3Com® Switch 8800 Family
Command Reference Guide

Advanced Software Version V5

Switch 8807
Switch 8810
Switch 8814

www.3Com.com
Part Number: 10016064 Rev. AA
Published: June, 2007

3Com Corporation
350 Campus Drive
Marlborough, MA
USA 01752-3064

ENVIRONMENTAL STATEMENT

It is the policy of 3Com Corporation to be environmentally-friendly in all operations. To uphold our policy, we are committed to:

Establishing environmental performance standards that comply with national legislation and regulations.

Conserving energy, materials and natural resources in all operations.

Reducing the waste generated by all operations. Ensuring that all waste conforms to recognized environmental standards. Maximizing the recyclable and reusable content of all products.

Ensuring that all products can be recycled, reused and disposed of safely.

Ensuring that all products are labelled according to recognized environmental standards.

Improving our environmental record on a continual basis.

End of Life Statement

3Com processes allow for the recovery, reclamation and safe disposal of all end-of-life electronic components.

Regulated Materials Statement

3Com products do not contain any hazardous or ozone-depleting material.

CONTENTS

4 MAC Address Table Management Configuration Commands

5 Link Aggregation Configuration Commands

6 GARP Configuration Commands

7 GVRP Configuration Commands

8 PORT MIRRORING CONFIGURATION COMMANDS

9 MSTP CONFIGURATION COMMANDS

27 IP PERFORMANCE CONFIGURATION COMMANDS

28 ROUTING POLICY CONFIGURATION COMMANDS

35 OSPF CONFIGURATION COMMANDS

36 IPv6 OSPFv3 Configuration Commands

39 BGP CONFIGURATION COMMANDS

40 IPv6 BGP Configuration Commands

44 IGMP CONFIGURATION COMMANDS

45 IGMP SNOOPING CONFIGURATION COMMANDS

46 PIM CONFIGURATION COMMANDS

47 MSDP CONFIGURATION COMMANDS

48 MLD CONFIGURATION COMMANDS

49 MLD SNOOPING CONFIGURATION COMMANDS

50 IPV6 PIM CONFIGURATION COMMANDS

51 UDP HELPER CONFIGURATION COMMANDS

52 DHCP SERVER CONFIGURATION COMMANDS

53 DHCP RELAY AGENT CONFIGURATION COMMANDS

54 DNS CONFIGURATION COMMANDS

55 IPV4-BASED VRRP CONFIGURATION COMMANDS

56 IPv6-Based VRRP Configuration Commands

57 GR Configuration Commands

58 Common Configuration Commands

59 IPv4 ACL Configuration Commands

60 IPv6 ACL Configuration Commands

61 Flow Template Configuration Commands

62 Traffic Shaping Configuration Commands

63 QoS Policy Class Defining Commands

64 QoS Policy Traffic Behavior Defining Commands

65 QoS Policy Defining Commands

72 EACL Configuration Commands

73 Outbound Traffic Statistics Configuration Commands

74 AAA Configuration Commands

75 RADIUS CONFIGURATION COMMANDS

76 HWTACACS CONFIGURATION COMMANDS

77 802.1X CONFIGURATION COMMANDS

78 SSH2.0 CONFIGURATION COMMANDS

79 SFTP CONFIGURATION COMMANDS

80 PASSWORD CONTROL CONFIGURATION COMMANDS

81 MAC AUTHENTICATION CONFIGURATION COMMANDS

82 NAT CONFIGURATION COMMANDS

83 DEVICE MANAGEMENT COMMANDS

84 POE CONFIGURATION COMMANDS

85 SYSTEM MAINTENANCE COMMANDS

86 SYSTEM DEBUGGING COMMANDS

87 FILE SYSTEM MANAGEMENT COMMANDS

88 CONFIGURATION FILE MANAGEMENT COMMANDS

89 FTP SERVER CONFIGURATION COMMANDS

90 FTP CLIENT CONFIGURATION COMMANDS

91 TFTP CLIENT CONFIGURATION COMMANDS

92 SNMP CONFIGURATION COMMANDS

93 RMON CONFIGURATION COMMANDS

94 NTP CONFIGURATION COMMANDS

95 NETSTREAM CONFIGURATION COMMANDS

96 NQA CONFIGURATION COMMANDS

99 INFORMATION CENTER CONFIGURATION COMMANDS

About This Guide

This guide describes the commands needed to configure the 3Com® Switch 8800 when using the Advanced Software.

This guide is intended for Qualified Service personnel who are responsible for configuring, using, and managing the switches. It assumes a working knowledge of local area network (LAN) operations and familiarity with communication protocols that are used to interconnect LANs.

Any command that the CLI displays, but is not described in this document set, is not supported in this software version. This product's document set describes the features that 3Com supports in this product.

Always download the Release Notes for your product from the 3Com World Wide Web site and check for the latest updates to software and product documentation:

`http://www.3com.com`

Conventions

Table 1 lists icon conventions that are used throughout this guide.

Table 1 Notice Icons

Icon	Notice Type	Description
	Information note	Information that describes important features or instructions.
	Caution	Information that alerts you to potential loss of data or potential damage to an application, system, or device.
	Warning	Information that alerts you to potential personal injury.

Table 2 lists text conventions that are used throughout this guide.

Table 2 Text Conventions

Convention	Description
`Screen displays`	This typeface represents information as it appears on the screen.
Keyboard key names	If you must press two or more keys simultaneously, the key names are linked with a plus sign (+), for example: Press Ctrl+Alt+Del

Table 2 Text Conventions

Convention	Description
The words "enter" and "type"	When you see the word "enter" in this guide, you must type something, and then press Return or Enter. Do not press Return or Enter when an instruction simply says "type."
Words in *italics*	Italics are used to: Emphasize a point. Denote a new term at the place where it is defined in the text. Identify menu names, menu commands, and software button names. Examples: From the *Help* menu, select *Contents*. Click *OK*.
Words in **`bold`**	Boldface type is used to highlight command names. For example, "Use the **`display user-interface`** command to..."

Related Documentation

The following manuals offer additional information necessary for managing your Switch 8800:

- *Switch 8800 Installation Guide*— Provides detailed descriptions about how to install the hardware, configure the software, and maintain the software and hardware for the Switch 8800. This guide also provides troubleshooting and support information for your switch.
- *Switch 8800 Configuration Guide Advanced Software Version*— Describes how to configure your Switch 8800 using the supported protocols and CLI commands.
- *Switch 8800 Release Notes* — Contains the latest information about your product. If information in this guide differs from information in the release notes, use the information in the *Release Notes*.

These documents are available in Adobe Acrobat Reader Portable Document Format (PDF) on the CD-ROM that accompanies your router or on the 3Com World Wide Web site:

`http://www.3com.com/`

About this Document

3Com supports only the commands that are described in this guide. You may encounter commands in the device's command line interface (CLI) that are not described in this guide. Any command that you see in the CLI but is not described in this guide is not supported in this version of the software. Unsupported commands may result in a loss of data and you enter them at your own risk.

1 BASIC CONFIGURATION COMMANDS

clock datetime

Syntax **clock datetime** *time date*

View User view

Parameter *time*: Current time in the format of *HH:MM:SS*, where *HH* is hours in the range 0 to 23, *MM* is minutes in the range 0 to 59, and *SS* is seconds in the range 0 to 59.

date: Current date in the format of *MM/DD/YYYY* or *YYYY/MM/DD*. *MM* is the month of the year in the range 1 to 12, *DD* is the day of the month that varies with months, and *YYYY* is a year in the range 2000 to 2035.

Description Use the **clock datetime** command to set the current time and date of the device.

The current time and date of the device must be set in an environment that requires the acquisition of absolute time.

You may choose not to provide seconds when inputting the time parameters.

After the configuration takes effect, you can use the **display clock** command to view it.

Example # Set the current system time to 14:10:20 08/01/2005.

```
<Sysname> clock datetime 14:10:20 08/01/2005
```

clock summer-time one-off

Syntax **clock summer-time** *zone-name* **one-off** *start-time start-date end-time end-date add-time*

undo clock summer-time

View User view

Parameter *zone-name*: Name of the summer time, a string of 1 to 32 characters. It is case sensitive.

start-time: Start time, in the format of *HH:MM:SS* (hours/minutes/seconds).

start-date: Start date, in the format of *MM/DD/YYYY* (months/days/years) or *YYYY/MM/DD*.

end-time: End time, in the format of *HH:MM:SS* (hours/minutes/seconds).

end-date: End date, in the format of *MM/DD/YYYY* (months/days/years) or *YYYY/MM/DD*.

add-time: Time added to the standard time of the device, in the format of *HH:MM:SS* (hours/minutes/seconds).

Description Use the **clock summer-time one-off** command to adopt summer time from the *start-time* of the *start-date* to the *end-time* of the *end-date*. Summer time adds the *add-time* to the current time of the device.

Use the **undo clock summer-time** command to cancel the configuration of the summer time.

After the configuration takes effect, you can use the **display clock** command to view it. Besides, the time of the log or debug information is the local time of which the time zone and summer time have been adjusted.

Note that:

- The time range from *start-time* in *start-date* to *end-time* in *end-date* must be longer than one day and shorter than one year. Otherwise, the argument is considered as invalid and the configuration fails.
- If the current system time is in the time range specified with this command, the system time automatically adds "add-time" after the execution of this command.

Related command: **clock timezone**.

Example # For summer time **abc1** from 06:00:00 on 08/01/2005 to 06:00:00 on 09/01/2005, set the system clock ahead one hour.

```
<Sysname> clock summer-time abc1 one-off 06:00:00 08/01/2005 06:00:0
0 09/01/2005 01:00:00
```

clock summer-time repeating

Syntax **clock summer-time** *zone-name* **repeating** *start-time start-date end-time end-date add-time*

undo clock summer-time

View User view

Parameter *zone-name*: Name of the daylight saving time, a string of 1 to 32 characters.

start-time: Start time, in the format of *HH:MM:SS* (hours/minutes/seconds).

start-date: Start date which can be set in two ways:

- Enter the year, month and date at one time, in the format of *MM/DD/YYYY* (months/days/years) or *YYYY/MM/DD*.
- Enter the year, month and date one by one, separated by spaces. The year ranges from 2000 to 2035; the month can be **January**, **February**, **March**, **April**, **May**, **June**, **July**, **August**, **September**, **October**, **November** or **December**; the start week can be the **first**, **second**, **third**, **fourth**, **fifth** or **last** week of the month; the start date is **Sunday**.

end-time: End time, in the format of *HH:MM:SS* (hours/minutes/seconds).

end-date: End date which can be set in two ways:

- Enter the year, month and date at one time, in the format of *MM/DD/YYYY* (months/days/years) or *YYYY/MM/DD*.
- Enter the year, month and date one by one, separated by spaces. The year ranges from 2000 to 2035; the month can be **January**, **February**, **March**, **April**, **May**, **June**, **July**, **August**, **September**, **October**, **November** or **December**; the end week can be the **first**, **second**, **third**, **fourth**, **fifth** or **last** week of the month; the end date is **Sunday**, **Monday**, **Tuesday**, **Wednesday**, **Thursday**, **Friday**, **Saturday**.

add-time: Time added to the standard time, in the format of *HH:MM:SS* (hours/minutes/seconds).

Description Use the **clock summer-time repeating** command to adopt summer-time repeatedly.

Use the **undo clock summer-time** command to cancel the configuration of the daylight saving time.

For example, when *start-date* and *start-time* are set to 2007/6/6 and 00:00:00, *end-date* and *end-time* to 2007/10/01 and 00:00:00, and *add-time* to 01:00:00, it specifies to adopt daylight saving time from 00:00:00 of June 6 until 00:00:00 of October 1 each year from 2007 (2007 inclusive). The daylight saving time adds one hour to the current device time.

After the configuration takes effect, use the **display clock** command to view the result. The information such as log file and debug adopts the local time modified by time-zone and daylight saving time.

Note that:

- The time range from "start-time" in "start-date" to "end-time" in "end-date" must be longer than one day and shorter than one year. Otherwise, the argument is considered as invalid and the configuration fails.
- If the current system time is in the time range specified with this command, the system time automatically adds "add-time" after the execution of this command.

Related command: **clock timezone**.

Example # For the summer time in **abc2** between 06:00:00 on 08/01/2007 and 06:00:00 on 09/01/2007 and from 06:00:00 08/01 to 06:00:00 on 09/01 each year after 2007, set the system clock ahead one hour.

```
<Sysname> clock summer-time abc2 repeating 06:00:00 08/01/2007 06:00
:00 09/01/2007 01:00:00
```

clock timezone

Syntax **clock timezone** *zone-name* { **add** | **minus** } *time*

undo clock timezone

View User view

Parameter *zone-name*: Time zone name, a string of 1 to 32 characters. It is case sensitive.

add: Positive offset to universal time coordinated (UTC) time.

minus: Negative offset to UTC time.

time: In the format of *HH*/*MM*/*SS* (hours/minutes/seconds), where *HH* is hours in the range 0 to 23, *MM* is minutes in the range 0 to 59, and *SS* is seconds in the range 0 to 59.

Description Use the **clock timezone** command to set the local time zone.

Use the **undo clock timezone** command to restore the local time zone to the default UTC time zone.

By default, the local time zone is UTC zone.

After the configuration takes effect, use the **display clock** command to view the result. The information such as log file and debug adopts the local time modified by time-zone and daylight saving time.

Related command: **clock summer-time**.

Example # Set the name of the local time zone to Z5, five hours ahead of UTC time.

```
<Sysname> clock timezone z5 add 05:00:00
```

command-privilege

Syntax **command-privilege level** *level* **view** *view command*

undo command-privilege view *view command*

View System view

Parameter *level*: Command level, in the range 0 to 3.

view: Specifies a view.

command: Command to be set in the specified view.

Description Use the **command-privilege** command to assign a level for the commands in the specified view.

Use the **undo command-privilege view** command to remove the configuration.

Command privilege falls into four levels: visit, monitor, system, and manage, which are identified by 0 through 3.

The administrator can assign a privilege level for a user according to his need. When the user logs on a device, the commands available depend on the user's privilege. For example, if a user's privilege is 3 and the command privilege of VTY 0 user interface is 1, and the user logs on the system from VTY 0, he can use all the commands with privilege smaller than three (inclusive).

Users are recommended to use the default user level; otherwise the change of user level may bring inconvenience to your maintenance and operation.

Table 1 describes the default level of the commands.

Table 1 Default level of the commands

Command level	Commands
Visit (0)	**ping**, **tracert**, **telnet**
Monitor (1)	**refresh**, **reset**, **send**
System (2)	Configuration commands
Manage (3)	FTP, Xmodem, TFTP, file system operation commands

Example # Set the command level of the **interface** command to 0.

```
<Sysname> system-view
[Sysname] command-privilege level 0 view system interface
```

display clipboard

Syntax **display clipboard**

View Any view

Parameter None

Description Use the **display clipboard** command to view the contents of the clipboard.

To copy the specified content to the clipboard:

- Move the cursor to the starting position of the content and press the <Esc+Shift+,> combination ("," is an English comma).
- Move the cursor to the ending position of the content and press the <Esc+Shift+.> combination ("." is an English dot) to copy the specified content to the clipboard.

Example # View the content of the clipboard.

```
<Sysname> display clipboard
---------------- CLIPBOARD-----------------
        ip route 10.1.0.0 255.0.0.0 eth 0
```

display clock

Syntax **display clock**

View Any view

Parameter None

Description Use the **display clock** command to view the current system time and date.

Related command: **clock datetime**.

Example # Display the current time and date.

```
<Sysname> display clock
09:27:21 UTC Mon 11/27/2006
```

display current-configuration

Syntax **display current-configuration** [**interface** [*interface-type* [*interface-number*]] | **configuration** [*configuration*] | [**by-linenum**] | [**|** { **begin** | **exclude** | **include** } *regular-expression*]] *

View Any view

Parameter **interface**: Displays the interface configuration.

interface-type interface-number: Interface type and interface number.

configuration [*configuration*]: Specifies to display the specified configuration, mainly the non-interface configuration. The value of the *configuration* argument is the keyword configured for the switch. For example:

- **isis**: Displays the isis configuration.
- **isp**: Displays the ISP configuration.
- **post-system**: Displays the **post-system** configuration.

- **radius-template**: Displays the Radius template configuration.
- **system**: Displays the system configuration.
- **user-interface**: Displays the user interface configuration.

by-linenum: Specifies to display the number of each line.

|: Specifies to use regular expression to filter the configuration of display device.

begin: Displays the configuration beginning with the specified text.

include: Displays the configuration including the specified text.

exclude: Displays the configuration excluding the specified text.

regular-expression: Regular expression in a string.

Table 2 Special characters in regular expressions

Character	Meaning	Note
^	Starting sign, the string following it appears only at the beginning of a line.	Regular expression "^user" matches a string begins with "user", not "Auser".
$	Ending sign, the string following it appears only at the end of a line.	Regular expression "user$" matches a string ends with "user", not "userA".
(	Left bracket, used as a stack symbol in a program	It is not recommended to user this character to establish a regular expression.
.	Full stop, a wildcard used in place of any character, including blank	None
*	Asterisk, used to match a subexpression zero or multiple times before it	zo* can map to "z" and "zoo".
+	Addition, used to match a subexpression one or multiple times before it	zo+ can map to "zo" and "zoo", but not "z".
-	Hyphen. It connects two values (the smaller one before it and the bigger one after it) to indicate a range together with [ ].	For example, "1-9" means numbers from 1 to 9 (inclusive); "a-h" means from a to h (inclusive).
[ ]	Selects one character from the group.	For example, [1-36A] can match only one character among 1, 2, 3, 6, and A.
( )	A group of characters. It is usually used with "+" or "*".	For example, (123A) means a string "123A"; "408(12)+" can match 40812 or 408121212. But it cannot match 408. That is, "12" can appear continuously and it must at least appear once.

Description Use the **display current-configuration** command to display the current validated configuration of a device.

A parameter is not displayed if it has the default configuration.

You can use the **display current-configuration** command to check the configuration to ensure its validity. A configuration is not displayed if it has not taken effect. For example, PPP has been configured on an interface. In this case, if you switch the link layer protocol to the X.25 protocol, the **display current-configuration** command does not display the PPP configuration on this interface.

Related command: **save**, **reset saved-configuration**, **display saved-configuration**.

Example # Display the configuration beginning with "user".

```
<Sysname> display current-configuration | begin user
user-interface aux 0
user-interface vty 0 4
```

display diagnostic-information

Syntax **display diagnostic-information**

View Any view

Parameter None

Description Use the **display diagnostic-information** command to display or save the statistics of each module's running status in the system.

When the system is out of order, you need to collect a lot of information to locate the problem. At this time you can use the **display diagnostic-information** command instead of many different **display** commands to collect prompt information of the following commands:

- **display clock**
- **display version**
- **display device**
- **display current-configuration**
- **display saved-configuration**
- **display interface**
- **display controller**
- **display fib**
- **display ip interface**
- **display ip statistics**
- **display memory**
- **display task**
- **display logbuffer**

- **display history all**

*You are recommended to execute the **display diagnostic-information** command for at least two consecutive times, so that you can compare the differences between the output running information to locate the fault. However, you should use this command only when necessary because execution of the command will continuously print lots of information, affecting the system operation.*

Example # Save the statistics of each module's running status in the system.

```
<Sysname> display diagnostic-information
Save or display diagnostic information (Y=save, N=display)?[Y/N]y
Please input the file name(*.diag)[flash:/default.diag]:aa.diag
Diagnostic information is outputting to flash:/aa.diag.
Please wait...
Save succeeded.
```

Display the statistics of each module's running status in the system.

```
<Sysname> display diagnostic-information
Save or display diagnostic information (Y=save, N=display)?[Y/N]n
```

display history-command

Syntax **display history-command**

View Any view

Parameter None

Description Use the **display history-command** command to display validated history commands performed last in current user view.

Refer to the **history-command max-size** command on page 73.

Example # Display validated history commands in current user view (the display information varies with configuration).

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

display hotkey

Syntax **display hotkey**

View Any view

Parameter None

Description Use the **display hotkey** command to display hotkey information.

Example # Display hotkey information.

```
<Sysname> display hotkey
----------------- HOTKEY -----------------

            =Defined hotkeys=
Hotkeys Command
CTRL_G  display current-configuration
CTRL_L  display ip routing-table
CTRL_O  undo debug all

           =Undefined hotkeys=
Hotkeys Command
CTRL_T  NULL
CTRL_U  NULL

            =System hotkeys=
Hotkeys Function
CTRL_A  Move the cursor to the beginning of the current line.
CTRL_B  Move the cursor one character left.
CTRL_C  Stop current command function.
CTRL_D  Erase current character.
CTRL_E  Move the cursor to the end of the current line.
CTRL_F  Move the cursor one character right.
CTRL_H  Erase the character left of the cursor.
CTRL_K  Kill outgoing connection.
CTRL_N  Display the next command from the history buffer.
CTRL_P  Display the previous command from the history buffer.
CTRL_R  Redisplay the current line.
CTRL_V  Paste text from the clipboard.
CTRL_W  Delete the word left of the cursor.
CTRL_X  Delete all characters up to the cursor.
CTRL_Y  Delete all characters after the cursor.
CTRL_Z  Return to the User View.
CTRL_]  Kill incoming connection or redirect connection.
ESC_B   Move the cursor one word back.
ESC_D   Delete remainder of word.
ESC_F   Move the cursor forward one word.
ESC_N   Move the cursor down a line.
ESC_P   Move the cursor up a line.
ESC_<   Specify the beginning of clipboard.
ESC_>   Specify the end of clipboard.
```

display memory

Syntax **display memory**

View Any view

Parameter None

Description Use the **display memory** command to display the usage of system memory.

Example # Display the current usage of the system memory.

```
<Sysname> system-view
[Sysname] display memory
System Total Memory(bytes): 41918976
Total Used Memory(bytes): 15949136
Used Rate: 38%
```

display this

Syntax **display this** [**by-linenum**]

View Any view

Parameter **by-linenum**: Specifies to display the number of each line.

Description Use the **display this** command to display the validated configuration information under the current view.

After finishing a set of configurations under a view, you can use the **display this** command to check whether the configuration takes effect.

Note that:

- A parameter is not displayed if it has the default configuration.
- A parameter is not displayed if the configuration has not taken effect.
- When you use the command under interface view, protocol view or protocol child view, the command displays the configuration corresponding to the current view.

Example # Display configuration information of the current view (the display information varies with configuration).

```
<Sysname> system-view
[Sysname] user-interface vty 0
[Sysname-ui-vty0] display this
#
user-interface con 0
user-interface vty 0
 history-command max-size 256
user-interface vty 1 4
#
return
```

display version

Syntax **display version**

View Any view

Parameter None

Description Use the **display version** command to view system version information.

By viewing system version information, you can learn about the current software version, rack type and the information related to the main control module and interface module.

Example # Display system version information.

```
<Sysname> display version
```

header

Syntax **header** { **incoming** | **legal** | **login** | **shell** } *text*

undo header { **incoming** | **legal** | **login** | **shell** }

View System view

Parameter **incoming**: Banner displayed when a user logs onto a terminal user interface by user name and password. If authentication is required, the banner is displayed after authentication.

legal: Authorization banner before login.

login: Login banner at authentication.

shell: Banner displayed for VTY users to enter user view.

text: Banner message. For the specific input methods, refer to the related contents in the System Basic Configuration section of the *3Com Switch 8800 Family Configuration Guide*.

Description Use the **header** command to create a banner.

Use the **undo header** command to clear a banner.

Example # Configure a banner in user view.

```
<Sysname> system-view
[Sysname] header incoming %
Input banner text, and quit with the character '%'.
Welcome to incoming(header incoming)%
```

```
[Sysname] header legal %
Input banner text, and quit with the character '%'.
Welcome to legal (header legal)%
[Sysname] header login %
Input banner text, and quit with the character '%'.
Welcome to login(header login)%
[Sysname] header motd %
Input banner text, and quit with the character '%'.
Welcome to motd(header motd)%
[Sysname] header shell %
Input banner text, and quit with the character '%'.
Welcome to shell(header shell)%
```

- *The character % is the starting/ending character of text in this example. Entering % after the displayed text quits the* ***header*** *command.*
- *As the starting and ending character, % is not a part of a banner.*

Test the configuration remotely using Telnet.

```
**************************************************************************
* All rights reserved (2004-2006)                                        *
* Without the owner's prior written consent,                             *
* no decompiling or reverse-switch fabricering shall be allowed.         *
**************************************************************************

Welcome to legal(header legal)
 Press Y or ENTER to continue, N to exit.
Welcome to motd(header motd)
Welcome to login(header login)



Login authentication


Password:
Welcome to shell(header shell)

<Sysname>
```

hotkey

Syntax **hotkey** { **CTRL_G** | **CTRL_L** | **CTRL_O** | **CTRL_T** | **CTRL_U** } *command*

undo hotkey { **CTRL_G** | **CTRL_L** | **CTRL_O** | **CTRL_T** | **CTRL_U** }

View System view

Parameter **CTRL_G**: Assigns the hot key <Ctrl+G> to a command.

CTRL_L: Assigns the hot key <Ctrl+L> to a command.

CTRL_O: Assigns the hot key <Ctrl+O> to a command.

CTRL_T: Assigns the hot key <Ctrl+T> to a command.

CTRL_U: Assigns the hot key <Ctrl+U> to a command.

command: The command line associated with the hot key.

Description Use the **hotkey** command to assign a hot key to a command line.

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

By default, the system specifies corresponding commands for <Ctrl+G>, <Ctrl+L> and <Ctrl+O>, while the others are null.

- <Ctrl+G> corresponds to **display current-configuration**
- <Ctrl+L> corresponds to **display ip routing-table**
- <Ctrl+O> corresponds to **undo debugging all**

You can customize this scheme as needed however.

Example # Assign the hot key <Ctrl+T> to the **display tcp status** command.

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

Display the configuration of hotkeys.

```
[Sysname] display hotkey
----------------- HOTKEY -----------------

            =Defined hotkeys=
Hotkeys Command
CTRL_G  display current-configuration
CTRL_L  display ip routing-table
CTRL_O  undo debug all
CTRL_T  display tcp status
          =Undefined hotkeys=
Hotkeys Command
CTRL_U  NULL

            =System hotkeys=
Hotkeys Function
CTRL_A  Move the cursor to the beginning of the current line.
CTRL_B  Move the cursor one character left.
CTRL_C  Stop current command function.
CTRL_D  Erase current character.
CTRL_E  Move the cursor to the end of the current line.
CTRL_F  Move the cursor one character right.
CTRL_H  Erase the character left of the cursor.
CTRL_K  Kill outgoing connection.
CTRL_N  Display the next command from the history buffer.
CTRL_P  Display the previous command from the history buffer.
CTRL_R  Redisplay the current line.
CTRL_V  Paste text from the clipboard.
CTRL_W  Delete the word left of the cursor.
CTRL_X  Delete all characters up to the cursor.
CTRL_Y  Delete all characters after the cursor.
CTRL_Z  Return to the user view.
CTRL_]  Kill incoming connection or redirect connection.
```

```
ESC_B   Move the cursor one word back.
ESC_D   Delete remainder of word.
ESC_F   Move the cursor forward one word.
ESC_N   Move the cursor down a line.
ESC_P   Move the cursor up a line.
ESC_<   Specify the beginning of clipboard.
ESC_>   Specify the end of clipboard.
```

quit

Syntax **quit**

View Any view

Parameter None

Description Use the **quit** command to exit to a lower-level view (if the current view is user view, you exit the system).

Example # Switch from Ethernet 1/1/1 interface view to system view, and then to user view.

```
[Sysname-Ethernet1/1/1] quit
[Sysname] quit
<Sysname>
```

return

Syntax **return**

View Any view except user view

Parameter None

Description Use the **return** command to return to user view from current view, as you do with the hot key <Ctrl+Z>.

Related command: **quit**.

Example # Return to user view from system view.

```
[Sysname] return
<Sysname>
```

super

Syntax **super** [*level*]

View User view

Parameter *level*: User level, in the range 0 to 3.

Description Use the **super** command to switch from the current user level to a specified user level.

There are four levels of commands:

- Visit: involves commands for network diagnosis (such as **ping** and **tracert**), commands for accessing an external device (such as Telnet client, SSH client, RLOGIN). Saving the configuration file is not allowed at this level.
- Monitor: includes the **display** and **debugging** commands for system maintenance, and service fault diagnosis. Saving the configuration file is not allowed at this level.
- System: provides service configuration commands, including routing and commands at each level of the network for providing services.
- Manage: influences the basic operation of the system and the system support modules for service support. Commands at this level involve file system, FTP, TFTP, Xmodem download and configuration file switch, power control, standby module control, user management, level setting, as well as parameter setting within a system (the last case involves those non-protocol or non RFC provisioned commands).

Login users are also classified into four levels that correspond to the four command levels. After users at different levels log in, they can only use commands at their own, or lower, levels.

Note that:

Users can switch to a lower user level unconditionally. To log in through AUX, or VTY user interface and switch to a higher user level, however, they need to enter the password (The password can be set with the **super password** command.). If the entered password is incorrect or no password is configured, the switch fails. Therefore, before switching to a higher user level, users should configure the password needed.

Related command: **super password**.

Example # Set the user level to 3.

```
<Sysname> super 3
User privilege level is 3, and only those commands can be used
whose level is equal or less than this.
Privilege note: 0-VISIT, 1-MONITOR, 2-SYSTEM, 3-MANAGE
```

super password

Syntax **super password** [**level** *user-level*] { **simple** | **cipher** } *password*

undo super password [**level** *user-level*]

View System view

Parameter *user-level*: User level in the range 1 to 3, with the default as 3.

simple: Plain text password.

cipher: Cipher text password.

password: Password, a string of characters. It is case-sensitive.

- For simple password, it is a string of 1 to 16 characters.
- For cipher password, it is a string of 1 to 16 characters in plain text or 24 characters in cipher text. For example, the simple text "1234567" corresponds to the cipher text "(TT8F]Y5SQ=^Q'MAF4<1!!".

Description Use the **super password** command to set the password needed to switch from a lower user level to a higher one.

Use the **undo super password** command to restore the default.

By default, no password is set to switch from a lower user level to a higher one.

Note that:

- If **simple** is specified, the configuration file saves a simple password.
- If **cipher** is specified, the configuration file saves the password in cipher text even if you input the password in plain text.
- The user must always enter a simple password, no matter **simple** or **cipher** is specified.
- Cipher passwords are recommended, as simple ones are easily getting cracked.

Example # Set the password to abc in simple form for switching user-level to 3.

```
<Sysname> system-view
[Sysname] super password level 3 simple abc
```

Display the password for switching user-level.

```
[Sysname] display current-configuration
#
 super password level 3 simple abc
```

Set the password to abc in cipher form for switching user-level to 3.

```
<Sysname> system-view
[Sysname] super password level 3 cipher abc
```

Display the password for switching user-level.

```
[Sysname] display current-configuration
#
 super password level 3 cipher =`*Y=F>*.%-a_SW8MYM2A!!
```

sysname

Syntax **sysname** *sysname*

undo sysname

View System view

Parameter *sysname*: Name of the device, a string of 1 to 30 characters.

Description Use the **sysname** command to set the name of the device.

Use the **undo sysname** demand to restore the device name to the default.

The default name of an Switch 8800 series switch is W8800.

Modifying device name affects the prompt of the CLI. For example, if the device name is 3Com, the prompt of user view is <SW8800>.

Example # Set the name of the device to R2000.

```
<SW8800> system-view
[SW8800] sysname R2000
[R2000]
```

Restore the device name to the default name 3Com.

```
[R2000] undo sysname
[SW8800]
```

system-view

Syntax **system-view**

View User view

Parameter None

Description Use the **system-view** command to enter system view from the current user view.

Related command: **quit**, **return**.

Example # Enter system view from the current user view.

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

2 USER INTERFACE CONFIGURATION COMMANDS

acl (user interface view)

Syntax For basic and advanced ACL, use the following commands:

acl [**ipv6**] *acl-number* { **inbound** | **outbound** }

undo acl [**ipv6**] *acl-number* { **inbound** | **outbound** }

For layer 2 ACL, use the following commands:

acl *acl-number* **inbound**

undo acl *acl-number* **inbound**

View VTY user interface view

Parameters **ipv6**: When this keyword is present, the command supports IPv6; otherwise, it supports IPv4.

acl-number: Number of access control list, in the range 2000 to 4999, where

- 2000 to 2999 are the basic ACL number
- 3000 to 3999 are the advanced ACL number
- 4000 to 4999 are the layer 2 ACL number

inbound: Controls dial-in for a user interface.

outbound: Controls dial-out for a user interface.

Description Use the **acl** command to reference an ACL to control dial-in or dial-out of the current users.

Use the **undo acl** command to remove the ACL.

For details regarding ACL, refer to the "Common Configuration Commands" page 981 .

By default, dial-in and dial-out of VTY users are not restricted.

Examples # Remove the restriction on outgoing calls for VTY 0.

```
<Sysname> system-view
[Sysname] user-interface vty 0
[Sysname-ui-vty0] undo acl 2001 outbound
```

auto-execute command

Syntax **auto-execute command** *command*

undo auto-execute command

View User interface view

Parameters *command*: Command to be automatically executed.

Description Use the **auto-execute command** command to specify a command to be executed automatically.

Use the **undo auto-execute command** command to disable this feature.

By default, command auto-execution is disabled.

Note that:

The **auto-execute command** command is supported on all types of user interfaces except the Console port and the AUX port functioning as the console port.

Once a command is configured using the **auto-execute command** command, the system automatically executes the command when a user logs on from the interface where the command is configured. After the command is completed, the connection breaks automatically.

A good example is configuring the **auto-execute command** *telnet* command to let users telnet to the specified host automatically.

CAUTION: *The **auto-execute command** command may disable you from configuring the system through the terminal line to which the command is applied. Therefore, before configuring the command and saving the configuration (using the **save** command), make sure that you can access the system by other means to remove the configuration in case a problem occurs.*

Examples # Automatically execute the **telnet 10.10.10.1** command after a user logs on from the VTY 0 interface.

```
<Sysname> system-view
[Sysname] user-interface vty 0
[Sysname-ui-vty0] auto-execute command telnet 10.10.10.1
% This action will lead to configuration failure through ui-vty0. Are you sure?[
Y/N] y
[Sysname-ui-vty0]
```

authentication-mode (User interface view)

Syntax **authentication-mode** { **none** | **password** | **scheme** [**command-authorization**] }

View User interface view

Parameters **none**: Performs no authentication.

password: Performs local password authentication.

scheme: Performs authorization and authentication of AAA. For details about AAA, refer to "AAA Configuration Commands" page 1073.

command-authorization: Performs command line authorization. HWTACACS allows per-command authorization. An input command is executed only after it passes authorization. For details about HWTACACS, refer to "HWTACACS Configuration Commands" page 1127.

Description Use the **authentication-mode** command to set the authentication mode when users log onto the device using the current user interface.

By default, the authentication mode is **password** for VTY and AUX user interfaces and is **none** for Console interfaces.

Related commands: **set authentication password**.

Examples # Set that no authentication is needed when users use VTY 0 interface to log onto the device. (This mode may be insecure.)

```
<Sysname> system-view
[Sysname] user-interface vty 0
[Sysname-ui-vty0] authentication-mode none
```

Set to use password authentication when users use VTY 0 interface to log onto the device. The authentication password is 321.

```
<Sysname> system-view
[Sysname] user-interface vty 0
[Sysname-ui-vty0] authentication-mode password
[Sysname-ui-vty0] set authentication password cipher 321
```

Set to use username and password authentication when users use VTY 0 interface to log onto the device. The username is 123 and the authentication password is 321.

```
<Sysname> system-view
[Sysname] user-interface vty 0
[Sysname-ui-vty0] authentication-mode scheme
[Sysname-ui-vty0] quit
[Sysname] local-user 123
[Sysname -luser-123] password cipher 321
[Sysname -luser-123] service-type telnet level 3
```

debugging modem

Syntax **debugging modem**

View User view

Parameters None

Description Use the **debugging modem** command to enable debugging of Modem.

Based on debugging output, you can verify the correctness of Modem scripts.

Examples # Enable debugging of Modem.

```
<Sysname> debugging modem
```

databits

Syntax **databits** { **5** | **6** | **7** | **8** }

undo databits

View User interface view

Parameters **5**: Five data bits.

6: Six data bits.

7: Seven data bits.

8: Eight data bits.

Description Use the **databits** command to set data bits on the user interface.

Use the **undo databits** command to restore the default, or eight bits.

*The command is only applicable to serial interfaces that work in asynchronous flow mode, which can be configured using the **async mode flow** command.*

Examples # Set data bits to 7.

```
<Sysname> system-view
[Sysname] user-interface aux 0
[Sysname-ui-aux0] databits 7
```

debugging vty

Syntax **debugging vty** { **fsm** | **negotiate** }

undo debugging vty { **fsm** | **negotiate** }

View User view

Parameters **fsm**: Enables/disables debugging of Telnet state machine.

negotiate: Enables/disables debugging of VTY negotiation.

Description Use the **debugging vty** command to enable debugging of VTY.

Use the **undo debugging vty** command to disable debugging of VTY.

Examples # Enable debugging of VTY negotiation.

```
<Sysname> debugging vty negotiate
```

display user-interface

Syntax **display user-interface** [*num1* | { **aux** | **console** | **vty** } *num2*] [**summary**]

View Any view

Parameters *num1*: Absolute number of a user interface. The value range normally starts from 0.

num2: Relative number of a user interface, in the following rules:

- For the AUX port, the value is 0.
- For the Console port, the value is 0.
- For VTY user interfaces, the value ranges from 0 to 4.

summary: Displays summary about user interfaces.

Description Use the **display user-interface** command to view information about the specified or all user interfaces.

- If the **summary** keyword is absent, the command displays the type of the user interface, the absolute or relative number, the speed, the user privilege level, the authentication mode and the physical location.
- If the **summary** keyword is present, the command displays all the number and type of user interfaces.

Examples # Display information about user interface 0.

```
<Sysname> display user-interface 0
  Idx  Type     Tx/Rx      Modem Privi Auth  Int
+ 0    CON 0    9600       -     3     N     -

  +    : Current user-interface is active.
  F    : Current user-interface is active and work in async mode.
  Idx  : Absolute index of user-interface.
```

```
  Type : Type and relative index of user-interface.
  Privi: The privilege of user-interface.
  Auth : The authentication mode of user-interface.
  Int  : The physical location of UIs.
  A    : Authentication use AAA.
  L    : Authentication use local database.
  N    : Current UI need not authentication.
  P    : Authentication use current UI's password.
```

Table 3 Description of the display user-interface command fields

Field	Description
+	The current user interface is active.
F	The current user interface is active and works in asynchronous mode.
Idx	The absolute number of the user interface.
Type	The type and relative number of the user interface.
Tx/Rx	The speed of the user interface
Modem	Whether the modem is allowed to dial in (in), dial out (out), or both (inout) By default, the character - is displayed to indicate that this function is disabled.
Privi	Indicates the command level of a user under that user interface
Auth	The authentication mode, uses one of the following, AAA (A), current user interface password (P), local database (L), none authentication (N).
Int	The physical location of the user interfaces

Display summary about all user interfaces.

```
<Sysname> display user-interface summary
User interface type : [CON]
            0:U
  User interface type : [AUX]
            1:X
  User interface type : [VTY]
            2:XXXX X

    1 character mode users.      (U)
    6 UI never used.             (X)
    1 total UI in use
```

Table 4 Field descriptions of the display user-interface summary command

Field	Description
User interface type	Type of user interface (CON/AUX/VTY)
0:U	0 represents the absolute number of the user interface. X means this user interface is not used; U means this user interface is in use; the number of the character X and U indicates the total number of user interfaces.
character mode users. (U)	Number of mode users, that is, the number of character U.

Table 4 Field descriptions of the display user-interface summary command

Field	Description
UI never used. (X)	Number of user interfaces not used, that is, the number of character X.
total UI in use	Total number of user interfaces in use

display users

Syntax **display users** [**all**]

View Any view

Parameters **all**: Displays information about users on all user interfaces.

Description Use the **display users** command to view the user information using the device.

Use the **display users all** command to view the user information of all the user interfaces supported on the device.

Examples # Display the user information of the current user interface.

```
<Sysname> display users
The user application information of the user interface(s):
  Idx UI      Delay   Type Userlevel
+ 178 VTY 0   00:00:00 TEL  3
  179 VTY 1   00:02:34 TEL  3

Following are more details.
VTY 0   :
        Location: 192.168.1.54
VTY 1   :
        Location: 192.168.1.58
+   : Current operation user.
F   : Current operation user work in async mode.
```

Table 5 Field descriptions offield descriptions of the display users command

Field	Description
Idx	Absolute number of the user interface
UI	The first number and the second number are respectively the absolute index and relative index of the user interface.
Delay	Interval since the last input, in the format of hh:mm:ss.
Type	User type, such as Telnet or SSH
Userlevel	User authority or level: 0 for visit, 1 for monitor, 2 for system, and 3 for manage.
+	User interface used by the current user
Location	Location of the user logging from the current user interface
F	The current user works in asynchronous mode

flow-control (User interface view)

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

undo flow-control

View User interface view

Parameters **hardware**: Hardware flow control , valid on the AUX port user interfaces only.

software: Software flow control.

none: No flow control.

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

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

By default, the flow control mode is **none**, that is, without flow control.

*The command is only applicable to serial interfaces that work in asynchronous flow mode, which can be configured using the **async mode flow** command.*

Examples # Configure software flow control in user interface view.

```
<Sysname> system-view
[Sysname] user-interface console 0
[Sysname-ui-console0] flow-control software
```

free user-interface

Syntax **free user-interface** { *num1* | { **aux** | **console** | **vty** } *num2* }

View User view

Parameters *num1*: Absolute number of a user interface. The value range normally starts from 0.

num2: Relative number of a user interface, in the following rules:

- For the AUX port, the value is 0.
- For the Console port, the value is 0.
- For VTY user interfaces, the value ranges from 0 to 4.

Description Use the **free user-interface** command to disconnect with the specified user interface.

Note that you cannot use this command to terminate your own connection.

Examples # Terminate the connection with user interface VTY1.

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

Terminate the connection with user interface VTY 0.

```
<Sysname> free user-interface vty 0
% Not allowed to clear current UI!
```

history-command max-size

Syntax **history-command max-size** *size-value*

undo history-command max-size

View User interface view

Parameters *size-value*: History buffer size in the range 0 to 256. It defaults to 10, that is, up to ten history commands can be stored.

Description Use the **history-command max-size** command to set the size of history command buffer of the current user interface.

Use the **undo history-command max-size** command to restore the default, or 10.

Examples # Set the size of the history command buffer to 20.

```
<Sysname> system-view
[Sysname] user-interface console 0
[Sysname-ui-console0] history-command max-size 20
```

idle-timeout

Syntax **idle-timeout** *minutes* [*seconds*]

undo idle-timeout

View User interface view

Parameters *minutes*: Specifies timeout time in minutes, in the range 0 to 35791.

seconds: Specifies timeout time in seconds, in the range 0 to 59.

Description Use the **idle-timeout** command to set the idle-timeout timer. When it expires, the user connection is terminated.

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

The default idle-timeout is 10 minutes.

- *The system automatically terminates user's connection if there is no information interaction between the device and the user in timeout time.*
- *Setting idle-timeout to zero disables the timer and the connection is maintained whether it is idle or not.*

Examples # Set the idle-timeout timer to 1 minute and 30 seconds.

```
<Sysname> system-view
[Sysname] user-interface console 0
[Sysname-ui-console0] idle-timeout 1 30
```

lock

Syntax **lock**

View User view

Parameters None

Description Use the **lock** command to set a password to prevent unauthorized users from operating under the active user interface.

After entering the **lock** command, you are prompted to input a password (up to 16 characters) and then confirm it by inputting the password again. The password is successfully set only when you input the exact password during the confirmation. After setting the password, you will be required to input the password next time you enter the system.

By default, this function is disabled.

Examples # Lock the active user interface.

```
<Sysname> lock
Please input password<1 to 16> to lock current user terminal interfa
ce:
Password:
Again:


                    locked !



Password:
<Sysname>
```

modem

Syntax **modem** [**call-in** | **call-out** | **both**]

undo modem [**call-in** | **call-out** | **both**]

View User interface view

Parameters **call-in**: Enables dial in.

call-out: Enables dial out.

both: Enables both dial in and dial out.

Description Use the **modem** command to enable the modem to dial in or dial out.

Use the **undo modem** command to disable this function.

By default, dial in and dial out are disabled on the modem.

This command takes effect on the AUX and VTY ports only, and cannot be applied to the Console port.

Examples # Set the modem dial in/out attribute on VTY 1.

```
<Sysname> system-view
[Sysname] user-interface vty 1
[Sysname-ui-vty1] modem call-in
```

modem auto-answer

Syntax **modem auto-answer**

undo modem auto-answer

View User interface view

Parameters None

Description Use the **modem auto-answer** command to set the answering mode to auto-answer.

Use the **undo modem auto-answer** command to restore the default, or manual answer.

This command takes effect on the AUX port and other asynchronous interfaces only, and cannot be applied to the Console port.

Examples # Set the answering mode to auto-answer.

```
<Sysname> system-view
[Sysname] user-interface aux 0
[Sysname-ui-aux0] modem auto-answer
```

modem timer answer

Syntax **modem timer answer** *time*

undo modem timer answer

View User interface view

Parameters *time*: Timeout time in the range 1 to 60 seconds.

Description Use the **modem timer answer** command to set the timeout interval spent waiting for the carrier signal after the off-hook action when setting up an incoming call connection.

Use the **undo modem timer answer** command to restore the default, or 30 seconds.

This command takes effect on the AUX port and other asynchronous interfaces only, and cannot be applied to the Console port.

Examples # Set the timeout interval to 50 seconds.

```
<Sysname> system-view
[Sysname] user-interface aux 0
[Sysname-ui-aux0] modem timer answer 50
```

parity

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

undo parity

View User interface view

Parameters **none**: No parity check.

even: Even parity check.

odd: Odd parity check.

mark: Mark parity check.

space: Space parity check.

Description Use the **parity** command to set the check bit of the user interface.

Use the **undo parity** command to restore the default, or **none**.

*The command is only applicable to serial interfaces that work in the asynchronous flow mode, which can be configured using the **async mode flow** command.*

Examples # Perform odd parity check on the AUX interface.

```
<Sysname> system-view
[Sysname] user-interface aux 0
[Sysname-ui-aux0] parity odd
```

protocol inbound (VTY user interface view)

Syntax **protocol inbound** { **all** | **ssh** | **telnet** }

View VTY user interface view

Parameters **all**: Supports all the protocols, including Telnet and SSH.

ssh: Supports SSH only.

telnet: Supports Telnet only.

Description Use the **protocol inbound** command to enable the current user interface to support either Telnet, PAD, SSH, or all of them.

By default, all the protocols are supported.

The configuration takes effect next time you log in.

CAUTION:

- *If SSH is configured, you must set the authentication mode to **scheme** using the **authentication-mode scheme** command to guarantee a successful login. The **protocol inbound ssh** command fails if the authentication mode is **password** or **none**. Related commands: **authentication-mode**.*
- *By default, the authentication mode of the Telnet protocol is **password**.*

Examples # Enable the VTYs 0 through 4 to support SSH only.

```
<Sysname> system-view
[Sysname] user-interface vty 0 4
[Sysname-ui-vty0-4] authentication-mode scheme
[Sysname-ui-vty0-4] protocol inbound ssh
```

screen-length

Syntax **screen-length** *screen-length*

undo screen-length

View User interface view

Parameters *screen-length*: Number of lines displayed on the screen, in the range 0 to 512, with zero meaning to disable multiple-screen output.

Description Use the **screen-length** command to set the number of lines displayed on the terminal screen.

Use the **undo screen-length** command to restore the default, or 24 lines.

Examples # Set the number of lines on the terminal screen to 30.

```
<Sysname> system-view
[Sysname] user-interface console 0
[Sysname-ui-console0] screen-length 30
```

send

Syntax **send** { **all** | *num1* | { **aux** | **console** | **vty** } *num2* }

View User view

Parameters **all**: Sends messages to all user interfaces.

num1: Absolute number of a user interface. The value range normally starts from 0.

num2: Relative number of a user interface, in the following rules:

- For the AUX port, the value is 0.
- For the Console port, the value is 0.
- For VTY user interfaces, the value ranges from 0 to 4.

Description Use the **send** command to send messages to the specified user interface(s).

Press <Ctrl+Z> to end message input and press <Ctrl+C> to remove this operation when inputting messages.

Examples # Send the message **hello abc** to the Console user interface.

```
<Sysname> send console 0
Enter message, end with CTRL+Z or Enter; abort with CTRL+C:
hello abc^Z
Send message? [Y/N]y
<Sysname>
***
***
***Message from con0 to con0
***
hello abc


<Sysname>
```

service modem-callback

Syntax **service modem-callback**

undo service modem-callback

View System view

Parameters None

Description Use the **service modem-callback** command to enable the modem callback function.

Use the **undo service modem-callback** command to disable the modem callback function.

By default, the function is disabled.

With the function enabled, a modem calls back once the modem line is activated (that is, it detects carriers or data from the peer device). In this case, no accounting system has been started yet, thus saving communication fees.

Examples # Enable the modem callback function.

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

service-type telnet

Syntax **service-type telnet** [**level** *level*]

undo service-type telnet

View User view

Parameters *level*: Command level available to a user logging in, in the range 0 to 3, and defaults to 2.

Description Use the **service-type telnet** command to configure the command level available to a user logging in.

Use the **undo service-type telnet** command to restore the default.

There are four command levels: visit, monitor, system, and manage.

- Visit: involves commands for network diagnosis, such as **ping** and **tracert**, commands for language mode switch on user interfaces, such as **language-mode,** and **telnet**. Saving the configuration file is not allowed at this level.

- Monitor: includes the **display** and **debugging** commands for system maintenance and service fault diagnosis. Saving the configuration file is not allowed at this level.
- System: provides service configuration commands including routing and commands at each level of the network for providing services.
- Manage: Commands at this level concern file system, file transfer protocol (FTP), trivial file transfer protocol (TFTP), downloading using XModem, user management, and level setting, which influence the basic operation of the system and the system support modules for service support.

Examples # Configure the command level to 0 for the user zbr after he logs in.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] local-user zbr
[Sysname-luser-zbr] service-type telnet level 0
```

set authentication password

Syntax **set authentication password** { **simple** | **cipher** } *password*

undo set authentication password

View User interface view

Parameters **simple**: Plain text password.

cipher: Cipher text password.

password: A case sensitive string. If the password format is set to **simple**, the *password* argument must be in plain text. If it is set to cipher, *password* can be either in cipher text or in plain text depending on what has been input. A plain text password can be a string of no more than 16 consecutive characters, 1234567 for example. A cipher text password, or the encrypted version of the plain text password, comprises 24 characters, such as _(TT8F]Y5SQ=^Q'MAF4<1!!.

Description Use the **set authentication password** command to set a local authentication password.

Use the **undo set authentication password** command to remove the local authentication password.

No local authentication password is set by default.

- When setting a password, you should specify **simple** to save it in plain text in the configuration file, or specify **cipher** to save it in cipher text.
- Whether the password format is plain text or cipher text, you must type in plain text password at authentication.

- Plain text password easily gets cracked. Therefore, you are recommended to use cipher text password.

By default, Telnet users must provide passwords at login, that is, the **authentication-mode password** command applies. If no password is configured, the following information appears:

```
Login password has not been set !
```

Related commands: **authentication-mode**.

Examples # Set the local authentication password for the user interface Console 0 to hello.

```
<Sysname> system-view
[Sysname] user-interface console 0
[Sysname-ui-console0] authentication-mode password
[Sysname-ui-console0] set authentication password simple hello
```

After setting the password, you will be required to input the password next time you enter the system.

shell

Syntax **shell**

undo shell

View User interface view

Parameters None

Description Use the **shell** command to enable terminal services on the user interface.

Use the **undo shell** command to disable this function.

By default, terminal services are enabled on all user interfaces.

There are a few restrictions on using the **undo shell** command:

- This command is not supported on the Console port.
- This command is not supported on the AUX port if the device has only a AUX port and no Console port.
- This command cannot be used on the user interface from which you log in.

Examples # Disable terminal services on the VTYs 0 through 4.

```
<Sysname> system-view
[Sysname] user-interface vty 0 4
[Sysname-ui-vty0-4] undo shell
% Disable ui-vty0-4 , are you sure ? [Y/N] y
[Sysname-ui-vty0-4]
```

The following information is displayed when a Telnet terminal logs in:

```
The connection was closed by the remote host!
```

speed (user interface view)

Syntax **speed** *speed-value*

undo speed

View User interface view

Parameters *speed-value*: Transmission rate in bps.

The transmission rates available with asynchronous serial interfaces include:

- 300 bps
- 600 bps
- 1200 bps
- 2400 bps
- 4800 bps
- 9600 bps
- 19200 bps
- 38400 bps
- 57600 bps
- 115200 bps

Description Use the **speed** command to set the transmission rate on the user interface.

Use the **undo speed** command to restore the default transmission rate.

By default, the transmission rate is 9600 bps.

*The command is only applicable to serial interfaces that work in asynchronous flow mode, which can be configured using the **async mode flow** command.*

Examples # Set the transmission rate on the user interface AUX 0 to 19200 bps.

```
<Sysname> system-view
[Sysname] user-interface aux 0
[Sysname-ui-aux0] speed 19200
```

stopbits

Syntax **stopbits** { **1.5** | **1** | **2** }

undo stopbits

View User interface view

Parameters **1.5**: 1.5 stop bits.

1: 1 stop bit.

2: 2 stop bits.

Description Use the **stopbits** command to set the stop bits on the user interface.

Use the **undo stopbits** command to restore the default, or one stop bit.

- *The command is only applicable to serial interfaces that work in asynchronous flow mode, which can be configured using the **async mode flow** command.*
- *Currently, the Switch 8800 routing switches do not support 1.5 stop bits.*

Examples # Set the stop bits on the user interface to 2.

```
<Sysname> system-view
[Sysname] user-interface aux 0
[Sysname-ui-aux0] stopbits 2
```

telnet

Syntax **telnet** [**vpn-instance** *vpn-instance-name*] { *hostname* | *ip-address* } [*service-port*] [**source** { **interface** *interface-type interface-number* | **ip** *ip-address* }]

View User view

Parameters **vpn-instance** *vpn-instance-name*: Specifies the name of an MPLS VPN instance, with *vpn-instance-name* being a string of 1 to 19 characters.

hostname: Host name of the remote switch, which has been configured with the **ip host** command.

ip-address: IP address of the remote switch.

service-port: Number of the TCP port providing the Telnet service on the remote switch, in the range 0 to 65535.

interface *interface-type interface-number*: Specifies the source interface, which can only be a VLAN one.

ip *ip-address*: Specifies the source IP address.

Description Use the **telnet** command to log in to other switches for remote management.

Press <Ctrl+k> to end the current Telnet login.

By default, the service port number is 23 if *service-port* is not specified.

Related commands: **display tcp status**, **ip host.**

Examples # Telnet a remote switch Sysname2 from the current switch Sysname1 with the IP address being 129.102.0.1.

```
<Sysname1> telnet 129.102.0.1
Trying 129.102.0.1...
Press CTRL+K to abort
Connected to 129.102.0.1...
<Sysname2>
```

terminal type

Syntax **terminal type { ansi | vt100 }**

undo terminal type

View User interface view

Parameters **ansi**: Specifies the terminal display type as ANSI.

vt100: Specifies the terminal display type as VT100.

Description Use the **terminal type** command to configure the type of terminal display.

Use the **undo terminal type** command to restore the default.

By default, the terminal display type is ANSI.

Note that the system supports two types of terminal display: ANSI and VT100. If the terminal display of the device and the client (for example, hyper terminal or Telnet terminal) is inconsistent or is set to ANSI, and if the total number of the characters of the currently using command line exceeds 80, anomalies such as cursor corruption or abnormal display of the terminal display may occur on the client. Therefore, you are recommended to set the display type of both the device and the client to VT100.

Examples # Set the terminal display type to VT100.

```
<Sysname> system-view
[Sysname] user-interface vty 0
[Sysname-ui-vty0] terminal type vt100
```

user privilege level

Syntax **user privilege level** *level*

undo user privilege level

View User interface view

Parameters *level*: Command level in the range 0 to 3.

Command level is divided into four levels of visit, monitor, system, and manage, corresponding to the number 0, 1, 2 and 3 respectively. The administrator can change the command level of a user when necessary.

Description Use the **user privilege level** command to configure the command level that the login users on the current user interface can access.

Use the **undo user privilege level** command to restore the default.

By default, the default command level is 3 for the Console user interface and 0 for other user interfaces.

Examples # Set the privilege level of the user logging in from VTY 0 to 0.

```
<Sysname> system-view
[Sysname] user-interface vty 0
[Sysname-ui-vty0] user privilege level 0
```

After the user telnets to the device from VTY 0, the terminal will only display level 0 commands, as follows:

```
<Sysname> ?
User view commands:
  language-mode  Specify the language environment
  ping           Send echo messages
  quit           Exit from current command view
  super          Privilege current user a specified priority level
  telnet         Establish one TELNET connection
  tracert        Trace route function
  undo           Undo a command or set to its default status
<Sysname>
```

Enable user 1 to access level 3 commands.

```
<Sysname> system-view
[Sysname] local-user user1
New local user added.
[Sysname-luser-user1] level 3
```

user-interface

Syntax **user-interface** { *first-num1* [*last-num1*] | { **aux** | **console** | **vty** } *first-num2* [*last-num2*] }

View System view

Parameters *first-num1*: Absolute number of the first user interface. The value range normally starts from 0.

last-num1: Absolute number of the last user interface. The value range normally starts from 0, but cannot be smaller than the *first-num1*.

first-num2: Relative number of the first user interface, in the following rules:

- For the AUX port, the value is 0.
- For the Console port, the value is 0.
- For VTY user interfaces, the value ranges from 0 to 4.

last-num2: Relative number of the last user interface, in the following rules:

- For VTY user interfaces, the value ranges from (*first-num2*+1) to 4.

Description Use the **user-interface** command to enter a single or multiple user interface view(s).

Examples # Enter Console user interface view.

```
<Sysname> system-view
[Sysname] user-interface console 0
[Sysname-ui-console0]
```

Enter the user interface view of VTY 0 to 3.

```
<Sysname> system-view
[Sysname] user-interface vty 0 3
[Sysname-ui-vty0-3]
```

3 ETHERNET INTERFACE CONFIGURATION COMMANDS

broadcast-suppression

Syntax **broadcast-suppression** *ratio*

undo broadcast-suppression

View Ethernet interface view, port group view

Parameters *ratio*: Broadcast storm suppression ratio to be set, in the range 1 to 100. Broadcast storm suppression ratio is the percentage of the maximum broadcast traffic allowed to the total transmission capability of an Ethernet interface. The smaller the ratio, the less the broadcast traffic allowed through the interface.

Description Use the **broadcast-suppression** command to set the broadcast storm suppression ratio.

Use the **undo broadcast-suppression** command to restore the default broadcast storm suppression ratio.

By default, all broadcast traffic is allowed to go through an Ethernet interface, that is, broadcast traffic is not suppressed.

If you execute this command in Ethernet interface view, the configuration takes effect only on the current interface. If you execute this command in port group view, the configuration takes effect on all ports in the port group.

With the broadcast storm suppression ratio set, when the broadcast traffic reaching the interface exceeds the maximum broadcast traffic allowed, the system will discard the extra packets so that the broadcast traffic ratio falls below the limit to ensure that the network functions properly.

If you set the broadcast suppression ratio repeatedly, the latest configuration takes effect.

Examples # Set the broadcast storm suppression ratio to 20 for Ethernet 1/1/1.

<Sysname> system-view

```
[Sysname] interface ethernet 1/1/1
[Sysname-Ethernet1/1/1] broadcast-suppression 20
```

Set the broadcast storm suppression ratio to 20 for all the interfaces in port group 1.

```
<Sysname> system-view
[Sysname] port-group manual group1
[Sysname-port-group manual group1] group-member ethernet 2/1/1
[Sysname-port-group manual group1] group-member ethernet 2/1/2
[Sysname-port-group manual group1] broadcast-suppression 20
```

description (Ethernet interface view)

Syntax **description** *text*

undo description

View Ethernet interface view

Parameters *text*: Interface description string to be set, a string of 1 to 80 characters.

Description Use the **description** command to set the description string of an Ethernet interface.

Use the **undo description** command to remove the description string.

By default, the description string of an interface is "interface index" + "interface".

Examples # Set the description string to "lanswitch-interface" for Ethernet 1//1/1.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1/1
[Sysname-Ethernet1/1/1] description lanswitch-interface
```

display brief interface

Syntax **display brief interface** [*interface-type* [*interface-number*]] [**|** { **begin** | **include** | **exclude** } *text*]

View Any view

Parameters *interface-type*: Interface type.

interface-number: Interface number.

|: Uses a regular expression to filter output information.

begin: Displays the configuration information from the line that contains the string specified by the *text* argument.

include: Displays all the lines that contain the string specified by the *text* argument.

exclude: Displays all the lines that do not contain the string specified by the *text* argument.

text: Regular expression, a string of 1 to 256 characters. This argument is case-sensitive and allows spaces.

Table 6 Special characters used in regular expressions

Character	Meaning	Notes on Use
^	Boundary matcher for the beginning of a line. This character specifies a string with which a line begins.	The regular expression "^user" matches lines that begin with the string "user". Lines that don t begin with the string "user", for example, "Auser", are not matched.
$	Boundary matcher for the end of a line. This character specifies a string with which a line ends.	The regular expression "user$" matches lines that end with the string "user". Lines that do not end with the string, for example, "userA", are not matched.
.	Full stop, used as the wildcard character, which matches any single character, including space.	None
*	Star, which matches the occurrences of the character to the left for zero or multiple times	zo* matches z and zoo.
+	Plus, which matches one or multiple occurrences of the character to the left	zo+ matches zo and zoo, but not z.
-	Hyphen, which is used to connect two numbers or characters. Note that the number to the left of this character needs to be larger than the one to the right. When used in a "[" and "]" pair, it represents a range.	1-9" represent a range from 1 to 9 ("1" and "9" included), and a-h represent a range from "a" to "h" ("a" and "h" included).
[ ]	Specifies a range.	[1-36A] matches a character, which can be a number in the range 1 to 36 or character A.
( )	Specifies a group of characters. Usually used with "+" and "*".	(123A) specifies the string "123A". 408(12)+ matchers "40812" or "408121212" (but not "408"). That is, "12" can appear for multiple times.

Description

Use the **display brief interface** command to display interface information in brief, including simple interface name, link state, protocol link state, protocol type, and main IP address.

- If neither interface type nor interface number is specified, all interface information will be displayed;
- If only interface type is specified, then only information of this particular type of interface will be displayed.

- If both interface type and interface number are specified, then only information of the specified interface will be displayed.

Related commands: **interface**.

Examples # Display the information about all the interfaces in brief.

```
<Sysname> display brief interface
The brief information of interface(s) under route mode:
Interface            Link      Protocol-link  Protocol type    Main IP
Loop0                UP        UP(spoofing)   LOOP             10.2.2.2
M-E0/0/0             UP        UP             ETHERNET         192.168.0.54
NULL0                UP        UP(spoofing)   NULL             --
Pos4/1/1             DOWN      DOWN           PPP              --
Pos4/1/2             DOWN      DOWN           PPP              --
Pos4/1/3             DOWN      DOWN           PPP              --
Pos4/1/4             DOWN      DOWN           PPP              --
Vlan1000             DOWN      DOWN           ETHERNET         10.110.10.1

The brief information of interface(s) under bridge mode:
Interface            Link      Speed     Duplex   Link-type  PVID
GE4/2/1              DOWN      auto      auto     access     1000
GE4/2/2              DOWN      auto      auto     access     1
GE4/2/4              DOWN      auto      auto     access     1
GE4/3/1              DOWN      auto      auto     access     1
GE4/3/2              DOWN      auto      auto     access     1
GE4/3/3              DOWN      auto      auto     access     1
GE4/3/4              DOWN      auto      auto     access     1
```

Table 7 Field descriptions of the display brief interface command.

Field	Description
The brief information of interface(s) under route mode:	Brief information of interface(s) in route mode
Interface	Interface name
Link	Interface physical link state, which can be up or down
Protocol-link	Interface protocol link state, which can be up or down
Protocol type	Interface protocol type
Main IP	Main IP
The brief information of interface(s) under bridge mode:	Brief information of interface(s) in bridge mode
Speed	Interface rate, in bps
Duplex	Duplex mode, which can be half (half duplex), full (full duplex), or auto (auto-negotiation).
PVID	Default VLAN ID

Table 8 Acronyms for different types of Interface

Interface name	Acronyms
Ethernet	Eth
GigabitEthernet	GE
Ten-GigabitEthernet	XGE

display counters

Syntax **display counters** { **inbound** | **outbound** } **interface** [*interface-type*]

View Any view

Parameters **inbound**: Displays statistics on inbound packets.

outbound: Displays statistics on outbound packets.

interface-type: Interface type.

Description Use the **display counters** command to display the statistics on specific packets.

- If you provide the *interface-type* argument, this command displays the statistics on the packets passing through all the interfaces that are of the specified type.
- If you do not provide the argument, this command displays the statistics on the packets passing through all the interfaces that support this command.

Examples # Display the statistics on the inbound packets passing through all the GigabitEthernet interfaces.

```
<Sysname> display counters inbound interface GigabitEthernet
Interface            Total(pkts)    Broadcast(pkts)    Multicast(pkts) Err(pkts)
GE5/1/1                    100               100                 0         0
GE5/1/2                 Overflow                 0          Overflow         0
GE5/1/3                        0                 0                 0         0
GE5/1/4                        0                 0                 0         0
GE5/2/1                        0                 0                 0         0
GE5/2/2                        0                 0                 0         0
GE5/2/3                        0                 0                 0         0
GE5/2/4                        0                 0                 0         0
GE5/3/1                        0                 0                 0         0
GE5/3/2                        0                 0                 0         0
GE5/3/3                        0                 0                 0         0
GE5/3/4                        0                 0                 0         0
Overflow: more than 14 decimal digits(7 digits for column "Err").
       --: not supported.
```

Table 9 Field descriptions of the display counters command

Field	Description
Interface	Interface name (in simplified format)
Total(pkts)	Total number of the packets received/sent through the interface. (You can specify the direction of the packets using the **inbound** and **outbound** keyword.)
Broadcast(pkts)	Total number of the broadcast packets received/sent through the interface. (You can specify the direction of the packets using the **inbound** and **outbound** keyword.)
Multicast(pkts)	Total number of the multicast packets received/sent through the interface. (You can specify the direction of the packets using the **inbound** and **outbound** keyword.)

Table 9 Field descriptions of the display counters command

Field	Description
Err(pkts)	Total number of the error packets received/sent through the interface. (You can specify the direction of the packets using the **inbound** and **outbound** keyword.)
Overflow: more than 14 decimal digits (7 digits for column "Err").	The value of the statistics item is larger than the maximum number a 14-digit decimal number can represent. For an Err item, Overflow means the value of the statistics item is larger than the maximum number a 7-digit decimal number can represent.
--: not supported.	The statistics item is not supported.

display counters rate

Syntax **display counters rate** { **inbound** | **outbound** } **interface** [*interface-type*]

View Any view

Parameters **inbound**: Displays the statistics on the rate of inbound packets.

outbound: Displays the statistics on the rate of outbound packets.

interface-type: Interface type.

Description Use the **display counters rate** command to display the statistics on the rate of the packets passing the interfaces that are in up state in the latest sampling interval.

- If you provide the *interface-type* argument, this command displays the statistics on the rate of the packets passing through all the interfaces that are in up state and are of the specified type.
- If you do not provide the argument, this command displays the statistics on the rate of the packets passing through all the interfaces that support this command.

  Sampling intervals can be set using the **flow-interval** command.

  By default, the sampling interval is 300 seconds.

Related commands: **flow-interval**.

Examples # Display the statistics on the rate of the inbound packets passing through all the GigabitEthernet interfaces.

```
<Sysname> display counters rate inbound interface GigabitEthernet
Interface           Total(pkts/sec)   Broadcast(pkts/sec)   Multicast(pkts/sec)
GE6/1/1                        200                   100                   100
GE6/1/2                        300                   200                   100
GE6/1/3                        300                   200                   100

Overflow: more than 14 decimal digits.
       --: not supported.
```

Table 10 Field descriptions of the display counters rate command

Field	Description
Interface	Interface name (in simplified format)
Total(pkts/sec)	Average rate (in packets per second) of receiving/sending packets during the sampling interval. You can specify the direction of the packets using the **inbound** and **outbound** keyword.
Broadcast(pkts/sec)	Average rate (packets per second) of receiving/sending broadcast packets during the sampling interval. You can specify the direction of the packets using the **inbound** and **outbound** keyword.
Multicast(pkts/sec)	Average rate (packets per second) of receiving/sending multicast packets during the sampling interval. You can specify the direction of the packets using the **inbound** and **outbound** keyword.
Overflow: more than 14 decimal digits(7 digits for column "Err").	The value of the statistics item is larger than the maximum number a 14-digit decimal number can represent.
--: not supported.	The statistics item is not supported.

*The **display counters** and **display counters rate** commands only count the statistics on the packets passing through RPR logical ports.*

display interface

Syntax **display interface** [*interface-type* [*interface-number*]]

View Any view

Parameters *interface-type*: Interface type.

interface-number: Interface number.

Description Use the **display interface** command to display the current state of an interface and related information.

- If neither interface type nor interface number is specified, all interface information will be displayed;
- If only interface type is specified, then only information of this particular type of interface will be displayed.
- If both interface type and interface number are specified, then only information of the specified interface will be displayed.

Related commands: **interface**.

Examples # Display the current state of the interface Ten-GigabitEthernet 5/1/2 and related information.

```
<Sysname> display interface Ten-GigabitEthernet5/1/2
 Ten-GigabitEthernet5/1/2 current state: DOWN
 IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 000f-e23f-32ce
 Description: Ten-GigabitEthernet5/1/2 Interface
 Loopback is not set
 Media type is not sure, Port hardware type is No Connector
Unknown-speed mode, unknown-duplex mode
Link speed type is autonegotiation, link duplex type is autonegotiation Flow
-control is not enabled
 The Maximum Frame Length is 1552
 Broadcast MAX-ratio: 100%
 PVID: 1
 Link delay is 1(sec)
 Ethernet port mode: WAN
        J0(Rx):""
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00     *..............*
        J0(Tx):""
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00     *..............*
        J1(Rx):""
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00     *..............*
        J1(Tx):""
        00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00     *..............*
     SDH error:
        section layer:  B1  0
        line    layer:  B2  0  M1  0
        path    layer:  B3  0  G1  0
 Port link-type: access
  Tagged   VLAN ID : none
  Untagged VLAN ID : 1
 Port priority: 0
 Last 300 seconds input:  0 packets/sec 0 bytes/sec
 Last 300 seconds output:  0 packets/sec 0 bytes/sec
 Input (total):  0 packets, 0 bytes
          0 broadcasts, 0 multicasts
 Input (normal):  0 packets, 0 bytes
          - broadcasts, - multicasts
 Input:  0 input errors, 0 runts, 0 giants, 0 throttles
          0 CRC, 0 frame, 0 overruns, - aborts
          0 ignored, - parity errors
 Output (total): 0 packets, 0 bytes
          0 broadcasts, 0 multicasts, 0 pauses
 Output (normal): 0 packets, 0 bytes
          - broadcasts, - multicasts, 0 pauses
 Output: 0 output errors, - underruns, - buffer failures
          0 aborts, 0 deferred, - collisions, 0 late collisions
          - lost carrier, - no carrier
```

Table 11 Field descriptions of the display interface command

Field	Description
Ten-GigabitEthernet5/1/2 current state	Ethernet interface physical state
IP Packet Frame Type	Ethernet frame type
Hardware address	Hardware address
Description	Description
Loopback is not set	Loopback is not set.
Media type, Port hardware type	Cable type, Port hardware type
Unknown-speed mode	Unknown-speed mode, in which mode speed is negotiated between the current host and the peer
unknown-duplex mode	unknown-duplex mode, in which mode speed is negotiated between the current host and the peer.

Table 11 Field descriptions of the display interface command

Field	Description
Link speed type is autonegotiation	Link speed type is autonegotiation.
link duplex type is autonegotiation	Link duplex type is autonegotiation.
Flow-control is not enabled	Flow-control is not enabled
The Maximum Frame Length	The maximum frame length allowed on an interface
Broadcast MAX-ratio	Broadcast storm suppression ratio (the maximum broadcast traffic allowed to overall traffic through an interface)
PVID	Default VLAN ID
Link delay	Link suppression time
Ethernet port mode	Ethernet port mode
SDH error	SDH error information
Port link-type	Interface link type, which could be access, trunk, and hybrid.
Tagged VLAN ID	Identify the VLANs that need Tag markers
Untagged VLAN ID	Identify the VLANs that do not need Tag markers
Port priority	Port priority
Last 300 seconds input	Average input rate within the latest 300 seconds
Last 300 seconds output	Average output rate within the latest 300 seconds
Input	Input packets
Output	Output packets

display port

Syntax **display port** { **hybrid** | **trunk** }

View Any view

Parameters **hybrid**: Displays the existing Hybrid ports.

trunk: Displays the existing Trunk ports.

Description Use the **display port** command to display the information about the existing ports that are of a specified type, including port name, default VLAN ID, and the VLAN ID of VLANs that the ports can pass through.

Examples # Display the existing hybrid ports.

```
<Sysname> display port hybrid
Interface            PVID  VLAN passing
GE4/2/2              100   Tagged:  1000, 1002, 1500, 1600-1611, 2000,
                                    2555-2558, 3000, 4000
                           Untagged:1, 10, 15, 18, 20-30, 44, 55, 67, 100,
                                    150-160, 200, 255, 286, 300-302
```

Display the existing trunk ports.

```
<Sysname> display port trunk
Interface            PVID  VLAN passing
GE4/3/2              2     1-4, 6-100, 145, 177, 189-200, 244, 289,
400,
                           555, 600-611, 1000, 2006-2008
```

Table 12 Field descriptions of the display port command.

Field	Description
Interface	Interface name
PVID	Default VLAN ID of a port
VLAN passing	ID of the VLANs permitted by the port

display port-group manual

Syntax **display port-group manual** [**all** | ***name*** *port-group-name*]

View Any view

Parameters **all**: Specifies all the manual port groups.

name *port-group-name*: Specifies the name of a manual port group, a string of 1 to 32 characters.

Description Use the **display port-group manual** command to display the information about a manual port group.

- If you provide the *port-group-name* argument, this command displays the information about the manual port group identified by the argument, including port group name and the Ethernet interface ports contained in the port group.
- If you provide the **all** keyword, this command displays the information about all the manual port groups, including their names and the Ethernet interface ports included.
- If you provide no keyword/argument, this command displays the names of all the manual port groups.

Examples # Display the names of all manual port groups.

```
<Sysname> display port-group manual
The following manual port group exist(s):
group1                                    group2
```

Display the information about all the manual port groups.

```
<Sysname> display port-group manual all
Member of group1:
    Ethernet1/1/1            Ethernet1/1/2            Ethernet1/1/3
    Ethernet1/1/4            Ethernet1/1/5            Ethernet1/1/6
    Ethernet2/1/1            Ethernet2/1/2            Ethernet2/1/3
    Ethernet2/1/4
```

```
Member of group2:
None
```

Display the information about the port group named "group1".

```
<Sysname> display port-group manual group1
Member of group1:
    Ethernet1/1/1            Ethernet1/1/2            Ethernet1/1/3
    Ethernet1/1/4            Ethernet1/1/5            Ethernet1/1/6
    Ethernet2/1/1            Ethernet2/1/2            Ethernet2/1/3
    Ethernet2/1/4
```

Table 13 Field descriptions of the display port-group manual command

Field	Description
Member of group	Member of the manual port group
Ethernet1/1/1 Ethernet1/1/2 Ethernet1/1/3	Ethernet ports in the manual port group
Ethernet1/1/4 Ethernet1/1/5 Ethernet1/1/6	
Ethernet2/1/1 Ethernet2/1/2 Ethernet2/1/3	
Ethernet2/1/4	

duplex

Syntax **duplex** { **auto** | **full** | **half** }

undo duplex

View Ethernet interface view

Parameters **auto**: Specifies the auto-negotiation mode.

full: Specifies the full-duplex mode.

half: Specifies the half-duplex state. This keyword is not applicable on GigabitEthernet interfaces.

Description Use the **duplex** command to set the duplex mode for an Ethernet interface.

Use the **undo duplex** command to restore the default duplex mode.

By default, the duplex mode of an Ethernet interface is determined through auto-negotiation.

Related commands: **speed**.

These two commands are not applicable to Ten-GigabitEthernet interface.

Examples # Configure interface Ethernet 1/1/1 to operate in the full-duplex mode.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1/1
[Sysname-Ethernet1/1/1] duplex full
```

flow-control (Ethernet interface view)

Syntax **flow-control**

undo flow-control

View Ethernet interface view

Parameters None

Description Use the **flow-control** command to enable flow control on an Ethernet interface.

Use the **undo flow-control** command to disable flow control on an Ethernet interface.

By default, flow control is disabled.

Flow control takes effect only when it is enabled on both sides.

Examples # Enable flow control on interface Ethernet1/1/1.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1/1
[Sysname-Ethernet1/1/1] flow-control
```

flow-interval

Syntax ***flow-interval*** *interval*

undo flow-interval

View Ethernet interface view

Parameters *interval*: Interval for generating interface statistics, in the range 5 to 300 (in seconds) and in step of 5. The system default is 300 seconds.

Description Use the **flow-interval** command to set the interval for generating interface statistics.

Use the **undo flow-interval** command to restore the default.

Examples # Set the time interval for generating interface statistics to 100 seconds for interface Ethernet1/1/1.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1/1
[Sysname-Ethernet1/1/1] flow-interval 100
```

group-member

Syntax **group-member** *interface-list*

undo group-member *interface-list*

View Manual port group view

Parameters *interface-list*: Ethernet interface list, in the format of {*interface-type interface-number* [***to*** *interface-type interface-number*] } &<1-10>, where *interface-type interface-number* is Ethernet interface type and number, and &<1-10> means that you can specify up to 10 interfaces/interface ranges for this argument.

Description Use the **group-member** command to add Ethernet interfaces to a manual port group.

Use the **undo group-member** command to remove Ethernet interfaces from a manual port group.

By default, a manual port group contains no Ethernet interface.

Examples # Add interfaces Ethernet1/1/1 and Ethernet1/1/2 to the manual port group named "group1".

```
<Sysname> system-view
[Sysname] port-group manual group1
[Sysname-port-group-manual-group1] group-member Ethernet 1/1/1 to Ethernet 1
/1/2
```

interface

Syntax ***interface*** *interface-type interface-number*

View System view

Parameters *interface-type interface-number*:

- *Interface is numbered using slot number, and interface number. For example, the interface number of Ethernet 1/1/1 is 1/1/1.*
- *For ease of user input, interface type can be abbreviated so long as it does not cause any confusion, for example, interface Ethernet 1/1/1 can be abbreviated as e1/1/1.*

Description Use the **interface** command to enter interface view.

Examples # Enter Ethernet1/1/1 interface view.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1/1
[Sysname-Ethernet1/1/1]
```

jumboframe enable

Syntax **jumboframe enable** [*jumboframe-value*] ***slot*** *slot-number*

undo jumboframe enable slot *slot-number*

View System view

Parameters *jumboframe-value*: Size of the jumbo frames allowed to pass through an Ethernet interface, in the range 1,552 to 10,240 (in bytes). By default, the size of the jumbo frames allowed is 1,552 bytes.

Description Use the **jumboframe enable** command to allow jumbo frames that are of specified size to pass through the interfaces on a module.

Use the **undo jumboframe enable** command to disable jumbo frames from passing through the interfaces on a module.

By default, jumbo frames are allowed to pass through Ethernet interfaces.

With the **undo jumboframe enable** command executed, the size of the jumbo frames allowed is 1,522 bytes.

- *The jumboframe-value argument is in the range 1,552 to 10,236 for the modules LSB1XP4B, LSB1XP4CA, LSB1XP4DB, LSB1GV48DA, 3C17532A, and LSB1GV48DB.*
- *By default, the modules 3C17548, 3C17542 and LSB1NATB0 allow jumbo frames with their size being 8,192 bytes. If you execute the* ***jumboframe enable*** *command for a module of this type, an error occurs.*
- *For FE interfaces, the size of the jumbo frames allowed is fixed to 1,552 bytes.*

Examples # Enable jumbo frames with their size being 1,552 bytes to pass through all the Ethernet interfaces on the module seated in slot 4.

```
<Sysname> system-view
[Sysname] jumboframe enable slot 4
```

link-delay

Syntax ***link-delay*** *delay-time*

undo link-delay

View Ethernet interface view

Parameters *delay-time*: Up/Down suppression time for the physical connection of an Ethernet interface, in the range 0 to 10 (in seconds).

Description Use the **link-delay** command to set the suppression time of physical-link-state changes on an Ethernet Interface.

Use the **undo link-delay** command to restore the default.

By default, the suppression time of physical-link-state changes on an Ethernet Interface is 1 second.

Examples # Set the up/down suppression time of the physical connection of Ethernet 1/1/1 interface to 2 seconds.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1/1
[Sysname-Ethernet1/1/1] link-delay 2
```

loopback

Syntax **loopback** { **external** | **internal** }

undo loopback

View Ethernet interface view

Parameters **external**: Enables external loopback testing.

internal: Enables internal loopback testing.

Description Use the **loopback** command to enable Ethernet interface loopback testing.

Use the **undo loopback** command to disable Ethernet interface loopback testing.

By default, Ethernet interface loopback testing is disabled.

- *Currently, Switch 8800s do not support external loopback testing.*
- *Loopback testing is required when you test certain functions, such as locating problems in an Ethernet.*
- *After you enable loopback testing on an Ethernet interface, the interface operates in full-duplex mode at the highest speed. The interface will return to its original state when loopback testing is disabled.*

Examples # Enable internal loopback testing on Ethernet 1/1/1.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1/1
[Sysname-Ethernet1/1/1] loopback internal
```

mdi

Syntax **mdi** { **across** | **auto** | **normal** }

undo mdi

View Ethernet interface view

Parameters **across**: Specifies cross-over cables for the Ethernet interface.

auto: Configures the Ethernet interface to be auto-sensing for the cable type.

normal: Specifies straight-through cables for the Ethernet interface

Description Use the **mdi** command to configure the cable type that can be sensed by an Ethernet interface.

Use the **undo mdi** command to restore the default.

By default, an Ethernet interface senses the type of the network cable connected to it automatically.

Examples # Configure the interface Ethernet1/1/1 to use cross-over cables.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1/1
[Sysname-Ethernet1/1/1] mdi across
```

port-group

Syntax **port-group** { ***manual*** *port-group-name* | ***aggregation*** *agg-id* }

undo port-group manual *port-group-name*

View System view

Parameters *port-group-name*: Name of a manual port group, a string of 1 to 32 characters.

aggregation *agg-id*: Specifies the ID of an existing aggregation port group.

Description Use the **port-group manual** command to create a manual port group. If the manual port group identified by the *port-group-name* argument already exists, this command leads you to manual port group view.

Use the **port-group aggregation** command to enter aggregation port group view.

Use the **undo port-group manual** command to remove a manual port group.

By default, no manual port group is created.

Examples # Create a manual port group named "group1".

```
<Sysname> system-view
[Sysname] port-group manual group1
[Sysname-port-group-manual-group1]
```

reset counters interface

Syntax ***reset counters interface*** [*interface-type* [*interface-number*]]

View User view

Parameters *interface-type*: Interface type.

interface-number: Interface number.

Description Use the **reset counters interface** command to clear the statistics on specific interfaces.

To obtain interface statistics within specific period of time, you need to clear the existing interface statistics first.

- If neither interface type nor interface number is specified, this command clears the statistics on all the interfaces.
- If only interface type is specified, this command clears the statistics on the interfaces that are of specific type.
- If both interface type and interface number are specified, this command clears the statistics on the specified interface.

Examples # Clear the statistics on Ethernet1/1/1.

```
<Sysname> reset counters interface ethernet 1/1/1
```

shutdown (Ethernet interface view)

Syntax **shutdown**

undo shutdown

View Ethernet interface view

Parameters None

Description Use the **shutdown** command to shut down an Ethernet interface.

Use the **undo shutdown** command to bring up an Ethernet interface.

By default, an Ethernet interface is up.

Examples # Shut down interface Ethernet1/1/1.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1/1
[Sysname-Ethernet1/1/1] shutdown
```

Bring up interface Ethernet1/1/1.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1/1
[Sysname-Ethernet1/1/1] undo shutdown
```

source-mac-tail

Syntax ***source-mac-tail*** *last-byte*

undo source-mac-tail

View Ethernet interface view

Parameters *last-byte:* Two-digit hexadecimal number to be used as the least octet of the source MAC address.

Description Use the **source-mac-tail** command to set the least octet of the source MAC address for an interface.

After you execute the **source-mac-tail** command, packets forwarded on Layer 3 through the interface uses the number set by this command as the least octet of their source MAC addresses.

Use the **undo source-mac-tail** command to remove the source MAC address setting.

By default, the source MAC address for an interface is that of the corresponding VLAN interface.

Currently, this command is not supported by the following modules: LSB1GV48DA, LSB1GV48DB, 3C17532A, 3C17538, LSB1XP4B, LSB1XP4CA, and LSB1XP4DB.

Examples # Set the least octet of the source MAC address to 0x12 for interface Ethernet 3/1/1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface Ethernet 3/1/1
[Sysname-Ethernet3/1/1] source-mac-tail 12
```

Remove the source MAC address setting for the interface Ethernet 3/1/1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface Ethernet 3/1/1
[Sysname-Ethernet3/1/1] undo source-mac-tail
```

speed (Ethernet interface view)

Syntax **speed** { **10** | **100** | **1000** | **auto** }

undo speed

View Ethernet interface view

Parameters **10**: Specifies the interface rate as 10 Mbps.

100: Specifies the interface rate as 100 Mbps.

1000: Specifies the interface rate as 1,000 Mbps.

auto: Specifies the interface rate is determined through auto-negotiation.

Description Use the **speed** command to set the operating rate for an Ethernet interface.

Use the **undo speed** command to restore the default operating rate.

By default, an Ethernet interface determines its operating rate through auto-negotiation.

Note that the **speed 1000** command is only applicable to GigabitEthernet interface.

Related commands: **duplex**.

This command is not applicable for Ten-GigabitEthernet interfaces.

Examples # Configure the operating rate of interface Ethernet1/1/1 as 100 Mbps.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1/1
[Sysname-Ethernet1/1/1] speed 100
```

4 MAC Address Table Management Configuration Commands

display mac-address

Syntax **display mac-address** [*mac-address* [**vlan** *vlan-id*] | [**dynamic** | **static**] [**interface** *interface-type interface-number*] [**vlan** *vlan-id*] [**count**]]

display mac-address blackhole [**vlan** *vlan-id*] [**count**]

View Any view

Parameters *mac-address*: Specifies a MAC address in the format of H-H-H.

static: Displays static MAC address entries, which do not age.

dynamic: Displays dynamic MAC address entries, which age.

blackhole: Displays blackhole MAC address entries. The attribute of the blackhole MAC address entries is the same as that of the static MAC address entries. The packets whose destination MAC addresses match blackhole MAC address entries are discarded..

interface-type interface-number: Displays MAC address learning status of the ports with the specified type and number.

vlan-id: Displays MAC address entries of the specified VLAN.

count: Displays the total number of MAC addresses in the MAC address table.

Description Use the **display mac-address** command to display information about the MAC address table.

Related commands: **mac-address**,**mac-address timer**.

Examples # Display the MAC address table entry.

```
<Sysname> display mac-address 00e0-fc01-0101
MAC ADDR     VLAN ID  STATE      PORT INDEX      AGING TIME(s)
00e0-fc01-0101 1   Learned   GigabitEthernet4/1/1  NOAGED
```

Table 14 Field descriptions of the display mac-address command

Field	Description
MAC ADDR	MAC address
VLAN ID	ID of the VLAN to which the MAC address belongs

Table 14 Field descriptions of the display mac-address command

Field	Description
STATE	State of a MAC address
PORT INDEX	Port name. The blackhole MAC address is displayed as "N/A"
AGING TIME(s)	Aging time, which could be: AGING, indicates that the entry is aging. NOAGED, indicates that the entry does not age.

display mac-address aging-time

Syntax **display mac-address aging-time**

View Any view

Parameters None

Description Use the **display mac-address aging-time** command to display the aging time of dynamic entries in the MAC address table.

Related commands: **mac-address**, **mac-address timer**, **display mac-address**.

Examples # Display the aging time of dynamic entries in the MAC address table.

```
<Sysname> display mac-address aging-time
Mac address aging time: 300s
```

The above information indicates that the aging time of dynamic entries in the MAC address table is 300 seconds.

display mac-address mac-learning

Syntax **display mac-address mac-learning** [*interface-type interface-number*]

View Any view

Parameters *interface-type interface-number*: Displays MAC address learning status of the port with the specified type and number.

Description Use the **display mac-address mac-learning** command to display MAC address learning status of the specified or all Ethernet ports.

Examples # Display MAC address learning status of all Ethernet ports.

```
<Sysname> display mac-address mac-learning
Mac address learning status of the switch: enable

PortName              Learning Status
```

```
GigabitEthernet1/1/1      enable
GigabitEthernet1/2/1      enable
GigabitEthernet1/3/1      enable
GigabitEthernet1/4/1      enable
GigabitEthernet2/1/1      enable
GigabitEthernet2/2/1      enable
GigabitEthernet2/3/1      enable
GigabitEthernet2/4/1      enable
......
```

Table 15 Field descriptions of display mac-address mac-learning

Field	Description
Mac address learning status of the switch	Global MAC address learning status, enabled or disabled.
PortName	Port name
Learning Status	Port MAC address learning status, enabled or disabled

mac-address (Ethernet interface view)

Syntax **mac-address** { **static** | **dynamic** } *mac-address* **vlan** *vlan-id*

undo mac-address { **static** | **dynamic** } *mac-address* **vlan** *vlan-id*

View Ethernet interface view

Parameters **dynamic**: Dynamic MAC address entries.

static: Static MAC address entries.

mac-address: Specifies a MAC address in the format of H-H-H.

vlan-id: VLAN ID.

Description Use the **mac-address** command to add or modify a MAC address entry on a specified Ethernet port.

Use the **undo mac-address** command to remove a MAC address entry on the Ethernet port.

As your MAC address entries configuration cannot survive a reboot, save it after completing the configuration. The dynamic MAC address table entries however will be lost whether you save the configuration or not.

Before using this command, you must add the port to the specified VLAN.

Do not configure dynamic or static MAC addresses on an aggregation port.

Related commands: **display mac-address**.

Examples # Add a static entry for MAC address 00e0-fc01-0101 on the GigabitEthernet 1/1/1 with VLAN ID 2.

```
<Sysname> system-view
[Sysname] interface gigabitEthernet 1/1/1
[Sysname-GigabitEthernet1/1/1] mac-address static 00e0-fc01-0101 vlan 2
```

mac-address (system view)

Syntax **mac-address** { **static** | **dynamic** } *mac-address* **interface** *interface-type interface-number* **vlan** *vlan-id*

mac-address blackhole *mac-address* **vlan** *vlan-id*

undo mac-address [{ **static** | **dynamic** } *mac-address* **interface** *interface-type interface-number* **vlan** *vlan-id*]

undo mac-address [**static** | **dynamic** | **blackhole**] [*mac-address*] **vlan** *vlan-id*

undo mac-address [**static** | **dynamic**] *mac-address* **interface** *interface-type interface-number* **vlan** *vlan-id*

undo mac-address [**static** | **dynamic**] **interface** *interface-type interface-number*

View System view

Parameters **static**: Static MAC address entries.

dynamic: Dynamic MAC address entries.

blackhole: Blackhole MAC address entries. These entries do not age but you can add or remove them. The packets whose destination MAC addresses match blackhole MAC address entries are discarded.

mac-address: Specifies a MAC address in the format of H-H-H.

interface-type interface-number: Specifies a port by its type and number.

vlan-id: Specifies a VLAN ID.

Description Use the **mac-address** command to add or modify a MAC address entry.

Use the **undo mac-address** command to remove one or all MAC address entries.

Note that**:**

- If the existing MAC address is a dynamic address, you can modify it as a static or blackhole address, and if the existing MAC address is a static address or blackhole address, you will be prompted that this MAC address already exists, and modification is not necessary.

- You can delete all the MAC address entries on a port or a VLAN, or you can delete the dynamic MAC address entry, the static MAC address entry or the blackhole MAC address entry.
- As your MAC address entries configuration cannot survive a reboot, save it after completing the configuration. The dynamic entries however will be lost whether you save the configuration or not.
- Before using this command, you must add the port to the specified VLAN.

Do not configure a dynamic, static or blackhole MAC address on an aggregation port.

Related commands: **display mac-address**.

Examples # Add a static entry for MAC address 00E0-FC01-0101. All frames destined to this MAC address are sent out of port Ethernet 1/1/1 which belongs to VLAN 2.

```
<Sysname> system-view
[Sysname] mac-address static 00e0-fc01-0101 interface ethernet 1/1/1 vlan 2
```

mac-address mac-learning disable

Syntax **mac-address mac-learning disable**

undo mac-address mac-learning disable

View System view/Ethernet interface view/port group view

Parameters None

Description Use the **mac-address mac-learning disable** command to disable MAC address learning globally or specify the MAC address learning function of the Ethernet port.

Use the **undo mac-address mac-learning disable** command to enable MAC address learning globally, or specify the MAC address learning function of the Ethernet port.

By default, MAC address learning is enabled globally.

Note that you need to disable MAC address learning sometimes to prevent the MAC address table from being saturated, for example, when your device is being attacked by a great deal of frames with different source MAC addresses. This somewhat affects update of the MAC address table.

Related commands: **display mac-address mac-learning**.

Examples # Disable global MAC address learning.

```
<Sysname> system-view
[Sysname] mac-address mac-learning disable
```

Disable MAC address learning on port Ethernet 1/1/1.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1/1
[Sysname-Ethernet1/1/1] mac-address mac-learning disable
```

mac-address max-mac-count (Ethernet interface view/port group view)

Syntax **mac-address max-mac-count** { *count* | **disable-forwarding** }

undo mac-address max-mac-count [**disable-forwarding**]

View Ethernet interface view/port group view

Parameters *count*: Maximum number of MAC addresses that can be learned on a port, in the range 0 to 14336. When the argument takes 0, the port is not allowed to learn MAC addresses.

disable-forwarding: Disables forwarding of frames after the number of learned MAC addresses reaches the upper limit.

Description Use the **mac-address max-mac-count** *count* command to configure the maximum number of MAC addresses that can be learned on an Ethernet port and whether forwarding frames is allowed after the maximum number of learned MAC addresses reaches the upper limit.

Use the **undo mac-address max-mac-count** command to restore the default maximum number of MAC addresses that can be learned on an Ethernet port.

Use the **undo mac-address max-mac-count disable-forwarding** command to allow forwarding frames received on an Ethernet port after the number of learned MAC addresses reaches the upper limit.

The default maximum number of MAC addresses that can be learned on a port is 14336, and forwarding is allowed when the upper limit is reached.

Executed in Ethernet interface view, this command takes effect only for the current port; executed in port group view, this command takes effect on all the ports under the port group.

Related commands: **mac-address (system view)**, **mac-address (Ethernet interface view)**, **mac-address timer**.

Examples # Set the maximum number of MAC addresses that can be learned on port Ethernet 1/1/1 to 600. After this upper limit is reached, frames received with unknown destination MAC addresses on the port will not be forwarded.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1/1
[Sysname-Ethernet1/1/1] mac-address max-mac-count 600
[Sysname-Ethernet1/1/1] mac-address max-mac-count disable-forwarding
```

mac-address max-mac-count (VLAN view)

Syntax **mac-address max-mac-count** *count*

undo mac-address max-mac-count

View VLAN view

Parameters *count*: Maximum number of MAC addresses that can be learned on a VLAN, in the range 0 to 172032, with 0 meaning that MAC address learning of this VLAN is not allowed.

Description Use the **mac-address max-mac-count** *count* command to configure the maximum number of MAC addresses that can be learned on a VLAN.

Use the **undo mac-address max-mac-count** command to restore the default maximum number of MAC addresses that can be learned on a VLAN.

A VLAN can learn up to 172032 MAC addresses by default.

Related commands: **mac-address**, **mac-address timer**.

There are no actual Layer 2 physical interfaces on the Super VLAN, and the number of the learned MAC addresses is always 0, so configuring the number of MAC addresses under Super VLAN is meaningless.

Examples # Set the maximum number of MAC addresses that can be learned on VLAN 10 to 600.

```
<Sysname> system-view
[Sysname] vlan 10
[Sysname-vlan10] mac-address max-mac-count 600
```

mac-address timer

Syntax **mac-address timer** { **aging** *seconds* | **no-aging** }

undo mac-address timer aging

View System view

Parameters **aging** *seconds*: Sets an aging time in seconds for dynamic MAC address entries.

no-aging: Sets dynamic MAC address entries not to age.

Description Use the **mac-address timer** command to configure the aging timer for dynamic MAC address entries.

Use the **undo mac-address timer** command to restore the default.

By default, the aging time for the MAC address dynamic entry is 300 seconds.

Set the aging timer appropriately: a short interval may result in removal of valid entries and hence unnecessary broadcasts which may affect device performance; a long aging interval may cause the MAC address table to retain outdated entries and fail to accommodate latest network changes. In this case, delay may result when a workstation is moved from one port to another.

Examples # Set the aging timer for dynamic MAC address entries to 500 seconds.

```
<Sysname> system-view
[Sysname] mac-address timer aging 500
```

5 LINK AGGREGATION CONFIGURATION COMMANDS

debugging lacp packet

Syntax **debugging lacp packet** [**interface** *interface-type interface-number* [**to** *interface-type interface-number*]]

undo debugging lacp packet [**interface** *interface-type interface-number* [**to** *interface-type interface-number*]]

View User view

Parameters *interface-type interface-number*: Port type and port number.

to: Specifies a port index range, with the two *interface-type interface-number* argument pairs around it as the two ends.

Description Use the **debugging lacp packet** command to enable debugging for LACP packets on specific ports.

Use the **undo debugging lacp packet** command to disable LACP packet debugging on specific ports.

By default, the debugging for LACP packets is disabled.

If no port is specified, these two commands apply to all the ports with the LACP enabled.

Table 16 Field descriptions of the debugging lacp packet command

Field	Description
size	Size of an LACP protocol packet, which is 128 bytes.
subtype	Protocol subtype of an LACP packet, which is 1 for LACP packets.
version	Protocol version. A value of 1 indicates LACP.

Table 16 Field descriptions of the debugging lacp packet command

Field	Description
Actor	Local port information contained in a protocol packet, in which: ■ tlv being 1 indicates that the information displayed is about the local port. ■ len indicates the length of the information. ■ sys-pri indicates the local system LACP priority. ■ sys-mac indicates the local system MAC address. ■ key indicates the operation key value assigned to the local port. ■ pri indicates the LACP priority of the local port. ■ p indicates the local port number. ■ state indicates the current LACP state of the local port.
Partner	Remote port information contained in a protocol packet and saved in the local system, in which: ■ tlv being 2 indicates that the information displayed is the remote port information saved in the local system. ■ len indicates the length of the information. ■ sys-pri indicates the remote system LACP priority. ■ sys-mac indicates the remote system MAC address. ■ key indicates the operational key value assigned to the remote port. ■ pri indicates the LACP priority of the remote port. ■ p indicates the remote port number. ■ state indicates the current LACP state of the remote port.
Collector	Collector field information contained in a protocol packet, in which: ■ tlv being 3 indicates the Collector field. ■ len indicates the length of the field. ■ col-max-delay indicates the maximum delay.
Terminator	Terminator field information contained in a protocol packet, in which: ■ tlv being 0 indicates the Terminator field, the end of a protocol packet. ■ len indicates the length of the field.

Examples # Enable debugging for LACP packets on port Ethernet 1/1/1.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1/1
```

```
[Sysname-Ethernet1/1/1] lacp enable
[Sysname-Ethernet1/1/1] return
<Sysname> terminal debugging
<Sysname> debugging lacp packet interface ethernet 1/1/1
*0.60323 Sysname LAGG/8/Pkt:
 Send LACP Packet via port Ethernet1/1/1
```

// An LACP packet was sent through Ethernet 1/1/1.

```
*0.60323 Sysname LAGG/8/Pkt:
 size=128, subtype =1, version=1
```

// The size of the packet is 128 bytes. The protocol subtype and the protocol version are all 1.

```
 Actor: tlv=1, len=20, sys-pri=0x8000, sys-mac=00e0-fc02-0300, key=0
x1, pri=0x8000, p=0x2, state=0x45
```

// The information about the local port carried in the packet is as follows.

- *Length of the information:20*
- *Local system LACP priority: 0x8000*
- *Local system MAC address: 00e0-fc02-0300*
- *Operation key value assigned to the local port: 0x1*
- *LACP priority of the local port: 0x8000*
- *Local port number: 0x2*
- *Current LACP state of the local port: 0x45*

```
Partner: tlv=2, len=20, sys-pri=0x0, sys-mac=0000-0000-0000, key=0x0
, pri=0x0, p=0x0, state=0x0
```

// The information about the remote port carried in the packet is as follows.

- *Length of the information:20*
- *Remote system LACP priority: 0x0*
- *Remote system MAC address: 0000-0000-0000*
- *Operation key value assigned to the remote port: 0x0*
- *LACP priority of the remote port: 0x0*
- *Remote port number: 0x0*
- *Current LACP state of the remote port: 0x0*

```
Collector: tlv=3, len=16, col-max-delay=0
```

// Information contained in the Collector field of the packet is as follows.

- *Length of the field: 16*
- *Maximum delay: 0*

```
Terminator: tlv=0, len=0
```

// The length of the Terminator field of the packet is 0.

```
*0.1221133 Sysname LAGG/8/Pkt:
 Receive LACP Packet via port Ethernet1/1/1
```

// A LACP packet was received through Ethernet 1/1/1.

```
*0.1221133 Sysname LAGG/8/Pkt:
 size=128, subtype =1, version=1
```

// The size of the packet is 128 bytes. The protocol subtype and the protocol version are all 1.

```
 Actor: tlv=1, len=20, sys-pri=0x8000, sys-mac=00e0-fc00-0000, key=0
x1, pri=0x8000, p=0x6, state=0x3d
```

// The information about the local port carried in the packet is as follows.

- *Length of the information:20*
- *Local system LACP priority: 0x8000*
- *Local system MAC address: 00e0-fc00-0000*
- *Operation key value assigned to the local port: 0x1*
- *LACP priority of the local port: 0x8000*
- *Local port number: 0x6*
- *Current LACP state of the local port: 0x3d*

```
Partner: tlv=2, len=20, sys-pri=0x8000, sys-mac=00e0-fc02-0300, key=
0x1, pri=0x8000, p=0x1, state=0xd
```

// The information about the remote port carried in the packet is as follows.

- *Length of the information:20*
- *Remote system LACP priority: 0x8000*
- *Remote system MAC address: 00e0-fc02-0300*
- *Operation key value assigned to the remote port: 0x1*
- *LACP priority of the remote port: 0x8000*
- *Remote port number: 0x1*
- *Current LACP state of the remote port: 0xd*

```
Collector: tlv=3, len=16, col-max-delay=0
```

// Information contained in the Collector field of the packet is as follows.

- *Length of the field: 16*
- *Maximum delay: 0*

```
Terminator: tlv=0, len=0
```

// The length of the Terminator field of the packet is 0.

Other similar information about LACP packets is omitted here.

debugging lacp state

Syntax **debugging lacp state** [**interface** *interface-type interface-number* [**to** *interface-type interface-number*]] { { **actor-churn** | **mux** | **partner-churn** | **ptx** | **rx** } * | **all** }

undo debugging lacp state [**interface** *interface-type interface-number* [**to** *interface-type interface-number*]] { { **actor-churn** | **mux** | **partner-churn** | **ptx** | **rx** } * | **all** }

View User view

Parameters *interface-type interface-number*: Port type and port number.

to: Specifies a port index range, with the two *interface-type interface-number* argument pairs around it as the two ends.

actor-churn: Enables/disables debugging for Actor-churn state machine.

mux: Enables/disables debugging for MUX state machine.

partner-churn: Enables/disables debugging for Partner-churn state machine.

ptx: Enables/disables debugging for PTX state machine.

rx: Enables/disables debugging for RX state machine.

all: Enables/disables debugging for all the state machines.

Description Use the **debugging lacp state** command to enable debugging for an LACP protocol state machine on specific ports.

Use the **undo debugging lacp state** command to disable debugging for an LACP protocol state machine on specific ports.

By default, debugging for any of the LACP protocol state machine is disabled.

If no port is specified, these two commands apply to all the ports with the LACP enabled.

Table 17 Field descriptions of the debugging lacp state command

Field	Description
from state XXX	The state before a state transition
to state XXX	The state after a state transition
stimulation	The condition that triggers a state transition.

Examples # Enable debugging for RX state machine on port Ethernet 1/1/2.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface ethernet1/1/2
[Sysname-Ethernet1/1/2] lacp enable
```

```
[Sysname-Ethernet1/1/2] return
<Sysname> terminal debugging
<Sysname> debugging lacp state interface ethernet 1/1/2 rx
*0.1360830 Sysname LAGG/8/FSM:
 Port Ethernet1/1/2: FSM Rx  transfers from state RESERVE to state INITIALIZE
 by the stimulation Begin_True
```

// The RX state machine has been initialized to the INITIALIZE state. The condition to the state is Begin_True (indicating the state machine starts).

```
*0.1360830 Sysname LAGG/8/FSM:
Port Ethernet1/1/2: FSM Rx  transfers from state INITIALIZE to state
 PORT_DISABLED
 by the stimulation UCT
```

// The RX state machine transited from the INITIALIZE state to the PORT-DISABLED state. The condition to the state is UCT (indicating no condition).

```
*0.1360830 Sysname LAGG/8/FSM:
Port Ethernet1/1/2: FSM Rx transfers from state PORT_DISABLED to state EXPIR
ED by the stimulation Lacp_Enabled
```

// The RX state machine transited from the PORT-DISABLED state to the EXPIRED state. The condition to the state is LACP_ENABLED (indicating LACP is enabled).

```
*0.1360862 Sysname LAGG/8/FSM:
 Port Ethernet1/1/2: FSM Rx  transfers from state EXPIRED to state CURRENT
 by the stimulation Pdu_Indicate
```

// The RX state machine transited from the EXPIRED state to the CURRENT state. The condition to the state is Pdu_Indicate (indicating a protocol packet is received from the peer).

debugging link-aggregation error

Syntax **debugging link-aggregation error**

undo debugging link-aggregation error

View User view

Parameters None

Description Use the **debugging link-aggregation error** command to enable debugging for link aggregation errors.

Use the **undo debugging link-aggregation error** command to disable debugging output.

By default, debugging for link aggregation errors is disabled.

Table 18 Field descriptions of the debugging link-aggregation error command

Field	Description
File	File where an error is detected

Table 18 Field descriptions of the debugging link-aggregation error command

Field	Description
Line	Line in the file where an error is detected.
ERROR	Error description

Examples # Enable debugging for link aggregation errors.

```
<Sysname> system-view
[Sysname] interface ethernet1/1/1
[Sysname-Ethernet1/1/1] lacp enable
[Sysname-Ethernet1/1/1] return
<Sysname> terminal debugging
<Sysname> debugging link-aggregation error
*0.21953 Sysname LAGG/8/lacpErrorEvent:
 File e:v500d05sp1softwarelacplacp_agm.c, Line: 1200
 ERROR------  Portindex: 1   LACP_SendLACPPacket ,g_ucLacpSysMAC NULL !
```

// An error occurred in the line numbered 1200 of the file e:v500d05sp1softwarelacplacp_agm.c. As indicated by the ERROR field, the system MAC address acquired was null.

debugging link-aggregation event

Syntax **debugging link-aggregation event**

undo debugging link-aggregation event

View User view

Parameters None

Description Use the **debugging link-aggregation event** command to enable debugging for link aggregation events.

Use the **undo debugging link-aggregation event** command to disable debugging output.

By default, debugging for link aggregation events is disabled.

Table 19 Field descriptions of the debugging link-aggregation event command

Field	Description
Port Index	Index of a port
Agg Index	ID of an aggregation group
Cfg MD5	MD5 summary
Restriction Value	Hardware restriction parameter
Admin Key	Administration key
Port Pri	Port LACP priority
Sys Mac	System MAC address
Sys Pri	System LACP priority

Table 19 Field descriptions of the debugging link-aggregation event command

Field	Description
Oper Key	Operational key assigned to a port
Unit Id	ID of a device

Examples # Enable debugging for link aggregation events.

```
<Sysname> debugging link-aggregation event
<Sysname> terminal debugging
<Sysname> display link-aggregation summary

Aggregation Group Type:D -- Dynamic, S -- Static , M -- Manual
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Actor ID: 0x8000, 00e0-fc57-367f

  AL  AL   Partner ID            Select Unselect Share Master
  ID  Type                       Ports  Ports    Type  Port
--------------------------------------------------------------------------
  10  M    none                  1      0        NonS  Ethernet2/1/1
```

// Link aggregation group 10 exists.

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

Remove link aggregation group 10.

```
[Sysname] undo link-aggregation group 10
*0.91991886 Sysname LAGG/8/AggDel:Link Aggregation 10 is deleted.
```

// Link aggregation group 10 was removed.

```
*0.91991961 Sysname LAGG/8/OperKeyDel:Oper key 1 is deleted.
```

// The operation key 1, which Ethernet 2/1/1 corresponds to, was removed.

```
*0.91992115 Sysname LAGG/8/AggDel:Slot=2;Link Aggregation 10 is deleted.
```

// Link aggregation group 10 was removed on the module seated in slot 2.

display lacp system-id

Syntax **display lacp system-id**

View Any view

Parameters None

Description Use the **display lacp system-id** command to display the local system ID (also known as actor system ID), which comprises the system LACP priority and the system MAC address.

Examples # Display the local system ID.

```
<Sysname> display lacp system-id
 Actor System ID: 0x8000, 00e0-fc00-0100
```

Table 20 Field descriptions of the display lacp system-id command

Field	Description
Actor System ID	Local system ID, comprising system LACP priority and system MAC address.

display link-aggregation interface

Syntax **display link-aggregation interface** *interface-type interface-number* [**to** *interface-type interface-number*]

View Any view

Parameters *interface-type interface-number*: Port type and port number.

to: Specifies a port index range, with the two *interface-type interface-number* arguments pairs around it as the two ends.

Description Use the **display link-aggregation interface** command to display the link aggregation-related information about specific ports.

Note that as ports in a manual link aggregation groups do not acquire the information about their peers automatically, so the entries in the information about the peer ports displayed are all 0 instead of the actual values. Moreover, this command does not display the statistics on the LACP packets processed by ports in manual aggregation groups.

Examples # Display the link aggregation-related information about port GigabitEthernet 4/2/1 (assuming that the port belongs to a manual aggregation group).

```
<Sysname> display link-aggregation interface gigabitEthernet4/2/1
Flags:  A -- LACP_Activity, B -- LACP_timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

 GigabitEthernet4/2/1:
   Selected AggID: 0
   Local:
     Port-Priority: 32768, Oper key: 0, Flag: {}
   Remote:
     System ID: 0x0, 0000-0000-0000
     Port Number: 0, Port-Priority: 0 , Oper-key: 0, Flag: {}
   Received LACP Packets: 0 packet(s), Illegal: 0 packet(s)
   Sent LACP Packets: 0 packet(s)
```

Display the link aggregation-related information about port Ethernet 1/1/2 (assuming that the port belongs to a dynamic aggregation group).

```
<Sysname> display link-aggregation interface ethernet1/1/2
Flags:  A -- LACP_Activity, B -- LACP_timeout, C -- Aggregation,
```

```
       D -- Synchronization, E -- Collecting, F -- Distributing,
       G -- Defaulted, H -- Expired

Ethernet1/1/2:
  Selected AggID: 2
  Local:
    Port-Priority: 32768, Oper key: 1, Flag: {ACDEF}
  Remote:
    System ID: 0x8000, 00e0-fc46-2a9a
    Port Number: 209, Port-Priority: 32768 , Oper-key: 1, Flag: {ACDEF}
  Received LACP Packets: 17 packet(s), Illegal: 0 packet(s)
  Sent LACP Packets: 16 packet(s)
```

Table 21 Field descriptions of the display link-aggregation interface command

Field	Description
Flags	LACP state flag, one byte in length. Each bit in this field is a flag and is represented by a character among A through H. When a bit is set, the corresponding character is displayed. Following describes the flags. ■ A" indicates LACP is enabled; absence of this character indicates LACP is not enabled. ■ B" indicates short LACP timeout; absence of this character indicates long LACP timeout. ■ C" indicates the link can be aggregated. ■ D" indicates the link is synchronized. ■ E" indicates the link is in collecting state. ■ F" indicates the link is in distributing state. ■ G" indicates the receiving state machine of the sending system is in the default state. ■ H" indicates the receiving state machine of the sending system is in the expired state.
Selected AggID	ID of the link aggregation group the port belongs to
Local:	Local system information.
Port-Priority	■ Port-Priority: Local port LACP priority
Oper key	■ Oper key: Operation key
Flag	■ Flag: LACP state flag
Remote:	Remote system information.
System ID	System ID: Remote system ID
Port Number	Port Number: Port number
Port-Priority	Port-Priority: Port LACP priority
Oper-key	Oper-key: Operation key
Flag	Flag: LACP state flag
Received LACP Packets:	Statistics on LACP packets.
Illegal	Packets: Number of the LACP packets received
Sent LACP Packets	Illegal: Number of the invalid LACP packets Sent LACP Packets: Number of the LACP packets sent

display link-aggregation service-type

Syntax **display link-aggregation service-type** [*agg-id*]

View Any view

Parameters *agg-id*: ID of an existing service loop group.

Description Use the **display link-aggregation service-type** command to display the information about a service loop group.

If no aggregation group is specified, this command displays the information about all the service loop groups.

Examples # Display the information about service loop group 1.

```
<Sysname> display link-aggregation service-type 1
 Service-Loop         Service                    Quote
   Group ID            Type                      Number
-------------------------------------------------------
     1                ipv6                         0
```

Table 22 Field descriptions of the display link-aggregation service-type command

Field	Description
Service-Loop Group ID	Service loop group ID
Service Type	Service type supported by the service loop group
Quote Number	Number of the ports to which the service loop group is applied. You can remove a service loop group only when it is applied to no port.

display link-aggregation summary

Syntax **display link-aggregation summary**

View Any view

Parameters None

Description Use the **display link-aggregation summary** command to display the summary of all the link aggregation groups.

Note that as ports in a manual link aggregation groups do not acquire the information about their peers automatically, so the entries in the information about the peer ports displayed are all 0 instead of the actual values.

Examples # Display the summary of all the link aggregation groups.

```
<Sysname> display link-aggregation summary

Aggregation Group Type:D -- Dynamic, S -- Static , M -- Manual
```

```
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Actor ID: 0x8000, 000f-e222-e5cd

  AL  AL   Partner ID            Select Unselect Share Master
  ID  Type                       Ports  Ports    Type  Port
------------------------------------------------------------------------------
----
  222 M    none                  0      2        NonS  GigabitEthernet4/2/1
```

Table 23 Field descriptions of the display link-aggregation summary command

Field	Description
Aggregation Group Type	Aggregation group type, which can be ■ S, for static LACP aggregation ■ M, for manual aggregation
Loadsharing Type	Load sharing type, which can be ■ Shar, for load sharing; ■ Nons, for non-load sharing.
Actor ID	Local system ID
AL ID	Link aggregation group ID
AL Type	Link aggregation group type
Partner ID	Remote system ID
Select Ports	Number of selected ports
Unselect Ports	Number of unselected ports
Share Type	Load sharing type
Master Port	Master port

display link-aggregation verbose

Syntax **display link-aggregation verbose** [*agg-id*]

View Any view

Parameters *agg-id*: ID of an existing link aggregation group.

Description Use the **display link-aggregation verbose** command to display the detailed information about a link aggregation group.

If you do not provide the *agg-id* argument, this command displays the detailed information about all the link aggregation groups.

Note that as ports in a manual link aggregation groups do not acquire the information about their peers automatically, so the entries in the information about the peer ports displayed are all 0 instead of the actual values.

Examples # Display the detailed information about link aggregation group 222.

```
<Sysname> display link-aggregation verbose 222
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Flags:  A -- LACP_Activity, B -- LACP_timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired
```

```
Aggregation ID: 222,  AggregationType: Manual,   Loadsharing Type: NonS
Aggregation Description:
System ID: 0x8000, 000f-e222-e5cd
Port Status: S -- Selected,  U -- Unselected
Local:
  Port             Status  Priority  Oper-Key  Flag
--------------------------------------------------------------------------------
----
  GE4/2/1          U       32768     1         {}
  GE4/2/2          U       32768     2         {}

Remote:
  Actor            Partner Priority  Oper-Key  SystemID               Flag
--------------------------------------------------------------------------------
----
  GE4/2/1          0       0         0         0x0000,0000-0000-0000  {}
  GE4/2/2          0       0         0         0x0000,0000-0000-0000  {}
```

Table 24 Field descriptions of the display link-aggregation verbose command

Field	Description
Loadsharing Type	Load sharing type, which can be ■ Shar, for load sharing; ■ Nons, for non-load sharing.
Flags	LACP state flag, one byte in length. Each bit in this field is a flag and is represented by a character among A through H. When a bit is set, the corresponding character is displayed. Following describes the flags. ■ A" indicates LACP is enabled; absence of this character indicates LACP is not enabled. ■ B" indicates short LACP timeout; absence of this character indicates long LACP timeout. ■ C" indicates the link can be aggregated. ■ D" indicates the link is synchronized. ■ E" indicates the link is in collecting state. ■ F" indicates the link is in distributing state. ■ G" indicates the receiving state machine of the sending system is in the default state. ■ H" indicates the receiving state machine of the sending system is in the expired state.
Aggregation ID	Link aggregation group ID
AggregationType	Link aggregation type, which can be manual or static LACP.
Aggregation Description	Link aggregation group name
System ID	Local system ID
Port State	Port state in a link aggregation group, which can be selected and unselected
Local: Port, Status, Priority, Oper-key, Flag	Other information about the local end, including member ports, port state, port LACP priority, operation key, and flags
Remote: Actor, Partner, Priority, Oper-key, SystemID, Flag	Detailed information about the remote end, including corresponding local port, port ID, port LACP priority, operation key, system ID, and flags

lacp enable

Syntax **lacp enable**

undo lacp enable

View Ethernet interface view

Parameters None

Description Use the **lacp enable** command to enable LACP on the port.

Use the **undo lacp enable** command to disable LACP on the port.

By default, LACP is disabled on a port.

Examples # Enable LACP on port Ethernet 1/1/1.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1/1
[Sysname-Ethernet1/1/] lacp enable
```

lacp port-priority

Syntax **lacp port-priority** *port-priority*

undo lacp port-priority

View Ethernet interface view

Parameters *port-priority*: Port LACP priority.

Description Use the **lacp port-priority** command to assign an LACP priority to the port.

Use the **undo lacp port-priority** command to restore the default.

By default, port LACP priority is 32768.

Related commands: **display link-aggregation interface**, **display link-aggregation verbose**.

Examples # Assign LACP priority 64 to a port.

```
<Sysname> system-view
[Sysname] interface ethernet1/1/1
[Sysname-Ethernet1/1/1] lacp port-priority 64
```

lacp system-priority

Syntax **lacp system-priority** *system-priority*

undo lacp system-priority

View System view

Parameters *system-priority*: System LACP priority.

Description Use the **lacp system-priority** command to assign an LACP priority to the local system.

Use the **undo lacp system-priority** command to restore the default.

By default, system LACP priority is 32768.

Examples # Assign LACP priority 64 to the local system.

```
<Sysname> system-view
[Sysname] lacp system-priority 64
```

link-aggregation group description

Syntax **link-aggregation group** *agg-id* **description** *agg-name*

undo link-aggregation group *agg-id* **description**

View System view

Parameters *agg-id*: Link aggregation group ID.

agg-name: Link aggregation group name.

Description Use the **link-aggregation group description** command to configure a name for the specified link aggregation group.

Use the **undo link-aggregation group description** command to remove the name of the specified link aggregation group.

Related commands: **display link-aggregation verbose**.

Examples # Name link aggregation group 22 as abc.

```
<Sysname> system-view
[Sysname] link-aggregation group 22 description abc
```

link-aggregation group mode

Syntax **link-aggregation group** *agg-id* **mode** { **manual** | **static** }

undo link-aggregation group *agg-id*

View System view

Parameters *agg-id*: Link aggregation group ID.

manual: Creates a manual link aggregation group.

static: Creates a static LACP link aggregation group.

Description Use the **link-aggregation group mode** command to create a manual or static LACP link aggregation group.

Use the **undo link-aggregation group** command to remove a link aggregation group. If the group is functioning as a service loop group, this can result in the removal of the service loop group.

- You can use the **undo** form of the command to remove static LACP link aggregation groups. In the case of removing a dynamic aggregation group, the member ports of the group form another dynamic aggregation group with an ID that can be the same as or different than the old one, depending on the current system configuration.
- An aggregation group being referenced by other modules cannot be removed.

Related commands: **display link-aggregation summary**.

Examples # Create manual link aggregation group 22.

```
<Sysname> system-view
[Sysname] link-aggregation group 22 mode manual
```

link-aggregation group service-type

Syntax **link-aggregation group** *agg-id* **service-type** { { **ipv6** | **ipv6mc** } * | **mpls** | **tunnel** }

undo link-aggregation group *agg-id* **service-type**

View System view

Parameters *agg-id*: ID of an existing manual aggregation group.

ipv6: Sets the service type to IPv6 (for supporting IPv6 unicast services).

ipv6mc: Sets the service type to IPv6mc (for supporting IPv6 multicast services).

tunnel: Sets the service type to tunnel (for supporting tunnel services).

mpls: Sets the service type to MPLS (for supporting MPLS services).

Description Use the **link-aggregation group service-type** command to configure an existing manual aggregation group as a service loop group that is of specific type.

Use the **undo link-aggregation group service-type** command to restore a service loop group to a manual aggregation group.

- *Currently, for Switch 8800s, the modules with their models suffixed with "DA", "DB", and "DC" support IPv6 unicast/multicast and tunnel service loop groups; those with their models suffixed with "C" and "CA" support MPLS service loop groups.*
- *There can be up to one service loop group for each service loop group type.*
- *You can change the type of an existing service loop group. The operation fails if it is currently referenced by a module or the service loop group contains ports whose attributes conflict with the intended service type.*
- *You can use the **undo link-aggregation group** command to remove an existing service loop group that is currently referenced by no module.*

Examples # Configure link aggregation group 5 as a tunnel service loop group.

```
<Sysname> system-view
[Sysname] link-aggregation group 5 service-type tunnel
```

port link-aggregation group

Syntax **port link-aggregation group** *agg-id*

undo port link-aggregation group

View Ethernet interface view

Parameters *agg-id*: Link aggregation group ID.

Description Use the **port link-aggregation group** command to assign the Ethernet port to the specified link aggregation group (manual or static LACP) or service loop group.

Use the **undo port link-aggregation group** command to remove the Ethernet port from the specified aggregation group or service loop group.

Note that Ethernet ports can only be added to existing link aggregation groups.

Related commands: **display link-aggregation verbose**.

Examples # Add port Ethernet 1/1/1 to link aggregation group 22.

```
<Sysname> system-view
[Sysname] interface ethernet1/1/1
[Sysname-Ethernet1/1/1] port link-aggregation group 22
```

port-group aggregation

Syntax **port-group aggregation** *agg-id*

View System view

Parameters *agg-id*: ID of an existing aggregation port group, same as the ID of its corresponding link aggregation group.

Description Use the **port-group aggregation** command to enter aggregation port group view.

Instead of being created administratively, an aggregation port group is created automatically upon creation of a link aggregation group and assigned the ID of the link aggregation group. In aggregation port group view, you can configure aggregation related settings such as STP, VLAN, QoS, GVRP, QinQ, BPDU tunnel, and MAC address learning, but cannot add or remove member ports.

Examples # Enter aggregation port group view.

```
<Sysname> system-view
[Sysname] port-group aggregation 10
[Sysname-port-group-aggregation-10]
```

reset lacp statistics

Syntax **reset lacp statistics** [**interface** *interface-type interface-number* [**to** *interface-type interface-number*]]

View User view

Parameters **interface** *interface-type interface-number* [**to** *interface-type interface-number*]: Specifies an interface range or an interface if the **to** keyword and the second interface are not specified.

Description Use the **reset lacp statistics** command to clear the LACP statistics on a port or all the ports.

Related commands: **display link-aggregation interface**.

Examples # Clear LACP statistics on all ports.

```
<Sysname> reset lacp statistics
```

6 GARP CONFIGURATION COMMANDS

debugging garp event

Syntax **debugging garp event**

undo debugging garp event

View User view

Parameters None

Description Use the **debugging garp event** command to enable GARP event debugging, in order to debug GARP timer events.

Use the **undo debugging garp event** command to disable GARP event debugging.

By default, GARP event debugging is disabled.

Examples # Enable GARP event debugging on a GARP-enabled device.

```
<Sysname> terminal debugging
<Sysname> debugging garp event
*0.1101110 Sysname GARP/8/Timer start:
Gvrp Start Join Timer for port Ethernet1/1/1 value = 200 millisec
```

// The above information shows the Join timer on port Ethernet1/1/1 started with a value of 200 ms.

```
*0.1101219 Sysname GARP/8/Timer expiry:
Gvrp Join Timer Expired for port Ethernet1/1/1
```

// The above information shows the Join timer on port Ethernet1/1/1 expired.

(Other timers' event information is omitted here.)

display garp statistics

Syntax **display garp statistics** [**interface** *interface-list*]

View Any view

Parameters *interface-list*: Ethernet port list, in the format of { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>, where &<1-10> indicates that you can specify up to 10 port ranges. A port range defined without the **to** *interface-type interface-number* portion comprises only one port.

Description Use the **display garp statistics** command to display statistics about GARP for specified or all ports.

Examples # Display statistics about GARP for port Ethernet1/1/1.

```
<Sysname> display garp statistics interface ethernet 1/1/1

        GARP statistics on port Ethernet1/1/1

        Number of GVRP Frames Received          : 0
        Number of GVRP Frames Transmitted       : 0
        Number of Frames Discarded              : 0
```

display garp timer

Syntax **display garp timer** [**interface** *interface-list*]

View Any view

Parameters *interface-list*: Ethernet port list, in the format of { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>, where &<1-10> indicates that you can specify up to 10 port ranges. A port range defined without the **to** *interface-type interface-number* portion comprises only one port.

Description Use the **display garp timer** command to display GARP timers.

Related commands: **garp timer**, **garp timer leaveall**.

Examples # Display GARP timers on port Ethernet1/1/1.

```
<Sysname> display garp timer interface ethernet 1/1/1

        GARP timers on port Ethernet1/1/1

                Garp Join Time          : 20 centiseconds
                Garp Leave Time         : 60 centiseconds
                Garp LeaveAll Time      : 1000 centiseconds
                Garp Hold Time          : 10 centiseconds
```

garp timer

Syntax **garp timer** { **hold** | **join** | **leave** } *timer-value*

undo garp timer { **hold** | **join** | **leave** }

View Ethernet interface view, port group view

Parameters **hold**: Sets the Hold timer. When a GARP application entity receives the first registration request, it starts the Hold timer and collects succeeding requests. When the timer expires, the entity sends all these requests in one Join message, thus saving bandwidth.

join: Sets the Join timer. A GARP application entity sends each Join message twice for reliability sake and uses the Join timer to set the interval between the two sending operations.

leave: Sets the Leave timer. This timer starts upon receipt of a Leave message from another GARP application entity for deregistering some attribute information. If no Join message is received before this timer expires, the GARP application entity removes the attribute information as requested.

timer-value: Timer value in centiseconds. Set it in steps of five. The default is 10 centiseconds for the Hold timer, 20 centiseconds for the Join timer, and 60 centiseconds for the Leave timer.

Description Use the **garp timer** command to set a GARP timer for an Ethernet port or all ports in a port group in compliance with the timer setting dependencies shown in Table 25.

Use the **undo garp timer** command to restore the default of a GARP timer. This may fail if the default does not satisfy the dependencies shown in Table 25.

When restoring the default GARP timers, you are recommended to do that on the timers in the order of Hold, Join, Leave, and LeaveAll.

When configuring GARP timers, note that their values are dependent on each other and must be a multiplier of five centiseconds. If the value range for a timer is not desired, you may change it by tuning the value of another timer as shown in the following table:

Table 25 Dependencies of GARP timers

Timer	Lower limit	Upper limit
Hold	10 centiseconds	Not greater than half of the Join timer setting
Join	Not less than two times the Hold timer setting	Less than half of the Leave timer setting
Leave	Greater than two times the Join timer setting	Less than the LeaveAll timer setting
LeaveAll	Greater than the Leave timer setting	32765 centiseconds

Related commands: **display garp timer**.

Examples # Set the GARP Join timer to 25 centiseconds, assuming that both the Hold timer and the Leave timer are using the default.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface ethernet 1/1/1
[Sysname-Ethernet1/1/1] garp timer join 25
```

garp timer leaveall

Syntax **garp timer leaveall** *timer-value*

undo garp timer leaveall

View System view

Parameters *timer-value*: Value for the LeaveAll timer in centiseconds, which is a multiple of 5. This value must be greater than the Leave timer values on all ports. The default LeaveAll timer is 1000 centiseconds, that is 10 seconds.

Description Use the **garp timer leaveall** command to set the LeaveAll timer of GARP.

Use the **undo garp timer leaveall** command to restore the default. This may fail if the default is less than the setting of the current Leave timer.

A LeaveAll timer starts upon the startup of a GARP application entity. When this timer expires, the entity sends a LeaveAll message so that other entities can re-register its attribute information, and, at the same time, the entity restarts the LeaveAll timer.

Different devices on a network may have different LeaveAll timer values. Each time a device on the network receives a LeaveAll message, it resets its LeaveAll timer. Therefore, each GARP application entity will send LeaveAll messages based on the shortest LeaveAll timer in the network. As a result, only the shortest LeaveAll timer in the network will take effect.

Related commands: **display garp timer**.

Examples # Set the LeaveAll timer to 100 centiseconds, assuming that the Leave timer is 60 centiseconds.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] garp timer leaveall 100
```

reset garp statistics

Syntax **reset garp statistics** [**interface** *interface-list*]

View User view

Parameters *interface-list*: Ethernet port list, in the format of { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>, where &<1-10> indicates that you can specify up to 10 port ranges. A port range defined without the **to** *interface-type interface-number* portion comprises only one port.

Description Use the **reset garp statistics** command to clear statistics about GARP on the specified or all ports.

Related commands: **display gvrp statistics**.

Examples # Clear statistics about GARP on all ports.

```
<Sysname> reset garp statistics
```

7 GVRP CONFIGURATION COMMANDS

debugging gvrp

Syntax **debugging gvrp** { **packet** | **event** }

undo debugging gvrp { **packet** | **event** }

View User view

Parameters **packet**: Specifies GVRP packet debugging.

event: Specifies GVRP event debugging.

Description Use the **debugging gvrp** command to enable GVRP packet or event debugging on all GVRP-enabled ports.

Use the **undo debugging gvrp** command to disable GVRP packet or event debugging.

By default, both GVRP packet debugging and GVRP event debugging are disabled.

Examples # Enable GVRP packet debugging on a GVRP-enabled device.

```
<Sysname> terminal debugging
<Sysname> debugging gvrp packet
*0.3440813 Sysname-wvrp GARP/8/debug_case:
Tx GVRP message on port Ethernet1/1/1
```

// The above information shows a GVRP message was transmitted on port Ethernet1/1/1.

```
*0.3440813 Sysname-wvrp GARP/8/Garp packet:
Vlan Attribute, Event = Join Empty, VLAN Id = 1
```

// The above information shows the GVRP message transmitted was a Join Empty message carrying a VLAN attribute (VLAN ID of 1).

Table 26 Field descriptions of the debugging gvrp packet command

Field	Description
Tx	This is a transmitted message.
Rx	This is a received message.
GVRP message	This is a GVRP message.

Table 26 Field descriptions of the debugging gvrp packet command

Field	Description
Port *portName*	Name of the port that transmits or receives the message
Vlan Attribute	The attribute carried in the message is a VLAN ID.
Event = { Leave All | Join Empty | Join In | Leave Empty | Leave In }	Event type of the message, which can be Leave All, Join Empty, Join In, Leave Empty or Leave In
VLAN Id = *n*	VLAN ID

Table 27 Field descriptions of the debugging gvrp event command

Field	Description
GVRP: Wrong VLAN Id = *n* to create	VLAN ID error occurred when a VLAN is created
GVRP: Number of static VLANs for port *portName* = *n*	Number of static VLANs on a port

display gvrp statistics

Syntax **display gvrp statistics** [**interface** *interface-list*]

View Any view

Parameters *interface-list*: Ethernet port list, in the format of { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>, where &<1-10> indicates that you can specify up to 10 port ranges. A port range defined without the **to** *interface-type interface-number* portion comprises only one port.

Description Use the **display gvrp statistics** command to display statistics about GVRP for specified or all trunk ports.

Note that if the **interface** *interface-list* is not provided, the GVRP statistics of all trunk ports will be displayed. Otherwise, only the GVRP statistics of all the specified trunk port will be displayed.

Examples # Display statistics about GVRP for trunk port Ethernet1/1/1.

```
<Sysname> display gvrp statistics interface ethernet 1/1/1

        GVRP statistics on port Ethernet1/1/1

                GVRP Status                     : Enabled
                GVRP Running                    : YES
                GVRP Failed Registrations       : 0
                GVRP Last Pdu Origin            : 0000-0000-0000
                GVRP Registration Type          : Normal
```

Table 28 Field descriptions of the display gvrp statistics command

Field	Description
GVRP Status	Indicates whether GVRP is enabled or disabled.
GVRP Running	Indicates whether GVRP is running.
GVRP Failed Registrations	Indicates the number of GVRP registration failures.
GVRP Last Pdu Origin	Indicates the source MAC address in the last GVRP PDU.
GVRP Registration Type	Indicates the GVRP registration type on the port.

display gvrp status

Syntax **display gvrp status**

View Any view

Parameters None

Description Use the **display gvrp status** command to display the global enable/disable state of GVRP.

Examples # Display the global GVRP enable/disable state.

```
<Sysname> display gvrp status
GVRP is enabled
```

gvrp

Syntax **gvrp**

undo gvrp

View System view, Ethernet interface view, port group view

Parameters None

Description Use the **gvrp** command to enable GVRP globally, on a port, or on all ports in a port group depending on the view you entered.

Use the **undo gvrp** command to disable GVRP globally, on a port, or on all ports in a port group depending on the view you entered.

Disabling GVRP globally also disables it on all ports.

By default, GVRP is disabled.

The port where you enable GVRP must be a trunk port. In addition, before you can enable GVRP on it, you must enable GVRP globally.

CAUTION:

- *BPDU Tunnel is incompatible with GVRP. Before enabling GVRP, disable BPDU Tunnel.*
- *Isolate-user-vlan is incompatible with global GVRP. Make sure that no Isolate-user-vlan has been created on the switch before enabling GVRP.*

Related commands: **display gvrp status**.

Examples # Enable GVRP globally.

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

gvrp registration

Syntax **gvrp registration** { **fixed** | **forbidden** | **normal** }

undo gvrp registration

View Ethernet interface view, port group view

Parameters **fixed**: Sets the registration type to fixed.

forbidden: Sets the registration type to forbidden.

normal: Sets the registration type to normal.

Description Use the **gvrp registration** command to configure the GVRP registration type on a port or all ports in a port group.

Use the **undo gvrp registration** command to restore the default.

The default GVRP registration type is normal.

GVRP provides the following three registration types on a port:

- Normal -- Enables the port to dynamically register/deregister VLANs, and to propagate both dynamic and static VLAN information.
- Fixed -- Disables the port from dynamically registering VLANs and from propagating information about dynamic VLANs, but allows the port to propagate information about static VLANs. On a trunk port with fixed registration type, GVRP can only propagate manually configured VLANs' information even though the port is configured to allow all VLANs to pass.
- Forbidden -- Disables the port from dynamically registering VLANs and from propagating any VLAN information except information about VLAN 1. On a trunk port with forbidden registration type, GVRP can only propagate the information of VLAN 1 (that is, the default VLAN) even though the port is configured to allow all VLANs to pass.

Note that this command is only available on trunk ports.

Related commands: **display garp statistics**.

Examples # Set the GVRP registration type to fixed on port Ethernet1/1/1.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface ethernet 1/1/1
[Sysname-Ethernet1/1/1] port link-type trunk
[Sysname-Ethernet1/1/1] gvrp registration fixed
```

8 PORT MIRRORING CONFIGURATION COMMANDS

display mirroring-group

Syntax **display mirroring-group** { *groupid* | **local** | **remote-source** | **remote-destination** | **all** }

View Any view

Parameters *groupid*: Port mirroring group number, in the range 1 to 24.

local: Specifies local port mirroring groups.

remote-source: Specifies remote source port mirroring groups.

remote-destination: Specifies remote destination port mirroring groups.

all: Specifies all the port mirroring groups.

Description Use the **display mirroring-group** command to display the information about a port mirroring group.

The output information varies with port mirroring group type and is organized by mirroring group numbers.

Examples # Display the information about all the port mirroring groups.

```
<Sysname> display mirroring-group all
mirroring-group 3:
    type: local
    status: active
    mirroring port:
        GigabitEthernet4/2/1  inbound
        GigabitEthernet4/2/2  outbound
    monitor port: GigabitEthernet4/3/1
mirroring-group 6:
    type: remote-source
    status: inactive
    mirroring port:
        GigabitEthernet4/3/4  inbound
    reflector port: GigabitEthernet4/2/4
    remote-probe vlan:
mirroring-group 9:
    type: remote-destination
    status: active
```

```
monitor port: GigabitEthernet4/2/1
remote-probe vlan: 2
```

Table 29 Field descriptions of the display mirroring-group command

Field	Description
mirroring-group	Port mirroring group number
type	Port mirroring group type, which can be local, remote-source, and remote-dest.
status	Status of a port mirroring group. "Active" for already effective, and "inactive" for not effective yet.
mirroring port	Source mirroring port
monitor port	Destination mirroring port
reflector port	Reflector mirroring port
remote-probe vlan	Remote mirroring VLAN

mirroring-group

Syntax **mirroring-group** *groupid* { **local** | **remote-source** | **remote-destination** }

undo mirroring-group { *groupid* | **local** | **remote-source** | **remote-destination** | **all** }

View System view

Parameters *groupid*: Port mirroring group number, in the range 1 to 24.

local: Creates/Removes a local port mirroring group.

remote-source: Creates/Removes a remote source port mirroring group.

remote-destination: Creates/Removes a remote destination port mirroring group.

all: Removes All the port mirroring groups.

Description Use the **mirroring-group** command to create a port mirroring group.

Use the **undo mirroring-group** command to remove a port mirroring group.

Specify the type of a port mirroring group to be created:

- With **local** specified, you create a local port mirroring group.
- With **remote-destination** specified, you create a remote destination port mirroring group.
- With **remote-source** specified, you create a remote source port mirroring group.

Specify the type or ID of the port mirroring group to be deleted:

- With *groupid* specified, you delete the port mirroring group with the *groupid*.
- With **all** specified, you delete all the port mirroring groups.
- With **local** specified, you delete all the local port mirroring groups.
- With **remote-destination** specified, you delete all the remote destination port mirroring groups.
- With **remote-source** specified, you delete all the remote source port mirroring groups.

Examples # Create a local port mirroring group numbered 1.

```
<Sysname> system-view
[Sysname] mirroring-group 1 local
```

mirroring-group mirroring-port

Syntax **mirroring-group** *groupid* **mirroring-port** *mirroring-port-list* { **inbound** | **outbound** | **both** }

undo mirroring-group *groupid* **mirroring-port** *mirroring-port-list* { **inbound** | **outbound** | **both** }

View System view

Parameters *groupid*: Port mirroring group number, in the range 1 to 24.

mirroring-port-list: List of ports to be added to the port mirroring group. You can specify multiple ports by providing this argument in the form of { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-8>, where the *interface-type* argument is port type, the *interface-number* argument is the port number, and &<1-8> means that you can provide up to eight port indexes/port index lists for this argument.

inbound: Specifies to duplicate inbound packets only.

outbound: Specifies to duplicate outbound packets only.

both: Specifies to duplicate both inbound and outbound packets.

Description Use the **mirroring-group mirroring-port** command to configure source ports for an existing port mirroring group.

Use the **undo mirroring-group mirroring-port** command to remove source ports from a port mirroring group.

- *You cannot configure source ports for a remote destination port mirroring group.*
- *When removing source ports from a port mirroring group using the **undo mirroring-group mirroring-port** command, make sure the keyword specified (that is, the **both**, the **inbound**, or the **outbound** keyword) matches the actual directions of the ports.*

Examples # Configure port Ethernet 1/1/1 through Ethernet 1/1/6 as the source ports of port mirroring group 1 (assuming that port mirroring group 1 already exists).

```
<Sysname> system-view
[Sysname] mirroring-group 1 mirroring-port ethernet 1/1/1 to ethernet 1/1/6
both
```

Remove port Ethernet 1/1/1 through Ethernet1/1/4 from port mirroring group 1.

```
<Sysname> system-view
[Sysname] undo mirroring-group 1 mirroring-port ethernet 1/1/1 to ethernet 1
/1/4 both
```

mirroring-group monitor-port

Syntax **mirroring-group** *groupid* **monitor-port** *monitor-port-id*

undo mirroring-group *groupid* **monitor-port** *monitor-port-id*

View System view

Parameters *groupid*: Port mirroring group number, in the range 1 to 24.

monitor-port-id: Index of the port to be configured as the destination port. You need to provide this argument in the format of { *interface-type interface-number* }, where *interface-type* is port type and *interface-number* is port number.

Description Use the **mirroring-group monitor-port** command to configure the destination port for a port mirroring group.

Use the **undo mirroring-group monitor-port** command to remove the destination port from a port mirroring group.

Note that:

- A port mirroring group can contain only one destination port.
- A remote source port mirroring group cannot contain destination ports.
- Member ports of existing port mirroring groups cannot be destination ports.
- To configure the destination port for a port mirroring group, make sure the port mirroring group already exists.

Examples # Configure Ethernet 1/1/1 as the destination port of port mirroring group 1 (a remote destination port mirroring group).

```
<Sysname> system-view
[Sysname] mirroring-group 1 remote-destination
[Sysname] mirroring-group 1 monitor-port ethernet 1/1/1
```

mirroring-group reflector-port

Syntax In system view:

mirroring-group *groupid* **reflector-port** *reflector-port-id*

undo mirroring-group *groupid* **reflector-port** *reflector-port-id*

In Ethernet interface view:

mirroring-group *groupid* **reflector-port**

undo mirroring-group *groupid* **reflector-port**

View System view, Ethernet interface view

Parameters *groupid*: Port mirroring group number, in the range 1 to 24.

reflector-port-id: Index of the port to be configured as a reflector port. You need to provide this argument in the form of *interface-type interface-number*, where *interface-type* is the port type and *interface-number* is the port number.

Description Use the **mirroring-group reflector-port** command to configure the reflector port for an existing remote source port mirroring group.

Use the **undo mirroring-group reflector-port** command to remove the reflector port from a remote source port mirroring group.

- *A remote source port mirroring group can contain only one reflector port.*
- *Only remote source port mirroring groups can contain reflector ports.*
- *Ports on XP4C, XP4B, GV48D, GP48D, and XP4DB modules cannot be configured as reflector ports.*

Examples # Configure port Ethernet 1/1/1 as the reflector port of port mirroring group 1 (a remote source port mirroring group).

```
<Sysname> system-view
[Sysname] mirroring-group 1 remote-source
[Sysname] mirroring-group 1 reflector-port ethernet 1/1/1
```

Configure port Ethernet 1/1/2 as the reflector port of port mirroring group 2 (a remote source port mirroring group).

```
<Sysname> system-view
[Sysname] mirroring-group 2 remote-source
[Sysname] interface ethernet 1/1/2
```

[Sysname-Ethernet1/1/2] mirroring-group 2 reflector-port

mirroring-group remote-probe vlan

Syntax **mirroring-group** *groupid* **remote-probe vlan** *rprobe-vlan-id*

undo mirroring-group *groupid* **remote-probe vlan** *rprobe-vlan-id*

View System view

Parameters *groupid*: Port mirroring group number, in the range 1 to 24.

rprobe-vlan-id: ID of the VLAN to be configured as the remote mirroring VLAN. Note that the VLAN must be an existing static VLAN.

Description Use the **mirroring-group remote-probe vlan** command to specify a VLAN as the mirroring VLAN for an existing remote source port mirroring group or an existing remote destination port mirroring group.

Use the **undo mirroring-group remote-probe vlan** command to remove the remote mirroring VLAN from a remote source mirroring group or a remote destination mirroring group.

- *Only remote source port mirroring groups or remote destination port mirroring groups with the remote mirroring VLANs not configured can have remote mirroring VLANs configured.*
- *It is recommended that you use a remote mirroring VLAN for remote mirroring only.*

Examples # Specify VLAN 2 as the remote mirroring VLAN of port mirroring group 1 (a remote source port mirroring group).

```
<Sysname> system-view
[Sysname] mirroring-group 1 remote-source
[Sysname] mirroring-group 1 remote-probe vlan 2
```

mirroring-port

Syntax [**mirroring-group** *groupid*] **mirroring-port** { **inbound** | **outbound** | **both** }

undo [**mirroring-group** *groupid*] **mirroring-port** { **inbound** | **outbound** | **both** }

View Ethernet interface view

Parameters *groupid*: Port mirroring group number, in the range 1 to 24.

inbound: Duplicates the inbound packets only.

outbound: Duplicates the outbound packets only.

both: Duplicates both inbound and outbound packets.

Description Use the **mirroring-port** command to configure a port as a source mirroring port of a port mirroring group.

Use the **undo mirroring-port** command to remove a source mirroring port from a port mirroring group.

If you do not specify the **mirroring-group** *groupid* keyword-argument combination, the **mirroring-port** command adds the current port to port mirroring group 1.

- *A remote destination mirroring group cannot contain source mirroring ports.*
- *When removing a source mirroring port from a port mirroring group using the **undo mirroring-port** command, make sure the keyword specified (that is, the **inbound**, the **outbound**, or the **both** keyword) matches the actual packet direction of the port.*

Examples # Configure port Ethernet 1/1/1 as a source mirroring port of remote source port mirroring group 2.

```
<Sysname> system-view
[Sysname] mirroring-group 2 remote-source
[Sysname] interface ethernet 1/1/1
[Sysname-Ethernet1/1/1] mirroring-group 2 mirroring-port both
```

monitor-port

Syntax [**mirroring-group** *groupid*] **monitor-port**

undo [**mirroring-group** *groupid*] **monitor-port**

View Ethernet interface view

Parameters *groupid*: Port mirroring group number, in the range 1 to 24.

Description Use the **monitor-port** command to configure a port as the destination mirroring port of a port mirroring group.

Use the **undo monitor-port** command to remove the destination mirroring port from a port mirroring group.

If you do not specify the **mirroring-group** *groupid* keyword-argument combination, the **monitor-port** command adds the current port to port mirroring group 1.

Note that:

- A remote source mirroring group cannot contain destination mirroring ports.
- Member ports of existing port mirroring groups cannot be destination ports.

Examples # Configure port Ethernet 1/1/1 as the destination port of port mirroring group 1 (a local port mirroring group).

```
<Sysname> system-view
[Sysname] mirroring-group 1 local
[Sysname] interface ethernet 1/1/1
[Sysname-Ethernet1/1/1] monitor-port
```

9 MSTP CONFIGURATION COMMANDS

active region-configuration

Syntax **active region-configuration**

View MST region view

Parameters None

Description Use the **active region-configuration** command to activate your MST region configuration.

When you carry out this command, MSTP will replace the currently running MST region-related parameters with the parameters you have just configured, and will perform spanning tree computing again.

Related commands: **instance**, **region-name**, **revision-level**, **vlan-mapping modulo**, and **check region-configuration**.

Examples # Activate MST region configuration manually.

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] active region-configuration
```

check region-configuration

Syntax **check region-configuration**

View MST region view

Parameters None

Description Use the **check region-configuration** command to view all the MST region configuration information, including the region name, VLAN-to-instance mapping and revision level settings.

CAUTION: *Be sure that your MST region configurations are correct, especially the VLAN-to-instance mapping table. MSTP-compliant devices are in the same MST region only when they have the same region name, the same VLAN-to-instance*

mapping table and the same MSTP revision level setting. A device will not be in a different region if it is different in any of these three settings. You can view all the MST region-related configuration information by using this command and determine the MST region the device is currently in, or check whether the MST region configuration is correct.

Related commands: **instance**, **region-name**, **revision-level**, **vlan-mapping modulo**, and **active region-configuration**.

Examples # View the inactivated configuration information of the MST region.

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] check region-configuration
Admin Configuration
   Format selector :0
   Region name     :00b010000001
   Revision level  :0

   Instance   Vlans Mapped
      0       1 to 4094
```

Table 30 Field descriptions of the check region-configuration command

Field	Description
Format selector	Format selector stipulated in MSTP
Region name	MST region name
Revision level	Revision level of the MST region
Instance Vlans Mapped	VLAN-to-instance mappings in the MST region

debugging stp

Syntax **debugging stp** { **all** | **global-error** | **global-event** }

undo debugging stp { **all** | **global-error** | **global-event** }

View User view

Parameters **all**: Enables all types of global MSTP debugging.

global-error: Enables debugging for global MSTP errors.

global-event: Enables debugging for global MSTP events.

Description Use the **debugging stp** command to enable a specific type of global MSTP debugging.

Use the **undo debugging stp** command to disable a specific type of global MSTP debugging.

By default, all types of global MSTP debugging are disabled.

Table 31 Field descriptions of the debugging stp global-error command

Field	Description
Port *Port Number* received BPDU packet is err for *String*	An error BPDU is received on a port. *Port Number*: Port number. *String*: Error description.
The protocol type ID is wrong	The protocol type ID is invalid.
The protocol version ID is wrong	The protocol version ID is invalid (the correct protocol version ID for STP, RSTP, and MSTP is 0, 2, and 3).
Instance *InstanceID* is wrong	The instance is invalid. *InstanceID*: Instance ID.
Creating mbuffer failed	Fail to create buffer.
P/V semaphore error	A P/V semaphore error occurs.
Set STP *String* error	Fail to issue STP-enabled state to the driver. *String*: STP state, which can be enable or disable.
Creating responsive message for configuration failed	Fail to generate response configuration messages.
Por*t Port Number* is inexistent	The port does not exist. *Port Number*: Port number.
Active region configuration error	Fail to activate region configuration.
Set instance *InstanceID*'s port *Port Number* STP state *String* error	Error occurs to setting STP forwarding state for a port in an instance. *InstanceID*: Instance ID. *Port Number*: Port number. *String*: STP forwarding state, which can be discarding, learning, or forwarding.
Write queue *String* error	Fail to write a queue. *String*: Queue name, which can be MstpMsgQue or MstpPktQue.
Write event *String* error	Fail to write an event. *String*: Event, which can be MSTP_BPDU_EVENT or MSTP_L2INF_EVENT.
Bind vlan to instance *InstanceID* error	Error occurs to binding a VLAN to an instance. *InstanceID*: Instance ID.
Instance *InstanceID* 's port *Port Number* enter unknown state of *String* state machine!	A port in an instance is in an unknown state of a state machine. *InstanceID*: Instance ID. *Port Number*: Port number. *String*: State machine name, which can be PIM, PPM, TCM, PRT_DAB, or PRT_RDM.
Port *Port Number* send packet error	Fail to send packets through a port. *Port Number*: Port number.

Table 32 Field descriptions of the debugging stp global-event command

Field	Description
Instance *InstanceID* Enters PRS Machine	An instance enters the PRS state machine. *InstanceID*: Instance ID.
Instance *InstanceID*'s all ports' dyna-Address are cleared	The dynamic MAC address entries of all the ports in an instance are removed.
All instances' all ports' dyna-Address are cleared	The dynamic MAC address entries of all the ports in all the instances are removed.

Examples # Enable debugging for global MSTP events after configuring multiple instances on an MSTP-enabled device, and then bring up a port.

```
<Sysname> terminal debugging
<Sysname> debugging stp global-event
%Feb  7 17:26:02:578 2006 Sysname IFNET/5/LINK UPDOWN:
 Ethernet1/1/1: link status is UP
*0.6848594 Sysname MSTP/8/PRS:Instance 0 Enters PRS Machine.
```

// Instance 0 entered the PRS state machine.

```
*0.6848594 Sysname MSTP/8/PRS:Instance 2 Enters PRS Machine.
```

// Instance 2 entered the PRS state machine.

```
*0.6848594 Sysname MSTP/8/PRS:Instance 0 Enters PRS Machine.
```

// Instance 0 entered the PRS state machine.

```
*0.6848594 Sysname MSTP/8/FLSHINS:Instance 0's all ports' dyna-Address are c
leared.
```

// The dynamic MAC address entries of all the ports in instance 0 were removed.

```
*0.6848610 Sysname MSTP/8/PRS:Instance 2 Enters PRS Machine.
```

// Instance 2 entered the PRS state machine.

```
*0.6848610 Sysname MSTP/8/FLSHINS:Instance 2's all ports' dyna-Address are c
leared.
```

// The dynamic MAC address entries of all the ports in instance 2 were removed.

debugging stp event

Syntax **debugging stp** [**interface** *interface-type interface-number*] **event**

undo debugging stp [**interface** *interface-type interface-number*] **event**

View User view

Parameters *interface-type interface-number*: Port type and port number.

Description Use the **debugging stp event** command to enable debugging for MSTP port events.

Use the **undo debugging stp event** disable debugging for MSTP port events.

By default, debugging for MSTP port events is disabled.

If the *interface-type interface-number* argument is not provided, these two commands apply to all the ports; otherwise, these two commands apply to the port identified by the argument.

Table 33 Field descriptions of the debugging stp event command

Field	Description
Instance *InstanceID*'s port *Port Number* enters *String* state	The state of a port in a valid instance *InstanceID*: Instance ID. *Port Number*: Port number. *String*: State in a state machine.
Instance *InstanceID*'s all ports' dyna-Address are cleared	The dynamic MAC address entries of all the ports in an instance are removed.
All instances' all ports' dyna-Address are cleared	The dynamic MAC address entries of all the ports in all the instances are removed.
Instance *InstanceID*'s Port *Port Number* is selected as *String* role	The role of a port in an instance *InstanceID*: Instance ID. *Port Number*: Port number. *String*: Role of a port in an instance, which can be DESIGNATED, ROOT, ALTERNATE, BACKUP, or MASTER.

Table 33 Field descriptions of the debugging stp event command

Field	Description
Port *ULONG* occurs *String* event	Event on a port *ULONG*: Port number. *String*: Event, which can one of the following: ■ ADD VLAN, indicating the event that the port is added to a VLAN. ■ DEL VLAN, indicating the event that the port is removed from a VLAN. ■ SPEED CHANGE, indicating the event that the speed of the port changes. ■ DUPLEX CHANGE, indicating the event that the duplex mode of the port changes. ■ LINK DOWN, indicating the event that the port is shut down) ■ LINK UP, indicating the event that the port is brought up. ■ NOT PA PORT, indicating the event that the port exits from a port aggregation group. ■ PA SUB PORT, indicating the event that the port joins a port aggregation group. ■ PA OLD BRIDGE PORT, indicating the old master port when the master port of a port aggregation group changes ■ PA NEW BRIDGE PORT indicating the new master port when the master port of a port aggregation group changes.

Examples # Connect two ports of Device A to two ports of Device B, configure Device A as the root bridge, enable MSTP on Device B, and enable debugging for MSTP port events on Ethernet 1/1/1.

```
<Sysname> display stp brief
 MSTID      Port                        Role  STP State     Protection
   0        Ethernet1/1/2               ROOT  FORWARDING    NONE
   0        Ethernet1/1/1               ALTE  DISCARDING    NONE
<Sysname> terminal debugging
<Sysname> debugging stp interface ethernet 1/1/1 event
**0.2307688 Sysname MSTP/8/MEXS:Instance 0's port385 enters PIM%CURRENT state.
```

// Ethernet 1/1/1 entered the CURRENT state of the PIM state machine in instance 0.

```
*0.2307688 Sysname-wvrp MSTP/8/MEXS:Instance 0's port385 enters PIM%
RECEIVED state.
```

// Ethernet 1/1/1 entered the RECEIVED state of the PIM state machine in instance 0.

```
*0.2307688 Sysname-wvrp MSTP/8/MEXS:Instance 0's port385 enters PIM%
REPEATED_DESIGNATED state.
```

// Ethernet 1/1/1 entered the REPEATED DESIGNATED state of the PIM state machine in instance 0.

```
*0.2307688 Sysname-wvrp MSTP/8/MEXS:Instance 0's port385 enters PRT%
ACTIVE_PORTstate.
```

// Ethernet 1/1/1 entered the ACTIVE PORT state of the PRT state machine in instance 0.

debugging stp instance

Syntax **debugging stp instance** *instance-id*

undo debugging stp instance *instance-id*

View User view

Parameters *instance-id*: MST instance ID, in the range 0 to 47. Note that a value of 0 specifies the common internal spanning tree (CIST).

Description Use the **debugging stp instance** command to enable debugging for an MST instance.

Use the **undo debugging stp instance** command to disable debugging for an MST instance.

By default, debugging for an MST instance is disabled.

Table 34 Field descriptions of the debugging stp instance command

Field	Description
Instance *InstanceID*'s port *Port Number* enters *String* state	The state of a port in an instance *InstanceID*: Instance ID. *Port Number*: Port number. *String*: State of a port in a state machine (the string before "%" represents the state machine name, and the string after "%" represents the state in the state machine), which could be one of the following values:

Table 34 Field descriptions of the debugging stp instance command

Field	Description
	■ PIM%ENABLED ■ PIM%AGED ■ PIM%CURRENT ■ PIM%RECEIVED, PIM%SUPERIOR_DESIGNATED ■ PIM%REPEATED_DESIGNATED ■ PIM%ROOT ■ PIM%OTHER ■ PPM%SEND_RSTP ■ PPM%SENDING_RSTP ■ PPM%SEND_STP ■ PPM%SENDING_STP ■ PRT%BLOCK_PORT ■ PRT%BLOCKED_PORT ■ PRT%BACKUP_PORT ■ PRT%ACTIVE_PORT ■ PRT%PROPOSED ■ PRT%PROPOSING ■ PRT%AGREES ■ PRT%SYNCED ■ PRT%AGREES ■ PRT%LEARN ■ PRT%FORWARD ■ PRT%REROOT ■ PRT%FORWARD ■ PRT%LEARN ■ PRT%LISTEN ■ PRT%REROOTED ■ PRT%ROOT ■ TCM%INIT ■ TCM%INACTIVE ■ TCM%DETECTED ■ TCM%ACTIVE ■ TCM%NOTIFIED_TCN ■ TCM%NOTIFIED_TC ■ TCM%PROPAGATING ■ TCM%ACKNOLEDGED

Examples # Connect the ports of Device A to those of Device B, configure Device A as the root bridge, configure MST instance 2 on Device B and enable debugging for MST instance 2.

```
<Sysname> terminal debugging
<Sysname> display stp brief
 MSTID      Port                        Role  STP State     Protection
```

```
   0        Ethernet1/1/1               ROOT  FORWARDING    NONE
   0        Ethernet1/1/2               ALTE  DISCARDING    NONE
   2        Ethernet1/1/1               MAST  FORWARDING    NONE
   2        Ethernet1/1/2               ALTE  DISCARDING    NONE
<Sysname> debugging stp instacne 2
*0.5919860 Sysname-wvrp MSTP/8/MEXS:Instance 2's port385 enters PRT%ACTIVE_P
ORT state.
*0.5919860 Sysname-wvrp MSTP/8/MEXS:Instance 2's port385 enters PRT%ACTIVE_P
ORT state.
*0.5921860 Sysname-wvrp MSTP/8/MEXS:Instance 2's port385 enters PRT%ACTIVE_P
ORT state.
*0.5921860 Sysname-wvrp MSTP/8/MEXS:Instance 2's port385 enters PRT%ACTIVE_P
ORT state.
```

// Ethernet 1/1/1 of instance 2 is in the ACTIVE PORT state of the PRT state machine.

debugging stp packet

Syntax **debugging stp** [**interface** *interface-type interface-number*] **packet** [**brief** | **verbose**]

undo debugging stp [**interface** *interface-type interface-number*] **packet** [**brief** | **verbose**]

View User view

Parameters *interface-type interface-number*: Port type and port number.

brief: Displays the brief information about MSTP packets. The **brief** keyword is adopted by default.

verbose: Displays the detailed information about MSTP packets.

Description Use the **debugging stp packet** command to enable MSTP packet debugging.

Use the **undo debugging stp packet** command to disable MSTP packet debugging.

By default, MSTP packet debugging is disabled.

Table 35 Field descriptions of the debugging stp packet brief command

Field	Description
Port *interface-number (interface-name) String type* Packet*(Length:number)*	*interface-number*: Port number. *interface-name*: Port name. *String*: Indicates packet direction (inbound or outbound). *Type*: Packet type, which can be Stp, Rstp, Mstp-dot1s, or Mstp-legacy. *Number*: Packet size (in bytes).
ProtocolVersionID	Protocol version
BPDUType	BPDU packet type
Instance(Flags)	Instance ID (flags carried in a BPDU)

Table 36 Field descriptions of the debugging stp packet verbose command

Field	Description
PKT	Packet debugging output information, including port number, port name, packet direction (inbound or outbound), packet type, packet size, and packet content (in hexadecimal characters)

Examples # Connect the ports of Device A to those of Device B, configure Device A as the root bridge, enable MSTP on Device B, and enable MSTP packet debugging on Device B to display the brief information about MSTP packets.

```
<Sysname> terminal debugging
<Sysname> debugging stp packet
*0.299531 Sysname-wvrp MSTP/8/PKT:
Port386(Ethernet1/1/1) Rcvd Mstp-legacy Packet(Length: 103)
ProtocolVersionID: 03
BPDUType         : 02
Instance(Flags)  : 0(6c)
```

// Ethernet 1/1/1 received an MSTP packet in legacy format. The size of the packet is 103 bytes, the protocol version is 3, BPDU type is 2, and the flag of instance 0 is 6c.

Enable MSTP packet debugging on an MSTP-enabled device to display detailed information about MSTP packets (assuming that at least one port is in up state).

```
<Sysname> debugging stp packet verbose
*0.1007594 Sysname-wvrp MSTP/8/PKT:
Port385(Ethernet1/1/1) Rcvd Mstp-legacy Packet(Length: 103)
00 00 03 02 6c 80 00 00 e0 fc 00 00 00 00 00 00
00 80 00 00 e0 fc 00 00 00 81 81 00 00 14 00 02
00 0f 00 00 00 00 40 30 30 65 30 66 63 30 30 30
30 30 30 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 ac 36 17 7f 50 28 3c
d4 b8 38 21 d8 ab 26 de 62 80 00 00 e0 fc 00 00
00 00 00 00 00 14 00
```

// Ethernet 1/1/1 received an MSTP packet in legacy format. The size of the packet is 103 bytes. The content of the packet is displayed in hexadecimal characters.

display stp

Syntax **display stp** [**instance** *instance-id*] [**interface** *interface-list* | **slot** *slot-num*] [**brief**]

View Any view

Parameters *instance-id*: MST instance ID, in the range 0 to 47. A value of 0 specifies the CIST.

interface-list: Ethernet port list. You can specify multiple Ethernet ports or port ranges by providing the this argument in the form of { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>, where,

interface-type is port type and *interface-number* is port number, and &<1-10> means that you can specify up to 10 ports or port ranges for this argument.

slot *slot-num*: Specifies the module seated in a specific slot.

brief: Displays brief MSTP information.

Description

Use the **display stp** command to view the MSTP status information and statistics information.

Based on the MSTP status information and statistics information, you can analyze and maintain the network topology or maintain the normal operation of MSTP.

Note that:

- If you do not specify an MST instance ID or a port list, this command displays the MSTP information about all the MST instances on all the ports by MST instance ID. The information about an MST instance is displayed by port number.
- If you specify an MST instance ID, this command displays the MSTP information about the specified MST instance on all the ports by port number.
- If you specify a port list, this command displays the MSTP information about all the MST instances on the specified ports by MST instance ID.
- If you specify both an MST instance ID and a port list, this command displays the MSTP information about the specified MST instance on the specified ports.

The MSTP status information includes:

- CIST global parameters, such as protocol work mode, device priority in the CIST instance (Priority), MAC address, hello time, max age, forward delay, maximum hops, common root of the CIST, external path cost from the device to the CIST common root, regional root, the internal path cost from the device to the regional root, CIST root port of the device, and states of the BPDU guard functions (enabled or disabled).
- CIST port parameters, such as port status, role, priority, path cost, designated bridge, designated port, edge port/non-edge port, whether connecting to a point-to-point link, maximum transmission rate (transmit limit), state of the root guard function (enabled or disabled), BPDU format, boundary port/non-boundary port, hello time, max age, forward delay, message age time, and remaining hops.
- MSTI global parameters, such as MSTI instance ID, bridge priority of the instance, regional root, internal path cost, MSTI root port, and master bridge.
- MSTI port parameters, such as port status, role, priority, path cost, designated bridge, designated port, and remaining hops.

The statistics information includes:

- The number of TCN BPDUs, configuration BPDUs, RST BPDUs, and MST BPDUs sent from each port
- The number of TCN BPDUs, configuration BPDUs, RST BPDUs, and MST BPDUs received on each port

Related commands: **reset stp**.

Examples # View the MSTP status information and statistics information.

```
<Sysname> display stp
Protocol Status    :disabled
 Protocol Std.      :IEEE 802.1s
 Version            :3
 CIST Bridge-Prio.  :32768
 MAC address        :000f-e222-e5cd
 Max age(s)         :20
 Forward delay(s)   :15
 Hello time(s)      :2
 Max hops           :20
```

Table 37 Field descriptions of the display stp command

Field	Description
Protocol Status	Protocol status
Protocol Std.	Protocol standard
Version	Protocol version
CIST Bridge-Prio	CIST priority of the bridge
MAC address	MAC address of the bridge
Max age(s)	Max age
Forward delays(s)	State transition delay
Hello time(s)	Interval of sending Hello packets
Max hops	Max hops

display stp ignored-vlan

Syntax **display stp ignored-vlan**

View Any view

Parameters None

Description Use the **display stp ignored-vlan** command to display VLAN Ignore-enabled VLANs.

Examples # Display VLAN Ignore-enabled VLANs.

```
<Sysname> display stp ignored-vlan
STP-Ignored VLAN:    1 to 2
```

Table 38 Field descriptions of the display stp ignored-vlan command

Field	Description
STP-Ignored VLAN	List of VLAN Ignore-enabled VLANs

display stp region-configuration

Syntax **display stp region-configuration**

View Any view

Parameters None

Description Use the **display stp region-configuration** command to view the currently effective MST region configuration information, including the region name, revision level, and VLAN-to-instance mappings.

Related commands: **stp region-configuration**.

Examples # View the currently effective MST region configuration information.

```
<Sysname> display stp region-configuration
Oper configuration
   Format selector    :0
   Region name        :000fe222e5cd
   Revision level     :0

   Instance   Vlans Mapped
      0       1 to 4094
```

Table 39 Field descriptions of the display stp region-configuration command

Field	Description
Format selector	MSTP-defined format selector
Region name	MST region name
Revision level	Revision level of an MST region
Instance Vlans Mapped	VLAN-to-instance mappings in an MST region

instance

Syntax **instance** *instance-id* **vlan** *vlan-list*

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

View MST region view

Parameters *instance-id*: MST instance ID, in the range 0 to 47. A value of 0 specifies the CIST.

vlan-list: VLAN list. You can specify multiple VLANs or VLAN ranges by providing this argument in the form of *vlan-list* = { *vlan-id* [**to** *vlan-id*] }&<1-10>, where, *vlan-id* is a VLAN ID, and &<1-10> means that you can specify up to 10 VLANs or VLAN ranges for this argument.

Description Use the **instance** command to map the specified VLAN(s) to an MST instance.

Use the **undo instance** command to remove the specified VLAN(s) from the specified MST instance and map the removed VLAN(s) to the CIST (MST instance 0).

By default, all VLANs are mapped to the CIST.

- If you specify no VLAN in the **undo instance** command, all VLANs mapped to the specified MST instance will be remapped to the CIST.
- You cannot map the same VLAN to different MST instances. If you map a VLAN that has been mapped to an instance to a new instance, the old mapping will be automatically removed.

Related commands: **region-name**, **revision-level**, **check region-configuration**, **vlan-mapping modulo**, and **active region-configuration**.

Examples # Map VLAN 2 to MST instance 1.

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] instance 1 vlan 2
```

region-name

Syntax **region-name** *name*

undo region-name

View MST region view

Parameters *name*: Name of the MST regions, a string of 1 to 32 characters.

Description Use the **region-name** command to configure the MST region name of your device.

Use the **undo region-name** command to restore the MST region name to the default setting.

By default, the MST region name of a device is its bridge MAC address.

The MST region name, the VLAN-to-instance mapping table and the MSTP revision level of a device jointly determine the MST region the device belongs to.

Related commands: **instance**, **revision-level**, **check region-configuration**, **vlan-mapping modulo**, and **active region-configuration**.

Examples # Set the MST region name of the device to "hello".

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] region-name hello
```

reset stp

Syntax **reset stp** [**interface** *interface-list*]

View User view

Parameters *interface-list*: Ethernet port list. You can specify multiple Ethernet ports or port ranges by providing the this argument in the form of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>, where, *interface-type* is port type and *interface-number* is port number, and &<1-10> means that you can specify up to 10 VLANs or VLAN ranges for this argument.

Description Use the **reset stp** command to clear the MSTP statistics information.

The MSTP statistics information includes the numbers of TCN BPDUs, configuration BPDUs, RST BPDUs and MST BPDUs sent/received through the specified port(s) (STP BPDUs and TCN BPDUs are counted only for the CIST).

Note that this command clears the spanning tree-related statistics information on the specified port(s) if you specify the *interface-list* argument; otherwise, this command clears the spanning tree-related statistics on all ports.

Related commands: **display stp**.

Examples # Clear the spanning tree-related statistics information on ports Ethernet 1/1/1 through Ethernet 1/1/3.

```
<Sysname> reset stp interface ethernet 1/1/1 to ethernet 1/1/3
```

revision-level

Syntax **revision-level** *level*

undo revision-level

View MST region view

Parameters *level*: MSTP revision level.

Description Use the **region-level** command to configure the MSTP revision level of your device.

Use the **undo region-level** command to restore the MSTP revision level to the default setting.

The MSTP revision level, the MST region name and the VLAN-to-instance mapping table of a device jointly determine the MST region the device belongs to.

Related commands: **instance**, **region-name**, **check region-configuration**, **vlan-mapping modulo**, and **active region-configuration**.

Examples # Set the MSTP revision level of the MST region to 5.

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] revision-level 5
```

stp

Syntax **stp** { **enable** | **disable** }

undo stp

View System view, Ethernet interface view, port group view

Parameters **enable**: Enables the MSTP feature.

disable: Disables the MSTP feature.

Description Use the **stp** command to enable or disable the MSTP feature globally or for a port or a group of ports.

Use the **undo stp** command to restore the default MSTP status globally or for a port or a group of ports.

By default, MSTP is enabled globally. With MSTP enabled globally, MSTP is enabled on all the ports by default.

Note that:

- To control MSTP flexibly, you can disable the MSTP feature for certain ports so that they will not take part in spanning tree computing and thus to save the device's CPU resources.
- Configured in system view, the setting is effective for the device globally; configured in Ethernet interface view, the setting is effective on the current port only; configured in port group view, the setting is effective on all the ports in the port group.
- After you enable MSTP, the device determines whether to work in STP-compatible mode, in RSTP mode or in MSTP mode according to your MSTP work mode setting. After MSTP is disabled, the device becomes a transparent bridge.
- After being enabled, MSTP dynamically maintains spanning tree status of the corresponding VLANs based the received configuration BPDUs. After being disabled, it stops maintaining the spanning tree status.

Related commands: **stp mode**.

Examples # Enable the MSTP feature globally.

```
<Sysname> system-view
[Sysname] stp enable
```

Disable MSTP on port Ethernet 1/1/1.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1/1
[Sysname-Ethernet1/1/1] stp disable
```

stp bpdu-protection

Syntax **stp bpdu-protection**

undo stp bpdu-protection

View System view

Parameters None

Description Use the **stp bpdu-protection** command to enable the BPDU guard function for the device.

Use the **undo stp bpdu-protection** command to disable the BPDU guard function for the device.

By default, the BPDU guard function is disabled.

Examples # Enable the BPDU guard function for the device.

```
<Sysname> system-view
[Sysname] stp bpdu-protection
```

stp bridge-diameter

Syntax **stp bridge-diameter** *bridgenum*

undo stp bridge-diameter

View System view

Parameters *bridgenum*: Network diameter of the spanning tree.

Description Use the **stp bridge-diameter** command to specify the network diameter, namely the maximum number of stations between any two terminal devices on the switched network.

Use the **undo stp bridge-diameter** command to restore the default network diameter of the switched network.

By default, the network diameter of the switched network is 7.

An appropriate setting of hello time, forward delay and max age can speed up network convergence. The values of these timers are related to the network size. You can set these three timers indirectly by setting the network diameter. Based on the network diameter you configured, MSTP automatically sets an optimal hello time, forward delay, and max age for the device. With the network diameter set to 7 (the default), the three timer are also set to their defaults.

Note that this configuration is effective for the CIST only and not for MSTIs, and this configuration must be configured on the root bridge.

Related commands: **stp timer forward-delay**, **stp timer hello**, and **stp timer max-age**.

Examples # Set the network diameter of the switched network to 5.

```
<Sysname> system-view
[Sysname] stp bridge-diameter 5
```

stp compliance

Syntax **stp compliance** { **legacy** | **dot1s** | **auto** }

undo stp compliance

View Ethernet interface view/port group view

Parameters **auto**: Configure the port to recognize the BPDU format automatically.

dot1s: Configures the port to receive and send standard-format (802.1s-compliant) MSTP packets.

legacy: Configures the port to receive and send compatible-format BPDUs.

Description Use the **stp compliance** command to configure the MSTP packet format for a port or a group of ports

Use the **undo stp compliance** command to restore the MSTP packet format to be default setting for a port or a group of ports.

By default, the MSTP packet format is set to **auto**, namely a port recognizes the BPDU format automatically.

Note that:

- Configured in Ethernet interface view, the setting is effective on the current port only; configured in port group view, the setting is effective on all ports in the port group.
- If the MSTP packet format is set to auto for a port, the port automatically recognizes and resolves the received compatible-format BPDUs or 802.1s-compliant BPDUs, and sends, when needed, compatible-format or 802.1s-compliant BPDUs.

- If you specify the BPDU format by using the legacy or dot1s keyword, the port can only receive and send BPDUs of the specified format. If the port is configured not to detect the packet format automatically while it works in the MSTP mode, and if it receives a packet in the format other than as configured, that port will become a designated port, and the port will remain in the discarding state to prevent the occurrence of a loop.

Examples # Configure port Ethernet 1/1/1 to receive and send standard-format (802.1s) MSTP packets.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1/1
[Sysname-Ethernet1/1/1] stp compliance dot1s
```

Restore the default MSTP packet format for port Ethernet 1/1/1.

```
[Sysname-Ethernet1/1/1] undo stp compliance
```

stp config-digest-snooping

Syntax **stp config-digest-snooping**

undo stp config-digest-snooping

View system view, Ethernet interface view, port group view

Parameters None

Description Use the **stp config-digest-snooping** command to enable Digest Snooping.

Use the **undo stp config-digest-snooping** command to disable Digest Snooping.

The feature is disabled by default.

Notice that:

- Configured in system view, the setting is effective for the device globally; configured in Ethernet interface view, the setting is effective on the current port only; configured in port group view, the setting is effective on all the ports in the port group.
- You need to enable this feature both globally and on ports connected to other vendors' devices to make it take effect. It is recommended to enable the feature on all the ports connected to other vendor's devices first and then enable it globally, to minimize the impact to the network. To disable the feature on all the ports, you can just disable it globally.
- It is not recommended to enable Digest Snooping on the MST region edge port to avoid loops.

Examples # Enable global Digest Snooping.

```
<Sysname> system-view
[Sysname] stp config-digest-snooping
```

Enable Digest Snooping on Ethernet 1/1/1.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1/1
[Sysname-Ethernet1/1/1] stp config-digest-snooping
```

stp cost

Syntax **stp** [**instance** *instance-id*] **cost** *cost*

undo stp [**instance** *instance-id*] **cost**

View Ethernet interface view, port group view

Parameters *instance-id:* MST instance ID.

cost *cost*: Specifies the path cost of a port.

Description Use the **stp cost** command to set the path cost of a port or a group or ports in the specified MST instance.

Use the **undo stp cost** command to restore the default path cost of a port or ports in a port group in the specified MST instance.

By default, the path cost of a port is determined by MSTP.

Note that:

- If you set *instance-id* to 0, you are setting the path cost of the port in the CIST. The path cost setting of a port can affect the role selection of the port. Setting different path costs for the same port in different MST instances allows different VLAN traffic flows to be forwarded along different physical links, thus to enable per-VLAN load balancing. When the path cost of a port is changed, MSTP will re-compute the role of the port and initiate a state transition.
- Configured in Ethernet interface view, the setting is effective on the current port only; configured in port group view, the setting is effective on all ports in the port group.
- If you do not provide **instance** *instance-id*, your configuration will take effect in the CIST instance only.

Examples # Set the path cost of port Ethernet 2/1/3 in MST instance 2 to 200.

```
<Sysname> system-view
[Sysname] interface ethernet 2/1/3
[Sysname-Ethernet2/1/3] stp instance 2 cost 200
```

stp edged-port

Syntax **stp edged-port** { **enable** | **disable** }

undo stp edged-port

View Ethernet interface view/port group view

Parameters **enable**: Configures the current port to be an edge port.

disable: Configures the current port to be a non-edge port.

Description Use the **stp edged-port enable** command to configure the current port to be an edge port.

Use the **stp edged-port disable** or **undo stp edged-port enable** command to configure the current port to be a non-edge port.

All Ethernet ports are non-edge ports by default.

Note that:

- Configured in Ethernet interface view, the setting is effective on the current port only; configured in port group view, the setting is effective on all ports in the port group.
- If a port directly connects to a user terminal rather than another device or a shared LAN segment, this port is regarded as an edge port. When the network topology changes, an edge port will not cause a temporary loop. Therefore, configuring a port as an edge port can enable the port to transition to the forwarding state rapidly. We recommend that you configure an Ethernet port directly connecting to a user terminal as an edge port before to enable it to transition to the forwarding state rapidly.
- Normally, configuration BPDUs from other devices cannot reach an edge port because it does not connect to any other device. Before the BPDU guard function is enabled, if a port receives a configuration BPDU, the port is working actually as a non-edge port even if you have configured in as an edge port.

Examples # Configure port Ethernet 2/1/1 as a non-edge port.

```
<Sysname> system-view
[Sysname] interface ethernet 2/1/1
[Sysname-Ethernet2/1/1] stp edged-port disable
```

stp ignored vlan

Syntax **stp ignored vlan** *vlan-list*

undo stp ignored vlan *vlan-list*

View System view

Parameters *vlan-list*: Indicates multiple VLAN IDs. *vlan-list*={ *vlan-id* [**to** *vlan-id*] }&<1-10>, *vlan-id* is in the range 1 to 4094, &<1-10> indicates you can enter the argument before it up to 10 times.

Description Use the **stp ignored vlan** command to enable VLAN Ignore in specified VLANs.

Use the **undo stp ignored vlan** command to disable VLAN Ignore in specified VLANs.

By default, VLAN ignore is disabled in a VLAN.

Examples # Enable VLAN Ignore in VLAN 2.

```
<Sysname> system-view
[Sysname] stp ignored vlan 2
```

stp loop-protection

Syntax **stp loop-protection**

undo stp loop-protection

View Ethernet interface view/port group view

Parameters None

Description Use the **stp loop-protection** command to enable the loop guard function for a port or a group of ports.

Use the **undo stp loop-protection** command to restore default loop guard setting for a port of a group of ports.

By default, the loop guard function is disabled.

Configured in Ethernet interface view, the setting is effective on the current port only; configured in port group view, the setting is effective on all ports in the port group.

Examples # Enable the loop guard function for port Ethernet 2/1/1.

```
<Sysname> system-view
[Sysname] interface ethernet 2/1/1
[Sysname-Ethernet2/1/1] stp loop-protection
```

stp max-hops

Syntax **stp max-hops** *hops*

undo stp max-hops

View System view

Parameters *hops*: Maximum hops.

Description Use the **stp max-hops** command to set the maximum hops of the MST region on the device.

Use the **undo stp max-hops** command to restore the maximum hops to the default setting.

By default, the maximum hops of an MST region is 20.

In the CIST or an MST instance, the maximum hops setting configured on the regional root bridge determines the maximum network diameter supported by the MST region. After a configuration BPDU leaves the root bridge, its hop count is decremented by 1 whenever it passes a device. When its hop count reaches 0, it will be discarded by the device that has received it. As a result, devices beyond the maximum hop count are unable to take part in spanning tree computing, and thereby the size of the MST region is limited.

When the current device becomes the root bridge of the CIST or an MSTI, the maximum hops setting configured on the device becomes the network diameter of that spanning tree and restricts the size of that spanning tree in the current MST region.

Devices other than the root bridge in an MST region use the maximum hops setting on the root bridge.

Examples # Set the maximum hops of the MST region to 35.

```
<Sysname> system-view
[Sysname] stp max-hops 35
```

stp mcheck

Syntax **stp mcheck**

View System view, Ethernet interface view

Parameters None

Description Use the **stp mcheck** command to carry out the mCheck operation globally or on a port.

In a switched network, if a port on the device running MSTP (or RSTP) connects to a device running STP, this port will automatically migrate to the STP-compatible mode. However, if the device running STP is removed, this will not be able to migrate automatically to the MSTP (or RSTP) mode, but will remain working in the STP-compatible mode. In this case, you can perform an mCheck operation to force the port to migrate to the MSTP (or RSTP) mode.

Note that the **stp mcheck** command is meaningful only when the device works in the MSTP (or RSTP) mode, not in the STP-compatible mode.

Related commands: **stp mode**.

Examples # Carry out mCheck on port Ethernet 2/1/1.

```
<Sysname> system-view
[Sysname] interface Ethernet 2/1/1
[Sysname-Ethernet2/1/1] stp mcheck
```

stp no-agreement-check

Syntax **stp no-agreement-check**

undo stp no-agreement-check

View Ethernet interface view/port group view

Parameters None

Description Use the **stp no-agreement-check** command to enable No Agreement Check on port(s).

Use the **undo stp no-agreement-check** command to disable No Agreement Check on port(s).

By default, No Agreement Check is disabled.

Configured in Ethernet interface view, the setting is effective on the current port only; configured in port group view, the setting is effective on all the ports in the port group.

The No Agreement Check feature can take effect only on root ports or alternate ports.

Examples # Enable No Agreement Check on Ethernet 1/1/1.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1/1
[Sysname-Ethernet1/1/1] stp no-agreement-check
```

stp mode

Syntax **stp mode** { **stp** | **rstp** | **mstp** }

undo stp mode

View System view

Parameters **stp**: Configures the MSTP-compliant device to work in STP-compatible mode.

rstp: Configures MSTP-compliant device to work in RSTP mode.

mstp: Configures MSTP-compliant device to work in MSTP mode.

Description Use the **stp mode** command to configure the MSTP work mode of the device.

Use the **undo stp mode** command to restore the MSTP work mode to the default setting.

By default, an MSTP-compliant device works in MSTP mode.

Related commands: **stp mcheck**, and **stp**.

Examples # Configure the MSTP-compliant device to work in STP-compatible mode.

```
<Sysname> system-view
[Sysname] stp mode stp
```

Configure the MSTP-compliant device to work in RSTP mode.

```
<Sysname> system-view
[Sysname] stp mode rstp
```

stp pathcost-standard

Syntax **stp pathcost-standard** { **dot1d-1998** | **dot1t** | **legacy** }

undo stp pathcost-standard

View System view

Parameters **dot1d-1998**: Adopts the IEEE 802.1D-1998 standard.

dot1t: Adopts the IEEE 802.1t standard.

legacy: Adopts the private standard.

Description Use the **stp pathcost-standard** command to specify the standard used to calculate the default path cost of the link connected with the device

Use the **undo stp pathcost-standard** command to restore the default setting of the calculation standard.

By default, a device uses the private standard to calculate the default path cost.

Note that if you change the standard that the device uses in calculating the default path cost, the port path cost value set through the **stp cost** command will be out of effect.

Table 40 Link speed vs. path cost

Link speed	Duplex state	802.1D-1998	IEEE 802.1t	Private standard
0	-	65535	200,000,000	200,000
10Mbps	Single Port	100	2,000,000	2,000
	Aggregated Link 2 Ports	100	1,000,000	1,800
		100	666,666	1,600
	Aggregated Link 3 Ports	100	500,000	1,400
	Aggregated Link 4 Ports			
100Mbps	Single Port	19	200,000	200
	Aggregated Link 2 Ports	19	100,000	180
		19	66,666	160
	Aggregated Link 3 Ports	19	50,000	140
	Aggregated Link 4 Ports			
1000Mbps	Single Port	4	20,000	20
	Aggregated Link 2 Ports	4	10,000	18
		4	6,666	16
	Aggregated Link 3 Ports	4	5,000	14
	Aggregated Link 4 Ports			
10Gbps	Single Port	2	2,000	2
	Aggregated Link 2 Ports	2	1,000	1
		2	666	1
	Aggregated Link 3 Ports	2	500	1
	Aggregated Link 4 Ports			

In the calculation of the path cost value of an aggregated link, 802.1D-1998 does not take into account the number of ports in the aggregated link. Whereas, 802.1T takes the number of ports in the aggregated link into account. The calculation formula is: Path Cost = 200,000,000/link speed (in 100 kbps), where link speed is the sum of the link speed values of the non-blocked ports in the aggregated link.

Examples # Configure the device to calculate the default path cost based on IEEE 802.1D-1998.

```
<Sysname> system-view
[Sysname] stp pathcost-standard dot1d-1998
```

Configure the device to calculate the default path cost based on IEEE 802.1t.

```
<Sysname> system-view
[Sysname] stp pathcost-standard dot1t
```

stp point-to-point

Syntax **stp point-to-point** { **force-true** | **force-false** | **auto** }

undo stp point-to-point

View Ethernet interface view/port group view

Parameters **auto**: Specifies MSTP detects automatically whether the current port connects to a point-to-point link.

force-false: Specifies the current port to connect to a non-point-to-point link.

force-true: Specifies the current port to connect to a point-to-point link.

Description Use the **stp point-to-point** command to specify whether the current port connects to a point-to-point link.

Use the **undo stp point-to-point** command to restore the default status of the link connected with the current port.

The default setting is **auto**; namely the MSTP-compliant device automatically detects whether an Ethernet port connects to a point-to-point link.

Configured in Ethernet interface view, the setting is effective on the current port only; configured in port group view, the setting is effective on all ports in the port group.

Note that:

- When connecting to a non-point-to-point link, a port is incapable of rapid state transition.
- If the current port is the master port of aggregated ports of if it works in full duplex mode, the link to which the current port connects is a point-to-point link. We recommend that you use the default setting, namely let MSTP detect the link status automatically.
- This setting is effective to the CIST and all MST instances. If a port is configured as connecting to a point-to-point link or a non-point-to-point link, the setting takes effect for the port in all MST instances. If the physical link to which the port connects is not a point-to-point link and you force it to be a point-to-point link by configuration, your configuration may incur a temporary loop.

Examples # Configure port Ethernet 2/1/3 as connecting to a point-to-point link.

```
<Sysname> system-view
[Sysname] interface Ethernet 2/1/3
[Sysname-Ethernet2/1/3] stp point-to-point force-true
```

stp port priority

Syntax **stp** [**instance** *instance-id*] **port priority** *priority*

undo stp [**instance** *instance-id*] **port priority**

View Ethernet interface view/port group view

Parameters *instance-id*: MST instance ID, in the range 0 to 47. A value of 0 specifies the CIST.

priority: Port priority, at the step of 16 (0, 16, 32..., for example).

Description Use the **stp port priority** command to set the priority of a port or a group or ports in the specified MST instance.

Use the **undo stp port priority** command to restore the default priority of a port or a group or ports in the specified MST instance.

By default, the port priority is 128.

Note that:

- Configured in Ethernet interface view, the setting is effective on the current port only; configured in port group view, the setting is effective on all ports in the port group.
- If you set *instance-id* to 0, you are setting the priority of the port in the CIST. The priority of a port can affect the role selection of the port in the specified MST instance.
- Setting different priorities for the same port in different MST instances allows different VLAN traffic flows to be forwarded along different physical links, thus to enable per-VLAN load balancing.
- When the priority of a port is changed, MSTP will re-compute the role of the port and initiate a state transition.
- If you do not provide **instance** *instance-id*, your configuration will take effect in the CIST instance only.

Examples # Set the priority of port Ethernet 2/1/3 in MST instance 2 to 16.

```
<Sysname> system-view
[Sysname] interface Ethernet 2/1/3
[Sysname-Ethernet2/1/3] stp instance 2 port priority 16
```

stp priority

Syntax **stp** [**instance** *instance-id*] **priority** *priority*

undo stp [**instance** *instance-id*] **priority**

View System view

Parameters *instance-id*: MST instance ID, in the range 0 to 47. A value of 0 specifies the CIST.

priority: Port priority, in the range of 0 to 61440 at the step of 4096, namely you can set up to 16 priority values, such as 0, 4096, 8192..., on the device.

Description Use the **stp priority** command to set the priority of the device in the specified MST instance.

Use the **undo stp priority** command to restore the device priority to the default setting.

By default, the device priority is 32768.

The device priority is involved in spanning tree computing. The device priority is set on a per-instance basis. An MSTP-compliant device can have different priorities in different MST instances.

If you do not provide **instance** *instance-id*, your configuration will take effect in the CIST instance only.

Examples # Set the device priority in MST instance 1 to 4096.

```
<Sysname> system-view
[Sysname] stp instance 1 priority 4096
```

stp region-configuration

Syntax **stp region-configuration**

undo stp region-configuration

View System view

Parameters None

Description Use the **stp region-configuration** command to enter MST region view.

Use the **undo stp region-configuration** command to restore the default MST region configurations.

By default, the default settings are used for all the three MST region parameters. Namely, the device's MST region name is the device's MAC address, all VLANs are mapped to the CIST, and the MSTP revision level is 0.

After you enter MST region view, you can configure the parameters related the MST region, including the region name, VLAN-to-instance mapping and revision level.

Examples # Enter MST region view.

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region]
```

stp root primary

Syntax **stp** [**instance** *instance-id*] **root primary** [**bridge-diameter** *bridgenum*] [**hello-time** *centi-seconds*]

undo stp [**instance** *instance-id*] **root**

View System view

Parameters *instance-id*: MST instance ID, in the range 0 to 47. A value of 0 specifies the CIST.

root primary: Specifies the current device as the root bridge of the specified MST instance.

bridgenum: Network diameter of the spanning tree, defaulting to 7.

centi-seconds: Hello time (in centiseconds) of the spanning tree.

Description Use the **stp root primary** command to specify the current device as the root bridge of the specified MST instance.

Use the **undo stp root** command to remove the current device as the root bridge of the specified MST instance.

By default, a device is not a root bridge.

Note that:

- If you do not provide **instance** *instance-id*, the setting is effective in the CIST instance only.
- There is only one root bridge in effect in a spanning tree instance. If two or more devices are configured as the root bridges of the same spanning tree instance, the one with smaller MAC address works as the root bridge.
- You can specify a root bridge for each MST instance without caring about the device priority.
- After specifying the current device as the root bridge or a secondary root bridge, you cannot change the priority of the device.
- When configuring a root bridge, you can use this command to specify the network diameter of the switched network, so that the MSTP-compliant device automatically calculates the three timers (hello time, forward delay and max age). As the calculated hello time value is not the optimal value, you can specify a hello time value by providing **hello-time** *centi-seconds* in the command, which will override the hello time value calculated by the device based on the network diameter. Generally, we recommend that you use the values of the other two timers calculated by the device based the specified network diameter.

- The configured network diameter and hello time settings are effective only for MST instance 0, namely the CIST. If you configure these two timers for any other instance, your configuration can succeed, but they will not actually work.

Examples # Configure the current device as the root bridge of MST instance 0, setting the network diameter to 4 and the hello time of the device to 500 centiseconds.

```
<Sysname> system-view
[Sysname] stp instance 0 root primary bridge-diameter 4 hello-time 500
```

stp root secondary

Syntax **stp** [**instance** *instance-id*] **root secondary** [**bridge-diameter** *bridgenum*] [**hello-time** *centi-seconds*]

undo stp [**instance** *instance-id*] **root**

View System view

Parameters *instance-id*: MST instance ID.

root secondary: Specifies the current device as a secondary root bridge of the specified MST instance.

bridgenum: Network diameter of the spanning tree, defaulting to 7.

centi-seconds: Hello time (in centiseconds) of the spanning tree.

Description Use the **stp root secondary** command to specify the current device as a secondary root bridge of the specified MST instance.

Use the **undo stp root** command to remove the current device as a secondary root bridge of the specified MST instance.

By default, a device is not a secondary root bridge.

Note that:

- If you do not provide **instance** *instance-id*, your configuration will take effect in the CIST instance only.
- You can configure one or more secondary root bridges for each MST instance. When the root bridge of an instance fails or is shut down, the secondary root bridge can take over the role of the instance of the specified MST instance. If you specify more than one secondary root bridge, the secondary root bridge with the lowest Mac address will become the root bridge.
- When configuration a secondary root bridge, you can specify the network diameter of the switched network and the hello time for the secondary root bridge, so that the MSTP-compliant device automatically calculates the other two timers (forward delay and max age) of the root bridge.

- The configured network diameter and hello time settings are effective only for MST instance 0, namely the CIST. If you configure these two timers for any other instance, your configuration can succeed, but they will not actually work.
- If you set *instance-id* to 0, you are specifying the current device as the secondary root bridge of the CIST.
- Upon specifying the current device as the root bridge or a secondary root bridge, you cannot change the priority of the device.

Examples # Define the current device as the secondary root bridge of MST instance 0 and set the network diameter to 5 and the hello time of the device to 300 centiseconds.

```
<Sysname> system-view
[Sysname] stp instance 0 root secondary bridge-diameter 5 hello-time 300
```

stp root-protection

Syntax **stp root-protection**

undo stp root-protection

View Ethernet interface view, port group view

Parameters None

Description Use the **stp root-protection** command to enable the root guard function for a port or a group of ports.

Use the **undo stp root-protection** command to restore default setting of the root guard function for the port(s).

By default, the root guard function is disabled.

Configured in Ethernet interface view, the setting is effective on the current port only; configured in port group view, the setting is effective on all ports in the port group.

Examples # Enable the root guard function for port Ethernet 2/1/1.

```
<Sysname> system-view
[Sysname] interface Ethernet 2/1/1
[Sysname-Ethernet2/1/1] stp root-protection
```

stp tc-protection

Syntax **stp tc-protection enable**

stp tc-protection disable

View System view

Parameters None

Description Use the **stp tc-protection enable** command to enable the TC-BPDU attack guard function for the device.

Use the **stp tc-protection disable** command to disable the TC-BPDU attack guard function for the device.

By default, the TC-BPDU attack guard function is enabled.

Examples # Enable the TC-BPDU attack guard function for the device.

```
<Sysname> system-view
[Sysname] stp tc-protection enable
```

stp timer forward-delay

Syntax **stp timer forward-delay** *centi-seconds*

undo stp timer forward-delay

View System view

Parameters *centi-seconds*: Forward delay in centiseconds.

Description Use the **stp timer forward-delay** command to set the forward delay timer of the device.

Use the **undo stp timer forward-delay** command to restore the forward delay timer of the device to the default setting.

By default, the forward delay timer is set to 1,500 centiseconds.

In order to prevent temporary loops, a port must go through an intermediate state, the learning state, before it transitions from the discarding state to the forwarding state, and must wait a certain period of time before it transitions from one state to another to keep synchronized with the remote device during state transition. The forward delay timer set on the root bridge determines the time interval of state transition.

If the current device is the root bridge, the state transition interval of the device depends on the set forward delay value; for a secondary root bridge, its state transition interval is determined by the forward delay timer set on the root bridge.

The setting of the hello time, forward delay and max age timers must meet the following formulae.

- 2 × (forward delay - 1 second) *f*¶ max age
- Max age *f*¶ 2 × (hello Time + 1 second)

MSTP can work effectively on the entire network only when the above-mentioned conditions are met; otherwise, network instability will frequently occur. We recommend that you specify the network diameter of the switched network in the **stp root primary** command and let MSTP automatically calculate an optimal setting of these three timers.

Related commands: **stp timer hello**, **stp timer max-age**, and **stp bridge-diameter**.

Examples # Set the forward delay timer of the device to 2,000 centiseconds.

```
<Sysname> system-view
[Sysname] stp timer forward-delay 2000
```

stp timer hello

Syntax **stp timer hello** *centi-seconds*

undo stp timer hello

View System view

Parameters *centi-seconds*: Hello time (in centiseconds).

Description Use the **stp timer hello** command to set the hello time of the device.

Use the **undo stp timer hello** command to restore the hello time of the device to the default setting.

By default, the hello time is set to 200 centiseconds.

Hello time is the time interval at which MSTP-compliant devices send configuration BPDUs to maintain spanning tree stability. If a device fails to receive configuration BPDUs within the set period of time, a new spanning tree computing process will be triggered due to timeout. The root bridge sends configuration BPDUs at the interval of the hello time set on the device, while secondary root bridges use the hello time set on the root bridge.

The setting of the hello time, forward delay and max age timers must meet the following formulae.

- 2 × (forward delay - 1 second) f max age
- Max age f 2 × (hello time + 1 second)

MSTP can work effectively on the entire network only when the above-mentioned conditions are met; otherwise, network instability will frequently occur. We recommend that you specify the network diameter of the switched network in the **stp root primary** command and let MSTP automatically calculate an optimal setting of these three timers.

Related commands: **stp timer forward-delay**, **stp timer max-age**, and **stp bridge-diameter**.

Examples # Set the hello time of the device to 400 centiseconds.

```
<Sysname> system-view
[Sysname] stp timer hello 400
```

stp timer max-age

Syntax **stp timer max-age** *centi-seconds*

undo stp timer max-age

View System view

Parameters *centi-seconds*: Max age (in centiseconds).

Description Use the **stp timer max-age** command to set the max age timer of the device.

Use the **undo stp timer max-age** command to restore the max age timer of the device to the default setting.

By default, the max age is set to 2,000 centiseconds.

MSTP can detect link faults and automatically restore the forwarding state of the redundant link. In the CIST, the device determines whether a configuration BPDU received on a port has expired based on the max age timer. If a port receives a configuration BPDU that has expired, that MST instance needs to re-computed.

The max age timer is not meaningful for MSTIs. If the current device is the root bridge of the CIST, it determines whether a configuration BPDUs has expired based on the configured max age timer; if the current device is not the root bridge of the CIST, it uses the max age timer set on the CIST root bridge.

The setting of the hello time, forward delay and max age timers must meet the following formulae.

- 2 × (forward delay - 1 second) $\geq$ max age
- Max age $\geq$ 2 × (hello time + 1 second)

MSTP can work effectively on the entire network only when the above-mentioned conditions are met; otherwise, network instability will frequently occur. We recommend that you specify the network diameter in the **stp root primary** command and let MSTP automatically calculate an optimal setting of these three timers.

Related commands: **stp timer forward-delay**, **stp timer hello**, and **stp bridge-diameter**.

Examples # Set the max age timer of the device to 1,000 centiseconds.

```
<Sysname> system-view
[Sysname] stp timer max-age 1000
```

stp timer-factor

Syntax **stp timer-factor** *number*

undo stp timer-factor

View System view

Parameters *number*: Timeout factor.

Description Use the **stp timer-factor** command to configure the timeout time of the device by setting the timeout factor. Timeout time = timeout factor × 3 × hello time.

Use the **undo stp timer-factor** command to restore the timeout factor to the default setting.

By default, the timeout factor of the device is set to 3.

A device sends a BPDU to the devices around it at a regular interval of hello time to check whether any link is faulty. Typically, if a device does not receive a BPDU from the upstream device within nine times the hello time, it will assume that the upstream device has failed and start a new spanning tree computing process.

In a very stable network, this kind of spanning tree computing may occur because the upstream device is busy. In this case, you can avoid such unwanted spanning tree computing by lengthening the timeout time (by setting the timeout factor to 4 or more). We recommend that you set the timeout factor to 5, or 6, or 7 for a stable network.

Examples # Set the timeout factor of the device to 7.

```
<Sysname> system-view
[Sysname] stp timer-factor 7
```

stp transmit-limit

Syntax **stp transmit-limit** *packetnum*

undo stp transmit-limit

View Ethernet interface view, port group view

Parameters *packetnum*: Maximum number of MSTP packets that the port can send within each hello time, namely the maximum transmission rate of the port.

Description Use the **stp transmit-limit** command to set the maximum number of configuration BPDUs that the current port can send within each hello time.

Use the **undo stp transmit-limit** command to restore the maximum number of configuration BPDUs that the current port can send within each hello time to the default setting.

By default, the maximum transmission rate of a port is 10.

- A larger maximum transmission rate value indicates that the current port sends more MSTP packets within each hello time, but this means that more device resources will be used. An appropriate maximum transmission rate setting can limit the number of MSTP packets that the current port sends within each hello time and prevent MSTP from using an excessive bandwidth resource during network topology instability.
- Configured in Ethernet interface view, the setting is effective on the current port only; configured in port group view, the setting is effective on all ports in the port group.

Examples # Set the maximum transmission rate of Ethernet 2/1/1 to 5.

```
<Sysname> system-view
[Sysname] interface Ethernet 2/1/1
[Sysname-Ethernet2/1/1] stp transmit-limit 5
```

vlan-mapping modulo

Syntax **vlan-mapping modulo** *modulo*

View MST region view

Parameters *modulo*: Modulo value.

Description Use the **vlan-mapping modulo** command to map VLANs in the current MST region to MST instances according to the specified modulo value.

By default, all VLANs are mapped to the CIST (instance 0).

You cannot map the same VLAN to different MST instances. If you map a VLAN that has been mapped to an instance to a new instance, the old mapping will be automatically removed.

*By using the **vlan-mapping modulo** command, you can quickly specify a VLAN for each MST instance. This command maps each VLAN to the MST instance whose ID is (VLAN ID-1) %modulo + 1, where (VLAN ID-1) %modulo is the modulo operation for (VLAN ID-1). If the modulo value is 16, for example, then VLAN 1 will be mapped to MSTI 1, VLAN 2 to MSTI 2, VLAN 16 to MSTI 16, VLAN 17 to MSTI 1, and so on.*

Related commands: **region-name**, **revision-level**, **check region-configuration**, and **active region-configuration**.

Examples # Map VLANs to MSTIs as per the modulo value of 16.

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] vlan-mapping modulo 16
```

10 TUNNELING CONFIGURATION COMMANDS

aggregation-group (Tunnel interface view)

Syntax **aggregation-group** *aggregation-group-ID*

undo aggregation-group

View Tunnel interface view

Parameters *aggregation-group-id*: Link aggregation group ID to be referenced.

Description Use the **aggregation-group** command to specify a link aggregation group to be referenced by a tunnel.

Use the **undo aggregation-group** command to remove the link aggregation group referenced by a tunnel.

By default, a tunnel does not reference any link aggregation group.

Before specifying a link aggregation group for a tunnel in tunnel interface view, you have configured the link aggregation group and set the service type of the link aggregation group to tunnel in system view.

One tunnel interface can reference only one link aggregation group.

Related commands: **link-aggregation group** in *Link Aggregation Commands* in *Access Volume*.

Examples # Create link aggregation group 1, and set the configuration mode to **manual** and the service type to **tunnel**.

```
<Sysname> system-view
[Sysname] link-aggregation group 1 mode manual
[Sysname] link-aggregation group 1 service-type tunnel
```

Add a Gigabit Ethernet interface to link aggregation group 1 on the module that supports IPv6.

```
[Sysname] interface GigabitEthernet 6/4/1
[Sysname-GigabitEthernet6/4/1] stp disable
[Sysname-GigabitEthernet6/4/1] port link-aggregation group 1
```

Reference link aggregation group 1 in tunnel interface view.

```
[Sysname] interface Tunnel 3/0/1
[Sysname-Tunnel3/0/1] aggregation-group 1
```

debugging ipv4-tunnel

Syntax **debugging ipv4-tunnel** { **all** | **error** | **packet** }

undo debugging ipv4-tunnel { **all** | **error** | **packet** }

View User view

Parameters **all**: Enables all types of debugging for the IPv4 tunnel module.

error: Enables error debugging for the IPv4 tunnel module.

packet: Enable packet debugging for the IPv4 tunnel module.

Description Use the **debugging ipv4-tunnel** command to enable debugging for the IPv4 tunnel module.

Use the **undo debugging ipv4-tunnel** command to disable debugging for the IPv4 tunnel module. By default, debugging for the IPv4 tunnel module is disabled.

Examples # Enable debugging for the IPv4 tunnel module, and use the **ping** command to view the debugging information.

```
<Sysname> debugging ipv4-tunnel all
<Sysname> terminal debugging
% Current terminal debugging is on
<Sysname> ping -c 1 5.5.5.2
  PING 5.5.5.2: 56  data bytes, press CTRL_C to break
*0.63272624 Sysname IPV4TUNN/8/debug:Slot=5
 Tunnel3/0/0 packet:Before encapsulation,
        Outer packet header 5.5.5.1->5.5.5.2(length = 84)
*0.2812422 Sysname IPV4-TUN/8/debug:
 Tunnel3/0/0 packet:After encapsulation,
        Outer packet header 192.168.19.41->192.168.19.42(length = 104)
*0.2812468 Sysname IPV4-TUN/8/debug:
 ipv4-tunnel_packet: Decapsulate tunnel packet
        Incoming packet header 192.168.19.42->192.168.19.41(length = 104)
*0.63272624 Sysname IPV4TUNN/8/debug:Slot=5
 Tunnel3/0/0 packet:After decapsulation,
        Outgoing packet header 5.5.5.2->5.5.5.1(length = 84)
    Reply from 5.5.5.2: bytes=56 Sequence=1 ttl=255 time=78 ms

  --- 5.5.5.2 ping statistics ---
    1 packet(s) transmitted
    1 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 78/78/78 ms
```

Table 41 Description on fields of the debugging ipv4-tunnel command

Field	Description
Sysname IPV4-TUN/8/debug	IPv4 tunnel debugging information on the switch

Table 41 Description on fields of the debugging ipv4-tunnel command

Field	Description
Tunnel3/0/0 packet:Before encapsulation, Outer packet header 5.5.5.1->5.5.5.2(length = 84)	On the interface Tunnel 3/0/0, the source address and destination address in the packet header before encapsulation are 5.5.5.1 and 5.5.5.2, and the packet is 84 bytes in length.
Tunnel3/0/0 packet:After encapsulation, Outer packet header 192.168.19.41->192.168.19.42(length = 104)	On the interface Tunnel3/0/0, the source address and destination address in the packet header after encapsulation are 192.168.19.41 and 192.168.19.42, and the packet is 104 bytes in length.
Ipv4-tunnel_packet: Decapsulate tunnel packet Incoming packet header 192.168.19.42->192.168.19.41(length = 104)	The source address and destination address in the packet header of an IPv4 tunnel packet before decapsulation are 192.168.19.42 and 192.168.19.41, and the packet is 104 bytes in length.
Tunnel3/0/0 packet:After decapsulation, Outgoing packet header 5.5.5.2->5.5.5.1(length = 84)	On the interface Tunnel3/0/0, the source address and destination address in the packet header after decapsulation are 5.5.5.2 and 5.5.5.1, and the packet is 84 bytes in length.

debugging ipv6-tunnel

Syntax **debugging ipv6-tunnel** { **all** | **error** | **packet** }

undo debugging ipv6-tunnel { **all** | **error** | **packet** }

View User view

Parameters **all**: Enables all types of debugging for the IPv6 tunnel module.

error: Enables error debugging for the IPv6 tunnel module.

packet: Enables packet debugging for the IPv6 tunnel module.

Description Use the **debugging ipv6-tunnel** command to enable debugging for the IPv6 tunnel module.

Use the **undo debugging ipv6-tunnel** command to disable debugging for the IPv6 tunnel module.

By default, debugging for the IPv6 tunnel is disabled.

Examples # Enable debugging for the IPv6 tunnel module, and conduct the ping operation, and use the **ping** command to view the debugging information.

```
<Sysname> debugging ipv6-tunnel all
<Sysname> terminal debugging
% Current terminal debugging is on
<Sysname> ping ipv6 -c 1 2005::2
  PING 2005::2 : 56  data bytes, press CTRL_C to break
*0.63750414 Sysname IPV6TUNN/8/debug:Slot=5
 Tunnel6/0/0 packet: Before encapsulation,
        Incoming packet header 2005::0001->2005::0002(length = 104)
```

```
*0.3760265 Sysname IPV6-TUN/8/debug:
 Tunnel6/0/0 packet: After encapsulation,
        Outgoing packet header 2003::0001->2003::0002(length = 144)
*0.3760297 Sysname IPV6-TUN/8/debug:
 ipv6-tunnel_event:transproto is ipv6.
*0.3760297 Sysname IPV6-TUN/8/debug:
 ipv6-tunnel_packet: Decapsulate tunnel packet
        Incoming packet header 2003::0002->2003::0001(length = 144)
*0.3760312 Sysname IPV6-TUN/8/debug:
 Tunnel6/0/0 packet: After decapsulation,
        Outgoing packet header 2005::0002->2005::0001(length = 104)
    Reply from 2005::2: Bytes=56 Sequence=1 hop limit=255  time = 78 ms

  --- 2005::2 ping statistics ---
    1 packet(s) transmitted
    1 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 78/78/78 ms
```

Table 42 Field descriptions of the debugging ipv6-tunnel command

Field	Description
Sysname IPV6-TUN/8/debug	IPv6 tunnel debugging information on the switch
Tunnel6/0/0 packet: Before encapsulation, Incoming packet header 2005::0001->2005::0002(length = 104).	On the interface Tunnel6/0/0, the source address and destination address of the encapsulated packet are 2005::0001 and 2005::0002, and the packet is 104 bytes in length.
Tunnel6/0/0 packet: After encapsulation, Outgoing packet header 2003::0001->2003::0002(length = 144)	On the interface Tunnel6/0/0, the source address and destination address of the decapsulated packet are 2003::0001 and 2003::0002, and the packet is 144 bytes in length.
Ipv6-tunnel_packet: Decapsulate tunnel packet Incoming packet header 2003::0002->2003::0001(length = 144).	On the interface Tunnel6/0/0, the source address and destination address of the packet before decapsulation are 2003::0002 and 2003::0001, and the packet is 144 bytes in length.
Tunnel6/0/0 packet: After decapsulation, Outgoing packet header 2005::0002->2005::0001(length = 104)	On the interface Tunnel6/0/0, the source address and destination address of the packet after decapsulation are 2005::0002 and 2005::0001, and the packet is 104 bytes in length.

debugging tunnel (User view)

Syntax **debugging tunnel** { **all** | **error** | **event | packet** }

undo debugging tunnel { **all** | **error** | **event | packet** }

View User view

Parameters **all**: Enables all types of debugging for the tunnel module.

error: Enables error debugging for the tunnel module.

event: Enables event debugging for the tunnel module.

packet: Enables packet debugging for the tunnel module.

Description Use the **debugging tunnel** command to enable debugging for the tunnel module. Use the **undo debugging tunnel** command to disable debugging for the tunnel module.

By default, debugging for the tunnel module is disabled.

Examples # Enable debugging for the tunnel module.

```
<Sysname> debugging tunnel all
<Sysname> terminal debugging
% Current terminal debugging is on
<Sysname>
*0.4445125 Sysname TUNNEL/8/debug:
Tunnel3/0/0 link state is DOWN, no change.
```

// When a tunnel source address is required but has not been configured, the following debugging information will be output.

```
*0.4450125 Sysname TUNNEL/8/debug:
Tunnel3/0/0 down, because the source ip is not set.
```

// When a tunnel destination address is required but has not been configured, the following debugging information will be output.

```
*0.4920140 Sysname TUNNEL/8/debug:
Tunnel3/0/0 down, because the dest address is required.
```

// When the tunnel needs to reference a link aggregation group ID but no link aggregation group has been configured, the following debugging information will be output.

```
*0.9505431 Sysname Switch 8807 TUNNEL/8/debug:
 Tunnel0/0/0 down, because the aggregation group is required.
*0.9505560 Sysname Switch 8807 TUNNEL/8/debug:
Tunnel0/0/0 link state is DOWN, no change.
```

// When the link aggregation group referenced by the tunnel is down, the following debugging information will be output.

```
*0.8565431 Sysname Switch 8807 TUNNEL/8/debug:
 Tunnel0/0/0 down, because the status of aggregation group 1 is down.
*0.8565570 Sysname Switch 8807 TUNNEL/8/debug:
Tunnel0/0/0 link state is DOWN, no change.
```

Table 43 Description on fields of the debugging tunnel command

Field	Description
Sysname TUNNEL/8/debug	Tunnel debugging information on the switch
Tunnel0/0/0 link state is DOWN, no change.	The link of the interface Tunnel0/0/0 is down and the link state is not changed.
Tunnel3/0/0 down, because the source ip is not set.	The interface Tunnel3/0/0 is down because no source address has been configured.
Tunnel3/0/0 down, because the dest address is required.	The interface Tunnel3/0/0 is down because no destination address has been configured.

Table 43 Description on fields of the debugging tunnel command

Field	Description
Tunnel3/0/0 down, because the aggregation group is required.	The interface Tunnel3/0/0 is down because the link aggregation group referenced by the tunnel is not configured. (This option is unavailable unless the link aggregation group ID is required.)
Tunnel0/0/0 down, because the status of aggregation group 1 is down.	The status of the Tunnel3/0/0 is down because the link aggregation group ID referenced by Tunnel is in down status (This check is not available unless the link aggregation group ID is a mandatory parameter).

destination (Tunnel interface view)

Syntax **destination** { *ip-address* | *ipv6-address* }

undo destination

View Tunnel interface view

Parameters *ip-address*: Tunnel destination IPv4 address on the interface.

ip-address: Tunnel destination IPv6 address on the interface.

Description Use the **destination** command to specify the tunnel destination address on the interface.

Use the **undo destination** command to remove the configured tunnel destination address.

By default, no tunnel destination address is configured on the interface.

Note that:

- The tunnel destination address on the interface is the address of the peer interface receiving packets and is usually the tunnel source address on the peer interface.
- Two or more tunnel interfaces using the same encapsulation protocol must have different source and destination addresses.
- At present, the Switch 8800 does not support the configuration of any tunnel destination IPv6 address on the interface.

Related commands: **interface tunnel**, **source**.

Examples # Set the interface VLAN-interface 10 (193.101.1.1) of Sysname 1 and the interface VLAN-interface 20 (192.100.1.1) of Sysname 2 to the source and destination interfaces of a tunnel between the two devices, respectively.

```
<Sysname1> system-view
[Sysname1] interface Tunnel 3/0/1
[Sysname1-Tunnel3/0/1] source 193.101.1.1
```

```
[Sysname1-Tunnel3/0/1] destination 192.100.1.1
[Sysname1-Tunnel3/0/1] return
<Sysname2> system-view
[Sysname2] interface Tunnel 4/0/1
[Sysname2-Tunnel4/0/1] source 192.100.1.1
[Sysname2-Tunnel4/0/1] destination 193.101.1.1
```

display interface tunnel (Any view)

Syntax **display interface tunnel** [*number*]

View Any view

Parameters *number*: Tunnel interface number, in the format of slot number./subslot number/Tunnel interface number. If the *number* argument is not specified, the information of all tunnel interfaces will be displayed.

Description Use the **display interface tunnel** command to display related information of a specified tunnel interface, such as source address, destination address, and encapsulation mode.

Related commands: **interface tunnel**, **source**, **destination**, **tunnel-protocol**.

Examples # Display information of the interface Tunnel 3/0/0.

```
<Sysname> display interface tunnel 3/0/0
Tunnel3/0/0 current state: UP
Line protocol current state: UP
Description: Tunnel3/0/0 Interface
The Maximum Transmit Unit is 64000
Internet Address is 10.1.2.1/24 Primary
Encapsulation is TUNNEL, aggregation ID not set
Tunnel source 192.13.2.1, destination 192.13.2.2
Tunnel protocol/transport GRE/IP
    GRE key disabled
    Checksumming of GRE packets disabled
    Last 300 seconds input:  0 bytes/sec, 0 packets/sec
    Last 300 seconds output:  0 bytes/sec, 0 packets/sec
    361 packets input,  9953388 bytes
    0 input error
    361 packets output,  30324 bytes
    0 output error
```

Description on fields of the **display interface tunnel** command

Field	Description
Tunnel3/0/0 current state: UP	The physical layer of the tunnel interface is reachable
Line protocol current state: UP	The link layer of the tunnel interface is reachable
Description	Descriptive information of a tunnel interface

Field	Description
Tunnel3/0/0 Interface	Tunnel interface number
Maximum Transmit Unit	Maximum transmission unit (MTU) in a tunnel
Encapsulation is TUNNEL	The encapsulation protocol is tunnel
aggregation ID	Link aggregation group ID referenced by a tunnel
Tunnel source	Tunnel source address
destination	Tunnel destination address
Tunnel protocol/transport	Tunnel protocol and transport protocol.
GRE key disabled	No key is configured for the GRE tunnel interface.
Checksumming of GRE packets disabled	Disables the GRE packet checksum function.
Last 300 seconds input	Number of bytes and packets input per second in the last five minutes.
Last 300 seconds output	Number of bytes and packets output per second in the last five minutes.
packets input	Total number of input packets.
input error	Number of error packets among all input packets.
packets output	Total number of output packets.
output error	Number of error packets in all output packets

display ipv6 interface tunnel (Any view)

Syntax **display ipv6 interface tunnel** *number*

View Any view

Parameters *number*: Tunnel interface number, in the format of slot No./subslot No./tunnel interface No.

Description Use the **display ipv6 interface tunnel** command to display related IPv6 information of a specified tunnel interface, including link state, IPv6 protocol state, and IPv6 address.

Examples # Display information of the interface Tunnel 3/0/0.

```
<Sysname> display ipv6 interface tunnel 3/0/0
Tunnel3/0/0 current state :UP
Line protocol current state :UP
IPv6 is enabled, link-local address is FE80::101:101
  Global unicast address(es):
    2002:101:101::1, subnet is 2002::/16
  Joined group address(es):
    FF02::1:FF01:101
    FF02::1:FF00:1
    FF02::2
    FF02::1
  MTU is 1500 bytes
```

```
ND reachable time is 30000 milliseconds
ND retransmit interval is 1000 milliseconds
Hosts use stateless autoconfig for addresses
```

Description on fields of the **display interface tunnel** command

Field	Description
Tunnel3/0/0 current state: UP	The physical layer of the tunnel interface is reachable.
Line protocol current state: UP	The link layer of the tunnel interface is reachable.
IPv6 is enabled	Enables IPv6 on a tunnel interface
link-local address	Link-local address of a tunnel interface
Global unicast address(es)	Aggregatable global unicast address of a tunnel interface.
Joined group address(es)	Multicast address of a tunnel interface.
MTU is 1500 bytes	Size of the MTU in a tunnel. The MTU in this example is 1,500 bytes.
ND reachable time	Neighbor reachable time
ND retransmit interval	Interval for retransmitting a neighbor discovery message.
Hosts use stateless autoconfig for addresses	Hosts use the stateless auto-configuration mode to acquire IPv6 addresses.

expediting enable (Tunnel interface view)

Syntax **expediting enable**

undo expediting enable

View Tunnel interface view

Parameters None

Description Use the **expediting enable** command to enable the expedite termination function.

Use the **expediting enable** command to disable the expedite termination function.

By default, the expedite termination function is disabled.

Examples # Enable the expedite termination function

```
<Sysname> system-view
[Sysname] interface tunnel 2/0/0
[Sysname-Tunnel2/0/0] expediting enable
```

expediting subnet

Syntax **expediting subnet** *ip-address mask*

undo expediting subnet

View Tunnel interface view

Parameters *ip-address*: Address of the expedite termination subnet of a tunnel

mask: Mask of the expedite termination subnet of a tunnel

Description Use the **expediting subnet** command to set an IP address and mask for the expedite termination subnet.

Use the **undo expediting subnet** command to remove the configuration.

By default, no expedite termination subnet is configured for a tunnel.

Note that:

- You must enable the expedite termination before configuring an expedite termination subnet in tunnel interface view.
- The expediting subnet is not applicable to configured tunnels (for example, GRE tunnel and IPv6 manually configured tunnel). After the expedite termination function is enabled, the system will automatically consider the destination address of a tunnel as the address of the expedite termination subnet, and the subnet mask as 255.255.255.255.
- For automatic tunnels (for example, 6to4 tunnel, ISATAP tunnel, and automatic IPv4-compatible IPv6 tunnel), you must carry out the expediting subnet command to designate an IP address and subnet for the expedite termination subnet after carrying out the **expediting enable** command.

*The configuration made by the **expediting enable** command will be invalid after you execute the **undo expediting subnet command**.*

Examples # Configure an expedite termination subnet for a 6to4 tunnel: First enable the expedite termination, and then set the address of the expedite termination subnet to 1.1.1.2 and the subnet mask to 255.255.255.0.

```
<Sysname> system-view
[Sysname] interface tunnel 2/0/0
[Sysname-Tunnel2/0/0] expediting enable
[Sysname-Tunnel2/0/0] expediting subnet 1.1.1.2 255.255.255.0
```

interface tunnel

Syntax **interface tunnel** *number*

undo interface tunnel *number*

View System view

Parameters *number*: Tunnel interface number, in the format of slot No./subslot No./tunnel interface No.

Description Use the **interface tunnel** command to create a tunnel interface and enter tunnel interface view.

Use the **undo interface tunnel** command to remove a specified tunnel interface.

By default, there is no tunnel interface on the device.

- Carry out the **interface tunnel** command to enter interface view of a specified tunnel. If the tunnel interface is not created, you must create it before entering tunnel interface view.
- A tunnel interface number has only local significance, and therefore, the same interface number or different interface numbers can be set at both ends of a tunnel.

Related commands: **display interface tunnel**, **source**, **destination**, **tunnel-protocol**.

Examples # Create the interface Tunnel 3/0/0.

```
<Sysname> system-view
[Sysname] interface tunnel 3/0/0
[Sysname-Tunnel3/0/0]
```

mtu (tunnel interface view)

Syntax **mtu** *mtu-size*

undo mtu

View Tunnel interface view

Parameters *mtu-size*: Tunnel interface MTU in bytes.

Description Use the **mtu** command to configure the tunnel interface MTU.

Use the **undo mtu** command to restore the default tunnel interface MTU.

The default value varies with devices.

Examples # Set the tunnel interface MTU to 10,000 bytes.

```
<Sysname> system-view
[Sysname] interface tunnel 4/0/6
[Sysname-Tunnel4/0/6] mtu 10000
```

source (Tunnel interface view)

Syntax **source** { *ip-address* | *ipv6-address* | *interface-type interface-num* }

undo source

View Tunnel interface view

Parameters *ip-address*: Source IPv4 address of a tunnel interface.

ip-address: Source IPv6 address of a tunnel interface.

interface-type interface-number: Type and number of a tunnel interface.

Description Use the **source** command to specify the tunnel source address on the interface.

Use the **undo source** command to remove the configured tunnel source address.

By default, no tunnel source address is configured on the interface.

Note that:

- The tunnel source address on the interface is the address of the interface sending packets and is usually the destination address of the peer tunnel interface.
- Two or more tunnel interfaces using the same encapsulation protocol must have different source addresses and destination addresses.
- At present, the Switch 8800 does not support the configuration of any tunnel source IPv6 address on the interface.

Related commands: **interface tunnel**, **destination**.

Examples # Set the tunnel source address to 192.100.1.1 on the interface Tunnel 5/0/0.

```
<Sysname> system-view
[Sysname] interface Tunnel 5/0/0
[Sysname-Tunnel5/0/0] source 192.100.1.1
```

tunnel-protocol (Tunnel interface view)

Syntax **tunnel-protocol** { **gre** | **ipv4-ipv4** | **ipv6-ipv4** [**6to4** | **auto-tunnel** | **isatap**] | **mpls te** }

undo tunnel-protocol

View Tunnel interface view

Parameters **gre:** Sets the tunnel to a GRE tunnel.

ipv4-ipv4: Sets the tunnel to an IPv4 over IPv4 tunnel.

ipv6-ipv4: Sets the tunnel to an IPv6 over IPv4 tunnel.

ipv6-ipv4 6to4: Sets the tunnel to IPv6 over IPv4 6to4 tunnel.

ipv6-ipv4 auto-tunnel: Sets the tunnel to an automatic IPv4 compatible IPv6 tunnel.

ipv6-ipv4 isatap: Sets the tunnel to an IPv6 over IPv4 ISATAP tunnel.

mpls te: Sets the tunnel to an MPLS TE tunnel.

Description Use the **tunnel-protocol** command to configure the tunnel type.

Use the **undo tunnel-protocol** to restore the tunnel type to the default.

By default, the tunnel is GRE tunnel.

Note that:

- A proper tunnel type can be selected for packet encapsulation according to the network topology and application. The same tunnel type must be configured at both ends of the tunnel. Otherwise, packet delivery will fail.
- Only one automatic tunnel can be configured at the same tunnel source.

Examples # Specify the tunnel type as IPv4 over IPv4 for a tunnel interface.

```
<Sysname> system-view
[Sysname] interface Tunnel 3/0/0
[Sysname-Tunnel3/0/0] tunnel-protocol ipv4-ipv4
```

11 BPDU TUNNELING CONFIGURATION COMMANDS

bpdu-tunnel dot1q stp

Syntax **bpdu-tunnel dot1q stp**

undo bpdu-tunnel dot1q stp

View Ethernet interface view/port group view

Parameters None

Description Use the **bpdu-tunnel dot1q stp** command to enable STP BPDU tunneling for a port or a group of ports.

Use the **undo bpdu-tunnel dot1q stp** command to disable STP BPDU tunneling for a port or a group of ports.

By default, the STP BPDU tunneling feature is disabled for all ports.

Configured in Ethernet interface view, the setting is effective on the current port only; configured in port group view, the setting is effective on all ports in the port group.

CAUTION: *Before you can enable the STP BPDU tunneling feature on a port, enable the BPDU tunneling feature and disable STP on the port first.*

Relative command: **bpdu-tunnel dot1q enable**.

Examples # Enable STP BPDU tunneling on Ethernet 1/1/1.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1/1
[Sysname-Ethernet1/1/1] stp disable
[Sysname-Ethernet1/1/1] bpdu-tunnel dot1q enable
[Sysname-Ethernet1/1/1] bpdu-tunnel dot1q stp
```

bpdu-tunnel dot1q enable

Syntax **bpdu-tunnel dot1q enable**

undo bpdu-tunnel dot1q enable

View System view/Ethernet interface view/port group view

Parameters None

Description Use the **bpdu-tunnel dot1q enable** command to enable BPDU tunneling.

Use the **undo bpdu-tunnel dot1q enable** command to disable BPDU tunneling.

Configured in system view, the command enables or disables BPDU tunneling globally; configured in Ethernet interface view, the setting is effective on the current port only; configured in interface view, the command enables or disables BPDU tunneling on the current port only; configured in port group view, the command enables or disables BPDU tunneling on all ports in the port group.

By default, BPDU tunneling is enabled globally but disabled for all ports.

- *The configured BPDU tunneling on a port cannot take effect unless BPDU tunneling is enabled globally.*
- *On the Ethernet interface, the BPDU tunneling feature is not compatible with the GVRP function. To enable this feature, you must disable the GVRP feature under the port.*

Examples # Enable BPDU tunneling globally.

```
<Sysname> system-view
[Sysname] bpdu-tunnel dot1q enable
```

Enable BPDU tunneling on the Ethernet 1/1/1 port.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1/1
[Sysname-Ethernet1/1/1] bpdu-tunnel dot1q enable
```

12 VLAN CONFIGURATION COMMANDS

description (VLAN view/VLAN interface view)

Syntax **description** *text*

undo description

View VLAN view/VLAN interface view

Parameters *text*: A string that describes the current VLAN or VLAN interface (Space can be included), case sensitive.

- For VLAN, this is a string of 1 to 32 characters.
- For VLAN interface, this is a string of 1 to 80 characters.

Description Use the **description** command to configure the descriptive string of the current VLAN or VLAN interface.

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

By default, the descriptive string for a VLAN is the VLAN ID, for example, "VLAN 0001"; for a VLAN interface is name of the current VLAN interface, for example, "Vlan-interface1 Interface"

Examples # Assign a descriptive string "RESEARCH" for VLAN 1.

```
<Sysname> system-view
[Sysname] vlan 1
[Sysname-vlan1] description RESEARCH
```

Assign a descriptive string "VLAN-INTERFACE-2" for VLAN-interface 2

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] quit
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] description VLAN-INTERFACE-2
```

display interface vlan-interface

Syntax **display interface vlan-interface** [*vlan-interface-id*]

View Any view

Parameters *vlan-interface-id*: VLAN interface ID.

Description Use the **display interface vlan-interface** command to display the relevant information of a VLAN interface.

If the *vlan-interface-id* argument specified, this command displays information about the specified VLAN interface; If the *vlan-interface-id* argument is not specified, information about all existing VLAN interfaces is displayed.

Related commands: **interface vlan-interface**.

Examples # Display the information of VLAN-interface 2.

```
<Sysname> display interface vlan-interface 2
Vlan-interface2 current state: DOWN
Line protocol current state: DOWN
Description: Vlan-interface2 Interface
The Maximum Transmit Unit is 1500
Internet protocol processing : disabled
IP Packet Frame Type: PKTFMT_ETHNT_2,  Hardware Address: 00e0-fc00-0001
IPv6 Packet Frame Type: PKTFMT_ETHNT_2,  Hardware Address: 00e0-fc00-0001
```

Table 44 Field descriptions of the display interface vlan-interface command

Field	Description
Vlan-interface2 current state	The physical state of a VLAN interface
Line protocol current state	The link state of a VLAN interface
Description	The description of a VLAN interface
The Maximum Transmit Unit	The MTU of a VLAN interface
Internet protocol processing	IP processing ability
IP Packet Frame Type	IPv4 outgoing frame format
Hardware address	MAC address corresponding to a VLAN interface
IPv6 Packet Frame Type	IPv6 outgoing frame format

display vlan

Syntax **display vlan** [*vlan-id1* [**to** *vlan-id2*] | **all** | **dynamic** | **interface** *interface-type interface-number.subnumber* | **reserved** | **static**]

View Any view

Parameters *vlan-id1*: Displays the information of a VLAN specified by VLAN ID.

vlan-id1 **to** *vlan-id2*: Displays the information of a range of VLANs specified by *vlan-id1* and *vlan-id2*. *vlan-id2* is greater than or equal to *vlan-id1*.

all: Displays information about all current VLANs except the reserved VLAN.

static: Displays information about static VLANs.

dynamic: Displays information about dynamic VLANs

reserved: Displays information about the reserved VLANs. Reserved VLANs are VLANs reserved by the device for function implementation. You cannot configure reserved VLANs..

Description Use the **display vlan** command to display VLAN information.

If specified with the *vlan-id* argument or the **all** keyword, this command displays information about the specified VLAN or all VLANs.

If specified with no parameter, this command displays the list of all the existing VLANs of the system.

If specified with the **static** or **dynamic** keyword, this command displays the list of the static or dynamic VLANs.

If specified with the **reserved** keyword, this command displays the information of the reserved VLANs of the system. Presently, Switch 8800s have no reserved VLANs.

Related commands: **vlan**.

Examples # Display VLAN 2 information.

```
<Sysname> display vlan 2
 VLAN ID: 2
 VLAN Type: static
 Route Interface: configured
 IP Address: 1.1.1.1
 Subnet Mask: 255.255.255.0
 Description: VLAN 0003
 Tagged   Ports: none
 Untagged Ports:
    GigabitEthernet4/2/4
```

Table 45 Field descriptions of the display vlan command

Field	Description
VLAN ID	VLAN ID
VLAN Type	VLAN type (static or dynamic)
Route interface	Whether the VLAN interface is configured for the VLAN: not configured or configured
Description	VLAN descriptive string
IP Address	IP address of the VLAN interface (not display if the VLAN interface has no IP address configured)
Subnet Mask	Subnet mask of the IP address (not display if the VLAN interface has no IP address configured)

Table 45 Field descriptions of the display vlan command

Field	Description
Tagged Ports	Tagged ports
Untagged Ports	Untagged ports

interface vlan-interface

Syntax **interface vlan-interface** *vlan-interface-id*

undo interface vlan-interface *vlan-interface-id*

View System view

Parameters *vlan-interface-id*: VLAN interface ID.

Description Use the **interface vlan-interface** command to enter the specified VLAN interface view.

Use the **undo interface vlan-interface** command to delete the specified VLAN interface. The VLAN interface must be created first before entering its view

Before creating a VLAN interface, make sure the corresponding VLAN has been created; otherwise, the VLAN interface cannot be created.

Related commands: **display interface vlan-interface**.

Examples # Create VLAN-interface 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] quit
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2]
```

ip address (VLAN interface view)

Syntax **ip address** *ip-address* { *mask* | *mask-length* } [**sub**]

undo ip address [*ip-address* { *mask* | *mask-length* } [**sub**]]

View VLAN interface view

Parameters *ip-address*: IP address of a VLAN interface, in dotted decimal format.

mask: Subnet mask that corresponds to the IP address of a VLAN interface, in dotted decimal format.

mask-length: Length of a sub-net mask, that is, the number of "1"s in the sub-net mask.

sub: Indicates the address is a sub-IP address of the VLAN interface.

Description Use the **ip address** command to specify the IP address and subnet mask for a VLAN interface.

Use the **undo ip address** command to remove the IP address and sub-net mask for a VLAN interface.

By default, no IP address is configured for a VLAN interface.

An interface normally has one IP address. To enable a switch to connect to multiple subnets, a maximum of 21 IP addresses can be configured on a VLAN interface, among which only one is the primary IP address and all the rest are secondary IP addresses. Their relationship is illustrated as follows:

- A newly configured primary IP address will replace the original one, if there is one.
- You can configure secondary IP addresses only for the interface that has primary IP address configured.
- Use the **undo ip address** command without any parameter to delete all IP addresses of the VLAN interface.
- Use the **undo ip address** *ip-address* { *mask* | *mask-length* } command to delete the primary IP address.
- Use the **undo ip address** *ip-address* { *mask* | *mask-length* } **sub** command to delete a secondary IP address.

Related commands: **display ip interface**.

Examples # Specify the IP address as 129.12.0.1, the sub-net mask as 255.255.255.0 for VLAN-interface 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ip address 129.12.0.1 255.255.255.0
```

shutdown (VLAN interface view)

Syntax **shutdown**

undo shutdown

View VLAN interface view

Parameters None

Description Use the **shutdown** command to shut down a VLAN interface.

Use the **undo shutdown** command to bring up a VLAN interface.

By default, the VLAN interface is down if all ports in the VLAN are down, as long as one port in the VLAN is up, the VLAN interface will be up

You can use the **undo shutdown** command to bring up a VLAN interface after configurations of the related parameter and protocol. When there is a fault in a VLAN interface, you can use the **shutdown** command to shut down the interface and then bring it up using the **undo shutdown** command. In this way, the interface will resume Shutting down/bringing up a VLAN interface does not affect any Ethernet ports in the VLAN. The state of an Ethernet port does not change with the VLAN interface state.

Examples # Shut down the VLAN-interface 2 and then bring it up.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] shutdown
[Sysname-Vlan-interface2] undo shutdown
```

vlan

Syntax **vlan** { *vlan-id1* [**to** *vlan-id2*] | **all** }

undo vlan { *vlan-id1* [**to** *vlan-id2*] | **all** }

View System view

Parameters *vlan-id1*: VLAN ID.

vlan-id2: VLAN ID, and is greater than or equal to *vlan-id1*.

vlan-id1 **to** *vlan-id2*: Specifies a VLAN range.

all: Indicates all VLANs.

Description Use the **vlan** *vlan-id* command to create a VLAN and enter its view. If the specified VLAN already exists, the command brings you to its view directly.

Use the **vlan** *vlan-id1* **to** *vlan-id2* command to create a range of VLANs specified by *vlan-id1* and *vlan-id2*.

Use the **vlan all** command to create all VLANs in a time.

Use the **undo vlan** *vlan-id* command to remove the specified VLAN.

Use the **undo vlan** *vlan-id1* **to** *vlan-id2* command to delete a range of VLANs specified by *vlan-id1* and *vlan-id2*.

Use the **undo vlan all** command to remove all VLANs in a time.

Note that:

- As the default VLAN, VLAN 1 cannot be created, or removed.
- Reserved VLANs are reserved by the system for specific function implementation. You cannot create/remove a reserved VLAN. Presently, the Switch 8800s have no reserved VLANs.
- Dynamic VLANs cannot be removed through the **undo vlan** command.
- A VLAN configured with QoS policies cannot be removed unless the QoS policies are removed.
- If an isolate-user-VLAN or a secondary VLAN is associated with another VLAN using the **isolate-user-vlan** command, the isolate-user-VLAN or secondary VLAN cannot be removed unless the association is removed.
- If a VLAN is configured as a remote mirroring VLAN, it cannot be removed through the **undo vlan** command unless its mirroring VLAN configuration is removed.

Note *When the VLAN removed by the **undo vlan** command is the default VLAN of a port: if the port is an Access port, its default VLAN reverts to VLAN 1; if the port is a Trunk or Hybrid port, its default VLAN keeps unchanged, that is, a Trunk or Hybrid port can use a nonexistent VLAN as its default VLAN.*

Related commands: **display vlan**.

Examples # Enter VLAN 1 view.

```
<Sysname> system-view
[Sysname] vlan 1
```

Create VLAN 4 through VLAN 100.

```
<Sysname> system-view
[Sysname] vlan 4 to 100
Please wait.............. Done.
```

13 PORT-BASED VLAN CONFIGURATION COMMANDS

port

Syntax **port** *interface-list*

undo port *interface-list*

View VLAN interface view

Parameters **interface** *interface-list*: Ethernet interface list, in the format of { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>, where &<1-10> indicates that you can specify up to 10 port or port ranges.

Description Use the **port** command to add one port or a group of ports to a VLAN.

Use the **undo port** command to remove one port or a group of ports from a VLAN.

Note

- *This command is only applicable to Access ports.*
- *All ports are Access ports by default; however, you can change the link type of a port by using the **port link-type** command in Ethernet interface view.*

Related commands: **display vlan**.

Examples # Add the ports from Ethernet 1/1/1 to Ethernet 1/1/3 to VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] port ethernet 1/1/1 to ethernet 1/1/3
```

port access vlan

Syntax **port access vlan** *vlan-id*

undo port access vlan

View Ethernet interface view, port group view

Parameters *vlan-id*: VLAN ID.

Description Use the **port access vlan** command to add the current Access port to a specified VLAN.

Use the **undo port access vlan** command to add the current Access port to the default VLAN.

Executed in Ethernet interface view, the command applies to the current port only, whereas in port group view, the command applies to all ports in the port group.

Ensure that the VLAN specified by the *vlan-id* argument exists.

Examples # Add Ethernet 1/1/1 to VLAN 3.

```
<Sysname> system-view
[Sysname] vlan 3
[Sysname-vlan3] quit
[Sysname] interface Ethernet 1/1/1
[Sysname-Ethernet1/1/1] port access vlan 3
```

port hybrid pvid vlan

Syntax **port hybrid pvid vlan** *vlan-id*

undo port hybrid pvid

View Ethernet interface view, port group view

Parameters *vlan-id*: VLAN ID.

Description Use the **port hybrid pvid vlan** command to configure the default VLAN ID for the Hybrid port.

Use the **undo port hybrid pvid** command to restore the default.

By default, the default VLAN of a Hybrid port is VLAN 1.

Executed in Ethernet interface view, the command applies to the current port only; whereas in port group view, the command applies to all ports in the port group.

The default VLAN ID of local Hybrid port must be consistent with that of the peer; otherwise, packets cannot be forwarded properly.

Related commands: **port link-type**.

Examples # Configure the default VLAN ID for the Hybrid port Ethernet 1/1/1 as 100.

```
<Sysname> system-view
[Sysname] vlan 100
[Sysname-vlan100] quit
[Sysname] interface ethernet 1/1/1
[Sysname-Ethernet1/1/1] port link-type hybrid
[Sysname-Ethernet1/1/1] port hybrid pvid vlan 100
```

port hybrid vlan

Syntax **port hybrid vlan** *vlan-id-list* { **tagged** | **untagged** }

undo port hybrid vlan *vlan-id-list*

View Ethernet interface view, port group view

Parameters *vlan-id-list*: The range of VLANs that the Hybrid ports will be added to, *vlan-id-list* = [*vlan-id1* [**to** *vlan-id2*]]&<1-10>, where &<1-10> indicates that you can specify up to 10 VLANs or VLAN ranges.

tagged: Specifies the port to keep the VLAN tag when sending packets of the specified VLAN (s).

untagged: Specifies the port to strip the VLAN tag when sending packets of the specified VLAN(s).

Description Use the **port hybrid vlan** command to add the current Hybrid port to the specified VLAN(s).

Use the **undo port hybrid vlan** command to remove the current Hybrid port from the specified VLAN(s).

The Hybrid port can allow multiple VLANs to pass. Repetitive execution of the **port hybrid vlan** command will yield a set of VLANs, to which the Hybrid port belongs.

Executed in Ethernet interface view, the command applies to the current port only whereas in port group view, the command applies to all ports in the port group.

Note that the configuration only applies to the existing VLANs among that specified by *vlan-id-list*.

Related commands: **port link-type**.

Examples # Add the Hybrid port Ethernet 1/1/1 to VLAN 2, VLAN 4, and the range of VLANs from VLAN 50 to VLAN 100 (all these VLANs already exist), and keep the VLAN tags of the outgoing packets of all these VLANs.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1/1
[Sysname-Ethernet1/1/1] port link-type hybrid
[Sysname-Ethernet1/1/1] port hybrid vlan 2 4 50 to 100 tagged
```

port link-type

Syntax **port link-type** { **access** | **hybrid** | **trunk** }

undo port link-type

View Ethernet interface view, port group view

Parameters **access**: Configures the link type of a port as Access.

hybrid: Configures the link type of a port as Hybrid.

trunk: Configures the link type of a port as Trunk.

Description Use the **port link-type** command to configure the link type of a port.

Use the **undo port link-type** command to restore the default link type of a port.

By default, the link type of all ports is Access.

Executed in Ethernet interface view, the command applies to the current port only whereas in port group view, the command applies to all ports in the port group.

Note *The Trunk and Hybrid ports cannot be converted to each other directly. You can convert either to the Access port, and then to the other type. For example, convert a Trunk port to an Access port, and then to a Hybrid port.*

Examples # Configure Ethernet 1/1/1(Access port) to be a Trunk port.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1/1
[Sysname-Ethernet1/1/1] port link-type trunk
```

port trunk permit vlan

Syntax **port trunk permit vlan** { *vlan-id-list* | **all** }

undo port trunk permit vlan { *vlan-id-list* | **all** }

View Ethernet interface view, port group view

Parameters *vlan-id-list*: The range of VLANs that the Hybrid ports will be added to, in the format of *vlan-id-list* = [*vlan-id1* [**to** *vlan-id2*]]&<1-10>, where &<1-10> indicates that you can specify up to 10 VLANs or VLAN ranges.

all: Adds the Trunk port to all VLANs.

Description Use the **port trunk permit vlan** command to add the current Trunk port to a specified VLAN, a selection of VLANs, or all VLANs.

Use the **undo port trunk permit vlan** command to remove the current Trunk port from a specified VLAN, a selection of VLANs, or all VLANs.

The Trunk port allows multiple VLANs to pass. Repetitive execution of the **port trunk permit vlan** command will yield a set of VLANs, to which the Trunk port belongs.

Executed in Ethernet interface view, the command applies to the current port only whereas in port group view, the command applies to all ports in the port group.

Related commands: **port link-type**.

Examples # Add the Trunk port Ethernet 1/1/1 to VLAN 2, VLAN 4, and the range of VLANs from VLAN 50 to VLAN 100.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1/1
[Sysname-Ethernet1/1/1] port link-type trunk
[Sysname-Ethernet1/1/1] port trunk permit vlan 2 4 50 to 100
Please wait.......... Done.
```

port trunk pvid vlan

Syntax **port trunk pvid vlan** *vlan-id*

undo port trunk pvid

View Ethernet interface view, port group view

Parameters *vlan-id*: VLAN ID.

Description Use the **port trunk pvid vlan** command to configure the default VLAN ID for the Trunk port.

Use the **undo port trunk pvid** command to restore the default.

By default, the default VLAN of a Trunk port is VLAN 1.

A Trunk port can use a nonexistent VLAN as its default VLAN.

Executed in Ethernet interface view, the command applies to the current port only whereas in port group view, the command apples to all ports in the port group.

You must configure the same default VLAN ID for the Trunk port of both the local device and the peer device. Otherwise, packets cannot be forwarded properly.

Related commands: **port link-type**.

Examples # Configure the default VLAN ID for the Trunk port Ethernet 1/1/1 as 100.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1/1
[Sysname-Ethernet1/1/1] port link-type trunk
[Sysname-Ethernet1/1/1] port trunk pvid vlan 100
```

14 PROTOCOL-BASED VLAN CONFIGURATION COMMANDS

display protocol-vlan interface

Syntax **display protocol-vlan interface** { *interface-listtype interface-number1* [**to** *interface-type interface-number2*] | **all** }

View Any view

Parameters *interface-type interface-number1*: Interface type and interface number.

interface-type interface-number1 **to** *interface-type interface-number2:* Specifies an interface range. The *interface-number* after **to** is greater than or equal to that before **to**.

all: Displays protocol information and protocol indexes of all ports.

Description Use the **display protocol-vlan interface** command to display protocol based VLAN information on the specified port(s).

Examples # Display protocol-based VLAN information on Ethernet 1/1/1.

```
[Sysname] display protocol-vlan interface ethernet 1/1/1
 Interface: Ethernet1/1/1
   VLAN ID   Protocol Index      Protocol Type
 ============================================================
       2           0                ipv4
       2           3                at
```

Table 46 Field descriptions of the display protocol-vlan interface command

Field	Description
Interface: Ethernet1/1/1	Interface type and number
VLAN ID	VLAN ID
Protocol Index	Protocol index value
Protocol Type	Protocol type

display protocol-vlan vlan

Syntax **display protocol-vlan vlan** { *vlan-id* [**to** *vlan-id*] | **all** }

View Any view

Parameters *vlan-id*: VLAN ID.

to: Specifies VLAN range, the value after this parameter must be greater than or equal to that before it.

all: All VLANs.

Description Use the **display protocol-vlan vlan** command to display the protocol information and protocol index configured on the specified VLAN(s).

Related commands: **display vlan**.

Examples # Display the protocol information and protocol index configured on VLAN 10 through VLAN 20.

```
<Sysname> display protocol-vlan vlan 10 to 20
 VLAN ID:15
    Protocol Index      Protocol Type
 ================================================
          0              ipv4
 VLAN ID:20
    Protocol Index      Protocol Type
 ================================================
          0              at
          1              ipv6
```

Refer to Table 46 for description of the output.

port hybrid protocol-vlan vlan

Syntax **port hybrid protocol-vlan vlan** *vlan-id* { *protocol-index* [**to** *protocol-end*] | **all** }

undo port hybrid protocol-vlan vlan *vlan-id* { *protocol-index* [**to** *protocol-end*] | **all** }

View Ethernet interface view, port group view

Parameters *vlan-id*: VLAN ID.

protocol-index: Initial value of the protocol index, must be smaller than the last value of the protocol index, automatically numbered according to the order in which protocols are associated with VLANs if not manually specified. You can use the **display protocol-vlan vlan all** command to display the protocol index. The value range varies with device models.

protocol-end: The last value of the protocol index, must be greater than or equal to the initial value of the protocol index.

all: All protocols.

Description Use the **port hybrid protocol-vlan vlan** command to associate a port with a protocol-based VLAN.

Use the **undo port hybrid protocol-vlan vlan** command to remove the association between the port and the protocol-based VLAN.

Executed in Ethernet interface view, the command applies the configuration to the current port only whereas in port group view, the command applies the configuration to all ports in the port group.

Note that only Hybrid ports support the above feature. Before issuing this command, ensure that the Hybrid port has been added to the VLAN to be associated with and that the VLAN has been assigned with a protocol.

Related commands: **display protocol-vlan interface**.

Examples # Associate Hybrid port Ethernet 1/1/1 with protocol 0 in the protocol-based VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-Vlan2] protocol-vlan at
[Sysname] interface ethernet 1/1/1
[Sysname-Ethernet1/1/1] port link-type hybrid
[Sysname-Ethernet1/1/1] port hybrid vlan 2 tagged
[Sysname-Ethernet1/1/1] port hybrid protocol-vlan vlan 2 0
```

protocol-vlan

Syntax **protocol-vlan** [*protocol-index*] { **at** | **ipv4 | ipv6** | **ipx** { **ethernetii** | **llc** | **raw** | **snap** } | **mode** { **ethernetii etype** *etype-id* | **llc** { **dsap** *dsap-id* [**ssap** *ssap-id*] | **ssap** *ssap-id* } | **snap etype** *etype-id* } }

undo protocol-vlan { *protocol-index* [**to** *protocol-end*] | **all** }

View VLAN view

Parameters **at**: Specifies the AppleTalk based VLAN.

ipv4: Specifies the IPv4 based VLAN.

ipv6: Specifies the IPv6 based VLAN.

ipx: Specifies the IPX based VLAN. The keywords **ethernetii**, **llc**, **raw**, and **snap** are four encapsulation formats of IPX, and default is **ethernetii**.

mode: Configures self-defined protocol template for the VLAN, which has four encapsulation formats: **ethernetii**, **llc**, **raw**, and **snap**.

ethernetii: Specifies the encapsulation format for Ethernet packets as **ethernetii**.

etype-id: Ethernet type of inbound packets, in the range of 0x0600 to 0xFFFF except 0x0800, 0x809B, 0x8137, and 0x86DD.

llc: Specifies the encapsulation format for Ethernet packets to be **llc**.

dsap-id: Destination service access point.

ssap-id: Source service access point.

CAUTION:

- *You cannot configure both dsap-id and ssap-id as 0xE0 or 0xFF; otherwise the matching packets will take the same encapsulation format as that of the **ipx llc** packets and the **ipx raw** packets respectively. If either dsap-id or ssap-id is configured, the system sets the other to 0xAA by default.*
- *When you use the **mode** keyword to configure a user-defined protocol template, do not set the etype-id argument for **ethernetii** packets to 0x0800, 0x809B, 0x8137, or 0x86DD; otherwise, the matching packets will take the same format as that of the IPv4, IPX, AppleTalk and IPv6 packets respectively.*

snap: Specifies the encapsulation format for Ethernet packets as **snap**.

etype-id: Ethernet type of inbound packets, cannot be **ipx snap** under the **snap** encapsulation format.

protocol-index: The initial value of the protocol index. System will automatically assign an index if this parameter is not specified.

protocol-end: The last value of the protocol index, must be greater than or equal to the initial value of the protocol index.

all: All protocol indexes.

Description Use the **protocol-vlan** command to configure the VLAN as a protocol based VLAN and the protocol template.

Use the **undo protocol-vlan** command to remove the configured protocol template.

Related commands: **display protocol-vlan vlan**.

CAUTION: *Due to the close relationship between IPv4 and ARP (the protocol index of ARP is 0x0806), it is recommended to bind the two protocols to the same VLAN and associate them to the same port to avoid that ARP packets and IP packets are not assigned to the same VLAN, which will cause abnormal communication.*

Examples # Specify VLAN 2 as the protocol-based VLAN to transmit IPv4 packets.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] protocol-vlan ipv4
```

15 SUPER VLAN CONFIGURATION COMMANDS

display supervlan

Syntax **display supervlan** [*supervlan-id*]

View Any view

Parameters *supervlan-id*: Super VLAN ID.

Description Use the **display supervlan** command to display the mapping between the specified super VLAN and the sub-VLANs, and their related information.

Related commands: **supervlan**, **subvlan**.

Examples # Display the mapping between a super VLAN and its sub-VLANs.

```
<Sysname> display supervlan 25
SuperVLAN ID :  25
 SubVLAN ID :  26-30

 VLAN ID: 25
 VLAN Type: static
 It is a Super VLAN.
 Route Interface: configured
 IP Address: 10.1.1.1
 Subnet Mask: 255.255.255.0
 Description: VLAN 0025
 Tagged   Ports: none
 Untagged Ports: none

 VLAN ID: 26
 VLAN Type: static
 It is a Sub VLAN.
 Route Interface: configured
 IP Address: 10.1.1.1
 Subnet Mask: 255.255.255.0
 Description: VLAN 0026
 Tagged   Ports: none
 Untagged Ports: none

 VLAN ID: 27
 VLAN Type: static
 It is a Sub VLAN.
 Route Interface: configured
 IP Address: 10.1.1.1
```

```
Subnet Mask: 255.255.255.0
Description: VLAN 0027
Tagged   Ports: none
Untagged Ports: none

VLAN ID: 28
VLAN Type: static
It is a Sub VLAN.
Route Interface: configured
IP Address: 10.1.1.1
Subnet Mask: 255.255.255.0
Description: VLAN 0028
Tagged   Ports: none
Untagged Ports: none

VLAN ID: 29
VLAN Type: static
It is a Sub VLAN.
Route Interface: configured
IP Address: 10.1.1.1
Subnet Mask: 255.255.255.0
Description: VLAN 0029
Tagged   Ports: none
Untagged Ports: none

VLAN ID: 30
VLAN Type: static
It is a Sub VLAN.
Route Interface: configured
IP Address: 10.1.1.1
Subnet Mask: 255.255.255.0
Description: VLAN 0030
Tagged   Ports: none
Untagged Ports: none
```

Table 47 Field descriptions of the display supervlan command

Field	Description
Route Interface	Whether VLAN interface is configured or not.
Tagged Ports	Ports through which packets are sent with VLAN tag kept.
Untagged Ports	Ports through which packets are sent with VLAN tag stripped.

subvlan

Syntax **subvlan** *vlan-list*

undo subvlan [*vlan-list*]

View VLAN view

Parameters *vlan-list*: Sub-VLAN list, in the format of *vlan-list* = { *vlan-id* [**to** *vlan-id2* }*&<1-10>*, in which *vlan-id* represents the sub-VLAN ID. *&<1-10>* indicates you can specify up to 10 sub-VLANs or sub-VLAN lists.

Description Use the **subvlan** command to establish the mapping between a super VLAN and the sub-VLAN (s).

The current VLAN is the super VLAN whereas the VLANs specified by the *vlan-list* aregument are the sub-VLANs.

Use the **undo subvlan** command to remove the mapping between a super VLAN and the sub-VLAN (s).

Note

- Ensure that a sub-VLAN already exists before mapping it onto a super VLAN.
- It is still possible to add /delete a port to/from a sub-VLAN after establishing a mapping between it and a super VLAN.
- Execution of the **undo subvlan** command without the *vlan-list* parameter will delete the mapping between the specified super VLAN and all sub-VLANs, while execution of the command with the parameter will only delete the mapping between the current super VLAN and the parameter specified sub-VLANs.

Related commands: **display supervlan**.

Examples # Establish a mapping between VLAN 10 (as a super VLAN) and VLAN 3, VLAN 4, VLAN 5, and VLAN 9 (all as sub-VLANs).

```
<Sysname> system-view
[Sysname] vlan 10
[Sysname-vlan10] subvlan 3 to 5 9
```

supervlan

Syntax **supervlan**

undo supervlan

View VLAN view

Parameters None

Description Use the **supervlan** command to configure the current VLAN as a super VLAN.

Use the **undo supervlan** command to remove the super VLAN configuration for the current VLAN.

Note that after a VLAN is specified as a super VLAN, it cannot be specified as a guest VLAN for a port any more, and vice versa. For more information about guest VLAN, refer to "802.1x Configuration Commands" page 1143.

CAUTION: *If a port is already added to a VLAN, the VLAN cannot be configured as a super VLAN.*

Related commands: **display supervlan**.

Examples # Configure VLAN 2 as a super VLAN.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] supervlan
```

16 ISOLATE-USER-VLAN CONFIGURATION COMMANDS

display isolate-user-vlan

Syntax **display isolate-user-vlan** [*isolate-user-vlan-id*]

View Any view

Parameters *isolate-user-vlan-id*: VLAN ID of an isolate-user-VLAN.

Description Use the **display isolate-user-vlan** command to display the mapping between an isolate-user-VLAN and the secondary VLAN(s).

Related commands: **isolate-user-vlan**, **isolate-user-vlan enable**.

Examples # Display the mapping between an isolate-user-VLAN and secondary VLANs.

```
<Sysname> display isolate-user-vlan
 Isolate-user-VLAN VLAN ID : 25
 Secondary VLAN ID : 26-27

 VLAN ID: 25
 VLAN Type: static
 Isolate-user-VLAN type : isolate-user-VLAN
 Route Interface: configured
IP Address: 10.0.0.1
 Subnet Mask: 255.255.255.0
 Description: VLAN 0025
 Tagged   Ports: none
 Untagged Ports:
    GigabitEthernet4/3/1     GigabitEthernet4/3/2     GigabitEthernet4/3/3
 VLAN ID: 26
 VLAN Type: static
 Isolate-user-VLAN type: secondary
 Route Interface: not configured
 Description: VLAN 0026
 Tagged   Ports: none
 Untagged Ports:
    GigabitEthernet4/3/1     GigabitEthernet4/3/2
 VLAN ID: 27
 VLAN Type: static
 Isolate-user-VLAN type: secondary
 Route Interface: not configured
 Description: VLAN 0027
 Tagged   Ports: none
 Untagged Ports:
    GigabitEthernet4/3/1     GigabitEthernet4/3/3
```

Table 48 Field descriptions of the display isolate-user-vlan command

Field	Description
Route Interface	Whether VLAN interface is configured or not.
Tagged Ports	Ports through which packets are sent with VLAN tag kept.
Untagged Ports	Ports through which packets are sent with VLAN tag stripped.

isolate-user-vlan

Syntax **isolate-user-vlan** *isolate-user-vlan-id* **secondary** *secondary-vlan-id* [**to** *secondary-vlan-id*]

undo isolate-user-vlan *isolate-user-vlan-id* [**secondary** *secondary-vlan-id* [**to** *secondary-vlan-id*]

View System view

Parameters *isolate-user-vlan-id*: VLAN ID of an isolate-user-VLAN.

secondary-vlan-id: VLAN ID of a secondary VLAN.

Description Use the **isolate-user-vlan** command to create the mapping between an isolate-user-vlan and the secondary VLAN(s).

Use the **undo isolate-user-vlan** command to delete the mapping between an isolate-user-vlan and the secondary VLANs.

By default, there is no mapping between the isolate-user-vlan and the secondary VLANs.

Note that:

- To use the **isolate-user-vlan** command, the isolate-user-VLAN and the secondary VLAN(s) must exist, and the VLAN specified by *isolate-user-vlan-id* is already configured as the isolate-user-VLAN.
- To use the **isolate-user-vlan** command, the secondary VLAN(s) must have at least one port (non Trunk port). The default VLAN of the port must be the secondary VLAN. Otherwise, the command can not be used. After the execution of the command, this kind of ports in the secondary VLAN(s) all change to Hybrid ports and the VLANs allowed on the ports change (it equals to execute the **port hybrid vlan** *isolate-user-vlan-id* **untagged** command on the ports). In this case, if you execute the **undo isolate-user-vlan** command, the port type does not change, but the VLANs allowed on the ports change (it equals to execute the **undo port hybrid vlan** *isolate-user-vlan-id* command on the ports automatically).
- To use the **isolate-user-vlan** command, the isolate-user-VLAN must have at least one port (non Trunk port). The default VLAN of the port must be the isolate-user-VLAN. Otherwise, the command can not be used. After the

execution of the command, this kind of ports all change to Hybrid ports and the VLANs allowed on the ports change (it equals to execute the **port hybrid vlan** *secondary-vlan-id* **untagged** command on the ports). In this case, if you execute the **undo isolate-user-vlan** command, the port type does not change, but the VLANs allowed on the ports change (it equals to execute the **undo port hybrid vlan** *secondary-vlan-id* command on the ports automatically).

- Executed without the **secondary** *secondary-vlan-id* parameter, the **undo isolate-user-vlan** command deletes the mapping between the specified isolate-user-VLAN and all secondary VLANs, while with the parameter specified, the commands deletes the mapping between the specified isolate-user-VLAN and the specified secondary VLANs.

Note *After the mapping between the isolate-user-VLAN and the secondary VLANs is created, no port can be added to or removed from the isolate-user-VLAN or the secondary VLAN(s), and the isolate-user-VLAN or the secondary VLAN(s) cannot be removed. Only after the mapping is deleted are the above operations possible.*

Related commands: **display isolate-user-vlan**.

Examples # Associate the isolate-user-VLAN 2 to the secondary VLANs VLAN 2 through VLAN 5.

```
<Sysname> system-view
[Sysname] isolate-user-vlan 10 secondary 2 to 5
```

isolate-user-vlan enable

Syntax **isolate-user-vlan enable**

undo isolate-user-vlan enable

View VLAN view

Parameters None

Description Use the **isolate-user-vlan enable** command to configure the current VLAN as an isolate-user-VLAN.

Use the **isolate-user-vlan enable** command to remove the isolate-user-VLAN configuration for a specified VLAN.

By default, no VLAN is an isolate-user-VLAN.

An isolate-user-VLAN may include multiple ports, including those that are connected to upstream devices.

Note *To create an isolate-user-VLAN, you need to disable the GVRP function of the switch first; otherwise, the isolate-user-VLAN cannot be created, and vice versa.*

Related commands: **display isolate-user-vlan**.

Examples # Configure VLAN 5 to be an isolate-user-VLAN.

```
<Sysname> system-view
[Sysname] vlan 5
[Sysname-vlan5] isolate-user-vlan enable
```

17 PORT ISOLATION COMMANDS

display port-isolate group

Syntax **display port-isolate group** [*group-number*]

View Any view

Parameters *group-number*: Specifies an isolation group number.

Description Use the **display port-isolate group** command to display an isolation group and information about it.

- If no isolation group number is specified, this command displays information of all the isolation groups of the device.
- If an isolation group number is specified, this command displays information of the specified isolation group.

Examples # On a switch, display information of Isolation Group 2.

```
<Sysname> display port-isolate group 2
 Port-isolate group information:
 Uplink port support: YES
 Group ID: 2
 Uplink port: GigabitEthernet4/3/2
    GigabitEthernet4/3/1
```

port-isolate enable

Syntax **port-isolate enable group** *group-number*

undo port-isolate enable

View Ethernet interface view or interface group view

Parameters **group** *group-number*: Specifies the isolation group number to add ports.

Description Use the **port-isolate enable** command to add a port to the isolation group as ordinary port only.

Use the **undo port-isolate enable** command to remove the port from the isolation group.

Before adding a port to an isolation group, it is necessary to create the isolation group first.

Configured in Ethernet interface view, the setting is effective on the current port only; configured in port group view, the setting is effective on all ports in the port group.

*For the same port, only one of the **port-isolate enable** command and the **port-isolate uplink-port** command is available, that is, a port cannot be configured as an ordinary port and an uplink port at the same time in the isolation group.*

Examples # On a switch, add port Ethernet 1/1/1 to the Isolation Group 2.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1/1
[Sysname-Ethernet1/1/1] port-isolate enable group 2
```

port-isolate group

Syntax **port-isolate group** *group-number*

undo port-isolate group { *group-number* **| all** }

View System view

Parameters *group-number*: Specifies an isolation group number.

all: All isolation groups.

Description Use the **port-isolate group** command to create an isolation group.

Use the **undo port isolate** command to remove an isolation group and its configuration.

In the **undo port-isolate group** command:

- If a number is specified, remove the specified isolation group and its configuration.
- If **all** is used, remove all the isolation groups and their configuration.

Examples # Create Isolation Group 2 on a switch.

```
<Sysname> system-view
[Sysname] port-isolate group 2
```

port-isolate uplink-port

Syntax **port-isolate uplink-port group** *group-number*

undo port-isolate uplink-port

View Ethernet interface view

Parameters *group-number*: Specifies an isolation group number.

Description Use the **port-isolate uplink-port** command to configure the specified port as the uplink port of the isolation group.

Use the **undo port-isolate uplink-port** command to remove the uplink port of the isolation group.

CAUTION:

- *This command is used to configure the uplink port of the specified isolation group, which must be created beforehand.*
- *For the same port, only one of the **port-isolate enable** command and the **port-isolate uplink-port** command is available, that is, a port cannot be configured as an ordinary port and an uplink port at the same time in the isolation group.*

Examples # On a switch, configure Ethernet1/1/1 as the uplink port of the isolation group.

```
<Sysname> system-view
[Sysname] interface Ethernet 1/1/1
[Sysname-Ethernet1/1/1] port-isolate uplink-port group 2
```

18 QinQ Configuration Commands

qinq enable

Syntax **qinq enable**

undo qinq enable

View Ethernet interface view, port group view

Parameters None

Description Use the **qinq enable** command to enable the basic QinQ function.

Use the **undo qinq enable** command to disable the basic QinQ function.

By default, the basic QinQ function is disabled.

With the basic QinQ function enabled on a port, the port tags each received frame with the VLAN tag of the default VLAN of the port.

When executed in Ethernet interface view, these two commands apply to the current port; when executed in port group view, these two commands apply to all the ports in the port group.

CAUTION: *As basic QinQ function affects layer-3 packet forwarding and MPLS switching, do not enable layer-3 packet forwarding or MPLS switching on ports with basic QinQ function enabled.*

Examples # Enable basic QinQ function on Ethernet 1/1/1.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1/1
[Sysname-Ethernet1/1/1] qinq enable
```

qing ethernet-type

Syntax **qinq ethernet-type** *hex-value*

undo qinq ethernet-type

View Ethernet interface view, port group view

Parameters *hex-value*: QinQ tag protocol identifier (TPID) to be set, a hexadecimal number, Note that this argument cannot be set to any of the values listed in Table 49.

Table 49 Commonly used TPIDs

Protocol type	Value
ARP	0x0806
PUP	0x0200
RARP	0x8035
IP	0x0800
IPv6	0x86DD
PPPoE	0x8863/0x8864
IPX/SPX	0x8137
LACP	0x8809
802.1x	0x888E
Cluster	0x88A7
Reserved	0xFFFD/0xFFFE/0xFFFF

Description Use the **qing ethernet-type** command to set the TPID.

Use the **undo ethernet-type** command to restore the TPID to the default value.

By default, the TPID is 0x8100.

Note that:

- A module supports only one TPID except the default TPID.
- When executed in Ethernet interface view, these two commands apply to the current port; when executed in port group view, these two commands apply to all the ports in the port group.
- If you execute the **qinq ethernet-type** command repeatedly, the latest TPID set takes effect.

Examples # Set the TPID to 0x9100 on Ethernet 1/1/1.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1/1
[Sysname-Ethernet1/1/1] qinq ethernet-type 9100
```

19 IP ROUTING TABLE DISPLAY COMMANDS

display ip routing-table

Syntax **display ip routing-table** [**vpn-instance** *vpn-instance-name*] [**verbose** | **|** { **begin** | **exclude** | **include** } *regular-expression*]

View Any view

Parameters **vpn-instance** *vpn-instance-name*: Displays routing table information for a VPN instance. The *vpn-instance-name* argument represents the instance name.

verbose: Displays detailed routing table information, including that for inactive routes. With this argument absent, the command displays only summary information about active routes.

|: Uses a regular expression to filter output information.

begin: Displays routing table entries starting from the one specified by the regular expression.

include: Displays routing table entries specified by the regular expression.

exclude: Displays routing table entries other than those specified by the regular expression.

regular-expression: Regular expression.

Table 50 Special characters for regular expressions

Character	Meaning	Remarks
_	Underscore, functions similarly as a wildcard and matches one of the following: (^|$|[,(){}]) or a space, the beginning of a string, the end of a string.	If it is not the first character in a regular expression, it can appear as many times as the command line length permits. If it is the first character in a regular expression, it can be followed with up to four underscores. If it appears intermittently in a regular expression, only the first group takes effect.
(	Left parenthesis, represents a stack push operation in a program.	It is not recommended to use this character in a regular expression.

Table 50 Special characters for regular expressions

Character	Meaning	Remarks
.	Full stop, a wildcard that matches any character, including a space.	-
*	Asterisk, indicates that the character(s) to its left can appear 0 or more times.	zo* matches z and zoo.
+	Plus, indicates that the character(s) to its left can appear one or more times.	zo+ matches zo and zoo, but not z.

Description

Use the **display ip routing-table** command to display brief information about active routes in the routing table.

Use the **display ip routing-table verbose** command to display detailed information about all routes in the routing table.

Examples

Display brief information about active routes in the routing table.

```
<Sysname> display ip routing-table
Routing Tables: Public
         Destinations : 6        Routes : 6

Destination/Mask    Proto  Pre  Cost         NextHop         Interface

2.2.2.0/24          Direct 0    0            2.2.2.1         vlan12
2.2.2.1/32          Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
192.168.80.0/24     Direct 0    0            192.168.80.10   vlan12
192.168.80.10/32    Direct 0    0            127.0.0.1       InLoop0
```

Table 51 Field descriptions of the display ip routing-table command

Field	Description
Destinations	Number of destination addresses
Routes	Number of routes
Destination/Mask	Destination address/mask length
Proto	Protocol that presents the route
Pre	Priority of the route
Cost	Cost of the route
NextHop	Address of the next hop on the route
Interface	Outbound interface for packets to be forwarded along the route

Display detailed information about all routes in the routing table.

```
<Sysname> display ip routing-table verbose
Routing Table : Public
         Destinations : 5        Routes : 5

  Destination: 10.1.1.0/24
     Protocol: Direct          Process ID: 0
   Preference: 0                     Cost: 0
      NextHop: 10.1.1.1         Interface: vlan-interface12
```

```
RelyNextHop: 0.0.0.0          Neighbour: 0.0.0.0
  Tunnel ID: 0x0                  Label: NULL
      State: Active Adv             Age: 00h00m30s
        Tag: 0

Destination: 10.1.1.1/32
   Protocol: Direct          Process ID: 0
 Preference: 0                     Cost: 0
    NextHop: 127.0.0.1        Interface: InLoopBack0
RelyNextHop: 0.0.0.0          Neighbour: 0.0.0.0
  Tunnel ID: 0x0                  Label: NULL
      State: Active NoAdv           Age: 00h00m30s
        Tag: 0

Destination: 10.1.1.2/32
   Protocol: Direct          Process ID: 0
 Preference: 0                     Cost: 0
    NextHop: 10.1.1.2         Interface: vlan-interface16
RelyNextHop: 0.0.0.0          Neighbour: 0.0.0.0
  Tunnel ID: 0x0                  Label: NULL
      State: Active Adv             Age: 00h00m30s
        Tag: 0

Destination: 127.0.0.0/8
   Protocol: Direct          Process ID: 0
 Preference: 0                     Cost: 0
    NextHop: 127.0.0.1        Interface: InLoopBack0
RelyNextHop: 0.0.0.0          Neighbour: 0.0.0.0
  Tunnel ID: 0x0                  Label: NULL
      State: Active NoAdv           Age: 00h00m36s
        Tag: 0

Destination: 127.0.0.1/32
   Protocol: Direct          Process ID: 0
 Preference: 0                     Cost: 0
    NextHop: 127.0.0.1        Interface: InLoopBack0
RelyNextHop: 0.0.0.0          Neighbour: 0.0.0.0
  Tunnel ID: 0x0                  Label: NULL
      State: Active NoAdv           Age: 00h00m36s
        Tag: 0
```

Displayed first are statistics for the whole routing table, followed by detailed description of each route (in sequence).

Table 52 Field descriptions of the display ip routing-table verbose command

Field	Description
Destination	Destination address/mask length
Protocol	Protocol that presents the route
Process ID	Process ID
Preference	Priority of the route
Cost	Cost of the route
NextHop	Address of the next hop on the route
Interface	Outbound interface for packets to be forwarded along the route

Table 52 Field descriptions of the display ip routing-table verbose command

Field	Description
RelyNextHop	The next hop address obtained through routing stack.
Neighbour	Neighboring address determined by Routing Protocol
Tunnel ID	Tunnel ID
Label	Label
State	Status of the route, which could be Active, Inactive, Adv, or NoAdv.
Age	Time that the route has been in the routing table, in the sequence of hour, minute, and second from left to right.
Tag	Route tag

display ip routing-table acl

Syntax **display ip routing-table acl** *acl-number* [**verbose**]

View Any view

Parameters *acl-number*: Basic ACL number.

verbose: Displays detailed routing table information, including that for inactive routes. With this argument absent, the command displays only brief information about active routes.

Description Use the **display ip routing-table acl** command to display information about routes permitted by a specified basic ACL.

This command is intended for the follow-up display of routing policies.

For more information about routing policy, refer to "Routing Policy Configuration Commands" page 351.

If the specified ACL does not exit or it has no rules configured, the entire routing table is displayed.

Examples # Define basic ACL 2000 and set the route filtering rules.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 10.1.0.0 0.0.255.255
[Sysname-acl-basic-2000] rule deny source any
```

Display brief information about active routes permitted by basic ACL 2000.

```
[Sysname-acl-basic-2000] display ip routing-table acl 2000
Routes Matched by Access list : 2000
Summary Count : 6
```

```
Destination/Mask    Proto   Pre  Cost         NextHop         Interface

10.1.1.0/24         Direct 0    0            10.1.1.2        Vlan1
10.1.1.2/32         Direct 0    0            127.0.0.1       InLoop0
10.1.2.0/24         Direct 0    0            10.1.2.1        Vlan12
10.1.2.1/32         Direct 0    0            127.0.0.1       InLoop0
10.1.3.0/24         Direct 0    0            10.1.3.1        Vlan14
10.1.3.1/32         Direct 0    0            127.0.0.1       InLoop0
```

For detailed description of the above output, see Table 51.

Display detailed information about both active and inactive routes permitted by basic ACL 2000.

```
<Sysname> display ip routing-table acl 2000 verbose
Routes Matched by Access list : 2000
Summary Count: 4

Destination: 10.1.1.0/24
     Protocol: Direct          Process ID: 0
   Preference: 0                     Cost: 0
      NextHop: 10.1.1.2         Interface: Vlan1
  RelyNextHop: 0.0.0.0          Neighbour: 0.0.0.0
    Tunnel ID: 0x0                  Label: NULL
        State: Active Adv             Age: 00h25m32s
          Tag: 0

Destination: 10.1.1.2/32
     Protocol: Direct          Process ID: 0
   Preference: 0                     Cost: 0
      NextHop: 127.0.0.1        Interface: InLoop0
  RelyNextHop: 0.0.0.0          Neighbour: 0.0.0.0
    Tunnel ID: 0x0                  Label: NULL
        State: Active NoAdv           Age: 00h41m34s
          Tag: 0

Destination: 10.1.2.0/24
     Protocol: Direct          Process ID: 0
   Preference: 0                     Cost: 0
      NextHop: 10.1.2.1         Interface: Vlan2
  RelyNextHop: 0.0.0.0          Neighbour: 0.0.0.0
    Tunnel ID: 0x0                  Label: NULL
        State: Active Adv             Age: 00h05m42s
          Tag: 0

Destination: 10.1.2.1/32
     Protocol: Direct          Process ID: 0
   Preference: 0                     Cost: 0
      NextHop: 127.0.0.1        Interface: InLoop0
  RelyNextHop: 0.0.0.0          Neighbour: 0.0.0.0
    Tunnel ID: 0x0                  Label: NULL
        State: Active NoAdv           Age: 00h05m42s
          Tag: 0

Destination: 10.1.3.0/24
     Protocol: Direct          Process ID: 0
   Preference: 0                     Cost: 0
```

```
      NextHop: 10.1.3.1          Interface: Vlan4
  RelyNextHop: 0.0.0.0           Neighbour: 0.0.0.0
    Tunnel ID: 0x0                   Label: NULL
        State: Active Adv              Age: 00h05m31s
          Tag: 0

Destination: 10.1.3.1/32
     Protocol: Direct           Process ID: 0
   Preference: 0                      Cost: 0
      NextHop: 127.0.0.1         Interface: InLoop0
  RelyNextHop: 0.0.0.0           Neighbour: 0.0.0.0
    Tunnel ID: 0x0                   Label: NULL
        State: Active NoAdv            Age: 00h05m32s
          Tag: 0
```

For detailed description of the above output, see Table 52.

display ip routing-table ip-address

Syntax **display ip routing-table** *ip-address* [*mask-length* | *mask*] [**longer-match**] [**verbose**]

display ip routing-table *ip-address1* { *mask-length* | *mask* } *ip-address2* { *mask-length* | *mask* } [**verbose**]

View Any view

Parameters *ip-address*: Destination IP address, in dotted decimal format.

mask-length: IP address mask length.

mask: IP address mask in dotted decimal format.

longer-match: Displays the matched route with the longest mask.

verbose: Displays detailed routing table information, including that for inactive routes. With this argument absent, the command displays only summary information about active routes.

Description Use the **display ip routing-table** *ip-address* command to display information about routes to a specified destination address.

Executing the command with different parameters yields different output:

- **display ip routing-table** *ip-address*

The system ANDs the input destination IP address with the subnet mask in each route entry; and ANDs the destination IP address in each route entry with its corresponding subnet mask.

If the two operations yield the same result for an entry and this entry is active, it is displayed.

- **display ip routing-table** *ip-address mask*

The system ANDs the input destination IP address with the input subnet mask; and ANDs the destination IP address in each route entry with the input subnet mask.

If the two operations yield the same result for an entry and the entry is active with a subnet mask less than or equal to the input subnet mask, the entry is displayed.

Only route entries that exactly match the input destination address and mask are displayed.

- **display ip routing-table** *ip-address* **longer-match**

The system ANDs the input destination IP address with the subnet mask in each route entry; and ANDs the destination IP address in each route entry with its corresponding subnet mask.

If the two operations yield the same result for multiple entries that are active, the one with longest mask length is displayed.

- **display ip routing-table** *ip-address mask* **longer-match**

The system ANDs the input destination IP address with the input subnet mask; and ANDs the destination IP address in each route entry with the input subnet mask.

If the two operations yield the same result for multiple entries with a mask less than or equal to the input subnet mask, the one that is active with longest mask length is displayed.

Use the **display ip routing-table** *ip-address1* { *mask-length* | *mask* } *ip-address2* { *mask-length* | *mask* } command to display route entries with destination addresses within a specified range.

Examples # Display route entries for the destination IP address 11.1.1.1.

```
[Sysname] display ip routing-table  11.1.1.1
Routing Table : Public
Summary Count : 4

Destination/Mask    Proto   Pre  Cost         NextHop         Interface

0.0.0.0/0           Static 60   0            0.0.0.0         NULL0
11.0.0.0/8          Static 60   0            0.0.0.0         NULL0
11.1.0.0/16         Static 60   0            0.0.0.0         NULL0
11.1.1.0/24         Static 60   0            0.0.0.0         NULL0
```

For detailed description about the output, see Table 51.

Display route entries by specifying a destination IP address and the **longer-match** keyword.

```
[Sysname] display ip routing-table  11.1.1.1 longer-match
Routing Table : Public
Summary Count : 1

Destination/Mask    Proto   Pre  Cost         NextHop         Interface

11.1.1.0/24         Static 60   0            0.0.0.0         NULL0
```

Display route entries by specifying a destination IP address and mask.

```
[Sysname] display ip routing-table  11.1.1.1 24
Routing Table : Public
Summary Count : 3

Destination/Mask    Proto  Pre  Cost         NextHop         Interface

11.0.0.0/8          Static 60   0            0.0.0.0         NULL0
11.1.0.0/16         Static 60   0            0.0.0.0         NULL0
11.1.1.0/24         Static 60   0            0.0.0.0         NULL0
```

Display route entries by specifying a destination IP address and mask and the **longer-match** keyword.

```
[Sysname] display ip routing-table  11.1.1.1 24 longer-match
Routing Table : Public
Summary Count : 1

Destination/Mask    Proto  Pre  Cost         NextHop         Interface

11.1.1.0/24         Static 60   0            0.0.0.0         NULL0
```

For detailed description of the above output, see Table 52.

Display route entries for destination addresses in the range 1.1.1.0 to 5.5.5.0.

```
<Sysname> display ip routing-table 1.1.1.0 24 5.5.5.0 24
Routing Table : Public

Destination/Mask    Proto  Pre  Cost         NextHop       Interface
1.1.1.0/24          Direct 0    0            1.1.1.1       Vlan1
1.1.1.1/32          Direct 0    0            127.0.0.1     InLoop0
2.2.2.0/24          Direct 0    0            2.2.2.1       Vlan2
3.3.3.0/24          Direct 0    0            3.3.3.1       vlan4
3.3.3.1/32          Direct 0    0            127.0.0.1     InLoop0
4.4.4.0/24          Direct 0    0            4.4.4.1       vlan6
```

4.4.4.1/32 Direct 0 0 127.0.0.1 InLoop0

display ip routing-table ip-prefix

Syntax **display ip routing-table ip-prefix** *ip-prefix-name* [**verbose**]

View Any view

Parameters *ip-prefix-name*: IP Prefix list name, which is a character string.

verbose: Displays detailed routing table information, including that for inactive routes. With this argument absent, the command displays only brief information about active routes.

Description Use the **display ip routing-table ip-prefix** command to display information about routes permitted by a specified prefix list.

This command is intended for the follow-up display of routing policies. If the specified prefix list is not configured, detailed information about all routes (with the **verbose** keyword) or brief information about all active routes (without the **verbose** keyword) is displayed.

Examples # Configure a prefix list named abc, permitting routes with a prefix of 2.2.2.0 and a mask length between 24 and 32.

```
<Sysname> system-view
[Sysname] ip ip-prefix abc permit 2.2.2.0 24 less-equal 32
```

Display brief information about active routes permitted by the prefix list abc.

```
[Sysname] display ip routing-table ip-prefix abc
Routes Matched by Prefix list : abc
Summary Count : 2
Destination/Mask   Proto  Pre  Cost        NextHop         Interface
2.2.2.0/24         Direct  0    0          2.2.2.1         Vlan2
2.2.2.1/32         Direct  0    0          127.0.0.1       InLoop0
```

For detailed description of the above output, see Table 51.

Display detailed information about both active and inactive routes permitted by IP prefix list abc.

```
[Sysname] display ip routing-table ip-prefix abc verbose
Routes Matched by Prefix list  abc :
Summary Count : 2

Destination: 2.2.2.0/24
     Protocol: Direct                 Process ID: 0
   Preference: 0                            Cost: 0
      NextHop: 2.2.2.1                 Interface: Vlan2
  RelyNextHop: 0.0.0.0                 Neighbour: 0.0.0.0
    Tunnel ID: 0x0                         Label: NULL
        State: Active Adv                    Age: 00h20m52s
          Tag: 0

Destination: 2.2.2.1/32
     Protocol: Direct                 Process ID: 0
   Preference: 0                            Cost: 0
      NextHop: 127.0.0.1               Interface: InLoop0
  RelyNextHop: 0.0.0.0                 Neighbour: 0.0.0.0
    Tunnel ID: 0x0                         Label: NULL
        State: Active NoAdv                  Age: 00h20m52s
          Tag: 0
```

For detailed description of the above output, see Table 52.

display ip routing-table protocol

Syntax **display ip routing-table protocol** *protocol* [**inactive** | **verbose**]

View Any view

Parameters *protocol*: Routing protocol. It can be **BGP**, **DIRECT**, **ISIS**, **OSPF**, **RIP**, or **STATIC**.

inactive: Displays information about only inactive routes. With this argument absent, the command displays information about both active and inactive routes.

verbose: Displays detailed routing table information. With this argument absent, the command displays brief routing table information.

Description Use the **display ip routing-table protocol** command to display routing information of a specified routing protocol.

Examples # Display brief information about direct routes.

```
<Sysname> display ip routing-table protocol direct
Public Routing Table : Direct
Summary Count : 6

Direct Routing table Status : < Active>
Summary Count :  6

Destination/Mask    Proto  Pre  Cost       NextHop         Interface

2.2.2.0/24          Direct 0    0          2.2.2.1         Vlan2
2.2.2.2/32          Direct 0    0          127.0.0.1       InLoop0
127.0.0.0/8         Direct 0    0          127.0.0.1       InLoop0
127.0.0.1/32          Direct 0    0          127.0.0.1       InLoop0
192.168.80.0/24     Direct 0    0          192.168.80.10   Vlan3
192.168.80.10/32    Direct 0    0          127.0.0.1       InLoop0

Direct Routing table Status : < Inactive>
Summary Count : 0
```

Display summary information about static routes.

```
<Sysname> display ip routing-table protocol static
Public Routing Table : Static
Summary Count : 2

Static Routing table Status : < Active>
Summary Count :  0

Static Routing table Status : < Inactive>
Summary Count : 2
Destination/Mask    Proto   Pre  Cost       NextHop      Interface
1.2.3.0/24          Static  60   0          1.2.4.5      Vlan10
3.0.0.0/8           Static  60   0           2.2.2.2     Vlan4
```

For detailed description of the above output, see Table 51.

display ip routing-table statistics

Syntax **display ip routing-table** [**vpn-instance** *vpn-instance-name*] **statistics**

View Any view

Parameters **vpn-instance** *vpn-instance-name*: Displays routing table information for a VPN instance. The VPN instance name is a character string.

Description Use the **display ip routing-table statistics** command to display statistics about the public network routing table or a VPN routing table.

Examples # Display statistics about the routes in the routing table.

```
<Sysname> display ip routing-table statistics
Proto      route       active      added       deleted       freed
DIRECT     24          4           25          1             0
STATIC     4           1           4           0             0
RIP        0           0           0           0             0
OSPF       0           0           0           0             0
IS-IS      0           0           0           0             0
BGP        0           0           0           0             0
Total      28          5           29          1             0
```

Table 53 Field descriptions of display ip routing-table statistics

Field	Description
Proto	Origin of the routes. Possible values include OSPF, RIP, BGP, direct or static.
route	Number of routes from the origin
active	Number of active routes from the origin
added	Number of routes added into the routing table since the device starts up or the last routing table reset operation
deleted	Number of routes marked as deleted, which will be freed after a period.
freed	Number of routes that got freed, that is, got removed permanently
Total	Sums for the numerical items above

display ipv6 routing-table

Syntax **display ipv6 routing-table**

View Any view

Parameters None

Description Use the **display ipv6 routing-table** command to display brief routing table information, including destination IP address and prefix, protocol type, priority, metric, next hop and outbound interface.

The command displays only active routes, namely, the brief information about the current optimal routes.

Examples # Display brief routing table information

```
<Sysname> display ipv6 routing-table
Routing Table :
        Destinations : 1        Routes : 1

Destination : ::1/128                           Protocol    : Direct
NextHop     : ::1                               Preference  : 0
Interface   : InLoop0                           Cost        : 0
```

Table 54 Field descriptions of the display ipv6 routing-table command

Field	Description
Destination	Destination IPv6 address
NextHop	Next hop
Preference	Routing preference
Interface	Outbound interface
Protocol	Routing protocol of the route
Cost	Routing cost
Tunnel ID	Tunnel ID
Label	Label

display ipv6 routing-table acl

Syntax **display ipv6 routing-table acl** *acl6-number* [**verbose**]

View Any view

Parameters *acl6-number:* Basic IPv6 ACL number.

Verbose: Displays both active and inactive verbose routing information permitted by the ACL. Without this keyword, only brief active routing information is displayed.

Description Use the **display ipv6 routing-table acl** command to display routing information permitted by the IPv6 ACL.

If the specified IPv6 ACL is not available, all routing information is displayed.

Examples # Display brief routing information permitted by ACL 2000.

```
<Sysname> display ipv6 routing-table acl 2000
Routes Matched by Access list  2000  :
Summary Count : 2

Destination : ::1/128                           Protocol   : Direct
NextHop     : ::1                               Preference : 0
Interface   : InLoop0                           Cost       : 0
Destination : 1:1::/64                            Protocol   : Static
NextHop     : ::                                Preference : 60
Interface   : NULL0                             Cost       : 0
```

Refer to Table 54 for description about the above output.

display ipv6 routing-table ipv6-address

Syntax **display ipv6 routing-table** *ipv6-address prefix-length* [**longer-match**] [**verbose**]

View Any view

Parameters *ipv6-address*: Destination IPv6 address.

prefix-length: Prefix length.

longer-match: Displays the matched route with the longest prefix.

verbose: Displays both active and inactive verbose routing information. Without this keyword, only brief active routing information is displayed.

Description Use the **display ipv6 routing-table** *ipv6-address* command to display routing information about the specified destination IPv6 address.

Executing the command with different parameters yields different output:

- **display ipv6 routing-table** *ipv6-address prefix-length*

The system ANDs the input destination IPv6 address with the input prefix length, and ANDs the destination IPv6 address in each route entry with the input prefix length.

If the two operations yield the same result for an entry and the entry is active with a prefix length less than or equal to the input prefix length, the entry is displayed.

Only route entries that exactly match the input destination address and prefix length are displayed.

- **display ipv6 routing-table** *ipv6-address prefix-length* **longer-match**

The system ANDs the input destination IPv6 address with the input prefix length; and ANDs the destination IPv6 address in each route entry with the input prefix length.

If the two operations yield the same result for multiple entries with a prefix length less than or equal to the input prefix length, the one that is active and has the longest prefix length is displayed.

Examples # Display brief information about the route matching the specified destination IPv6 address.

```
<Sysname> display ipv6 routing-table 10::1 127
```

Routing Table:

Summary Count: 3

Destination: 10::/64 Protocol : Static

NextHop : :: Preference: 60

Interface : NULL0 Cost : 0

Destination: 10::/68 Protocol : Static

NextHop : :: Preference: 60

Interface : NULL0 Cost : 0

Destination: 10::/120 Protocol : Static

NextHop : :: Preference: 60

Interface : NULL0 Cost : 0

Display brief information about the route matching the specified destination IPv6 address and having the longest prefix.

```
<Sysname> display ipv6 routing-table 10:: 127 longer-match
```

Routing Tables:

Summary Count : 1

Destination: 10::/120 Protocol : Static

NextHop : :: Preference: 60

```
Interface  : NULL0                                    Cost      : 0
```

Refer to Table 54 for description about the above output.

display ipv6 routing-table ipv6-address1 ipv6-address2

Syntax **display ipv6 routing-table** *ipv6-address1 prefix-length1 ipv6-address2 prefix-length2* [**verbose**]

View Any view

Parameters *ipv6-address1*/*ipv6-address2*: An IPv6 address range from IPv6 address1 to IPv6 address2.

prefix-length1/*prefix-length2*: Prefix length.

verbose: Displays both active and inactive verbose routing information. Without this keyword, only brief active routing information is displayed.

Description Use the **display ipv6 routing-table** *ipv6-address1 ipv6-address2* command to display routes with destinations falling into the specified IPv6 address range.

Examples # Display routes with destinations falling into the IPv6 address range.

```
<Sysname> display ipv6 routing-table 3:: 32 4:4:: 64
Routing Table :
Summary Count : 3

Destination: 100::/64                                  Protocol  : Static
NextHop    : ::                                        Preference: 60
Interface  : NULL0                                     Cost      : 0

Destination: 200::/64                                  Protocol  : Static
NextHop    : ::                                        Preference: 60
Interface  : NULL0                                     Cost      : 0

Destination: 300::/64                                  Protocol  : Static
NextHop    : ::                                        Preference: 60
Interface  : NULL0                                     Cost      : 0
```

Refer to Table 54 for description about the above output.

display ipv6 routing-table ipv6-prefix

Syntax **display ipv6 routing-table ipv6-prefix** *ipv6-prefix-name* [**verbose**]

View Any view

Parameters *ipv6-prefix-name*: Name of the IPv6 prefix list.

verbose: Displays both active and inactive verbose routing information. Without this keyword, only brief active routing information is displayed.

Description Use the **display ipv6 routing-table ipv6-prefix** command to display routes permitted by the IPv6 prefix list.

Examples # Display brief active routing information permitted by the IPv6 prefix list abc2.

```
<Sysname> display ipv6 routing-table ipv6-prefix abc2
Routes Matched by Prefix list  abc2  :
Summary Count : 1

Destination: 100::/64                                  Protocol  : Static
NextHop    : ::                                        Preference: 60
Interface  : NULL0                                     Cost      : 0
```

Refer to Table 54 for description about the above output.

display ipv6 routing-table protocol

Syntax **display ipv6 routing-table protocol** *protocol* [**inactive** | **verbose**]

View Any view

Parameters *protocol*: Displays routes of a routing protocol, which can be **bgp4+**, **direct**, **isisv6**, **ospfv3**, **ripng** and **static**.

inactive: Displays only inactive routes. Without the keyword, all active and inactive routes are displayed.

verbose: Displays both active and inactive verbose routing information. Without this keyword, only brief active routing information is displayed.

Description Use the **display ipv6 routing-table protocol** command to display routes of a specified routing protocol.

Examples # Display brief information about all direct routes.

```
<Sysname> display ipv6 routing-table protocol direct
Direct Routing Table :
Summary Count : 1

Direct Routing Table's Status : < Active >
Summary Count : 1

Destination: ::1/128                                    Protocol  : Direct
NextHop    : ::1                                        Preference: 0
Interface  : InLoop0                                    Cost      : 0

Direct Routing Table's Status : < Inactive >
Summary Count : 0
```

Refer to Table 54 for description about the above output.

display ipv6 routing-table statistics

Syntax **display ipv6 routing-table statistics**

View Any view

Parameters None

Description Use the **display ipv6 routing-table statistics** command to display routing statistics, including total route number, added route number and deleted route number.

Examples # Display routing statistics.

```
<Sysname> display ipv6 routing-table statistics
Protocol   route      active     added      deleted     freed
DIRECT      1           1          1           0           0
STATIC      3           0          3           0           0
RIPng       0           0          0           0           0
OSPFv3      0           0          0           0           0
IS-ISv6     0           0          0           0           0
BGP4+       0           0          0           0           0
Total       4           1          4           0           0
```

Table 55 Field descriptions of the display ipv6 routing-table statistics command

Field	Description
Protocol	Routing protocol

Table 55 Field descriptions of the display ipv6 routing-table statistics command

Field	Description
route	Route number of the protocol
active	Active route number
added	Routes added after the last startup of the router
deleted	Deleted routes, which will be released after a specified time
freed	Released (totally removed from the routing table) route number
Total	Total route number

display ipv6 routing-table verbose

Syntax **display ipv6 routing-table verbose**

View Any view

Parameters None

Description Use the **display ipv6 routing-table verbose** command to display detailed information about all active and inactive routes, including the statistics of the entire routing table and information for each route.

Examples # Display detailed information about all active and inactive routes.

```
<Sysname> display ipv6 routing-table verbose
Routing Table :
         Destinations : 1        Routes : 1

 Destination  : ::1                                    PrefixLength : 128
 NextHop      : ::1                                    Preference   : 0
 RelayNextHop : ::                                     Tag          : 0H
 Neighbour    : ::                                     ProcessID    : 0
 Interface    : InLoopBack0                            Protocol     : Direct
 State        : Active NoAdv                           Cost         : 0
 Tunnel ID    : 0x0                                    Label        : NULL
 Age          : 22161sec
```

Table 56 Field descriptions of the display ipv6 routing-table verbose command

Field	Description
Destination	Destination IPv6 address
PrefixLength	Prefix length of the address
Nexthop	Next hop
Preference	Routing preference
RelayNextHop	Relay next hop
Tag	Tag of the route
Neighbour	Neighbor address
ProcessID	Process ID
Interface	Outbound interface
Protocol	Routing protocol
State	State of the route, Active, Inactive, Adv (advertised), or NoAdv (not advertised)

Table 56 Field descriptions of the display ipv6 routing-table verbose command

Field	Description
Cost	Cost of the route
Tunnel ID	Tunnel ID
Label	Label
Age	Time that has elapsed since the route was generated

reset ip routing-table statistics protocol

Syntax **reset ip routing-table statistics protocol** [**vpn-instance** *vpn-instance-name*] { **all** | *protocol* }

View User view

Parameters *vpn-instance-name*: VPN instance name, which is a character string.

all: All protocols.

protocol: Routing protocol. It can be **BGP**, **DIRECT**, **ISIS**, **OSPF**, **RIP**, or **STATIC**.

Description Use the **reset ip routing-table statistics protocol** command to clear routing statistics for the public network routing table or VPN routing table.

Examples # Clear private network routing statistics for the VPN instance Sysname1.

```
<Sysname> reset ip routing-table statistics protocol vpn-instance Sysname1 all
```

reset ipv6 routing-table statistics (User view)

Syntax **reset ipv6 routing-table statistics protocol** { **all** | *protocol* }

View User view

Parameters **all**: Clears statistics for all routing protocols.

protocol: Clears statistics for the routing protocol, which can be **bgp4+**, **direct**, **isisv6**, **ospfv3**, **ripng**, or **static**.

Description Use the **reset ipv6 routing-table statistics** command to clear the route statistics of the routing table.

Examples # Clears statistics for all routing protocols.

```
<Sysname> reset ipv6 routing-table statistics protocol all
```

20 IP ADDRESSING CONFIGURATION COMMANDS

display ip interface

Syntax **display ip interface** [*interface-type interface-number*]

View Any view

Parameters *interface-type interface-number*: Specifies an interface by its type and number.

Description Use the **display ip interface** command to display information about a specified or all Layer 3 interfaces.

Examples # Display information about the interface Vlan-interface1.

```
<Sysname> display ip interface vlan-interface 1
Vlan-interface1 current state :DOWN
Line protocol current state :DOWN
Internet Address is 2.2.2.2/24 Primary
Broadcast address : 2.2.2.255
The Maximum Transmit Unit : 1500 bytes
input packets : 0, bytes : 0, multicasts : 0
output packets : 0, bytes : 0, multicasts : 0
ARP packet input number:           0
  Request packet:                  0
  Reply packet:                    0
  Unknown packet:                  0
TTL invalid packet number:         0
ICMP packet input number:          0
  Echo reply:                      0
  Unreachable:                     0
  Source quench:                   0
  Routing redirect:                0
  Echo request:                    0
  Router advert:                   0
  Router solicit:                  0
  Time exceed:                     0
  IP header bad:                   0
  Timestamp request:               0
  Timestamp reply:                 0
  Information request:             0
  Information reply:               0
  Netmask request:                 0
  Netmask reply:                   0
  Unknown type:                    0
DHCP packet deal mode:  global
```

Table 57 Description on fields of the display ip interface command

Field	Description
current state	Current physical state of an interface
Line protocol current state	Current state of the link layer protocol
Internet Address	IP address of an interface. Primary behind an IP address indicates the IP address is a primary one, and Sub indicates the IP address is a secondary one.
Broadcast address	Broadcast address of the subnet attached to an interface
The Maximum Transmit Unit	Maximum transmission units on an interface
input packets : 0, bytes : 0, multicasts : 0	Unicast packets, bytes, and multicast packets received on an interface
output packets : 0, bytes : 0, multicasts : 0	Unicast packets, bytes, and multicast packets sent on an interface
ARP packet input number	Total number of ARP packets received on an interface
Request packet	Number of ARP request packets received on an interface
Reply packet	Number of ARP reply packets received on an interface
Unknown packet	Number of unknown packets received on an interface
TTL invalid packet number	Number of TTL-invalid packets received on an interface
ICMP packet input number: 0 Echo reply: 0 Unreachable: 0 Source quench: 0 Routing redirect: 0 Echo request: 0 Router advert: 0 Router solicit: 0 Time exceed: 0 IP header bad: 0 Timestamp request: 0 Timestamp reply: 0 Information request: 0 Information reply: 0 Netmask request: 0 Netmask reply: 0 Unknown type: 0	Total number of ICMP packets received on an interface, including the following packets: ■ Echo reply packet ■ Unreachable packets ■ Source quench packets ■ Routing redirect packets ■ Echo request packets ■ Router advertisement packets ■ Router solicitation packets ■ Time exceed packets ■ IP header bad packets ■ Timestamp request packets ■ Timestamp reply packets ■ Information request packets ■ Information reply packets ■ Netmask request packets ■ Netmask reply packets ■ Unknown type packets
DHCP packet deal mode	DHCP packet processing mode.

display ip interface brief

Syntax **display ip interface brief** [*interface-type interface-number*]

View Any view

Parameters *interface-type interface-number*: Specifies an interface by its type and number.

Description Use the **display ip interface brief** command to display brief information about a specified or all Layer 3 interfaces.

Related commands: **display ip interface**.

Examples # Display brief information about Vlan-interface22.

```
<Sysname> display ip interface brief vlan-interface 22
*down: administratively down
(s): spoofing
Interface                         Physical   Protocol   IP Address
Vlan-interface22                    down       down     10.2.2.2
```

Table 58 Description on fields of the display ip interface brief command

Field	Description
*down	The interface is administratively shut down with the **shutdown** command.
(s)	Spoofing attribute of the interface. It indicates that an interface whose link layer protocol is displayed up may have no link present or the link is set up only on demand.
Interface	Interface name
Physical	Physical state of interface
Protocol	Link layer protocol state of interface
IP Address	IP address of interface (if no IP address is configured, "unassigned" is displayed.)

ip address (Interface view)

Syntax **ip address** *ip-address* { *mask* | *mask-length* } [**sub**]

undo ip address [*ip-address* { *mask* | *mask-length* } [**sub**]]

View Interface view

Parameters *ip-address*: IP address of interface, in dotted decimal notation.

mask: Subnet mask in dotted decimal notation.

mask-length: Subnet mask length, the number of consecutive ones in the mask.

sub: Indicates the specified IP address is a secondary IP address.

Description Use the **ip address** command to assign an IP address and mask to the specified interface.

Use the **undo ip address** command to remove all IP addresses from the interface.

Use the **undo ip address** *ip-address* { *mask* | *mask-length* } command to remove the primary IP address.

Use the **undo ip address** *ip-address* { *mask* | *mask-length* } **sub** command to remove a secondary IP address.

You cannot assign a secondary IP address when the interface is configured to obtain an IP address through DHCP or PPP negotiation, or to borrow an IP address through IP unnumbered.

By default, no IP address is assigned to any interface.

When assigning IP addresses to an interface, consider the following:

- You can assign only one primary IP address to an interface.
- The primary and secondary IP addresses can be located in the same network segment.
- Before removing the primary IP address, remove all secondary IP addresses.

Related commands: **display ip interface**.

Examples # Assign Vlan-interface1 a primary IP address and a secondary IP address, with subnet masks being 255.255.255.0.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ip address 129.12.0.1 255.255.255.0
[Sysname-Vlan-interface1] ip address 202.38.160.1 255.255.255.0 sub
```

21 ARP CONFIGURATION COMMANDS

arp check enable

Syntax **arp check enable**

undo arp check enable

View System view

Parameters None

Description Use the **arp check enable** command to enable ARP entry check, preventing the device from learning multicast MAC addresses.

Use the **undo arp check enable** command to disable the function, allowing the device to learn multicast MAC addresses.

By default, ARP entry check is enabled.

Examples # Disable the device from learning multicast MAC addresses.

```
<Sysname> system-view
[Sysname] undo check enable
```

arp max-learning-num

Syntax **arp max-learning-num** *number*

undo arp max-learning-num

View VLAN interface view

Parameters *number*: Maximum number of dynamic ARP entries that the interface can learn. The default is 4096.

Description Use the **arp max-learning-num** command to set the maximum number of dynamic ARP entries that the interface can learn.

Use the **undo arp max-learning-num** command to restore the default.

Examples # Specify VLAN interface 40 to learn up to 500 dynamic ARP entries.

```
<Sysname> system-view
[Sysname] interface vlan-interface 40
[Sysname-Vlan-interface40]arp max-learning-num 500
```

arp static

Syntax **arp static** *ip-address mac-address* [*vlan-id interface-type interface-number*] [**vpn-instance** *vpn-instance-name*]

undo arp *ip-address* [*vpn-instance-name*]

View System view

Parameters *ip-address*: IP address of the static ARP entry.

mac-address: MAC address of the static ARP entry, in the format H-H-H.

vlan-id: ID of a VLAN to which the static ARP entry belongs to.

interface-type interface-number: Interface type and interface number.

vpn-instance-name: Name of a VLAN instance.

Description Use the **arp static** command to configure a static ARP entry in the ARP mapping table.

Use the **undo arp** command to remove an ARP entry.

ARP entries fall into two categories: dynamic and static.

1. A dynamic entry is automatically created and maintained by ARP. It can get aged, be updated by a new ARP packet, or be overwritten by a static ARP entry. When the aging timer expires or the interface goes down, the corresponding dynamic ARP entry will be removed.
2. A static ARP entry is manually configured and maintained. It can be permanent or non-permanent.
   - A permanent static ARP entry can be directly used to forward data. When configuring a permanent static ARP entry, you must configure a VLAN and outbound interface for the entry besides the IP address and MAC address.
   - A non-permanent static ARP entry cannot be directly used for forwarding data. When configuring a non-permanent static ARP entry, you only need to configure the IP address and MAC address. When forwarding IP packets, the device sends an ARP request. If the source IP and MAC addresses in the received ARP reply are the same as the configured IP and MAC addresses, the entry can be used for forwarding IP packets.

By default, the ARP entry table is empty and ARP dynamically obtains IP-to-MAC mappings. Only in special cases, manual configuration is needed. ARP entries are used for resolution of addresses in the same LAN. There are other methods for address resolution in WANs, such as reverse address resolution in FR.

Note that:

- A static ARP entry is effective when the device works normally. However, when the VLAN or VLAN interface to which an ARP entry corresponds is deleted, the entry, if permanent, will be deleted, and if non-permanent and resolved, will become unresolved.
- The *vlan-id* argument is used to specify the corresponding VLAN of an ARP entry and must be the ID of an existing VLAN. In addition, the Ethernet interfaces following the argument must belong to that VLAN.
- Switch 8800s support both permanent and non-permanent ARP entries configuration.

Related commands: **reset arp**, **display arp**, and **debugging arp**.

Examples # Configure a static ARP entry, with the IP address being 202.38.10.2, the MAC address being 00e0-fc01-0000, and the outbound interface being Ethernet 1/1/1 of VLAN 10.

```
<Sysname> system-view
[Sysname] arp static 202.38.10.2 00e0-fc01-0000 10 ethernet 1/1/1
```

arp timer aging

Syntax **arp timer aging** *aging-time*

undo arp timer aging

View System view

Parameters *aging-time*: Aging time for dynamic ARP entries in minutes.

Description Use the **arp timer aging** command to set aging time for dynamic ARP entries.

Use the **undo arp timer aging** command to restore the default.

The default aging time is 20 minutes.

Related commands: **display arp timer aging**.

Examples # Set aging time for dynamic ARP entries to 10 minutes.

```
<Sysname> system-view
[Sysname] arp timer aging 10
```

debugging arp

Syntax **debugging arp** { **packet** | **status** }

undo debugging arp { **packet** | **status** }

View User view

Parameters **packet**: ARP packet debugging.

status: ARP status debugging.

Description Use the **debugging arp** command to enable specified ARP debugging.

Use the **undo debugging arp** command to disable specified ARP debugging.

No ARP debugging is enabled by default.

Related commands: **arp static**, **display arp**.

Examples # Enable ARP packet debugging.

```
<Sysname> debugging arp packet
*Dec 29 14:56:23:132 2006 S95 ARP/7/arp_send:Slot=3; Send an ARP Packet, ope
ration : 1, sender_eth_addr :
 00e0-fc00-3500,sender_ip_addr : 10.110.91.159, target_eth_addr : 0000-0000-
0000, target_ip_addr : 10.110.91.193
*Dec 29 14:56:22:876 2006 S95 ARP/7/arp_rcv:Slot=3; Receive an ARP Packet, o
peration : 2, sender_eth_addr :
 0050-ba22-6fd7, sender_ip_addr : 10.110.91.193, target_eth_addr : 00e0-fc00
-3500, target_ip_addr : 10.110.91.159
```

Table 59 Field descriptions of the debugging arp packet command

Field	Description
operation	ARP operation code: 1 for ARP request, 2 for ARP response
sender_eth_addr	Source Ethernet address
sender_ip_addr	Source IP address
target_eth_addr	Destination Ethernet address, all zeros for a request
target_ip_addr	Destination IP address

display arp

Syntax **display arp** { { **all** | **dynamic** | **static** } [**slot** *slot-id*] | **vlan** *vlan-id* | **interface** *interface-type interface-number* } [[**verbose**] [**|** { **begin** | **exclude** | **include** } *text*] | **count**]

View Any view

Parameters **all**: Displays all ARP entries.

dynamic: Displays dynamic ARP entries.

static: Displays static ARP entries.

slot-id: Displays the ARP entries of the specified slot.

vlan-id: Displays the ARP entries of the specified VLAN.

interface-type interface-number: Displays the ARP entries of the specified interface.

verbose: Displays detailed information about ARP entries.

|: Uses a regular expression to specify the ARP entries to be displayed.

begin: Displays ARP entries from the first one containing the specified string.

exclude: Displays the ARP entries that do not contain the specified string.

include: Displays the ARP entries containing the specified string.

text: A string for matching.

count: Displays the number of ARP entries.

Description Use the **display arp** command to display ARP entries in the ARP mapping table. Using the **display arp all** command displays all ARP entries.

Related commands: **arp static**, **reset arp**, and **debugging arp**.

Examples # Display the detailed information of all ARP entries.

```
<Sysname> display arp all verbose
                Type: S-Static    D-Dynamic
IP Address       MAC Address     VLAN ID  Interface              Aging Type
Vpn-instance Name
20.1.1.1         00e0-fc00-0001  N/A      N/A                    N/A   S
test
193.1.1.70       00e0-fe50-6503  100      GE1/1/1                DIS    D
[No Vrf]
192.168.0.115    000d-88f7-9f7d  1        GE1/1/4                DIS    D
[No Vrf]
192.168.0.39     0012-a990-2241  1        GE1/1/4                DIS    D
[No Vrf]
```

Table 60 Field descriptions of the display arp command

Field	Description
IP Address	IP address in an ARP entry
MAC Address	MAC address in an ARP entry
VLAN ID	VLAN ID contained a static ARP entry
Interface	Outbound interface in an ARP entry
Aging	Aging time for a dynamic ARP entry in minutes
DIS	Indicates the ARP entry was not learned by the module.
Type	ARP entry type: D stands for dynamic and S for static.
Vpn-instance Name	Name of VPN instance. [No Vrf] means no VPN instance is configured for the corresponding ARP.

Display the number of all ARP entries

```
<Sysname> display arp all count
Total entry(ies): 4
```

display arp ip-address

Syntax **display arp** *ip-address* [**slot** *slot-id*] [**verbose**] [**|** { **begin** | **exclude** | **include** } *text*]

View Any view

Parameters *ip-address:* Displays the ARP entry for the specified IP address.

slot-id: Displays the ARP entry for the specified slot.

verbose: Displays the detailed information about ARP entries.

|: Uses a regular expression to specify the ARP entries to be displayed.

begin: Displays the ARP entries from the first one containing the specified string.

exclude: Displays the ARP entries that do not contain the specified string.

Include: Displays the ARP entries that contain the specified string.

text: A character string.

Description Use the **display arp** *ip-address* command to display the ARP entry for a specified IP address.

Related commands: **arp static**, and **reset arp**.

Examples # Display the corresponding ARP entry for the IP address 20.1.1.1.

```
<Sysname> display arp 20.1.1.1
  Type: S-Static    D-Dynamic
IP Address       MAC Address     VLAN ID  Interface             Aging Type
20.1.1.1         00e0-fc01-0001  22       GE4/2/4               N/A   S
```

Table 61 Field descriptions of the display arp ip-address command

Field	Description
IP Address	IP address of the ARP entry
MAC Address	MAC address of the ARP entry
VLAN ID	VLAN ID of the ARP entry
Interface	Interface of the ARP entry
Aging	Remaining aging time for a dynamic ARP entry, in minutes
Type	ARP entry type: D for dynamic, S for static

display arp timer aging

Syntax **display arp timer aging**

View Any view

Parameters None

Description Use the **display arp timer aging** command to display the aging time for dynamic ARP entries.

Related commands: **arp timer aging**.

Examples # Display the aging time for dynamic ARP entries.

```
<Sysname> display arp timer aging
Current ARP aging time is 20 minute(s)(default)
```

display arp vpn-instance

Syntax **display arp vpn-instance** *vpn-instance-name* [**|** { **begin** | **exclude** | **include** } *text* | **count**]

View Any view

Parameters *vpn-instance-name*: Name of VPN instance, a case-insensitive string of 1 to 31 characters.

|: Uses a regular expression to specify the ARP entries to be displayed.

begin: Displays the ARP entries from the first one that contains the specified string.

exclude: Displays the ARP entries that do not contain the specified string.

include: Displays the ARP entries that contain the specified string.

text: A character string.

count: Displays the number of ARP entries.

Description Use the **display arp vpn-instance** command to display the ARP entries for a specified VPN instance.

Related commands: **arp static** and **reset arp.**

Examples # Display ARP entries for the VPN instance named test.

```
<Sysname> display arp vpn-instance test
                Type: S-Static    D-Dynamic
IP Address       MAC Address     VLAN ID  Interface             Aging Type
Vpn-instance Name
20.1.1.1         00e0-fc00-0001  N/A      N/A                   N/A   S
test
```

Table 62 Field descriptions of the display arp vpn-instance command

Field	Description
IP Address	IP address of the ARP entry

Table 62 Field descriptions of the display arp vpn-instance command

Field	Description
MAC Address	MAC address of the ARP entry
VLAN ID	VLAN ID of the ARP entry
Interface	Interface of the ARP entry
Aging	Remaining aging time for a dynamic ARP entry, in minutes
Type	ARP entry type: D for dynamic, S for static
Vpn-instance Name	VPN instance name

naturemask-arp enable

Syntax **naturemask-arp enable**

undo naturemask-arp enable

View System view

Parameters None

Description Use the **naturemask-arp enable** command to cancel the restriction that ARP requests must be from the same subnet. In this case, ARP requests from a natural network are supported.

Use the **undo naturemask-arp enable** command to restore the default.

By default, the support for ARP requests from a natural network is disabled.

Examples # Enable the support for ARP requests from a natural network.

```
<Sysname> system-view
[Sysname] naturemask-arp enable
```

reset arp

Syntax **reset arp** { **all** | **dynamic** | **static** | **slot** *slot-id* | **interface** *interface-type interface-number* }

View User view

Parameters **all:** Clears all ARP entries.

dynamic: Clears all dynamic ARP entries.

static: Clears all static ARP entries.

slot-id: Clears the ARP entries for the specified slot.

interface *interface-type interface-number*: Clears the ARP entries for the specified interface.

Description Use the **reset arp** command to clear ARP entries from the ARP mapping table.

With **interface** *interface-type interface-number* specified, the command clears only dynamic entries for the interface.

Related commands: **arp static** and **display arp**.

Examples # Clear all static ARP entries.

```
<Sysname> reset arp static
```

22 GRATUITOUS ARP CONFIGURATION COMMANDS

gratuitous-arp-sending enable

Syntax **gratuitous-arp-sending enable**

undo gratuitous-arp-sending enable

View System view

Parameters None

Description Use the **gratuitous-arp-sending enable** command to enable a device to send gratuitous ARP packets.

Use the **undo gratuitous-arp-sending enable** command to disable a device from sending gratuitous ARP packets.

By default, a Switch 8800 cannot send gratuitous ARP packets.

Related commands: **gratuitous-arp-learning enable**.

Examples # Disable a device from sending gratuitous ARP packets

```
<Sysname> system-view
[Sysname] undo gratuitous-arp-sending enable
```

gratuitous-arp-learning enable

Syntax **gratuitous-arp-learning enable**

undo gratuitous-arp-learning enable

View System view

Parameters None

Description Use the **gratuitous-arp-learning enable** command to enable the gratuitous ARP packet learning function.

Use the **undo gratuitous-arp-learning enable** command to disable the function.

By default, the function is disabled.

Examples # Enable the gratuitous ARP packet learning function.

```
<Sysname> system-view
[Sysname] gratuitous-arp-learning enable
```

23 ARP SOURCE SUPPRESSION CONFIGURATION COMMANDS

arp source-suppression enable

Syntax **arp source-suppression enable**

undo arp source-suppression enable

View System view

Parameters None

Description Use the **arp source-suppression enable** command to enable the ARP source address suppression function.

Use the **undo arp source-suppression enable** command to disable the function.

By default, the ARP source address suppression function is disabled.

With the function enabled, whenever the number of packets with unresolvable IP addresses that a host sends to the device within five seconds exceeds the specified threshold, the device drops all subsequent packets with the same source IP address in another five coming seconds. This helps in protecting the device against the attack.

Related commands: **display arp source-suppression**.

Examples # Enable the ARP source suppression function.

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

arp source-suppression limit

Syntax **arp source-suppression limit** *limit-value*

undo arp source-suppression limit

View System view

Parameters *limit-value*: Maximum number of packets with the same source IP address but unresolvable destination IP addresses that a port can receive in five seconds.

Description Use the **arp source-suppression limit** command to set the maximum number of packets with the same source IP address but unresolvable destination IP addresses that a port can receive in five seconds.

Use the **undo arp source-suppression limit** command to restore the default value, which is 10.

Related commands: **display arp source-suppression**.

Examples # Set to 100 the maximum number of packets with the same source address but unresolvable destination IP addresses that a port can receive in five seconds.

```
<Sysname> system-view
[Sysname] arp source-suppression limit 100
```

display arp source-suppression

Syntax **display arp source-suppression**

View Any view

Parameters None

Description Use the **display arp source-suppression** command to display information about the current ARP source suppression configuration.

Examples # Display information about the current ARP source suppression configuration.

```
<Sysname> display arp source-suppression
ARP source suppression is enabled
 Current suppression limit: 10
 Current cache length: 16
```

Table 63 Description on fields of display arp source-suppression

Field	Description
ARP source suppression is enabled	The ARP source suppression function is enabled
Current suppression limit	Maximum number of packets with the same source IP address but unresolvable IP addresses that the device can receive in five seconds
Current cache length	Size of cache used to record source suppression information

24 ARP DEFENSE AGAINST IP PACKET ATTACK CONFIGURATION COMMANDS

arp resolving-route enable

Syntax **arp resolving-route enable**

undo arp resolving-route enable

View System view

Parameters None

Description Use the **arp resolving-route enable** command to enable ARP defense against IP packet attacks.

Use the **undo arp resolving-route enable** command to disable the function.

By default, this function is enabled.

With this function enabled and after receiving an IP packet that ARP cannot resolve the MAC address of the next hop, the hardware forwarding chip of the switch simply drops all packets to the destination in the next 25 seconds. This protects the device against the IP packet attack efficiently, reducing the load of the CPU.

Examples # Enable ARP defense against IP packet attacks.

```
<Sysname> system-view
[Sysname] arp resolving-route enable
```

25 PROXY ARP CONFIGURATION COMMANDS

proxy-arp enable

Syntax **proxy-arp enable**

undo proxy-arp enable

View VLAN interface view

Parameters None

Description Use the **proxy-arp enable** command to enable proxy ARP.

Use the **undo proxy-arp enable** command to disable proxy ARP.

By default, proxy ARP is disabled.

With this command enabled, the device can implement the layer 3 communication between two hosts that reside in the same subnet but connect to different VLAN interfaces.

Related commands: **display proxy-arp**.

Examples # Enable proxy ARP on VLAN-interface 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] proxy-arp enable
```

local-proxy-arp enable

Syntax **local-proxy-arp enable**

undo local-proxy-arp enable

View VLAN interface view

Parameters None

Description Use the **local-proxy-arp enable** command to enable local proxy ARP.

Use the **undo local-proxy-arp enable** command to disable local proxy ARP.

By default, local proxy ARP is disabled.

Related commands: **display local-proxy-arp**.

Examples # Enable local proxy ARP on VLAN-interface 2.

```
<Sysname> system-view
[Sysname] interface Vlan-interface 2
[Sysname-Vlan-interface2] local-proxy-arp enable
```

display proxy-arp

Syntax **display proxy-arp** [**interface** *interface-type interface-number*]

View Any view

Parameters *interface-type interface-number*: Displays the proxy ARP status of the specified interface.

Description Use the **display proxy-arp** command to display the proxy ARP status.

Related commands: **proxy-arp enable**.

Examples # Display the proxy ARP status on VLAN-interface 22.

```
<Sysname> display arp proxy interface Vlan-interface22
Interface Vlan-interface22
Proxy ARP status: enabled
```

display local-proxy-arp

Syntax **display local-proxy-arp** [**interface** *interface-type interface-number*]

View Any view

Parameters *interface-type interface-number*: Displays the local proxy ARP status of the specified interface.

Description Use the **display local-proxy-arp** command to display the status of the local proxy ARP.

Related commands: **local-proxy-arp enable**.

Examples # Display the status of the local proxy ARP on VLAN-interface 2.

```
<Sysname> display local-proxy-arp interface vlan-interface 2
Interface Vlan-interface2
 Local Proxy ARP status: enabled
```

26 IPv6 Basics Configuration Commands

debugging ipv6 icmpv6

Syntax **debugging ipv6 icmpv6**

undo debugging ipv6 icmpv6

View User view

Parameters None

Description Use the **debugging ipv6 icmpv6** command to enable ICMPv6 debugging to display the received and transmitted ICMPv6 packets.

Use the **undo debugging ipv6 icmpv6** command to disable ICMPv6 debugging.

By default, ICMPv6 debugging is disabled.

Examples # Enable ICMPv6 debugging on an IPv6 interface of an IPv6-supported device.

```
<Sysname> debugging ipv6 icmpv6
*0.375970 Sysname ICMPV6/8/debug_ipv6 ICMPv6:
ICMPv6 Sent: Type=128, Code=0, Dst = 5007::100
```

// An ICMPv6 packet is sent.

```
*0.375972 AR19-62 ICMPV6/8/debug_ipv6 ICMPv6:
ICMPv6 Received: Type=129, Code=0,
Src = 5007::100, Dst = 5007::46
```

// An ICMPv6 packet is received.

Table 64 Table 21-1 Description on fields of the debugging ipv6 icmpv6 command

Field	Description
Sent	Send a packet
Received	Receive a packet
Type	Type of an ICMP packet
Code	Code of an ICMP packet
Src	Source IP address
Dst	Destination IP address

debugging ipv6 nd

Syntax **debugging ipv6 nd**

undo debugging ipv6 nd

View User view

Parameters None

Description Use the **debugging ipv6 nd** command to enable debugging for neighbor state and neighbor messages.

Use the **undo debugging ipv6 nd** command to disable the debugging.

By default, the debugging for neighbor state and neighbor messages is disabled.

Examples # Enable debugging for neighbor state and neighbor messages on an IPv6 interface of an IPv6-supported device.

```
<Sysname> debugging ipv6 nd
*0.20683530 Sysname ND/8/debug_ipv6 ND:
 Adding INCOMPLETE NB Entry: 2008::6 on Vlan-interface500
```

// A neighbor entry in the incomplete state is added.

```
*0.20683560 Sysname ND/8/debug_ipv6 ND:
 Address Resolution started for 2008::6 on Vlan-interface500
```

// Resolution of the IP address 2008::6 of the neighbor starts.

```
*0.20683690 Sysname ND/8/debug_ipv6 ND:
 Sending NS to FF02::1:FF00:6, on the interface Vlan-interface500
```

// An NS message is sent to the MAC address FF02::1:FF00:6.

```
*0.20684701 Sysname ND/8/debug_ipv6 ND:
 Received NA from 2008::6, on the interface Vlan-interface500
```

// An NA message is received from 2008::6.

```
*0.20684840 Sysname ND/8/debug_ipv6 ND:
 INCOMPLETE->REACHABLE : 2008::6 on Vlan-interface500
```

// The state of a neighbor entry is changed from incomplete to reachable.

Table 65 Table 21-2 Description on fields of the debugging ipv6 nd command

Field	Description
Adding	Add a neighbor entry
Deleting	Delete a neighbor entry
Address Resolution	Start address resolution
Sending	Send a packet

Table 65 Table 21-2 Description on fields of the debugging ipv6 nd command

Field	Description
Received	Receive a packet
NS	Neighbor solicitation message
NA	Neighbor advertisement message
RS	Router solicitation message
RA	Router advertisement message
Prefix	Prefix

debugging ipv6 packet

Syntax **debugging ipv6 packet**

undo debugging ipv6 packet

View User view

Parameters None

Description Use the **debugging ipv6 packet** command to enable IPv6 packet debugging.

Use the **undo debugging ipv6 packet** command to disable the debugging.

By default, IPv6 packet debugging is disabled.

Examples # Enable IPv6 packet debugging on an IPv6 interface of an IPv6-supported device.

```
<Sysname> terminal debugging
% Current terminal debugging is on
<Sysname> debugging ipv6 packet
*0.65250 Sysname IPV6 PRO/8/debug_ipv6:
Discarding, interface = Vlan-interface 12, version = 6, traffic class = 0,
flow label = 0, payload length = 92, protocol = 17, hop limit = 255,
Src = FE80:C00:C18:7::, Dst = FF02::9,
prompt: Ingress interface did not join the group address!/Invalid IPv6 contr
ol block!
```

// A packet is discarded possibly due to the error as prompted above.

```
*0.685761 AR19-62 IPV6PP/8/debug_ipv6:
Sending, interface = Vlan-interface 12, version = 6, traffic class = 0,
flow label = 0, payload length = 32, protocol = 58, hop limit = 255,
Src = FE80::20F:E2FF:FE00:2, Dst = FE80::2E0:FCFF:FE01:71,
prompt: Sending the packet from local at Vlan-interface 12
```

// A packet is sent.

```
*0.685764 AR19-62 IPV6PP/8/debug_ipv6:
Receiving, interface = Vlan-interface 12, version = 6, traffic class = 0,
flow label = 0, payload length = 24, protocol = 58, hop limit = 255,
Src = FE80::2E0:FCFF:FE01:71, Dst = FE80::20F:E2FF:FE00:2,
prompt: Input an IPv6 Package
```

// A packet is received from the Ethernet.

```
*0.685765 AR19-62 IPV6PP/8/debug_ipv6:
Delivering, interface = Vlan-interface 12, version = 6, traffic class = 0,
flow label = 0, payload length = 24, protocol = 58, hop limit = 255,
Src = FE80::2E0:FCFF:FE01:71, Dst = FE80::20F:E2FF:FE00:2,
prompt: IPv6 packet is delivering up!
```

// The received packet is delivered to the upper layer.

Table 66 Table 21-3 Description on major fields of the debugging ipv6 packet command

Field	Description
Discarding	Discard a packet.
Sending	Send a packet.
Receiving	Receive a packet.
Delivering	The packet is delivered from the IP layer to the upper layer.
Interface	Receiving/sending interface
Version	Version of the IP protocol
Traffic class	Class of the traffic
Protocol	Next packet header
Src	Source IP address
Dst	Destination IP address

debugging ipv6 pathmtu

Syntax **debugging ipv6 pathmtu**

undo debugging ipv6 pathmtu

View User view

Parameters None

Description Use the **debugging ipv6 pathmtu** command to enable IPv6 path maximum transmission unit (PMTU) debugging.

Use the **undo debugging ipv6 pathmtu** command to disable the debugging.

By default, the IPv6 PMTU debugging is disabled.

Examples # Enable PMTU debugging.

```
<Sysname> terminal debugging
% Current terminal debugging is on
<Sysname> debugging ipv6 pathmtu
```

Add a PMTU entry to view the corresponding debugging information.

```
<Sysname> system-view
[Sysname] ipv6 pathmtu 2000::8 1500
*0.85010 Sysname IPV6 PAT/8/Debug_ipv6_pathmtu:
```

```
Information-> Adding PMTU Entry at MultipleIndex,
Value = 4097,
```

// A PMTU entry is added.

```
Prompt-> Successful Addition of PMTU entry
*0.1307224 AR19-62 IPV6PMTU/8/Debug_ipv6_pathmtu:
Information-> Delete PMTU Entry at Multiple Index,
Value = 128,
Prompt-> Successul Deletion of  PMTU Entry
```

// A PMTU entry is deleted.

```
*0.2387611 AR19-62 IPV6PMTU/8/Debug_ipv6_pathmtu:
Information-> Pathmtu Notification UnRegister,
Value = 0,
Prompt-> UnRegistering is Succssful..
```

// A PMTU entry is deregistered at the transport layer.

Table 67 Table 21-4 Description on major fields of the debugging ipv6 pathmtu command

Field	Description
Adding	Add a PMTU entry
Delete	Delete a PMTU entry
Value	PMTU entry index

debugging tcp ipv6

Syntax **debugging tcp ipv6** { **event** | **packet** } [*task-id socket-id*]

undo debugging tcp ipv6 { **event** | **packet** } [*task-id socket-id*]

View User view

Parameters **event**: Enables event debugging.

packet: Enables packet debugging.

task-id socket-id: Task ID and socket ID. All tasks and sockets apply if this argument is not specified.

Description Use the **debugging tcp ipv6** command to enable TCPv6 packet and event debugging for the specified task ID or socket ID.

Use the **undo debugging tcp ipv6** command to disable TCPv6 packet and event debugging.

By default, TCPv6 packet and event debugging is disabled.

The packet debugging displays information of each input and output packet, and the event debugging displays only the TCP packet header information.

Examples # Enable the telnet server function on an IPv6 interface of an IPv6-supported device.

```
<Sysname> telnet server enable
 Telnet server is started!
```

Create a VTY user.

```
<Sysname> user-interface vty 0 4
[Sysname-ui-vty0-4] authentication-mode none
[Sysname-ui-vty0-4] user privilege level 3
```

Enable IPv6 TCP event debugging.

```
<Sysname> terminal debugging
% Current terminal debugging is on
<Sysname> debugging tcp ipv6 event
```

Use the telnet ipv6 function to telnet the local device from another device. The debugging information is displayed as follows:

```
*0.2021569 Sysname IPV6TCP/8/TCP6 EVENT:
956752441: task = VTYD(31), socketid = 0,
TCP6CB 0x03a85a04 created
```

// A TCP control block is created.

```
*0.2021570 Sysname IPV6TCP/8/TCP6 EVENT:
956752441: task = VTYD(31), socketid = 0,
state Closed changed to Listening
```

// The state is changed.

```
*0.2021581 Sysname IPV6TCP/8/TCP6 EVENT:
956752441: task = VTYD(31), socketid = 0,
Received MSS 1440, LA = 5007::100:23, FA = 5007::46:1024
```

// The maximum segment size (MSS) is received from the peer.

```
*0.2021600 Sysname IPV6TCP/8/TCP6 EVENT:
956752441: task = VTYD(31), socketid = 0,
Advertising MSS 1440, LA = 5007::100:23, FA = 5007::46:1024
```

// The local MSS is advertised to the peer.

Enable IPv6 TCP packet debugging.

```
<Sysname> debugging tcp ipv6 packet
*0.2378222 Sysname IPV6TCP/8/TCP6 PACKET:
956752802: Input: task = VTYD(31), socketid = 3, state = Established,
src = 5007::46->1024, dst = 5007::100->23,
seq = 254158666, ack = 255508488, datalen = 1, optlen = 12, flag = ACK PSH,
window = 8192
```

// A packet is received.

```
*0.2378230 Sysname IPV6TCP/8/TCP6 PACKET:
956752802: Output: task = VTYD(31), socketid = 3, state = Established,
src = 5007::100->23, dst = 5007::46->1024,
seq = 255508488, ack = 254158667, datalen = 1, optlen = 12, flag = ACK PSH,
window = 8192
```

// A packet is sent.

Table 68 Table 21-5 Description on fields of the debugging tcp ipv6 command

Field	Description
Task	TCP connection establishment task
Socketid	Socket ID used for establishing a TCP connection
State	TCP connection state
Received MSS	MSS advertised by the peer.
LA	Local IP address and port number
FA	Peer IP address and port number
Advertising	The local end advertises the local information to the peer.
State	Current stat
Src	Source IP address
Dst	Destination IP address
Seq	Packet sequence number
Ack	Packet acknowledgement number
Datalen	Packet data length
Optlen	Packet option length
Flag	Flag bit
Window	Window size

debugging udp ipv6 packet

Syntax **debugging udp ipv6 packet** [*task-id socket-id*]

undo debugging udp ipv6 packet [*task-id socket-id*]

View User view

Parameters *task-id socket-id*: Task ID and socket ID. All tasks and sockets apply if this argument is not specified.

Description Use the **debugging udp ipv6 packet** command to enable IPv6 User Datagram Protocol (UDP) packet debugging.

Use the **undo debugging udp ipv6 packet** command to disable IPv6 UDP packet debugging.

By default, IPv6 UDP packet debugging is disabled.

Examples # Use the tracert ipv6 function to telnet an IPv6-supported device with the interfaces configured with IPv6 IP addresses.

Enable IPv6 UDP packet debugging for all sockets and tasks.

```
<Sysname> debugging udp ipv6 packet
```

Enable IPv6 UDP packet debugging for task 3 and socket 5.

```
<Sysname> debugging udp ipv6 packet 3 5
UDP6:
  IPv6 UDP packet debugging switch is on for task any socket any
  IPv6 UDP packet debugging switch is on for task 3 socket 5
```

Disable IPv6 UDP packet debugging.

```
<Sysname> undo debugging udp ipv6 packet 3 5
*0.3216710 Sysname IPV6UDP/8/debug_case:
956753649: O: task = au0(3), socketid = 2,
src = ::1->30003,
dst = 5007::100->33435, datalen = 12
```

// A UDP packet is output.

```
*0.3216720 Sysname IPV6UDP/8/debug_case:
956753649: I: unreachable port
src = ::1->30003,
dst = 5007::100->33435, datalen = 12
```

// A UDP packet is input.

Table 69 Table 21-6 Field descriptions of the debugging udp ipv6 command

Field	Description
Task	TCP connection establishment task
Socketid	Socket ID used for establishing a TCP connection
Src	Source IP address
Dst	Destination IP address
I	Input packets
O	Output packets
Datalen	Data length

display dns ipv6 dynamic-host

Syntax **display dns ipv6 dynamic-host**

View Any view

Parameters None

Description Use the **display dns ipv6 dynamic-host** command to display IPv6 dynamic domain name cache information.

Examples # Display IPv6 dynamic domain name cache information.

```
<Sysname> display dns ipv6 dynamic-host
No  Host                Ipv6Address     TTL
1       aaa             3001::2         6
```

Table 70 Table 21-7 Description on fields of the display dns ipv6 dynamic-host command

Field	Description
No	Sequence number
Host	Host name
Ipv6Address	IPv6 address of the host
TTL	Time an entry can be cached in seconds

display ipv6 fib

Syntax **display ipv6 fib** [*slot-number*] [*ipv6-address*]

View Any view

Parameters *slot-number*: Number of the slot whose IPv6 forwarding information base (FIB) entries are to be displayed.

ipv6-address: Destination IPv6 address whose IPv6 FIB entries are to be displayed.

Description Use the **display ipv6 fib** command to display IPv6 FIB entries. If no argument is specified, all FIB entries will be displayed.

Examples # Display all IPv6 FIB entries.

```
<Sysname> display ipv6 fib
FIB Table:
 Total number of Routes : 1

Flag:
  U:Useable   G:Gateway   H:Host   B:Blackhole   D:Dynamic   S:Static

Destination:    ::1                      PrefixLength    : 128
NextHop  :  ::1                        Flag            : HU
Label     : NULL                           Tunnel ID   : 0
TimeStamp     : Date- 12/5/2004, Time- 9:15:18
Interface    :  InLoopBack0
```

Table 71 Table 21-8 Description on fields of the display ipv6 fib command

Field	Description
Total number of Routes	Total number of routes in the FIB
Destination	Destination address to which a packet is to be forwarded
PrefixLength	Prefix length of the destination address
NextHop	Next hop of the route to the destination

Table 71 Table 21-8 Description on fields of the display ipv6 fib command

Field	Description
Flag	Route flag: ■ l U - Usable route ■ l G - Gateway route ■ l H - Host route ■ l B - Black hole route ■ l D - Dynamic route ■ l S - Static route
Label	Label
Tunnel ID	ID of a tunnel
TimeStamp	Generation time of a FIB entry
Interface	Outgoing interface that forwards packets

display ipv6 fibcache

Syntax **display ipv6 fibcache** *slot-number*

View Any view

Parameters None

Description Use the **display ipv6 fibcache** command to display the total number of routes in the FIB cache.

Examples # Display the IPv6 FIB information in the cache.

```
<Sysname> display ipv6 fibcache
FIB Cache:
 Total number of Routes : 0
```

display ipv6 host

Syntax **display ipv6 host**

View Any view

Parameters None

Description Use the **display ipv6 host** command to display the mappings between host names and IPv6 addresses in the static DNS database.

Examples

Display the mappings between host names and IPv6 addresses.

```
<Sysname> display ipv6 host
Host                  Age          Flags           IPv6Address
aaa                   0            static           2002::1
bbb                   0            static           2002::2
```

Table 72 Table 21-9 Description on fields of the display ipv6 host command

Field	Description
Host	Host name
Age	Time for the entry to live. "0" is displayed in the case of static configuration.
Flags	Flag indicating the type of mapping between a host name and an IPv6 address. Static indicates a static mapping.
IPv6Address	IPv6 address of a host

display ipv6 interface

Syntax **display ipv6 interface** [*interface-type interface-number* | **brief**]

View Any view

Parameters *interface-type interface-number*: Specifies an interface.

brief: Displays brief IPv6 information of an interface.

Description Use the **display ipv6 interface** command to display the IPv6 information of an interface for which an IPv6 interface can be configured.

When *interface-type interface-number* is not specified, the IPv6 information of all interfaces for which IPv6 addresses can be configured is displayed.

Examples # Display the IPv6 information of an interface.

```
<Sysname> display ipv6 interface vlan-interface 2
Vlan-interface2 current state :DOWN
Line protocol current state :DOWN
IPv6 is enabled, link-local address is FE80::1234:56FF:FE65:4322 [TENTATIVE]
  Global unicast address(es):
    2001::1, subnet is 2001::/64 [TENTATIVE]
  Joined group address(es):
    FF02::1:FF00:1
    FF02::1:FF65:4322
    FF02::2
    FF02::1
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  Hosts use stateless autoconfig for addresses
```

Table 73 Table 21-10 Description on fields of the display ipv6 interface command (on a switch)

Field	Description
Vlan-interface2 current state	Physical state of the interface

Table 73 Table 21-10 Description on fields of the display ipv6 interface command (on a switch)

Field	Description
Line protocol current state	Link layer protocol state of the interface
IPv6 is enabled	IPv6 packet forwarding state of the interface (IPv6 packet forwarding is enabled in the example)
link-local address	Link-local address configured for the interface
Global unicast address(es)	Global unicast address(es) configured for the interface(s)
Joined group address(es)	Address(es) of multicast group(s) that the interface joins
MTU	Maximum transmission unit of the interface
ND DAD is enabled, number of DAD attempts	Number of DAD attempts, with DAD enabled
ND reachable time	Neighbor reachable time
ND retransmit interval	Interval for retransmitting a neighbor solicitation (NS) message
Hosts use stateless autoconfig for addresses	Hosts use stateless auto-configuration mode to acquire IPv6 addresses

Display the brief IPv6 information of all interfaces for which IPv6 addresses can be configured.

```
<Sysname> display ipv6 interface brief
*down: administratively down
(s): spoofing
Interface                 Physical      Protocol        IPv6 Address
Vlan-interface1             down         down            Unassigned
Vlan-interface2             down         down            Unassigned
Vlan-interface100           down         down            Unassigned
```

Table 74 Table 21-11 Description on fields of display ipv6 interface brief (on a switch)

Field	Description
*down	The interface is down, that is, the interface is closed by using the **shutdown** command.
(s)	Spoofing attribute of the interface, that is, the link protocol state of the interface is up, but the link does not exist, or the link is established on demand, instead of being permanent.
Interface	Name of the interface
Physical	Physical state of the interface
Protocol	Link protocol state of the interface
IPv6 Address	IPv6 address of the interface. (If no address is configured for the interface, "Unassigned" will be displayed.)

display ipv6 neighbors

Syntax **display ipv6 neighbors** { { *ipv6-address* | **all** | **dynamic** | **static** } [**slot** *slot-number*] | **interface** *interface-type interface-number* | **vlan** *vlan-id* } [**|** { **begin** | **exclude** | **include** } *text*]

View Any view

Parameters *ipv6-address*: IPv6 address whose neighbor information is to be displayed.

all: Displays information of all neighbors, including neighbors acquired dynamically and configured statically.

dynamic: Displays information of all neighbors acquired dynamically.

static: Displays information of all neighbors configured statically.

slot *slot-number*: Displays information of the neighbors of a specified slot.

interface *interface-type interface-number*: Displays information of the neighbors of a specified interface.

vlan *vlan-id*: Displays information of the neighbors of a specified VLAN.

|: Filters the output information.

begin: Displays the neighbor entries from the first one containing the specified character string.

include: Displays the neighbor entries containing the specified character string.

exclude: Displays the neighbor entries without the specified character string.

text: Character string.

Description Use the **display ipv6 neighbors** command to display neighbor information.

Examples # Display all neighbor information.

```
<Sysname> display ipv6 neighbors all
                Type: S-Static    D-Dynamic
IPv6 Address              Link-layer      VID  Interface  State  T  Age
FE80::200:5EFF:FE32:B800  0000-5e32-b800  100  GE4/2/1    REACH  S   -
```

Table 75 Table 21-12 Description on fields of the display ipv6 neighbors command

Field	Description
IPv6 Address	IPv6 address
Link-layer	Link layer address (MAC address of a neighbor)
VID	VLAN to which the interface connected with a neighbor belongs
Interface	Interface connected with a neighbor

Table 75 Table 21-12 Description on fields of the display ipv6 neighbors command

Field	Description
State	State of a neighbor, including: ■ l INCMP: The address is being resolved. The link layer address of the neighbor is unknown. ■ l REACH: The neighbor is reachable. ■ l STALE: The reachability of the neighbor is unknown. The device will not verify the reachability any longer unless data is sent to the neighbor. ■ l DELAY: The reachability of the neighbor is unknown. The device sends an NS message after a delay. ■ l PROBE: The reachability of the neighbor is unknown. The device sends an NS message to verify the reachability of the neighbor.
T	Type of neighbor information, including static configuration and dynamic acquisition.
Age	For a static entry, a hyphen "-" is displayed. For a dynamic entry, the reachable time (in seconds) elapsed is displayed. Therefore, the aging time can only be displayed after a neighbor goes into the REACH state. If the directly generated ND entry is in the STALE state, "#" is displayed (for a neighbor acquired dynamically).

display ipv6 neighbors count

Syntax **display ipv6 neighbors** { { **all** | **dynamic** | **static** } [**slot** *slot-number*] | **interface** *interface-type interface-number* | **vlan** *vlan-id* } **count**

View Any view

Parameters **all**: Displays the total number of all neighbor entries, including neighbor entries acquired dynamically and configured statically.

dynamic: Displays the total number of all neighbor entries acquired dynamically.

static: Displays the total number of neighbor entries configured statically.

slot *slot-number*: Displays the total number of neighbor entries of a specified slot.

interface *interface-type interface-number*: Displays the total number of neighbor entries of a specified interface.

vlan *vlan-id*: Displays the total number of neighbor entries of a specified VLAN.

Description Use the **display ipv6 neighbors count** command to display the total number of neighbor entries satisfying the specified condition.

Examples # Display the total number of neighbor entries acquired dynamically.

```
<Sysname> display ipv6 neighbors dynamic count
Total dynamic entry(ies):  2
```

display ipv6 pathmtu

Syntax **display ipv6 pathmtu** { *ipv6-address* | **all** | **dynamic** | **static** }

View Any view

Parameters *ipv6-address*: IPv6 address whose PMTU is to be displayed.

all: Displays all PMTU information.

dynamic: Displays all dynamic PMTU information.

dynamic: Displays all static PMTU information.

Description Use the **display ipv6 pathmtu** command to display the PMTU information of IPv6 addresses.

Examples # Display all PMTU values.

```
<Sysname> display ipv6 pathmtu all
Ipv6 Destination Address    ZoneID  PathMTU     Age     Type
 fe80::12                   0       1300            40      Dynamic
 2222::3                    0       1280            -       Static
```

Table 76 Table 21-13 Description on fields of the display ipv6 pathmtu command

Field	Description
Ipv6 Destination Address	Destination IPv6 address
ZoneID	ID of address zone, currently invalid
PathMTU	PMTU of an IPv6 address
Age	Time for a PMTU to live. For a static PMTU, a hyphen "-" is displayed.
Type	Indicates the PMTU is dynamically negotiated or statically configured.

display ipv6 socket

Syntax **display ipv6 socket** [**socktype** *socket-type*] [*task-id socket-id*] [**slot** *slot-number*]

View Any view

Parameters *socket-type*: Type of a socket. The value "1" represents a TCP socket, "2" a UDP socket, and "3" a raw IP socket.

task-id: ID of a task.

socket-id: ID of a socket.

slot-number: Number of a slot.

Description Use the **display ipv6 socket** command to display information about a socket.

Examples # Display the information of a specified socket.

```
<Sysname> display ipv6 socket
SOCK_STREAM:
Task = VTYD(14), socketid = 4, Proto = 6,
LA = ::->22, FA = ::->0,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_ACCEPTCONN SO_REUSEPORT SO_SENDVPNID,
socket state = SS_PRIV SS_ASYNC

Task = VTYD(14), socketid = 3, Proto = 6,
LA = ::->23, FA = ::->0,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_ACCEPTCONN SO_REUSEPORT SO_SENDVPNID,
socket state = SS_PRIV SS_ASYNC

SOCK_DGRAM:
SOCK_RAW:
```

Table 77 Table 21-14 Description on fields of the display ipv6 socket command

Field	Description
SOCK_STREAM	TCP socket
Task	Task ID of the created socket
Socketid	ID assigned by the kernel to the created socket
Proto	Protocol ID
LA	Local address and local port number
FA	Remote address and remote port number
Sndbuf	Size of the send buffer
Rcvbuf	Size of the receive buffer
sb_cc	Number of bytes sent by the send buffer
rb_cc	Number of bytes received by the receive buffer
Socket option	Socket option set by the application
Socket state	State of the socket

display ipv6 statistics

Syntax **display ipv6 statistics** [**slot** *slot-number*]

View Any view

Parameters *slot-number*: Number of a slot.

Description Use the **display ipv6 statistics** command to display statistics of IPv6 packets and IPv6 ICMP packets.

Examples # Display the statistics of IPv6 packets and IPv6 ICMP packets.

```
<Sysname> display ipv6 statistics
  IPv6 Protocol:

    Sent packets:
      Total:      0
        Local sent out:     0            forwarded:         0
        raw packets:             0               discarded:            0
        routing failed:     0            fragments:         0
        fragments failed:        0

    Received packets:
      Total:      0
        local host:         0            hopcount exceeded: 0
        format error:            0            option error:      0
        protocol error:     0            fragments:         0
        reassembled:             0            reassembly failed:    0
        reassembly timeout: 0

  ICMPv6 protocol:

    Sent packets:
      Total:      0
        unreached:          0               too big:               0
        hopcount exceeded:  0               reassembly timeout: 0
        parameter problem:  0
        echo request:       0               echo replied:           0
        neighbor solicit:   0               neighbor advert:       0
        router solicit: 0           router advert:      0
        redirected:     0
      Send failed:
        ratelimited:        0               other errors:       0

    Received packets:
      Total:      0
        checksum error: 0              too short:           0
        bad code:           0
        unreached:          0              too big:             0
        hopcount exceeded:  0              reassembly timeout:  0
        parameter problem:  0              unknown error type:  0
        echoed:         0              echo replied:             0
        neighbor solicit:   0              neighbor advert:     0
        router solicit: 0              router advert:            0
        redirected:     0              router renumbering:  0
        unknown info type:  0
      Deliver failed:
        bad length:         0          ratelimited:         0
```

Table 78 Table 21-15 Description on fields of the display ipv6 statistics command

Field	Description
IPv6 Protocol:	Statistics of IPv6 packets

Table 78 Table 21-15 Description on fields of the display ipv6 statistics command

Field	Description
Sent packets: Total: 0 Local sent out: 0 forwarded: 0 raw packets: 0 discarded: 0 routing failed: 0 fragments: 0 fragments failed: 0	Statistics of sent IPv6 packets, including: ■ l Total number of sent packets ■ l Number of packets sent locally ■ l Number of forwarded packets ■ l Number of packets sent via raw socket ■ l Number of discarded packets ■ l Number of packets failing to be routed ■ l Number of sent fragment packets ■ l Number of fragments failing to be sent
Received packets: Total: 0 local host: 0 hopcount exceeded: 0 format error: 0 option error: 0 protocol error: 0 fragments: 0 reassembled: 0 reassembly failed: 0 reassembly timeout: 0	Statistics of received IPv6 packets, including ■ l Total number of received packets ■ l Number of packets received locally ■ l Number of packets exceeding the hop limit ■ l Number of packets in an incorrect format ■ l Number of packets with incorrect options ■ l Number of packets with incorrect protocol ■ l Number of received fragment packets ■ l Number of reassembled packets ■ l Number of packets failing to be reassembled ■ l Number of packets whose reassembly times out
ICMPv6 protocol:	Statistics of IPv6 ICMP packets

Table 78 Table 21-15 Description on fields of the display ipv6 statistics command

Field	Description
Sent packets: Total: 0 unreached: 0 too big: 0 hopcount exceeded: 0 reassembly timeout: 0 parameter problem: 0 echo request: 0 echo replied: 0 neighbor solicit: 0 neighbor advert: 0 router solicit: 0 router advert 0 redirected: 0 Send failed: ratelimited: 0 other errors: 0	Statistics of sent IPv6 ICMP packets, including ■ l Total number of sent packets ■ l Number of packets whose destination is unreachable ■ l Number of too large packets ■ l Number of packets exceeding the hop limit ■ l Number of packets whose fragmentation and reassembly times out ■ l Number of packets with parameter errors ■ l Number of request packets ■ l Number of response packets ■ l Number of neighbor solicitation packets ■ l Number of neighbor advertisement packets ■ l Number of router solicitation packets ■ l Number of router advertisement packets ■ l Number of redirected packets ■ l Number of packets failing to be sent because of rate limitation ■ l Number of packets with other errors

Table 78 Table 21-15 Description on fields of the display ipv6 statistics command

Field	Description
Received packets: Total: 0 checksum error: 0 too short: 0 bad code 0 unreached: 0 too big: 0 hopcount exceeded: 0 reassembly timeout: 0 parameter problem: 0 unknown error type: 0 echoed: 0 echo replied: 0 neighbor solicit: 0 neighbor advert: 0 router solicit: 0 router advert 0 redirected: 0 router renumbering 0 unknown info type: 0 Deliver failed: bad length: 0 ratelimited: 0	Statistics of received IPv6 ICMP packets, including ■ l Total number of received packets ■ l Number of packets with checksum errors ■ l Number of too small packets ■ l Number of packets with error codes ■ l Number of packets whose destination is unreachable ■ l Number of too large packets ■ l Number of packets exceeding the hop limit ■ l Number of packets whose fragmentation and reassembly times out ■ l Number of packets with parameter errors ■ l Number of packets with unknown errors ■ l Number of request packets ■ l Number of response packets ■ l Number of neighbor solicitation messages ■ l Number of neighbor advertisement packets ■ l Number of router solicitation packets ■ l Number of router advertisement packets ■ l Number of redirected packets ■ l Number of recounted routers ■ l Number of unknown type of packets ■ l Number of packets with a incorrect size ■ l Number of packets failing to be received because of rate limitation

display tcp ipv6 statistics

Syntax **display tcp ipv6 statistics**

View Any view

Parameters None

Description Use the **display tcp ipv6 statistics** command to display IPv6 TCP statistics.

Examples # Display the statistics of received and sent IPv6 TCP packets.

```
<Sysname> display tcp ipv6 statistics
Received packets:
     Total: 0
     packets in sequence: 0 (0 bytes)
     window probe packets: 0, window update packets: 0
     checksum error: 0, offset error: 0, short error: 0

     duplicate packets: 0 (0 bytes), partially duplicate packets: 0 (0 bytes)
     out-of-order packets: 0 (0 bytes)
     packets with data after window: 0 (0 bytes)
     packets after close: 0

     ACK packets: 0 (0 bytes)
     duplicate ACK packets: 0, too much ACK packets: 0

Sent packets:
     Total: 0
     urgent packets: 0
     control packets: 0 (including 0 RST)
     window probe packets: 0, window update packets: 0

     data packets: 0 (0 bytes) data packets retransmitted: 0 (0 bytes)
     ACK only packets: 0 (0 delayed)

Retransmitted timeout: 0, connections dropped in retransmitted timeout: 0
Keepalive timeout: 0, Keepalive probe: 0, keepalive timeout, so connections disco
nnected : 0
Initiated connections: 0, accepted connections: 0, established connections: 0
Closed connections: 0 (dropped: 0, initiated dropped: 0)
```

Table 79 Table 21-16 Description on fields of the display tcp ipv6 statistics command

Field	Description
Received packets:	Statistics of received packets, including
Total: 0	■ l Total number of received packets
packets in sequence: 0 (0 bytes)	■ l Number of packets received in sequence
window probe packets: 0	■ l Number of window probe packets
window update packets: 0	■ l Number of window size update packets
checksum error: 0	■ l Number of packets with checksum errors
offset error: 0	■ l Number of packets with offset errors
short error: 0	■ l Number of packets whose total length is less than specified in the packet header
duplicate packets: 0 (0 bytes), partially duplicate packets: 0 (0 bytes)	■ l Number of duplicate packets ■ l Number of partially duplicate packets
out-of-order packets: 0 (0 bytes)	■ l Number of out-of-order packets
packets with data after window: 0 (0 bytes)	■ l Number of packets exceeding the size of the receiving window
packets after close: 0	■ l Number of packets received after the connection is closed
ACK packets: 0 (0 bytes)	
duplicate ACK packets: 0	■ l Number of ACK packets
too much ACK packets: 0	■ l Number of duplicate/excessive ACK packets

Table 79 Table 21-16 Description on fields of the display tcp ipv6 statistics command

Field	Description
Sent packets:	Statistics of sent packets, including
Total: 0	■ l Total number of packets
urgent packets: 0	■ l Number of packets containing an urgent indicator
control packets: 0 (including 0 RST)	■ l Number of control packets
window probe packets: 0	■ l Number of window probe packets
window update packets: 0	■ l Number of window update packets
data packets: 0 (0 bytes) data	■ l Number of data packets
packets retransmitted: 0 (0 bytes)	■ l Number of retransmitted packets
ACK only packets: 0 (0 delayed)	■ l Number of ACK packets
Retransmitted timeout	Number of packets whose retransmission times out
connections dropped in retransmitted timeout	Number of connections dropped because of retransmission timeout
Keepalive timeout	Number of keepalive timeouts
Keepalive probe	Number of keepalive probes
Keepalive timeout, so connections disconnected	Number of connections dropped because of keepalive response timeout
Initiated connections	Number of initiated connections
accepted connections	Number of accepted connections
established connections	Number of established connections
Closed connections	Number of closed connections
dropped	Number of dropped connections (after SYN is received from the peer)
initiated dropped	Number of initiated but dropped connections (before SYN is received from the peer)

display tcp ipv6 status

Syntax **display tcp ipv6 status**

View Any view

Parameters None

Description Use the **display tcp ipv6** command to display the IPv6 TCP connection status.

Examples # Display the IPv6 TCP connection status.

```
<Sysname> display tcp ipv6 status
TCP6CB       Local Address       Foreign Address      State
045d8074     ::->21                ::->0              Listening
```

Table 80 Table 21-17 Description on fields of the display tcp ipv6 status command

Field	Description
TCP6CB	IPv6 address of the TCP control block (hexadecimal)

Table 80 Table 21-17 Description on fields of the display tcp ipv6 status command

Field	Description
Local Address	Local IPv6 address
Foreign Address	Remote IPv6 address
State	TCP connection status, including ■ l Closed ■ l Listening ■ l Syn_Sent ■ l Syn_Rcvd ■ l Established ■ l Close_Wait ■ l Fin_Wait1 ■ l Closing ■ l Last_Ack ■ l Fin_Wait2 ■ l Time_Wait

display udp ipv6 statistics

Syntax **display udp ipv6 statistics**

View Any view

Parameters None

Description Use the **display udp ipv6 statistics** command to display statistics of IPv6 UDP packets.

Examples # Display statistics information of IPv6 UDP packets.

```
<Sysname> display udp ipv6 statistics
Received packets:
     Total: 0
     checksum error: 0
     shorter than header: 0, data length larger than packet: 0
     unicast(no socket on port): 0
     broadcast/multicast(no socket on port): 0
     not delivered, input socket full: 0
     input packets missing pcb cache: 0
Sent packets:
     Total: 0
```

Table 81 Table 21-18 Description on fields of the display udp ipv6 statistics command

Field	Description
Total	Total number of received/sent packets
checksum error	Total number of packets with a checksum error
shorter than header	Total number of IPv6 UDP packets whose total length is less than specified by the packet header

Table 81 Table 21-18 Description on fields of the display udp ipv6 statistics command

Field	Description
data length larger than packet	Total number of packets whose data length exceeds that specified by the packet header
unicast(no socket on port)	Total number of unicast packets without any socket received on a port
broadcast/multicast(no socket on port)	Total number of broadcast/multicast packets without any socket received on a port
not delivered, input socket full	Number of packets not handled because of the receive buffer being full
input packet missing pcb cache	Number of packets failing to match the PCB cache

dns server ipv6

Syntax **dns server ipv6** *ipv6-address* [*interface-type interface-number*]

undo dns server ipv6 *ipv6-address* [*interface-type interface-number*]

View System view

Parameters *ipv6-address*: IPv6 address of a DNS server.

interface-type interface-number: Specifies an interface. When the IPv6 address of the DNS server is a link-local address, this argument must be specified.

Description Use the **dns server ipv6** command to configure an IPv6 address for a DNS server.

Use the **undo dns server ipv6** command to remove the configured DNS server.

By default, no DNS server is configured.

Examples # Configure the IPv6 address 2002::1 for a DNS server.

```
<Sysname> system-view
[Sysname] dns server ipv6 2002::1
```

ipv6 (System view)

Syntax **ipv6**

undo ipv6

View System view

Parameters None

Description Use the **ipv6** command to enable the IPv6 packet forwarding function.

Use the **undo ipv6** command to disable the IPv6 packet forwarding function.

By default, the IPv6 packet forwarding function is disabled.

Examples # Enable the IPv6 packet forwarding function.

```
<Sysname> system-view
[Sysname] ipv6
```

ipv6 address (Interface view)

Syntax **ipv6 address** { *ipv6-address prefix-length* | *ipv6-address***/***prefix-length* }

undo ipv6 address [*ipv6-address prefix-length* | *ipv6-address***/***prefix-length*]

View Interface view

Parameters *ipv6-address*: IPv6 address.

prefix-length: Prefix length of an IPv6 address.

Description Use the **ipv6 address** command to configure a site-local address or global unicast address for an interface.

Use the **undo ipv6 address** command to remove the manually configured interface address.

By default, no site-local address or global unicast address is configured for an interface.

Note that you will remove all IPv6 addresses except the automatically configured link-local address if you carry out the **undo ipv6 address** command without any parameter specified.

Examples # Set the global unicast address of the interface VLAN-interface 1 to 2001::1/64.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ipv6 address 2001::1/64
```

ipv6 address auto link-local (Interface view)

Syntax **ipv6 address auto link-local**

undo ipv6 address auto link-local

View Interface view

Parameters None

Description Use the **ipv6 address auto link-local** command to automatically generate a link-local address for an interface.

Use the **undo ipv6 address auto link-local** command to remove the automatically generated link-local address for an interface.

By default, no link-local address is automatically generated for an interface.

Examples # Configure the interface VLAN-interface 1 to automatically generate a link-local address.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ipv6 address auto link-local
```

ipv6 address eui-64 (Interface view)

Syntax **ipv6 address** *ipv6-address*/*prefix-length* **eui-64**

undo ipv6 address *ipv6-address*/*prefix-length* **eui-64**

View Interface view

Parameters *ipv6-address*/*prefix-length*: IPv6 address and IPv6 prefix. The *ipv6-address* and *prefix-length* arguments jointly specify the prefix of an IPv6 address in the EUI-64 format.

Description Use the **ipv6 address eui-64** command to configure a site-local address or global unicast address in the EUI-64 format for an interface.

Use the **undo ipv6 address eui-64** command to remove the configured site-local address or global unicast address in the EUI-64 format for an interface.

By default, no site-local or global unicast address in EUI-64 format is configured for an interface.

Examples # Configure an IPv6 address in EUI-64 format for the interface VLAN-interface 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ipv6 address 2001::1/64 eui-64
```

ipv6 address link-local (Interface view)

Syntax **ipv6 address** *ipv6-address* **link-local**

undo ipv6 address *ipv6-address* **link-local**

View Interface view

Parameters *ipv6-address*: IPv6 link-local address. The first ten bits of an address must be 1111111010 (binary), that is, the first group of hexadecimals in the address must be FE80 to FEBF.

Description Use the **ipv6 address link-local** command to configure a link-local address manually for a specified interface. Use the **undo ipv6 address link-local** command to remove the configured link-local address for an interface.

Examples # Configure a link-local address for the interface VLAN-interface 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ipv6 address fe80::1 link-local
```

ipv6 fibcache

Syntax **ipv6 fibcache** { *slot-number* | **all** }

undo ipv6 fibcache { *slot-number* | **all** }

View System view

Parameters *slot-number*: Slot number.

all: Specifies all slots.

Description Use the **ipv6 fibcache** command to enable the caching function of the IPv6 FIB.

Use the **undo ipv6 fibcache** command to disable the caching function of the IPv6 FIB.

By default, the caching function of the IPv6 FIB is disabled.

Note that the caching function of the IPv6 FIB is valid only for packets to be forwarded.

Examples # Enable the caching function of the IPv6 FIB.

```
<Sysname> system-view
[Sysname] ipv6 fibcache all
```

ipv6 fib-loadbalance-type hash-based

Syntax **ipv6 fib-loadbalance-type hash-based**

undo ipv6 fib-loadbalance-type hash-based

View System view

Parameters None

Description Use the **ipv6 fib-loadbalance-type hash-based** command to specify the load sharing mode based on the HASH algorithm for packet forwarding.

Use the **undo ipv6 fib-loadbalance-type hash-based** command to restore the load sharing mode to the default.

By default, the load sharing based on polling is adopted, that is, each equal cost multi-path (ECMP) route is used in turn to forward packets.

Examples # Specify the load sharing mode based on the HASH algorithm for packet forwarding.

```
<Sysname> system-view
[Sysname] ipv6 fib-loadbalance-type hash-based
```

ipv6 host

Syntax **ipv6 host** *hostname ipv6-address*

undo ipv6 host *hostname* [*ipv6-address*]

View System view

Parameters *hostname*: Host name, a character string containing letters, numerals, "_", "-", or "." and must contain at least one letter.

ipv6-address: IPv6 address.

Description Use the **ipv6 host** command to configure the mappings between host names and IPv6 addresses.

Use the **undo ipv6 host** command to remove the mappings between host names and IPv6 addresses.

Each host name can correspond to only one IPv6 address.

Examples # Configure the mapping between a host name and an IPv6 address.

```
<Sysname> system-view
[Sysname] ipv6 host aaa 2001::1
```

ipv6 icmp-error

Syntax **ipv6 icmp-error** { **bucket** *bucket-size* | **ratelimit** *interval* } *

undo ipv6 icmp-error

View System view

Parameters *bucket-size*: Number of tokens in a token bucket.

interval: Update period of the token bucket in milliseconds. The update period "0" indicates that the number of ICMPv6 error packets sent is not restricted.

Description Use the **ipv6 icmp-error** command to configure the maximum number of ICMPv6 error packets that can be sent within the specified period.

Use the **undo ipv6 icmp-error** command to restore the default size and update period of the token bucket.

By default, the size is 10 and the update period is 100 milliseconds. That is, at most 10 IPv6 ICMP error packets can be sent within these 100 milliseconds.

Examples # Set the capacity of the token bucket to 50 and the update period to 100 milliseconds.

```
<Sysname> system-view
[Sysname] ipv6 icmp-error bucket 50 ratelimit 100
```

ipv6 mtu (Interface view)

Syntax **ipv6 mtu** *mtu-size*

undo ipv6 mtu

View Interface view

Parameters *mtu-size*: Size of the maximum transmission units (MTUs) of an interface in bytes.

Description Use the **ipv6 mtu** command to set the MTU of IPv6 packets sent over an interface.

Use the **undo ipv6 mtu** command to restore the default.

Examples # Set the MTU of IPv6 packets sent over the interface VLAN-interface 12 to 1,280 bytes.

```
<Sysname> system-view
[Sysname] interface vlan-interface 12
[Sysname-Vlan-interface12] ipv6 mtu 1280
```

ipv6 nd autoconfig managed-address-flag

Syntax **ipv6 nd autoconfig managed-address-flag**

undo ipv6 nd autoconfig managed-address-flag

View Interface view

Parameters None

Description Use the **ipv6 nd autoconfig managed-address-flag** command to set the managed address configuration (M) flag to 1 so that the host can acquire an IPv6 address through stateful auto-configuration (for example, DHCP server).

Use the **undo ipv6 nd autoconfig managed-address-flag** command to restore the M flag to the default value "0" so that the host can acquire an IPv6 address through stateless auto-configuration.

By default, the M flag is set to **0**.

Examples # Configure the host to acquire an IPv6 address through stateful auto-configuration.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ipv6 nd autoconfig managed-address-flag
```

ipv6 nd autoconfig other-flag

Syntax **ipv6 nd autoconfig other-flag**

undo ipv6 nd autoconfig other-flag

View Interface view

Parameters None

Description Use the **ipv6 nd autoconfig other-flag** command to set the other stateful configuration flag (O) flag to 1 so that the host can acquire information other than IPv6 address through stateful auto-configuration (for example, DHCP server).

Use the **undo ipv6 nd autoconfig other-flag** command to remove the setting so that the host can acquire other information through stateless auto-configuration.

By default, the O flag is set to **0**.

Examples # Configure the host to acquire information other than IPv6 address through stateless auto-configuration.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] undo ipv6 nd autoconfig other-flag
```

ipv6 nd dad attempts

Syntax **ipv6 nd dad attempts** *value*

undo ipv6 nd dad attempts

View Interface view

Parameters *value*: Number of attempts to send a neighbor solicitation message for DAD. The default value is **1**. When it is set to **0**, the DAD is disabled.

Description Use the **ipv6 nd dad attempts** command to configure the number of attempts to send a neighbor solicitation message for DAD.

Use the **undo ipv6 nd dad attempts** command to restore the default.

By default, the number of attempts to send a neighbor solicitation message for DAD is 1.

Examples # Set the number of attempts to send a neighbor solicitation message for DAD to 20.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ipv6 nd dad attempts 20
```

ipv6 nd hop-limit

Syntax **ipv6 nd hop-limit** *value*

undo ipv6 nd hop-limit

View System view

Parameters *value*: Number of hops. When it is set to **0**, the Cur Hop Limit field in RA messages sent by the device is **0**. That is, the number of hops is determined by the host itself, but not specified by the device.

Description Use the **ipv6 nd hop-limit** command to configure the hop limit advertised by the device.

Use the **undo ipv6 nd hop-limit** command to restore the default.

By default, the hop limit advertised by the device is 64.

Examples # Set the hop limit advertised by the device to 100.

```
<Sysname> system-view
[Sysname] ipv6 nd hop-limit 100
```

ipv6 nd ns retrans-timer

Syntax **ipv6 nd ns retrans-timer** *value*

undo ipv6 nd ns retrans-timer

View Interface view

Parameters *value*: Interval for sending NS messages in milliseconds.

Description Use the **ipv6 nd ns retrans-timer** command to set the interval for sending NS messages. The local interface sends NS messages at intervals of this value. Furthermore, the Retrans Timer field in RA messages sent by the local interface is equal to this value.

Use the **undo ipv6 nd ns retrans-timer** command to restore the default interval.

By default, the local interface sends NS messages at intervals of 1,000 milliseconds and the Retrans Timer field in RA messages sent by the local interface is 0.

Examples # Specify Vlan-interface100 to send NS messages at intervals of 10,000 milliseconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ipv6 nd ns retrans-timer 10000
```

ipv6 nd nud reachable-time

Syntax **ipv6 nd nud reachable-time** *value*

undo ipv6 nd nud reachable-time

View Interface view

Parameters *value*: Neighbor reachable time in milliseconds.

Description Use the **ipv6 nd nud reachable-time** command to configure the neighbor reachable time on an interface. This time value serves as not only the neighbor reachable time on the local interface, but also the value of the Reachable Timer field in RA messages sent by the local interface.

Use the **undo ipv6 nd nud reachable-time** command to restore the default neighbor reachable time and to specify the value of the Reachable Timer field in RA messages as 0 so that the number of hops is determined by the host itself, but not specified by the device.

By default, the neighbor reachable time on the local interface is 30,000 milliseconds and the Reachable Timer field in RA messages is 0.

Examples # Set the neighbor reachable time on the interface VLAN-interface 1 to 10,000 milliseconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ipv6 nd nud reachable-time 10000
```

ipv6 nd ra halt

Syntax **ipv6 nd ra halt**

undo ipv6 nd ra halt

View Interface view

Parameters None

Description Use the **ipv6 nd ra halt** command to suppress RA messages.

Use the **undo ipv6 nd ra halt** command to disable the RA message suppression.

By default, RA messages are suppressed.

Examples # Suppress RA messages on the interface VLAN-interface 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ipv6 nd ra halt
```

ipv6 nd ra interval

Syntax **ipv6 nd ra interval** *max-interval-value min-interval-value*

undo ipv6 nd ra interval

View Interface view

Parameters *max-interval-value*: Maximum interval for advertising RA messages in seconds.

min-interval-value: Minimum interval for advertising RA messages in seconds.

Description Use the **ipv6 nd ra interval** command to set the maximum and minimum interval for advertising RA messages. The device advertises RA messages at intervals of a random value between the maximum interval and the minimum interval.

Use the **undo ipv6 nd ra interval** command to restore the default.

By default, the maximum interval between RA messages is 600 seconds, and the minimum interval is 200 seconds.

Note the following:

- l The minimum interval should be three-fourths of the maximum interval or less.
- l The maximum interval for sending RA messages should be less than or equal to the router lifetime in RA messages.

Examples # Set the maximum interval for advertising RA messages to 1,000 seconds and the minimum interval to 700 seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ra interval 1000 700
```

ipv6 nd ra prefix

Syntax **ipv6 nd ra prefix** { *ipv6-address prefix-length* | *ipv6-address/prefix-length* } *valid-lifetime preferred-lifetime* [**no-autoconfig** | **off-link**] *

undo ipv6 nd ra prefix *ipv6-prefix*

View Interface view

Parameters *ipv6-address*: IPv6 address or IPv6 address prefix.

prefix-length: Prefix length of an IPv6 address.

ipv6-prefix: IPv6 address prefix.

valid-lifetime: Valid lifetime of a prefix in seconds.

preferred-lifetime: Preferred lifetime of a prefix used for stateless auto-configuration in seconds.

no-autoconfig: Specifies a prefix not to be used for stateless auto-configuration. If this keyword is not provided, the prefix is used for stateless auto-configuration.

off-link: Specifies the address with the prefix not to be directly reachable on the link. If this keyword is not provided, the address with the prefix is directly reachable on the link.

Description Use the **ipv6 nd ra prefix** command to configure the prefix information in RA messages.

Use the **undo ipv6 nd ra prefix** command to remove the prefix information from RA messages.

By default, no prefix information is configured in RA messages and the IPv6 address of the interface is used as the prefix information.

Examples # Configure the prefix information for RA messages on the interface VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ra prefix 2001:10::100/64 100 10
[Sysname-Ethernet1/0] ipv6 nd ra prefix 2001:10::100/64 100 10
```

ipv6 nd ra router-lifetime

Syntax **ipv6 nd ra router-lifetime** *value*

undo ipv6 nd ra router-lifetime

View Interface view

Parameters *value*: Routing device lifetime in seconds. When it is set to **0**, the device does not serve as the default routing device.

Description Use the **ipv6 nd ra router-lifetime** command to configure the routing device lifetime in RA messages.

Use the **undo ipv6 nd ra router-lifetime** command to restore the default.

By default, the routing device lifetime in RA messages is 1,800 seconds.

Note that the routing device lifetime in RA messages should be greater than or equal to the advertising interval.

Examples # Set the routing device lifetime in RA messages on the interface VLAN-interface 1 to 1,000 seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ipv6 nd ra router-lifetime 1000
```

ipv6 neighbor

Syntax **ipv6 neighbor** *ipv6-address mac-address* { *vlan-id port-type port-number* | **interface** *interface-type interface-number* }

undo ipv6 neighbor *ipv6-address interface-type interface-number*

View System view

Parameters *ipv6-address*: IPv6 address in a static neighbor entry.

mac-address: Link layer address in a static neighbor entry (48 bits long, in the format of H-H-H).

vlan-id: VLAN ID in a static neighbor entry.

port-type port-number: Type and number of a Layer 2 port in a static neighbor entry.

interface-type interface-number: Type and number of a Layer 3 interface in a static neighbor entry.

Description Use the **ipv6 neighbor** command to configure a static neighbor entry.

Use the **undo ipv6 neighbor** command to remove a static neighbor entry.

Note that you can adopt the IPv6 address and link layer address of the Layer 3 VLAN interface or those of the VLAN port to configure a static neighbor entry.

- l If a static neighbor entry is configured by using the first method, the neighbor entry is in the INCMP state. After the device obtains the corresponding Layer 2 VLAN port information through resolution, the neighbor entry will go into the REACH state.
- l If a static neighbor entry is configured by using the second method, the corresponding VLAN interface must exist and the port specified by *port-type port-number* must belong to the VLAN specified by *vlan-id*. After a static neighbor entry is configured, the device will relate the VLAN interface with the IPv6 address to identify a static neighbor entry uniquely and the entry will be in the REACH state.

You only need to specify the corresponding VLAN interface before removing a static neighbor entry.

Examples # Configure a static neighbor entry for layer 2 port Ethernet 4/1/1 of VLAN 1.

```
<Sysname> system-view
[Sysname] ipv6 neighbor 2000::1 fe-e0-89 1 ethernet4/1/1
```

ipv6 neighbors max-learning-num

Syntax **ipv6 neighbors max-learning-num** *number*

undo ipv6 neighbors max-learning-num

View Interface view

Parameters *number*: Maximum number of neighbors that can be dynamically learned by an interface.

Description Use the **ipv6 neighbors max-learning-num** command to configure the maximum number of neighbors that can be dynamically learned on a specified interface.

Use the **undo ipv6 neighbors max-learning-num** command to restore the default.

By default, the maximum number of neighbors that can be dynamically learned on an interface is 1024.

Examples # Set the maximum number of neighbors that can be dynamically learned on the interface VLAN-interface 1 to 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ipv6 neighbors max-learning-num 10
```

ipv6 pathmtu

Syntax **ipv6 pathmtu** *ipv6-address* [*value*]

undo ipv6 pathmtu *ipv6-address*

View System view

Parameters *ipv6-address*: Specified IPv6 address.

value: PMTU of a specified IPv6 address in bytes.

Description Use the **ipv6 pathmtu** command to configure a static PMTU for a specified IPv6 address.

Use the **undo ipv6 pathmtu** command to remove the PMTU configuration for a specified IPv6 address.

By default, no static PMTU is configured.

Examples # Configure a static PMTU for a specified IPv6 address.

```
<Sysname> system-view
[Sysname] ipv6 pathmtu fe80::12 1300
```

ipv6 pathmtu age

Syntax **ipv6 pathmtu age** *age-time*

undo ipv6 pathmtu age

View System view

Parameters *age-time*: Aging time for PMTU in minutes.

Description Use the **ipv6 pathmtu age** command to configure the aging time for a dynamic PMTU.

Use the **undo ipv6 pathmtu age** command to restore the default.

By default, the aging time is 10 minutes.

Note that the aging time is invalid for a static PMTU.

Related commands: **display ipv6 pathmtu**.

Examples # Set the aging time for a dynamic PMTU to 40 minutes.

```
<Sysname> system-view
[Sysname] ipv6 pathmtu age 40
```

reset dns ipv6 dynamic-host

Syntax **reset dns ipv6 dynamic-host**

View User view

Parameters None

Description Use the **reset dns ipv6 dynamic-host** command to clear IPv6 dynamic domain name cache information.

Examples # Clear IPv6 dynamic domain name cache information.

```
<Sysname> reset dns ipv6 dynamic-host
```

reset ipv6 fibcache

Syntax **reset ipv6 fibcache** { *slot-number* | **all** }

View User view

Parameters *slot-number*: Slot number.

all: All slots.

Description Use the **reset ipv6 fibcache** command to clear IPv6 FIB cache entries.

Examples # Clear FIB cache entries.

```
<Sysname> reset ipv6 fibcache
```

reset ipv6 neighbors

Syntax **reset ipv6 neighbors** { **all** | **dynamic** | **interface** *interface-type interface-number* | **slot** *slot-number* | **static** }

View User view

Parameters **all**: Clears the static and dynamic neighbor information on all interfaces.

dynamic: Clears the dynamic neighbor information on all interfaces.

interface *interface-type interface-number*: Clears dynamic neighbor information on a specified interface.

slot *slot-number*: Clears the dynamic neighbor information on a specified slot.

static: Clears the static neighbor information on all interfaces.

Description Use the **reset ipv6 neighbors** command to clear corresponding IPv6 neighbor information.

Examples # Clear neighbor information on all interfaces.

```
<Sysname> reset ipv6 neighbors all
```

reset ipv6 pathmtu

Syntax **reset ipv6 pathmtu** { **all** | **static** | **dynamic** }

View User view

Parameters **all**: Clears all PMTUs.

static: Clears all static PMTUs.

dynamic: Clears all dynamic PMTUs.

Description Use the **reset ipv6 pathmtu** the command to clear the corresponding PMTU information.

Examples # Clear all PMTUs.

```
<Sysname> reset ipv6 pathmtu all
```

reset ipv6 statistics

Syntax **reset ipv6 statistics** [**slot** *slot-number*]

View User view

Parameters *slot number*: Slot number.

Description Use the **reset ipv6 statistics** command to clear the statistics of IPv6 packets.

Examples # Clear the statistics of IPv6 packets.

```
<Sysname> reset ipv6 statistics
```

reset tcp ipv6 statistics

Syntax **reset tcp ipv6 statistics**

View User view

Parameters None

Description Use the **reset tcp ipv6 statistics** command to clear the statistics of all IPv6 TCP connections.

Examples # Clear the statistics of all IPv6 TCP connections.

```
<Sysname> reset tcp ipv6 statistics
```

reset udp ipv6 statistics

Syntax **reset udp ipv6 statistics**

View User view

Parameters None

Description Use the **reset udp ipv6 statistics** command to clear the statistics of all IPv6 UDP packets.

Examples # Clear the statistics of all IPv6 UDP packets.

```
<Sysname> reset udp ipv6 statistics
```

tcp ipv6 timer fin-timeout

Syntax **tcp ipv6 timer fin-timeout** *wait-time*

undo tcp ipv6 timer fin-timeout

View System view

Parameters *wait-time*: Length of the finwait timer for IPv6 TCP connections in seconds.

Description Use the **tcp ipv6 timer fin-timeout** command to set the finwait timer for IPv6 TCP connections.

Use the **undo tcp ipv6 timer fin-timeout** command to restore the default.

By default, the length of the finwait timer is 675 seconds.

Examples # Set the finwait timer length of IPv6 TCP connections to 800 seconds.

```
<Sysname> system-view
[Sysname] tcp ipv6 timer fin-timeout 800
```

tcp ipv6 timer syn-timeout

Syntax **tcp ipv6 timer syn-timeout** *wait-time*

undo tcp ipv6 timer syn-timeout

View System view

Parameters *wait-time*: Length of the synwait timer for IPv6 TCP connections in seconds.

Description Use the **tcp ipv6 timer syn-timeout** command to set the synwait timer for IPv6 TCP connections

Use the **undo tcp ipv6 timer syn-timeout** command to restore the default.

By default, the length of the synwait timer of IPv6 TCP connections is 75 seconds.

Examples # Set the synwait timer length of IPv6 TCP connections to 100 seconds.

```
<Sysname> system-view
[Sysname] tcp ipv6 timer syn-timeout 100
```

tcp ipv6 window

Syntax **tcp ipv6 window** *size*

undo tcp ipv6 window

View System view

Parameters *size*: Size of the IPv6 TCP packet buffer in KB (kilobyte).

Description Use the **tcp ipv6 window** command to set the size of the IPv6 TCP packet buffer.

Use the **undo tcp ipv6 window** command to restore the default.

By default, the size of the IPv6 TCP packet buffer is 8 KB.

Examples # Set the size of the IPv6 TCP packet buffer to 4 KB.

```
<Sysname> system-view
[Sysname] tcp ipv6 window 4
```

27 IP PERFORMANCE CONFIGURATION COMMANDS

debugging fib errmsg

Syntax **debugging fib errmsg**

undo debugging fib errmsg

View User view

Parameters None

Description Use the **debugging fib errmsg** command to enable FIB error debugging.

Use the **undo debugging fib errmsg** command disable FIB error debugging.

By default, FIB error debugging is disabled.

Examples # Enable FIB error debugging.

```
<Sysname> terminal debugging
<Sysname> debugging fib errmsg
```

debugging fib synmsg

Syntax **debugging fib synmsg**

undo debugging fib synmsg

View User view

Parameters None

Description Use the **debugging fib synmsg** command to enable debugging for FIB entry synchronization information.

Use the **undo debugging fib synmsg** command to disable debugging for FIB entry synchronization information.

By default, debugging is disabled for FIB entry synchronization information.

Examples # Enable debugging for FIB entry synchronization information.

```
<Sysname> terminal debugging
<Sysname> debugging fib synmsg
```

debugging fib rtmsg

Syntax **debugging fib rtmsg**

undo debugging fib rtmsg

View User view

Parameters None

Description Use the **debugging fib rtmsg** command to enable FIB entry operation debugging.

Use the **undo debugging fib rtmsg** command to disable FIB entry operation debugging.

By default, FIB entry operation debugging is disabled.

Examples # Enable FIB entry operation debugging.

```
<Sysname> terminal debugging
<Sysname> debugging fib rtmsg
```

debugging ip error

Syntax **debugging ip error**

undo debugging ip error

View User view

Parameters None

Description Use the **debugging ip error** command to enable IP forwarding error debugging.

Use the **undo debugging ip error** command to disable IP forwarding error debugging.

By default, IP forwarding error debugging is disabled.

Examples # Enable IP forwarding error debugging.

```
<Sysname> terminal debugging
<Sysname> debugging ip error
```

debugging ip icmp

Syntax **debugging ip icmp**

undo debugging ip icmp

View User view

Parameters None

Description Use the **debugging ip icmp** command to enable ICMP debugging.

Use the **undo debugging ip icmp** command to disable ICMP debugging.

By default, ICMP debugging is disabled.

Table 82 Description on fields of the debugging ip icmp command

Field	Description
ICMP Send	Operation of sending ICMP packets
ICMP Receive	Operation of receiving ICMP packets
Type	ICMP packet type
Code	ICMP packet code
Src	Source IP address
Dst	Destination IP address

Examples # Enable ICMP debugging and execute a ping operation.

```
<Sysname> terminal debugging
<Sysname> debugging ip icmp
<Sysname> ping 10.1.1.2
*Dec 30 11:18:36:659 2006 Sysname IPDBG/7/debug_icmp:
ICMP Send: echo(Type=8, Code=0), Dst = 10.1.1.2
```

// An ICMP packet with destination IP address 10.1.1.2 is sent.

```
*Dec 30 11:18:37:789 2006 Sysname IPDBG/7/debug_icmp:Slot=3;
ICMP Receive: echo-reply(Type=0, Code=0), Src = 10.1.1.2, Dst = 10.1.1.1
```

// An ICMP packet with source IP address 10.1.1.2 and destination IP address 10.1.1.1 is received.

debugging ip packet

Syntax **debugging ip packet** [**acl** *acl-number*]

undo debugging ip packet

View User view

Parameters *acl-number*: ACL number, specifying an ACL to match specific IP packets for which debugging information is displayed.

Description Use the **debugging ip packet** command to enable IP packet debugging.

Use the **undo debugging ip packet** command to disable IP packet debugging.

By default, IP packet debugging is disabled.

Table 83 Description on fields of the debugging ipv6 packet command

Field	Description
Sending	Operation of sending packets
Receiving	Operation of receiving packets
Delivering	The packet is delivered from the IP layer to the upper layer
interface	Receiving/transmitting interface
version	IP protocol version
headlen	Length of the packet header
tos	Type of service
pktlen	Total length of the packet
pktid	Packet identifier
offset	Offset
ttl	TTL
protocol	Protocol
checksum	Checksum
s	Source IP address
d	Destination IP address
prompt	Prompt message

Examples # Enable IP packet debugging and execute a ping operation.

```
<Sysname> terminal debugging
<Sysname> debugging ip packet
<Sysname> ping 10.1.1.2
*Dec 30 11:19:11:661 2006 Sysname IPFWD/7/debug_case:
Sending, interface = Vlan-interface100, version = 4, headlen = 20, tos = 0,
pktlen = 84, pktid = 2521, offset = 0, ttl = 255, protocol = 1,
checksum = 39883, s = 10.1.1.1, d = 10.1.1.2
prompt: Sending the packet from local at Vlan-interface100
```

// The packet is sent.

```
*Dec 30 11:19:11:925 2006 Sysname IPFWD/7/debug_case:Slot=4;
Receiving, interface = Vlan-interface100, version = 4, headlen = 20, tos = 0,
pktlen = 84, pktid = 2525, offset = 0, ttl = 255, protocol = 1,
checksum = 39879, s = 10.1.1.2, d = 10.1.1.1
prompt: Receiving IP packet from Vlan-interface100
```

// The packet is received.

```
*Dec 30 11:19:12:301 2006 Sysname IPDBG/7/debug_case:Slot=4;
Delivering, interface = Vlan-interface100, version = 4, headlen = 20
, tos = 0,
```

```
pktlen = 84, pktid = 2525, offset = 0, ttl = 255, protocol = 1,
checksum = 39879, s = 10.1.1.2, d = 10.1.1.1
prompt: IP packet is delivering up!
```

// The received packet is delivered to the upper layer for processing.

debugging tcp event

Syntax **debugging tcp event** [*task-id socket-id slot-number*]

undo debugging tcp event [*task-id socket-id slot-number*]

View User view

Parameters *task-id*: Task ID.

socket-id: Socket ID.

slot-number: Slot number.

Description Use the **debugging tcp event** command to enable TCP event debugging.

Use the **undo debugging tcp event** command to disable TCP event debugging.

By default, TCP event debugging is disabled.

Table 84 Description on fields of the debugging tcp event command

Field	Description
task	Task ID for establishing a TCP connection
socketid	Socket ID for establishing a TCP connection
state	TCP connection state
received MSS	Maximum segment size (MSS) that the peer end advertises to the local end
LA	Local IP address and port number
FA	Peer IP address and port number
advertising	Maximum segment size that the local end advertises to the peer end

Examples # Enable telnet server.

```
<Sysname> system-view
[Sysname] telnet server enable
```

Create a VTY user.

```
[Sysname] user-interface vty 0 4
[Sysname-ui-vty0-4] authentication-mode none
[Sysname-ui-vty0-4] user privilege level 3
```

Enable TCP event debugging.

```
<Sysname> terminal debugging
<Sysname> debugging tcp event
```

Telnet to the local device from another device. The debugging information on the local device is displayed as follows.

```
*Dec 30 11:19:50:967 2006 Sysname SOCKET/7/TCP EVENT:
1141227210: task = VTYD(38), socketid = 0,
TCPCB 0x06af1204 created
```

// A TCP control block is created.

```
*Dec 30 11:19:51:111 2006 Sysname SOCKET/7/TCP EVENT:
1141227210: task = VTYD(38), socketid = 0,
state Closed changed to Listening
```

// The TCP connection state is changed from Closed to Listening.

```
*Dec 30 11:19:51:270 2006 Sysname SOCKET/7/TCP EVENT:
1141227210: task = VTYD(38), socketid = 0,
received MSS = 1460,
LA = 10.1.1.1:23, FA = 10.1.1.2:1025
```

// The local end receives the MSS advertised by the peer end.

```
*Dec 30 11:19:51:460 2006 Sysname SOCKET/7/TCP EVENT:
1141227210: task = VTYD(38), socketid = 0,
state Listening changed to Syn_Rcvd
```

// The TCP connection state is changed from Listening to Syn_Rcvd.

```
*Dec 30 11:19:51:620 2006 Sysname SOCKET/7/TCP EVENT:
1141227210: task = VTYD(38), socketid = 0,
advertising MSS = 1460,
LA = 10.1.1.1:23, FA = 10.1.1.2:1025
```

// The local end advertises the MSS to the peer end.

```
*Dec 30 11:19:51:820 2006 Sysname SOCKET/7/TCP EVENT:
1141227210: task = VTYD(38), socketid = 3,
state Syn_Rcvd changed to Established
```

// The TCP connection state is changed from Syn_Rcvd to Established.

debugging tcp md5

Syntax **debugging tcp md5**

undo debugging tcp md5

View User view

Parameters None

Description Use the **debugging tcp md5** command to enable MD5 authentication debugging for TCP connections.

Use the **undo debugging tcp md5** command to disable MD5 authentication debugging for TCP connections.

By default, MD5 authentication debugging is disabled for TCP connections.

Examples # Enable MD5 authentication debugging for TCP connections.

```
<Sysname> terminal debugging
<Sysname> debugging tcp md5
```

debugging tcp packet

Syntax **debugging tcp packet** [*task-id socket-id slot-number*]

undo debugging tcp packet [*task-id socket-id slot-number*]

View User view

Parameters *task-id*: Task ID.

socket-id: Socket ID.

slot-number: Slot number.

Description Use the **debugging tcp packet** command to enable TCP packet debugging.

Use the **undo debugging tcp packet** command to disable TCP packet debugging.

By default, TCP packet debugging is disabled.

Table 85 Description on fields of the debugging tcp packet command

Field	Description
task	Task ID
socketid	Socket ID
state	Current TCP connection state
src	Source IP address
dst	Destination IP address
seq	Sequence number
ack	Acknowledgement sequence number
optlen	Length of packet data
flag	Flag bit
window	Buffer size

Examples # Enable telnet server.

```
<Sysname> system-view
[Sysname] telnet server enable
```

Create a VTY user.

```
[Sysname] user-interface vty 0 4
[Sysname-ui-vty0-4] authentication-mode none
[Sysname-ui-vty0-4] user privilege level 3
```

Enable TCP packet debugging.

```
<Sysname> terminal debugging
<Sysname> debugging tcp packet
```

Telnet to the local device from another device. The debugging information on the local device is displayed as follows.

```
*Dec 30 11:20:23:347 2006 Sysname SOCKET/7/TCP PACKET:
1141233312: Input: task = VTYD(38), socketid = 1, state = Listening,
src = 10.1.1.2:1026, dst = 10.1.1.1:23,
seq = 948064152, ack = 0, optlen = 4, flag = SYN,
window = 8192
```

// A TCP packet is received. The current TCP connection state is Listening.

```
*Dec 30 11:20:23:630 2006 Sysname SOCKET/7/TCP PACKET:
1141233312: Output: task = VTYD(38), socketid = 0, state = Syn_Rcvd,
src = 10.1.1.1:23, dst = 10.1.1.2:1026,
seq = 994298079, ack = 948064153, optlen = 4, flag = ACK SYN,
window = 8192
```

// A TCP packet is sent. The current TCP connection state is Syn_Rcvd.

debugging udp packet

Syntax **debugging udp packet** [*task-id socket-id slot-number*]

undo debugging udp packet [*task-id socket-id slot-number*]

View User view

Parameters *task-id*: Task ID.

socket-id: Socket ID.

slot-number: Slot number.

Description Use the **debugging udp packet** command to enable UDP packet debugging.

Use the **undo debugging udp packet** command to disable UDP packet debugging.

By default, UDP packet debugging is disabled.

Table 86 Description on fields of the debugging udp packet command

Field	Description
task	Task ID
socketid	Socket ID
src	Source IP address and source UDP port number
dst	Destination IP address and destination UDP port number
datalen	Data length of the UDP packet

Examples # Enable UDP packet debugging and execute a tftp operation.

```
<Sysname> terminal debugging
<Sysname> debugging udp packet
<Sysname> tftp 192.168.0.66 get 1.txt
*Aug 3 06:05:25:800 2006 Sysname SOCKET/7/UDP:
1141236065: Output: task = co0(1), socketid = 1,
src = 192.168.0.62:1025, dst = 192.168.0.66:69, datalen = 14
```

display fib

Syntax **display fib** [**|** { **begin** | **include** | **exclude** } *text* | **acl** *acl-number* | **ip-prefix** *ip-prefix-name*]

View Any view

Parameters **|** { **begin** | **include** | **exclude** } *text*: Displays FIB information in the buffer related to the specified string according to a regular expression.

- The **begin** keyword specifies to display from the first FIB entry that contains the specified string *text*.
- The **include** keyword specifies to display only the FIB entries that include the specified string *text*.
- The **exclude** keyword specifies to display only the FIB entries that do not include the specified string *text*.
- The *text* argument is a string.

acl *acl-number*: Displays FIB information matching a specified ACL numbered from 2000 to 2999.

ip-prefix *ip-prefix-name*: Displays FIB information matching a specified IP prefix list, a string of 1 to 19 characters.

Description Use the **display fib** command to display FIB forwarding information. If no parameters are specified, all FIB information will be displayed.

Examples # Display all FIB information.

```
<Sysname> display fib
FIB Table:
Total number of Routes : 2
```

```
Flag:
  U:Useable   G:Gateway   H:Host   B:Blackhole   D:Dynamic   S:Static
  R:Reject   L:Generated by ARP or ESIS

Destination/Mask    Nexthop     Flag     TimeStamp      Interface   Token
127.0.0.0/8     127.0.0.1   U    t[1141138116]  InLoop0     invalid
127.0.0.1/32        127.0.0.1   HU   t[1141138116]  InLoop0     invalid
```

Table 87 Description on fields of the display fib command

Field	Description
Total number of Routes	Total number of routes in the FIB table
Destination/Mask	Destination address/length of mask
Nexthop	Address of next hop
Flag	Flags of routes: ■ U"-Usable route ■ G"-Gateway route ■ H"-Host route ■ B"-Blackhole route ■ D"-Dynamic route ■ S"-Static route ■ R"-Refused route ■ L"-Route generated by ARP or ESIS
TimeStamp	Time stamp
Interface	Forwarding interface
Token	LSP index number

Display FIB information matching ACL 2000

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 10.2.0.0 0.0.255.255
[Sysname-acl-basic-2000] display fib acl 2000
Route entry matched by access-list 2000:
Summary counts: 1
Flag:
  U:Useable   G:Gateway   H:Host   B:Blackhole   D:Dynamic   S:Static
  R:Reject   L:Generated by ARP or ESIS
Destination/Mask    Nexthop     Flag     TimeStamp      Interface   Token
10.2.1.1/32     127.0.0.1    HU  t[1150900568]  InLoop0     invalid
```

Display all entries starting from the one that contains the string "127".

```
<Sysname> display fib | begin 127
Flag:
  U:Useable   G:Gateway   H:Host   B:Blackhole   D:Dynamic   S:Static
  R:Reject   L:Generated by ARP or ESIS

Destination/Mask    Nexthop     Flag     TimeStamp      Interface   Token
10.2.1.1/32     127.0.0.1    HU  t[1150900568]  InLoop0     invalid
127.0.0.0/8     127.0.0.1    U   t[1150623094]  InLoop0     invalid
127.0.0.1/32        127.0.0.1    HU  t[1150623094]  InLoop0     invalid
```

For description about the above output, refer to Table 87.

display fib ip-address

Syntax **display fib** *ip-address1* [{ *mask1* | *mask-length1* } [*ip-address2* { *mask2* | *mask-length2* } | **longer**] | **longer**]

View Any view

Parameters *ip-address1, ip-address2*: Destination IP address, in dotted decimal notation. *ip-address1* and *ip-address2* together determine an address range for the FIB entries to be displayed.

mask1, mask2: IP address mask.

mask-length1, mask-length2: Length of IP address mask.

longer: Displays FIB entries that match the specified address/mask and have masks longer than or equal to the mask that a user enters. If no masks are specified, FIB entries that match the natural network address and have the masks longer than or equal to the natural mask will be displayed.

Description Use the **display fib** *ip-address* command to display FIB entries that match the specified destination IP address.

Examples # Display the FIB entries that match the natural network of 10.1.0.0 and have the masks longer than or equal to the natural mask.

```
<Sysname> display fib 10.1.0.0 longer
  Route Entry Count: 1
 Flag:
  U:Useable   G:Gateway   H:Host   B:Blackhole   D:Dynamic   S:Static
  R:Reject   L:Generated by ARP or ESIS
Destination/Mask    Nexthop     Flag     TimeStamp      Interface   Token
10.1.1.1/32     127.0.0.1   HU   t[1141140133]  InLoop0     invalid
```

For description about the above output, refer to Table 87.

display fib statistics

Syntax **display fib statistics**

View Any view

Parameters None

Description Use the **display fib statistics** command to display statistics about the FIB entries.

Examples # Display statistics about the FIB entries.

```
<Sysname> display fib statistics
Route Entry Count          : 2
```

Table 88 Description on fields of the display fib statistics command

Field	Description
Route Entry Count	Number of FIB entries

display icmp statistics

Syntax **display icmp statistics** [**slot** *slot-number*]

View Any view

Parameters *slot-number*: Number of a slot.

Description Use the **display icmp statistics** command to display ICMP statistics.

Related commands: **display ip interface** (in *IP Addressing Commands* of *IP Services Volume*) and **reset ip statistics**.

Examples # Display ICMP statistics.

```
<Sysname> display icmp statistics
  Input: bad formats   0                  bad checksum            0
         echo          5                  destination unreachable 0
         source quench 0                  redirects               0
         echo reply    10                 parameter problem       0
         timestamp     0                  information request     0
         mask requests 0                  mask replies            0
         time exceeded 0
  Output:echo          10                 destination unreachable 0
         source quench 0                  redirects               0
         echo reply    5                  parameter problem       0
         timestamp     0                  information reply       0
         mask requests 0                  mask replies            0
         time exceeded 0
```

Table 89 Description on fields of the display icmp statistics command

Field	Description
bad formats	Number of input wrong format packets
bad checksum	Number of input wrong checksum packets
echo	Number of input/output echo packets
destination unreachable	Number of input/output destination unreachable packets
source quench	Number of input/output source quench packets
redirects	Number of input/output redirection packets
echo reply	Number of input/output replies
parameter problem	Number of input/output parameter problem packets
timestamp	Number of input/output time stamp packets
information request	Number of input information request packets
mask requests	Number of input/output mask requests

Table 89 Description on fields of the display icmp statistics command

Field	Description
mask replies	Number of input/output mask replies
information reply	Number of output information reply packets
time exceeded	Number of input/output expiration packets

display ip socket

Syntax **display ip socket** [**socktype** *sock-type*] [*task-id socket-id*] [**slot** *slot-number*]

View Any view

Parameters *sock-type*: Type of socket, in the range of 1 to 3, corresponding to TCP, UDP and raw IP respectively.

task-id: Task ID.

socket-id: Socket ID.

slot-number: Slot number.

Description Use the **display ip socket** command to display socket information.

Examples # Display all socket information.

```
<Sysname> display ip socket
SOCK_STREAM:
Task = LDP(89), socketid = 2, Proto = 6,
LA = 0.0.0.0:646, FA = 0.0.0.0:0,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_ACCEPTCONN SO_REUSEADDR SO_REUSEPORT SO_SENDVPNID(0),
socket state = SS_PRIV SS_ASYNC

SOCK_DGRAM:
Task = DHCP(59), socketid = 2, Proto = 17,
LA = 0.0.0.0:67, FA = 0.0.0.0:0,
sndbuf = 9216, rcvbuf = 41600, sb_cc = 0, rb_cc = 0,
socket option = SO_BROADCAST SO_REUSEPORT SO_UDPCHECKSUM,
socket state = SS_PRIV SS_ASYNC

Task = LDP(89), socketid = 1, Proto = 17,
LA = 0.0.0.0:646, FA = 0.0.0.0:0,
sndbuf = 9216, rcvbuf = 41600, sb_cc = 0, rb_cc = 0,
socket option = SO_REUSEADDR SO_UDPCHECKSUM SO_SENDVPNID(0),
socket state = SS_PRIV SS_ASYNC

Task = RDSO(74), socketid = 1, Proto = 17,
LA = 0.0.0.0:1024, FA = 0.0.0.0:0,
sndbuf = 9216, rcvbuf = 41600, sb_cc = 0, rb_cc = 0,
socket option = SO_UDPCHECKSUM,
socket state = SS_PRIV

Task = LSSO(72), socketid = 1, Proto = 17,
LA = 0.0.0.0:1645, FA = 0.0.0.0:0,
sndbuf = 9216, rcvbuf = 41600, sb_cc = 0, rb_cc = 0,
socket option = SO_UDPCHECKSUM,
```

```
socket state = SS_PRIV

Task = LSSO(72), socketid = 2, Proto = 17,
LA = 0.0.0.0:1646, FA = 0.0.0.0:0,
sndbuf = 9216, rcvbuf = 41600, sb_cc = 0, rb_cc = 0,
socket option = SO_UDPCHECKSUM,
socket state = SS_PRIV

SOCK_RAW:
Task = DHCP(59), socketid = 1, Proto = 1,
LA = 0.0.0.0, FA = 0.0.0.0,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = 0,
socket state = SS_PRIV SS_ASYNC

Task = ROUT(83), socketid = 2, Proto = 65,
LA = 0.0.0.0, FA = 0.0.0.0,
sndbuf = 32767, rcvbuf = 256000, sb_cc = 0, rb_cc = 0,
socket option = 0,
socket state = SS_PRIV SS_NBIO SS_ASYNC

Task = ROUT(83), socketid = 1, Proto = 2,
LA = 0.0.0.0, FA = 0.0.0.0,
sndbuf = 32767, rcvbuf = 256000, sb_cc = 0, rb_cc = 0,
socket option = SO_SENDVPNID(0),
socket state = SS_PRIV SS_NBIO SS_ASYNC

Task = RSVP(88), socketid = 1, Proto = 46,
LA = 0.0.0.0, FA = 0.0.0.0,
sndbuf = 4194304, rcvbuf = 4194304, sb_cc = 0, rb_cc = 0,
socket option = 0,
socket state = SS_PRIV SS_NBIO SS_ASYNC
```

Table 90 Description on fields of the display ip socket command

Field	Description
SOCK_STREAM	TCP socket
SOCK_DGRAM	UDP socket
SOCK_RAW	raw IP socket
Task	Task number
Socketid	Socket ID
Proto	Protocol number of the socket
LA	Local address and local port number
FA	Remote address and remote port number
Sndbuf	sending buffer size of the socket
Rcvbuf	receiving buffer size of the socket
sb_cc	Current data size in the sending buffer (It is available only for TCP that can buffer data)
rb_cc	Data size currently in the receiving buffer
socket option	Socket option
socket state	Socket state

display ip statistics

Syntax **display ip statistics** [**slot** *slot-number*]

View Any view

Parameters *slot-number*: Slot number.

Description Use the **display ip statistics** command to display statistics of IP packets.

Related commands: **display ip interface** (in *IP Addressing Commands* of *IP Services Volume*) and **reset ip statistics**.

Examples # Display statistics of IP packets.

```
<Sysname> display ip statistics
  Input:    sum            0                local             0
            bad protocol   0                bad format        0
            bad checksum   0                bad options       0
  Output:   forwarding     0                local             1
            dropped        0                no route          1
            compress fails 0
  Fragment:input           0                output            0
            dropped        0
            fragmented     0                couldn't fragment 0
  Reassembling:sum         0                timeouts          0
```

Table 91 Description on fields of the display ip statistics command

Field		Description
Input:	sum	Total number of packets received
	local	Total number of packets with destination being local
	bad protocol	Total number of unknown protocol packets
	bad format	Total number of packets with incorrect format
	bad checksum	Total number of packets with incorrect checksum
	bad options	Total number of packets with incorrect option
Output:	forwarding	Total number of packets forwarded
	local	Total number of packets sent from the local
	dropped	Total number of packets discarded
	no route	Total number of packets for which no route is available
	compress fails	Total number of packets failed to compress
Fragment:	input	Total number of fragments received
	output	Total number of fragments sent
	dropped	Total number of fragments dropped
	fragmented	Total number of packets successfully fragmented
	couldn't fragment	Total number of packets that can't be fragmented
Reassembling	sum	Total number of packets reassembled
	timeouts	Total number of reassembly timeout fragments

display tcp statistics

Syntax **display tcp statistics**

View Any view

Parameters None

Description Use the **display tcp statistics** command to display statistics of TCP traffic.

Related commands: **display tcp status** and **reset tcp statistics**.

Examples # Display statistics of TCP traffic.

```
<Sysname> display tcp statistics
Received packets:
     Total: 0
     packets in sequence: 0 (0 bytes)
     window probe packets: 0, window update packets: 0
     checksum error: 0, offset error: 0, short error: 0

     duplicate packets: 0 (0 bytes), partially duplicate packets: 0 (0 bytes)
     out-of-order packets: 0 (0 bytes)
     packets of data after window: 0 (0 bytes)
     packets received after close: 0

     ACK packets: 0 (0 bytes)
     duplicate ACK packets: 0, too much ACK packets: 0

Sent packets:
     Total: 0
     urgent packets: 0
     control packets: 0 (including 0 RST)
     window probe packets: 0, window update packets: 0

     data packets: 0 (0 bytes) data packets retransmitted: 0 (0 bytes)
     ACK-only packets: 0 (0 delayed)

Retransmitted timeout: 0, connections dropped in retransmitted timeout: 0
Keepalive timeout: 0, keepalive probe: 0, Keepalive timeout, so connections disco
nnected : 0
Initiated connections: 0, accepted connections: 0, established connections: 0
Closed connections: 0 (dropped: 0, initiated dropped: 0)
Packets dropped with MD5 authentication: 0
Packets permitted with MD5 authentication: 0
```

Table 92 Description on fields of the display tcp statistics command

Field		Description
Received packets:	Total	Total number of packets received
	packets in sequence	Number of packets arriving in sequence
	window probe packets	Number of window probe packets received
	window update packets	Number of window update packets received
	checksum error	Number of checksum error packets received
	offset error	Number of offset error packets received
	short error	Number of received packets with length being too small
	duplicate packets	Number of completely duplicate packets received
	partially duplicate packets	Number of partially duplicate packets received
	out-of-order packets	Number of out-of-order packets received
	packets of data after window	Number of packets outside the receiving window
	packets received after close	Number of packets that arrived after connection is closed
	ACK packets	Number of ACK packets received
	duplicate ACK packets	Number of duplicate ACK packets received
	too much ACK packets	Number of ACK packets for data unsent
Sent packets:	Total	Total number of packets sent
	urgent packets	Number of urgent packets sent
	control packets	Number of control packets sent
	window probe packets	Number of window probe packets sent; in the brackets are resent packets
	window update packets	Number of window update packets sent
	data packets	Number of data packets sent
	data packets retransmitted	Number of data packets retransmitted
	ACK-only packets: 40	Number of ACK packets sent; in brackets are delayed ACK packets
Retransmitted timeout		Number of retransmission timer timeouts
connections dropped in retransmitted timeout		Number of connections broken due to retransmission timeouts
Keepalive timeout		Number of keepalive timer timeouts
keepalive probe		Number of keepalive probe packets sent
Keepalive timeout, so connections disconnected		Number of connections broken due to keepalive probe failures
Initiated connections		Number of connections initiated
accepted connections		Number of connections accepted
established connections		Number of connections established
Closed connections		Number of connections closed; in brackets are connections closed accidentally (before receiving SYN from the peer) and connections closed initiatively (after receiving SYN from the peer)

Table 92 Description on fields of the display tcp statistics command

Field	Description
Packets dropped with MD5 authentication	Number of packets dropped with MD5 authentication
Packets permitted with MD5 authentication	Number of packets permitted with MD5 authentication

display tcp status

Syntax **display tcp status**

View Any view

Parameters None

Description Use the **display tcp status** command to display status of all TCP connection for monitoring TCP connections.

Examples # Display status of all TCP connections

```
<Sysname> display tcp status
*: TCP MD5 Connection
TCPCB           Local Add:port      Foreign Add:port        State
0690bac4      0.0.0.0:646          0.0.0.0:0            Listening
```

Table 93 Description on fields of the display tcp status command

Field	Description
*	If the status information of a TCP connection contains *, the TCP adopts the MD5 algorithm for authentication.
TCPCB	TCP control block
Local Add:port	Local IP address and port number
Foreign Add:port	Remote IP address and port number
State	State of the TCP connection

display udp statistics

Syntax **display udp statistics**

View Any view

Parameters None

Description Use the display udp statistics command to display statistics of UDP packets.

Related commands: **reset udp statistics**.

Examples # Display statistics of UDP packets.

```
<Sysname> display udp statistics
Received packets:
     Total: 0
     checksum error: 0
     shorter than header: 0, data length larger than packet: 0
     unicast(no socket on port): 0
     broadcast/multicast(no socket on port): 0
     not delivered, input socket full: 0
     input packets missing pcb cache: 0
Sent packets:
     Total: 1
```

Table 94 Description on fields of the display udp statistics command

Table 95	Field	Description
Received packet:	Total	Total number of UDP packets received
	checksum error	Total number of packets with incorrect checksum
	shorter than header	Number of packets with data shorter than head
	data length larger than packet	Number of packets with data longer than packet
	unicast(no socket on port)	Number of unicast packets with no socket on port
	broadcast/multicast(no socket on port)	Number of broadcast/multicast packets without socket on port
	not delivered, input socket full	Number of packets not delivered to upper layer due to socket buffer being full
	input packets missing pcb cache	Number of packets without matching PCB cache
Sent packet:	Total	Total number of UDP packets sent

ip forward-broadcast (interface view)

Syntax **ip forward-broadcast** [**acl** *acl-number*]

undo ip forward-broadcast

View VLAN/POS/tunnel interface view

Parameters *acl-number*: Number of an ACL from 2000 to 3999. From 2000 to 2999 are numbers for basic ACLs, and from 3000 to 3999 are numbers for advanced ACLs. Only directed broadcasts permitted by the ACL can be forwarded.

Description Use the **ip forward-broadcast** command to enable the interface to forward directed broadcasts.

Use the **undo ip forward-broadcast** command to disable an interface from forwarding directed broadcasts.

By default, an interface is disabled from forwarding directed broadcasts.

Examples # Allow VLAN interface2 to forward directed broadcasts permitted by ACL 2001.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ip forward-broadcast acl 2001
```

ip forward-broadcast (system view)

Syntax **ip forward-broadcast**

undo ip forward-broadcast

View System view

Parameters None

Description Use the **ip forward-broadcast** command to enable the device to forward directed broadcasts.

Use the **undo ip forward-broadcast** command to disable the device from forwarding directed broadcasts.

By default, the device is disabled from forwarding directed broadcasts in system view.

Examples # Enable the device to forward directed broadcasts in system view.

```
<Sysname> system-view
[Sysname] ip forward-broadcast
```

ip redirects enable

Syntax **ip redirects enable**

undo ip redirects

View System view

Parameters None

Description Use the **ip redirects enable** command to allow sending ICMP redirection packets.

Use the **undo ip redirects** command to disable sending ICMP redirection packets.

This feature is enabled by default.

Examples # Disable sending ICMP redirection packets.

```
<Sysname> system-view
[Sysname] undo ip redirects
```

ip ttl-expires enable

Syntax **ip ttl-expires enable**

undo ip ttl-expires

View System view

Parameters None

Description Use the **ip ttl-expires enable** command to enable the sending of ICMP timeout packets.

Use the **undo ip ttl-expires** command to disable sending ICMP timeout packets.

Sending ICMP timeout packets is enabled by default.

If the feature is disabled, the device will not send TTL timeout ICMP packets, but still send "reassembly timeout" ICMP packets.

Examples # Disable sending ICMP timeout packets.

```
<Sysname> system-view
[Sysname] undo ip ttl-expires
```

ip unreachables enable

Syntax **ip unreachables enable**

undo ip unreachables

View System view

Parameters None

Description Use the **ip unreachables enable** command to enable the sending of ICMP destination unreachable packets.

Use the **undo ip unreachables** command to disable sending ICMP destination unreachable packets.

Sending ICMP destination unreachable packets is enabled by default.

If the feature is disabled, the device will not send network unreachable and source route failure ICMP packets, but still send other destination unreachable ICMP packets.

Examples # Disable sending ICMP destination unreachable packets.

```
<Sysname> system-view
[Sysname] undo ip unreachables
```

reset ip statistics

Syntax **reset ip statistics** [**slot** *slot-number*]

View User view

Parameters **slot** *slot-number*: Clears IP packet statistics on the specified slot.

Description Use the **reset ip statistics** command to clear statistics of IP packets.

Related commands: **display ip interface** (in *IP Addressing Commands* of *IP Services Volume*) and **display ip statistics**.

Examples # Clear statistics of IP packets.

```
<Sysname> reset ip statistics
```

reset tcp statistics

Syntax **reset tcp statistics**

View User view

Parameters None

Description Use the **reset tcp statistics** command to clear statistics of TCP traffic.

Related commands: **display tcp statistics**.

Examples # Display statistics of TCP traffic.

```
<Sysname> reset tcp statistics
```

reset udp statistics

Syntax **reset udp statistics**

View User view

Parameters None

Description Use the **reset udp statistics** command to clear statistics of UDP traffic.

Examples # Display statistics of UDP traffic.

```
<Sysname> reset udp statistics
```

tcp mss

Syntax **tcp mss** *value*

undo tcp mss

View POS/tunnel interface view

Parameters *value*: TCP maximum segment size (MSS) in bytes.

Description Use the **tcp mss** command to configure the TCP MSS.

Use the **undo tcp mss** command to restore the default.

As the default MTU on an interface is 1500 bytes, and there are link layer cost and IP packet header, so the recommended TCP MSS is about 1,200 bytes.

By default, the TCP MSS is 1,460 bytes.

Examples # Set the TCP MSS to 1300 bytes on interface POS4/1/4.

```
<Sysname> system-view
[Sysname] interface pos 4/1/4
[Sysname-Pos4/1/4] tcp mss 1300
```

tcp timer fin-timeout

Syntax **tcp timer fin-timeout** *time-value*

undo tcp timer fin-timeout

View System view

Parameters *time-value*: Length of the TCP finwait timer in seconds.

Description Use the **tcp timer fin-timeout** command to configure the length of the TCP finwait timer.

Use the **undo tcp timer fin-timeout** command to restore the default.

By default, the length of the finwait timer is 675 seconds.

Note that the actual length of the finwait timer is determined by the following formula:

Actual length of the finwait timer = (Configured length of the finwait timer - 75) + configured length of the synwait timer

Related commands: **tcp timer syn-timeout** and **tcp window**.

Examples # Set the length of the TCP finwait timer to 800 seconds.

```
<Sysname> system-view
[Sysname] tcp timer fin-timeout 800
```

tcp timer syn-timeout

Syntax **tcp timer syn-timeout** *time-value*

undo tcp timer syn-timeout

View System view

Parameters *time-value*: Length of the TCP finwait timer in seconds.

Description Use the **tcp timer syn-timeout** command to configure the length of the TCP synwait timer.

Use the **undo tcp timer syn-timeout** command to restore the default.

By default, the length of the TCP synwait timer is 75 seconds.

Related commands: **tcp timer fin-timeout** and **tcp window**.

Examples # Set the length of the TCP synwait timer to 80 seconds.

```
<Sysname> system-view
[Sysname] tcp timer syn-timeout 80
```

tcp window

Syntax **tcp window** *window-size*

undo tcp window

View System view

Parameters *window-size*: Receiving/sending buffer size of TCP connection in KB.

Description Use the **tcp window** command to configure the receiving/sending buffer size of TCP connection.

Use the **undo tcp window** command to restore the default.

The TCP receiving/sending buffer is 8 KB by default.

Related commands: **tcp timer fin-timeout** and **tcp timer syn-timeout**.

Examples # Configure the receiving/sending buffer of TCP connection as 3 KB.

```
<Sysname> system-view
[Sysname] tcp window 3
```

28 ROUTING POLICY CONFIGURATION COMMANDS

apply as-path

Syntax **apply as-path** *as-number*&<1-10> [**replace**]

undo apply as-path

View Routing policy view

Parameters *as-number*: Autonomous system number.

&<1-10>: Indicates you can enter *as-number* up to 10 times.

replace: Replaces the original AS number.

Description Use the **apply as-path** command to apply the specified AS numbers to BGP routes.

Use the **undo apply as-path** command to remove the clause configuration.

No AS_PATH attribute is set by default.

With the **replace** keyword, using the **apply as-path** command replaces the original AS_PATH attribute with specified AS numbers. Without the **replace** keyword, using this command adds the specified AS numbers before the original AS_PATH attribute.

Examples # Create routing policy "policy1" with node 10, matching mode as permit. If BGP routing information matches AS-path-ACL 1, add AS number 200 before the original AS_PATH attribute.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match as-path 1
[Sysname-route-policy] apply as-path 200
```

apply comm-list delete

Syntax **apply comm-list** *comm-list-number* **delete**

undo apply comm-list

View Routing policy view

Parameters *comm-list-number*: Community list number. The basic community list number ranges from 1 to 99. The advanced community list number ranges from 100 to 199.

Description Use the **apply comm-list delete** command to remove community attributes in BGP routing information specified by the community list.

Use the **undo apply comm-list** command to remove the clause configuration.

No community attributes are removed by default.

Examples # Create routing policy "policy1" with node 10, matching mode as permit. If BGP routing information matches AS-path-ACL 1, remove community attributes specified in community list 1.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match as-path 1
[Sysname-route-policy] apply comm-list 1 delete
```

apply community

Syntax **apply community** { **none** | **additive** | { *community-number*&<1-16> | *aa:nn*&<1-16> | **internet** | **no-export-subconfed** | **no-export** | **no-advertise** } * [**additive**] }

undo apply community

View Routing policy view

Parameters **none**: Removes community attributes of BGP routes.

community-number: Community sequence number.

aa:nn: Community number.

&<1-16>: Indicates the argument before it can be entered up to 16 times.

internet: Sets the **internet** community attribute for matched BGP routes. Routes with this attribute are advertised to all BGP peers.

no-export-subconfed: Sets the **no-export-subconfed** community attribute for matched BGP routes. Routes with this attribute are not advertised out the sub autonomous system.

no-advertise: Sets the **no-advertise** community attribute for matched BGP routes. Routes with this attribute are not advertised to any peers.

no-export: Sets the **no-export** community attribute for matched BGP routes. Routes with this attribute are not advertised out the autonomous system or confederation, but can be advertised to other sub ASs in the confederation.

additive: Adds the specified community attribute to the original community attribute of a matched BGP route.

Description Use the **apply community** command to set the specified community attribute for BGP routes.

Use the **undo apply community** command to remove the apply clause.

No community attribute is set by default.

Related commands: **ip community-list**, **if-match community**, **route-policy**.

Examples # Create routing policy "setcommunity" with node 16 with matching mode as permit. Set the no-export community attribute for BGP routes passing AS-path-ACL 8.

```
<Sysname> system-view
[Sysname] route-policy setcommunity permit node 16
[Sysname-route-policy] if-match as-path 8
[Sysname-route-policy] apply community no-export
```

apply cost

Syntax **apply cost** [**+** | **-**] *value*

undo apply cost

View Routing policy view

Parameters **+**: Increases cost value.

+: Decreases cost value.

cost: Cost for routing information.

Description Use the **apply cost** command to set a cost for routing information.

Use the **undo apply cost** command to remove the clause configuration.

No cost is set for routing information by default.

Related commands: **if-match interface**, **if-match acl**, **if-match ip-prefix**, **if-match ip next-hop**, **if-match cost**, **if-match tag**, **route-policy**, **apply ip-address next-hop**, **apply local-preference**, **apply origin** and **apply tag**.

Examples # Create routing policy "policy1" with node 10, matching mode as permit. If a route matches the outbound Vlan-interface100, set the cost for the route to 120.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match interface vlan-interface 100
[Sysname-route-policy] apply cost 120
```

apply cost-type

Syntax **apply cost-type** { **external** | **internal** | **type-1** | **type-2** }

undo apply cost-type

View Routing policy view

Parameters **external**: IS-IS external route.

internal: IS-IS internal route.

type-1: Type-1 external route of OSPF.

type-2: Type-2 external route of OSPF.

Description Use the **apply cost-type** command to set a cost type for routing information.

Use the **undo apply cost-type** command to remove the clause configuration.

No cost type is set for routing information by default.

Examples # Create routing policy "policy1" with node 10, matching mode as permit. If a route matches tag 8, set the cost type for the route to IS-IS internal route.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match tag 8
[Sysname-route-policy] apply cost-type internal
```

apply extcommunity

Syntax **apply extcommunity** { **rt** *route-target* }&<1-16> [**additive**]

undo apply extcommunity

View Routing policy view

Parameters **rt** *route-target*: Sets the route target extended community attribute. *route-target* has two forms:

16-bit AS number: 32-bit self-defined number, for example, 101:3;

32-bit IP address: 16-bit self-defined number, for example, 192.168.122.15:1.

&<1-16>: Indicates the argument before it can be entered up to 16 times.

additive: Adds to the original community attribute of a route..

Description Use the **apply extcommunity** command to apply the specified extended community attribute to BGP routes.

Use the **undo apply extcommunity** command to remove the clause configuration.

No extended community attribute is set for routing information by default.

Examples # Create routing policy "policy1" with node 10, matching mode as permit. If a BGP route matches AS-path-ACL 1, add the RT extended community attribute 100:2 to the route.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match as-path 1
[Sysname-route-policy] apply extcommunity rt 100:2 additive
```

apply isis

apply isis { **level-1** | **level-1-2** | **level-2** }

undo apply isis

View Routing policy view

Parameters **level-1**: Redistributes routes into IS-IS level-1 area.

level-2: Redistributes routes into IS-IS level-2 area.

level-1-2: Redistributes routes into both IS-IS level-1 and level-2 areas.

Description Use the **apply isis** command to redistribute routes into a specified ISIS level.

Use the **undo apply isis** command to remove the clause configuration.

No level is set by default.

Related commands: **if-match interface**, **if-match acl**, **if-match ip-prefix**, **if-match ip next-hop**, **if-match cost**, **if-match tag**, **route-policy**, **apply cost**, **apply origin** and **apply tag**.

Examples # Create routing policy "policy1" with node 10, matching mode as permit. If a route matches tag 8, redistribute the route to IS-IS level-2 area.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match tag 8
[Sysname-route-policy] apply isis level-2
```

apply local-preference

Syntax **apply local-preference** *preference*

undo apply local-preference

View Routing policy view

Parameters *preference*: BGP local preference.

Description Use the **apply local-preference** command to apply the specified local preference to BGP routes.

Use the **undo apply local-preference** command to remove the clause configuration.

No local preference is set for BGP routing information by default.

Related commands: **route-policy**.

Examples # Create routing policy "policy1" with node 10, matching mode as permit. If a route matches AS-path-ACL 1, set the local preference for the route to 130.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match as-path 1
[Sysname-route-policy] apply local-preference 130
```

apply mpls-label

Syntax **apply mpls-label**

undo apply mpls-label

View Routing policy view

Parameters None

Description Use the **apply mpls-label** command to set MPLS label for routing information.

Use the **undo apply mpls-label** command to remove the clause configuration.

No MPLS label is set by default.

If MPLS label failed to apply, the routing information can not be advertised.

Examples # Create routing policy "policy1" with node 10, matching mode as permit. If a route matches AS-path-ACL 1, set MPLS label for the route.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match as-path 1
[Sysname-route-policy] apply mpls-label
```

apply origin

Syntax **apply origin** { **igp** | **egp** *as-number* | **incomplete** }

undo apply origin

View Routing policy view

Parameters **igp**: Sets the origin of BGP routing information to IGP.

egp: Sets the origin of BGP routing information to EGP.

as-number: Autonomous system number for EGP routes.

incomplete: Sets the origin of BGP routing information to unknown.

Description Use the **apply origin** command to apply the specified origin attribute to BGP routes.

Use the **undo apply origin** command to remove the clause configuration.

No origin attribute is set for routing information by default.

Related commands: **if-match interface**, **if-match acl**, **if-match ip-prefix**, **if-match ip next-hop**, **if-match cost**, **if-match tag**, **route-policy**, **apply ip-address next-hop**, **apply local-preference**, **apply cost** and **apply tag**.

Examples # Create routing policy "policy1" with node 10, matching mode as permit. If a route matches AS-path-ACL 1, set the origin for the route to IGP.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match as-path 1
[Sysname-route-policy] apply origin igp
```

apply preference

Syntax **apply preference** *preference*

undo apply preference

View Routing policy view

Parameters *preference*: Routing preference.

Description Use the **apply preference** command to set a preference for a routing protocol.

Use the **undo apply preference** command to remove the clause configuration.

No preference is set for a routing protocol by default.

*If you set a preference for a routing protocol with the **preference** command, using the **apply preference** command will set a new preference for the matched routing protocol. Other routing protocols not satisfying the criteria still use the preferences set by the **preference** command.*

Examples # Create routing policy "policy1" with node 10, matching mode as permit. If a route matches OSPF external route type, set the preference for the routing protocol to 90.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match route-type external-type1or2
[Sysname-route-policy] apply preference 90
```

apply preferred-value

Syntax **apply preferred-value** *preferred-value*

undo apply preferred-value

View Routing policy view

Parameters *preferred-value*: Preferred value.

Description Use the **apply preferred-value** command to apply a preferred value to BGP routes.

Use the **undo apply preferred-value** command to remove the clause configuration.

No preferred value is set for BGP routes by default.

Examples # Create routing policy "policy1" with node 10, matching mode as permit. If a BGP route matches AS-path-ACL 1, set the preferred value 66 for the BGP route.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match as-path 1
[Sysname-route-policy] apply preferred-value 66
```

apply tag

Syntax **apply tag** *value*

undo apply tag

View Routing policy view

Parameters *value*: Tag value.

Description Use the **apply tag** command to set a specified tag value for RIP, OSPF or IS-IS routing information.

Use the **undo apply tag** command to remove the clause configuration.

No routing tag is set for RIP, OSPF or IS-IS routing information by default.

Related commands: **if-match interface**, **if-match acl**, **if-match ip-prefix**, **if-match ip next-hop**, **if-match cost**, **if-match tag**, **route-policy**, **apply ip-address next-hop**, **apply local-preference**, **apply cost** and **apply origin**.

Examples # Create routing policy "policy1" with node 10, matching mode as permit. If a route matches OSPF external route type 1, set the tag of the route to 100.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match route-type external-type1
[Sysname-route-policy] apply tag 100
```

display ip as-path

Syntax **display ip as-path** [*as-path-number*]

View Any view

Parameters *as-path-number*: AS path list number.

Description Use the **display ip as-path-acl** command to display BGP AS path list information.

Information about all BGP AS path lists will be displayed if no *as-path-acl-number* is specified.

Related commands: **ip as-path-acl**, **if-match as-path** and **apply as-path**.

Examples # Display the information of BGP AS path list 1.

```
<Sysname> display ip as-path 1
ListID    Mode      Expression
1         permit    2
```

Table 96 Field descriptions of the display ip as-path command

Field	Description
ListID	AS path list ID
Mode	Matching mode: permit, deny
Expression	Regular expression for matching

display ip community-list

Syntax **display ip community-list** [*basic-community-list-number* | *adv-community-list-number*]

View Any view

Parameters *basic-community-list-number*: Basic community list number.

adv-community-list-number: Advanced community list number.

Description Use the **display ip community-list** command to display BGP community list information.

All BGP community list information will be displayed if no *basic-community-list-number* or *adv-community-list-number* is specified.

Related commands: **ip community-list**, **if-match community** and **apply community**.

Examples # Display the information of the BGP community list 1.

```
<Sysname> display ip community-list 1
Community List Number 1
         permit  1:1 1:2 2:2
```

display ip extcommunity-list

Syntax **display ip extcommunity-list** [*ext-comm-list-number*]

View Any view

Parameters *ext-comm-list-number*: Extended community list number.

Description Use the **display ip extcommunity-list** command to display BGP extended community list information.

All BGP extended community list information will be displayed if no *ext-comm-list-number* is specified.

Related commands: **ip extcommunity-list**, **if-match extcommunity**, **apply extcommunity**.

Examples # Display the information of BGP extended community list 1.

```
<Sysname> display ip extcommunity-list 1
Extended Community List Number 1
         permit rt : 9:6
```

display route-policy

Syntax **display route-policy** [*route-policy-name*]

View Any view

Parameters *route-policy-name*: Routing policy name.

Description Use the **display route-policy** command to display routing policy information.

All routing policy information will be displayed if no *route-policy-name* is specified.

Related commands: **route-policy**.

Examples # Display the information of routing policy 1.

```
<Sysname> display route-policy policy1
Route-policy : policy1
  permit : 10
         if-match ip-prefix abc
         apply cost 120
```

Table 97 Field descriptions of the display route-policy command.

Field	Description
Route-policy	Routing policy name
Permit	permit mode: permit, deny
if-match ip-prefix abc	Match criterion
apply cost 120	If the match criterion is satisfied, set the route cost to 120.

if-match as-path

Syntax **if-match as-path** *as-path-number*&<1-16>

undo if-match as-path [*as-path-number*&<1-16>]

View Routing policy view

Parameters *as-path-number*: AS path list number.

&<1-16>: Indicates the argument before it can be entered up to 16 times.

Description Use the **if-match as-path** command to use AS path list(s) for matching against the AS path attribute of BGP routing information.

Use the **undo if-match as-path** command to remove the match criterion.

The match criterion is not configured by default.

This command is one of the if-match clauses of a route policy, used for filtering BGP routing information and specifying match criteria according to the AS path attribute of routing information.

Related commands: **route-policy**, **ip as-path-acl**.

Examples # Define as-path list 2, allowing routing information containing AS 200 or 300 to pass. Define routing policy "test" with node 10, and set an if-match clause using the as-path list for matching.

```
<Sysname> system-view
[Sysname] ip as-path-acl 2 permit _*200.*300
[Sysname] route-policy test permit node 10
[Sysname-route-policy] if-match as-path 2
```

if-match community

Syntax **if-match community** { *basic-community-list-number* [**whole-match**] | *adv-community-list-number* }&<1-16>

undo if-match community [*basic-community-list-number* | *adv-community-list-number*]&<1-16>

View Routing policy view

Parameters *basic-community-list-number*: Basic community list number.

adv-community-list-number: Advanced community list number.

whole-match: Specifies the exact match. All and only the specified communities must be present.

&<1-16>: Indicates the argument before it can be entered up to 16 times.

Description Use the **if-match community** command to specify community list(s) for matching against the community attribute of BGP routing information.

Use the **undo if-match community** command to remove the match criterion.

The match criterion is not configured by default.

This command is one of the if-match clauses of route policy, used for filtering BGP routing information and specifying match criterion according to the community attribute of BGP routing information.

Related commands: **route-policy** and **ip community-list**.

Examples # Define community-list 1, allowing routing information with community number 100 or 200 to pass. Then define a routing policy named test, whose node 10 is defined with an if-match clause to reference the community-list 1 for matching.

```
<Sysname> system-view
[Sysname] ip community-list 1 permit 100 200
[Sysname] route-policy test permit node 10
[Sysname-route-policy] if-match community 1
```

if-match cost

Syntax **if-match cost** *value*

undo if-match cost

View Routing policy view

Parameters *cost*: Specifies the cost to match.

Description Use the **if-match cost** command to specify a cost for matching against the cost of a route.

Use the **undo if-match cost** command to remove the match criterion.

The match criterion is not configured by default.

This command is one of the if-match clauses of routing policy, used for matching routes with the specified route cost.

Related commands: **if-match interface**, **if-match acl**, **if-match ip-prefix**, **if-match ip next-hop**, **if-match tag**, **route-policy**, **apply ip-address next-hop**, **apply cost, apply local-preference**, **apply origin** and **apply tag**.

Examples # Create routing policy "policy1" with node 10, matching mode as permit. Define an if-match clause to permit routing information with a cost of 8.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match cost 8
```

if-match extcommunity

Syntax **if-match extcommunity** *ext-comm-list-number*&<1-16>

undo if-match extcommunity [*ext-comm-list-number*&<1-16>]

View Routing policy view

Parameters *ext-comm-list-number*: Extended community list number.

&<1-16>: Indicates the argument before it can be entered up to 16 times.

Description Use the **if-match extcommunity** command to specify extended community list(s) for matching against the extended community attribute of routing information.

Use the **undo if-match extcommunity** command to remove the match criterion.

The match criterion is not configured by default.

Examples # Create a routing policy named policy1 with node 10, matching mode as permit. Match the extended community attribute of routes against extended community lists 100 and 150.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match extcommunity 100 150
```

if-match interface

Syntax **if-match interface** { *interface-type interface-number* }

undo if-match interface [*interface-type interface-number*]

View Routing policy view

Parameters *interface-type*: Interface type

interface-number: Interface number

Description Use the **if-match interface** command to specify an interface for matching against the outbound interface of routing information.

Use the **undo if-match interface** command to remove the match criterion.

The match criterion is not configured by default.

Related commands: **if-match acl**, **if-match ip-prefix**, **if-match ip next-hop**, **if-match cost**, **if-match tag**, **route-policy**, **apply ip-address next-hop**, **apply cost**, **apply local-preference**, **apply origin**, **apply tag**.

Examples # Create a routing policy named policy1 with node 10, matching mode as permit. Define an if-match clause to match the routing information with the outbound interface as Vlan-interface 1.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match interface vlan-interface 1
```

if-match mpls-label

Syntax **if-match mpls-label**

undo if-match mpls-label

View Routing policy view

Parameters None

Description Use the **if-match mpls-label** command to specify the MPLS label match criterion.

Use the **undo if-match mpls-label** command to remove the match criterion.

The match criterion is not configured by default.

Examples # Match MPLS label of routing updates.

```
<Sysname> system-view
[Sysname] route-policy setcommunity permit node 16
[Sysname-route-policy] if-match mpls-label
```

if-match route-type

Syntax **if-match route-type** { **internal** | **external-type1** | **external-type2** | **external-type1or2** | **is-is-level-1** | **is-is-level-2** | **nssa-external-type1** | **nssa-external-type2** | **nssa-external-type1or2** } *

undo if-match route-type [**internal** | **external-type1** | **external-type2** | **external-type1or2** | **is-is-level-1** | **is-is-level-2** | **nssa-external-type1** | **nssa-external-type2** | **nssa-external-type1or2**] *

View Routing policy view

Parameters **internal**: Internal routes (OSPF intra-area and inter-area routes).

external-type1: OSPF Type 1 external routes.

external-type2: OSPF Type 2 external routes.

external-type1or2: OSPF Type 1 or 2 external routes.

is-is-level-1: IS-IS Level-1 routes.

is-is-level-2: IS-IS Level-2 routes.

nssa-external-type1: OSPF NSSA Type 1 external routes.

nssa-external-type2: OSPF NSSA Type 2 external routes.

nssa-external-type1or2: OSPF NSSA Type 1 or 2 external routes.

Description Use the **if-match route-type** command to configure a route type match criterion.

Use the **undo if-match route-type** command to remove the match criterion.

The match criterion is not configured by default.

Examples # Create a routing policy named policy1 with node 10, matching mode as permit. Define an if-match clause to match internal routes.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match route-type internal
```

if-match tag

Syntax **if-match tag** *value*

undo if-match tag

View Routing policy view

Parameters *value*: Specifies a tag value.

Description Use the **if-match tag** command to specify a tag for matching against the tag field of RIP, OSPF and IS-IS routes.

Use the **undo if-match tag** command to remove the match criterion.

The match criterion is not configured by default.

Related commands: **if-match interface**, **if-match acl**, **if-match ip-prefix**, **if-match ip next-hop**, **if-match cost**, **route-policy**, **apply ip-address next-hop**, **apply cost**, **apply local-preference**, **apply origin** and **apply tag**.

Examples # Create a routing policy named policy1 with node 10, matching mode as permit. Define an if-match clause to permit RIP, OSPF and IS-IS routing information with the tag as 8.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match tag 8
```

ip as-path

Syntax **ip as-path** *as-path-number* { **deny** | **permit** } *regular-expression*

undo ip as-path *as-path-number*

View System view

Parameters *as-path-number*: AS path list number.

deny: Specifies the matching mode for the AS path ACL as deny.

permit: Specifies the matching mode for the AS path ACL as permit.

regular-expression: Regular expression of AS path.

BGP routing information contains the AS path attribute field that identifies the autonomous systems through which routing information has passed. Used to compare with the AS path attribute, a regular expression is a formula comprised of characters, for example, ^200. *100$, which matches AS path attribute fields that start with AS200 and end with AS100.

The meanings of special characters used in regular expressions are shown below:

Character	Meaning
.	Matches any single character, including blank space.
*	Matches 0 or more patterns.
+	Matches 1 or more patterns.
^	Matches the beginning of an input string.
$	Matches the end of an input string.
_	Matches a comma, left brace, right brace, left parenthesis, right parenthesis, the beginning of an input string, the end of an input string, or a space.
[range]	Means the range of single-character patterns.
-	Separates the ending points of a range.

Description Use the **ip as-path** command to create an AS path list.

Use the **undo ip as-path** command to remove an AS path list.

No AS path list is created by default.

Examples # Create an AS path ACL numbered 1, permitting routing information whose AS_PATH starts with 10.

```
<Sysname> system-view
[Sysname] ip as-path 1 permit ^10
```

ip community-list

Syntax **ip community-list** *basic-comm-list-num* { **deny** | **permit** } [*community-number-list*] [**internet** | **no-advertise** | **no-export** | **no-export-subconfed**] *

undo ip community-list *basic-comm-list-num* [*community-number-list*] [**internet** | **no-advertise** | **no-export** | **no-export-subconfed**] *

ip community-list *adv-comm-list-num* { **deny** | **permit** } *regular-expression*

undo ip community-list *adv-comm-list-num* [*regular-expression*]

View System view

Parameters *basic-comm-list-num*: Basic community list number.

adv-comm-list-num: Advanced community list number.

regular-expression: Regular expression of advanced community attribute.

deny: Specifies the matching mode of the community list as deny.

permit: Specifies the matching mode of the community list as permit.

community-number-list: Community number list, in the *community number* or *aa:nn* format. Each format can be entered up to 16 times.

internet: Routes with this attribute can be advertised to all the BGP peers. By default, all routes have this attribute.

no-advertise: Routes with this attribute will not be advertised to other BGP peers.

no-export: Routes with this attribute will not be advertised out the local AS, or the confederation but can be advertised to other ASs in the confederation.

no-export-subconfed: Routes with this attribute can not be advertised out the local AS, or to other sub ASs in the confederation.

Description Use the **ip community-list** to define a community list.

Use the **undo ip community-list** command to remove a community list.

No community list is defined by default.

Examples # Define basic community list 1 to permit routing information with the **internet** community attribute.

```
<Sysname> system-view
[Sysname] ip community-list 1 permit internet
```

Define advanced community list 100 to permit routing information with the community attribute starting with 10.

```
<Sysname> system-view
[Sysname] ip community-list 100 permit ^10
```

ip extcommunity-list

Syntax **ip extcommunity-list** *ext-comm-list-number* { **deny** | **permit** } { **rt** *route-target* }&<1-16>

undo ip extcommunity-list *ext-comm-list-number*

View System view

Parameters *ext-comm-list-number*: Extended community list number.

permit: Specifies the matching mode for the extended community list as permit.

deny: Specifies the matching mode for the extended community list as deny.

rt *route-target*: Specifies the route target extended community attribute. *route-target* has two forms:

- 16-bit AS number: 32-bit self-defined number, for example, 101:3;
- 32-bit IP address: 16-bit self-defined number, for example, 192.168.122.15:1.

&<1-16>: Indicates the argument before it can be entered up to 16 times.

Description Use the **ip extcommunity-list** to define an extended community list entry.

Use the **undo ip extcommunity-list** command to remove an extended community list.

Examples # Define extended community list 1 to permit routing information with RT 200:200.

```
<Sysname> system-view
[Sysname] ip extcommunity-list 1 permit rt 200:200
```

route-policy

Syntax **route-policy** *route-policy-name* { **permit** | **deny** } **node** *node-number*

undo route-policy *route-policy-name* [**node** *node-number*]

View System view

Parameters *route-policy-name*: Routing policy name.

permit: Specifies the matching mode of the routing policy node as permit. If a route satisfies all the if-match clauses of the node, it passes through the filtering of the node and then is executed with the apply clauses of the node. If not, it goes to the next node of the routing policy.

deny: Specifies the matching mode of the routing policy node as deny. If a route satisfies all the if-match clauses of the node, it does not pass the filtering of the node and will not go to the next node.

node *node-number*: Node number. The node with a smaller *node-number* will be tested first when the routing policy is used for filtering routing information.

Description Use the **route-policy** command to create a routing policy and enter its view.

Use the **undo route-policy** command to remove a routing policy.

No routing policy is created by default.

A routing policy is used for routing information filtering or policy routing. It contains several nodes and each node comprises some if-match and apply clauses. The if-match clauses define the matching criteria of the node and the apply clauses define the actions performed after a packet passes the filtering of the node. The relation among the if-match clauses of a node is logic AND, namely all the if-match clauses must be satisfied. The filter relation among different route-policy nodes is logic OR, namely a packet passing a node passes the routing policy.

Related commands: **if-match interface**, **if-match acl**, **if-match ip-prefix**, **if-match ip next-hop**, **if-match cost**, **if-match tag**, **apply ip-address next-hop**, **apply local-preference**, **apply cost**, **apply origin** and **apply tag**.

Examples # Create routing policy "policy1" with node 10 with matching mode as permit, and then enter routing policy view.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy]
```

29 IPv4 Routing Policy Configuration Commands

apply ip-address next-hop

Syntax **apply ip-address next-hop** *ip-address*

undo apply ip-address next-hop

View Routing policy view

Parameters *ip-address*: IP address of the next hop.

Description Use the **apply ip-address next-hop** command to set a next hop for IPv4 routing information.

Use the **undo apply ip-address next-hop** command to remove the clause configuration.

No next hop address is set for IPv4 routing information by default.

It is invalid to use the **apply ip-address next-hop** command to set a next hop when redistributing routes.

Related commands: **if-match interface**, **if-match acl**, **if-match ip-prefix**, **if-match ip next-hop**, **if-match cost**, **if-match tag**, **route-policy**, **apply local-preference**, **apply cost**, **apply origin** and **apply tag**.

Examples # Create routing policy "policy1" with node 10, matching mode "permit". If passing AS path ACL 1, a route's next hop is set to 193.1.1.8.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match as-path 1
[Sysname-route-policy] apply ip-address next-hop 193.1.1.8
```

display ip ip-prefix

Syntax **display ip ip-prefix** [*ip-prefix-name*]

View Any view

Parameters *ip-prefix-name*: IP prefix list name.

Description Use the **display ip ip-prefix** command to display the statistics of an IPv4 prefix list. If no ip-prefix-name is specified, statistics for all IPv4 prefix lists will be displayed.

Related commands: **ip ip-prefix**.

Examples # Display the statistics of IPv4 prefix list "abc".

```
<Sysname> display ip ip-prefix abc
Prefix-list abc
Permitted 0
Denied 0
        index: 10               permit  1.0.0.0/11              ge  22  le  32
```

Table 98 Field descriptions of the display ip ip-prefix command.

Field	Description
Prefix-list	Name of the IPv4 prefix list
Permitted	Number of routes satisfying the match criterion
Denied	Number of routes not satisfying the match criterion
index	Internal serial number of the IPv4 prefix list
permit	Matching mode: permit or deny
1.0.0.0/11	Match IP address and mask
ge	greater-equal, the lower limit mask
le	less-equal, the upper limit mask

if-match acl

Syntax **if-match acl** *acl-number*

undo if-match acl

View Routing policy view

Parameters *acl-number*: ACL number.

Description Use the **if-match acl** command to configure an ACL match criterion.

Use the **undo if-match acl** command to remove the match criterion.

No ACL match criterion is configured by default.

Related commands: **if-match interface**, **if-match ip next-hop**, **if-match cost**, **if-match tag**, **route-policy**, **apply ip-address next-hop**, **apply cost**, **apply local-preference**, **apply origin** and **apply tag**.

Examples # Create routing policy "policy1" with node 10, matching mode as permit. Define an if-match clause to permit routes matching ACL 2000.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match acl 2000
```

if-match ip

Syntax **if-match ip** { **next-hop** | **route-source** } { **acl** *acl-number* | **ip-prefix** *ip-prefix-name* }

undo if-match ip { **next-hop** | **route-source** } [**acl** | **ip-prefix**]

View Routing policy view

Parameters **next-hop**: Matches next hop.

route-source: Matches source address.

acl *acl-number*: Matches an ACL.

ip-prefix *ip-prefix-name*: Matches an IP prefix list.

Description Use the **if-match ip** command to configure a next hop or source address match criterion for IPv4 routes.

Use the **undo if-match ip** command to remove the match criterion.

The match criterion is not configured by default.

Related commands: **route-policy**.

Examples # Create routing policy "policy1" with node 10, matching mode permit. Define an if-match clause to permit routing information whose next hop address matches IP prefix list p1.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match ip next-hop ip-prefix p1
```

if-match ip-prefix

Syntax **if-match ip-prefix** *ip-prefix-name*

undo if-match ip-prefix

View Routing policy view

Parameters *ip-prefix-name*: Matches an IP prefix list.

Description Use the **if-match ip-prefix** command to configure an IP prefix list based match criterion.

Use the **undo if-match ip-prefix** command to remove the match criterion.

No IP prefix list based match criterion is configured by default.

Related commands: **if-match interface**, **if-match ip next-hop**, **if-match cost**, **if-match tag**, **route-policy**, **apply ip-address next-hop**, **apply cost**, **apply local-preference**, **apply origin** and **apply tag**.

Examples # Create routing policy "policy1" with node 10, matching mode as permit. Define an if-match clause to permit a route whose destination address matches IP prefix list "p1".

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match ip-prefix p1
```

ip ip-prefix

Syntax **ip ip-prefix** *ip-prefix-name* [**index** *index-number*] { **permit** | **deny** } *ip-address mask-length* [**greater-equal** *min-mask-length*] [**less-equal** *max-mask-length*]

undo ip ip-prefix *ip-prefix-name* [**index** *index-number*]

View System view

Parameters *ip-prefix-name*: IPv4 prefix list name.

index-number: Index number, for uniquely specifying an item of the IPv4 prefix list. The index with a smaller number is tested first.

permit: Specifies the matching mode for the IPv4 prefix list as permit, that is, when a route to be filtered is in the range of the IPv4 prefix list, the route passes the IPv4 prefix list without needing to enter the next item for testing. If the route to be filtered is not in the prefix range, it will enter the next item for testing.

deny: Specifies the matching mode for the IPv4 prefix list as deny, that is, when a route to be filtered is in the IPv4 prefix list range, the route neither passes the filter nor enters the next node for testing. If not in the range, the route will enter the next item test.

ip-address mask-length: Specifies an IPv4 address prefix and mask length.

min-mask-length, *max-mask-length*: Specifies the range for prefix if the IPv4 address and prefix length are matched. **greater-equal** means "greater than or equal to" and **less-equal** means "less than or equal to". The range relation is *mask-length* <= *min-mask-length* <= *max-mask-length* <= 32. If only *min-mask-length* is specified, the prefix length range is [min-mask-length, 32]. If only *max-mask-length* is specified, the prefix length range is [mask-length,

max-mask-length]. If both min-mask-length and max-mask-length are specified, the prefix length range is [min-mask-length, max-mask-length].

Description Use the **ip ip-prefix** command to configure an IPv4 prefix list item.

Use the **undo ip ip-prefix** command to remove an IPv4 prefix list or an item.

No IPv4 prefix list is configured by default.

An IPv4 prefix list is used to filter IPv4 addresses. It may have multiple items, each of which specifies a range of IPv4 prefix. The filtering relation among items is logic OR, namely, passing any item means the IPv4 prefix list is passed. If no item is passed, the IP prefix list cannot be passed.

The IP prefix range is determined by *mask-length* and [*min-mask-length, max-mask-length*]. If both *mask-length* and [*min-mask-length, max-mask-length*] are specified, then the IP address to be filtered must satisfy both of them.

If *ip-address mask-length* is specified as 0.0.0.0 0, then only the default routes will be matched.

To match all the routes, use 0.0.0.0 0 **less-equal** 32.

Examples # Create a routing policy named policy1 with node 10 with matching mode as permit. Define an IP prefix list named p1 to permit only the routes in the network segment 10.0.192.0/8 and with mask length 17 or 18.

```
<Sysname> system-view
[Sysname] ip ip-prefix p1 permit 10.0.192.0 8 greater-equal 17 less-equal 18
```

reset ip ip-prefix

Syntax **reset ip ip-prefix** [*ip-prefix-name*]

View User view

Parameters *ip-prefix-name*: IP prefix list name.

Description Use the **reset ip ip-prefix** command to clear the statistics of a specified IPv4 prefix list. If no *ip-prefix-name* is specified, the statistics of all the IPv4 prefix lists will be cleared.

Examples # Clear the statistics of IPv4 prefix list "abc".

```
<Sysname> reset ip ip-prefix abc
```

30 IPv6 Routing Policy Configuration Commands

apply ipv6 next-hop

Syntax **apply ipv6 next-hop** *ipv6-address*

undo apply ipv6 next-hop

View Routing policy view

Parameters *ipv6-address*: Next hop IPv6 address.

Description Use the **apply ipv6 next-hop** command to apply a next hop to IPv6 routes.

Use the **undo apply ipv6 next-hop** command to remove the clause configuration.

No next hop address is set for IPv6 routing information by default.

Using the **apply ipv6 next-hop** command to set a next hop when redistributing routes does not take effect.

Examples # Create routing policy "policy1" with node 10 with matching mode being "permit". If a route matches AS path list 1, set next hop 3ff3:506::1 for it.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match as-path 1
```

[Sysname-route-policy] apply ipv6 next-hop 3ffe:506::1

display ip ipv6-prefix

Syntax **display ip ipv6-prefix** [*ipv6-prefix-name*]

View Any view

Parameters *ipv6-prefix-name*: IPv6 prefix list name, a string of 1 to 19 characters.

Description Use the **display ip ipv6-prefix** command to display the statistics of the specified IPv6 prefix list. If no IPv6 prefix list is specified, the statistics of all the IPv6 prefix lists will be displayed.

Examples # Display the statistics of all the IPv6 prefix lists.

```
<Sysname> display ip ipv6-prefix
Prefix-list6 abc
Permitted 0
Denied 0
         index:   10            permit  ::/0
         index:   20             permit  ::/1                ge  1   le  128
```

Table 99 Field descriptions of the display ip ipv6-prefix command

Field	Description
Prefix-list6	Name of the IPv6 prefix list
Permitted	Number of routes satisfying the match criterion
Denied	Number of routes not satisfying the match criterion
Index	Internal serial number of address prefix list
Permit	Matching mode: permit, deny
::/1	IPv6 address and its prefix length for matching
ge	greater-equal, the lower limit prefix length
Le	less-equal, the upper limit prefix length

if-match ipv6

Syntax **if-match ipv6** { **address** | **next-hop** | **route-source** } { **acl** *acl6-number* | **prefix-list** *ipv6-prefix-name* }

undo if-match ipv6 { **address** | **next-hop** | **route-source** } [**acl** | **prefix-list**]

View Routing policy view

Parameters **address**: Matches the destination address of IPv6 routing information.

next-hop: Matches the next hop of IPv6 routing information.

route-source: Matches the source address of IPv6 routing information.

acl *acl6-number*: Specifies the number of an IPv6 ACL for filtering, in the range 2000 to 3999 for **address**, and 2000 to 2999 for **next-hop** and **route-source**.

prefix-list *ipv6-prefix-name*: Specifies the name of a IPv6 prefix list for filtering, a string of 1 to 19 characters.

Description Use the **if-match ipv6** command to configure a destination, next hop or source address based match criterion for IPv6 routes.

Use the **undo if-match ipv6** command to remove the match criterion.

The match criterion is not configured by default.

Examples # Create a routing policy named policy1 with node 10, matching mode as permit. Define an if-match clause to permit the routing information whose next hop address matches IPv6 prefix list p1.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
```

[Sysname-route-policy] if-match ipv6 next-hop prefix-list p1

ip ipv6-prefix

Syntax **ip ipv6-prefix** *ipv6-prefix-name* [**index** *index-number*] { **deny** | **permit** } *ipv6-address prefix-length* [**greater-equal** *min-prefix-length*] [**less-equal** *max-prefix-length*]

undo ip ipv6-prefix *ipv6-prefix-name* [**index** *index-number*]

View System view

Parameters *ipv6-prefix-name*: IPv6 prefix list name for uniquely specifying an IPv6 prefix list.

index-number: Index number for uniquely specifying an IPv6 prefix list item. The item with a smaller *index-number* will be tested first.

permit: Specifies the matching mode for the IPv6 prefix list as permit, that is, if a route matches the IPv6 prefix list, it passes the IPv6 prefix list without needing to enter the next item for test. If not, it will enter the next item's test.

deny: Specifies the matching mode for the IPv6 prefix list as deny, that is, if a route matches the IPv6 prefix list, the route neither passes the filter nor enters the next node for test; if not, the route will enter the next item's test.

ipv6-address prefix-length: Specifies an IPv6 prefix and prefix length. When specified as :: 0, it matches the default route.

greater-equal *min-prefix-length:* Greater than or equal to the minimum prefix length.

less-equal *max-prefix-length*: Less than or equal to the maximum prefix length.

The length relation is *mask-length* <= *min-mask-length* <= *max-mask-length* <= 32. If only min-prefix-length is specified, the prefix length range is [min-prefix-length, 128]. If only max-prefix-length is specified, the prefix length range is [prefix-length, max-prefix-length]. If both min-prefix-length and max-prefix-length are specified, the prefix length range is [min-prefix-length, max-prefix-length].

Description Use the **ip ipv6-prefix** command to configure an IPv6 prefix list item.

Use the **undo ip ipv6-prefix** command to remove an IPv6 prefix list or an item.

No IPv6 prefix list is configured by default.

The IPv6 prefix list is used to filter IPv6 addresses. It may have multiple items, and each of them specifies a range of IPv6 prefix. The filtering relation among items is logic OR, namely, a route passing an item will pass the prefix list.

The IPv6 prefix range is determined by *prefix-length* and [*min-prefix-length, max-prefix-length*]. If both *mask-length* and [*min-mask-length, max-mask-length*] are specified, then the IPv6 addresses must satisfy both of them.

If *ipv6-address prefix-length* is specified as :: 0, then only the default route matches.

If you want it to match all the routes, configure it as :: 0 **less-equal** 128.

Examples # Permit the IPv6 addresses with mask length between 32 bits and 64 bits.

```
<Sysname> system-view
```

[Sysname] ip ipv6-prefix abc permit :: 0 greater-equal 32 less-equal 64

Deny the IPv6 addresses with prefix as 3FFE:D00::/32, prefix length greater than or equal to 32 bits.

```
<Sysname> system-view
```

[Sysname] ip ipv6-prefix abc deny 3FEE:D00:: 32 less-equal 128

reset ip ipv6-prefix

Syntax **reset ip ipv6-prefix** [*ipv6-prefix-name*]

View User view

Parameters *ipv6-prefix-name*: IPv6 prefix list name, a string of 1 to 19 characters.

Description Use the **reset ip ipv6-prefix** command to clear the statistics of the specified IPv6 prefix list. If no name is specified, the statistics of all IPv6 prefix lists will be cleared.

Examples # Clear the statistics of IPv6 prefix list "abc".

<Sysname> reset ip ipv6-prefix abc

31 STATIC ROUTING CONFIGURATION COMMANDS

delete static-routes all

Syntax **delete** [**vpn-instance** *vpn-instance-name*] **static-routes all**

View System view

Parameters *vpn-instance-name*: Name of a VPN instance.

Description Use the **delete static-routes all** command to delete all static routes.

When you use this command to delete static routes, the system will prompt you to confirm the operation before deleting all the static routes.

Related commands: **display ip routing-table** and **ip route-static**.

Examples # Delete all static routes on the router.

```
<Sysname> system-view
[Sysname] delete static-routes all
This will erase all ipv4 static routes and their configurations, you
 must reconfigure all static routes
Are you sure?[Y/N]:Y
```

ip route-static

Syntax **ip route-static** *dest-address* { *mask* | *mask-length* } { *gateway-address* | *interface-type interface-number* [*gateway-address*] | **vpn-instance** *d-vpn-instance-name gateway-address* } [**preference** *preference-value*] [**tag** *tag-value*] [**description** *description-text*]

undo ip route-static *dest-address* { *mask* | *mask-length* } [*gateway-address* | *interface-type interface-number* [*gateway-address*] | **vpn-instance** *d-vpn-instance-name gateway-address*] [**preference** *preference-value*]

ip route-static vpn-instance *s-vpn-instance-name*&<1-6> *dest-address* { *mask* | *mask-length* } { *gateway-address* [**public**] | *interface-type interface-number* [*gateway-address*] | **vpn-instance** *d-vpn-instance-name gateway-address* } [**preference** *preference-value*] [**tag** *tag-value*] [**description** *description-text*]

undo ip route-static vpn-instance *s-vpn-instance-name*&<1-6> *dest-address* { *mask* | *mask-length* } [*gateway-address* [**public**] | *interface-type*

interface-number [*gateway-address*] | **vpn-instance** *d-vpn-instance-name gateway-address*] [**preference** *preference-value*]

View System view

Parameters **vpn-instance** *s-vpn-instance-name*&<1-6>: Specifies the VPN instance name. &<1-6> indicates the argument before it can be entered up to 6 times. Each VPN instance has its own routing table, and the configured static route is installed in the routing tables of the specified VPN instances.

dest-address: Destination IP address of the static route, in dotted decimal notation.

mask: Mast of the IP address, in dotted decimal notation.

mask-length: Mask length.

gateway-address: IP address of the next hop, in dotted decimal notation.

interface-type interface-number: Specifies the output interface by its type and number. If the output interface is a broadcast interface, the next hop address must be specified.

vpn-instance *d-vpn-instance-name*: Name of the destination VPN instance. If a destination VPN instance name is specified, the router will search the output interface in the destination VPN instance based on the configured *gateway-address*.

gateway-address **public**: Indicates that the specified *gateway-address* is a public network address, rather than a VPN instance address.

preference *preference-value* : Specifies the preference of the static route. The default is 60.

tag *tag-value*: Sets a tag value for the static route from 1 to 4294967295. The default is 0. Tags of routes are used in routing policies to control routing.

description *description-text*: Configures a description for the static route, which consists of 1 to 60 characters, including special characters like space, but excluding "?".

Description Use the **ip route-static** command to configure a unicast static route.

Use the **undo ip route-static** command to delete a unicast static route.

When configuring a unicast static route, note that:

1. If the destination IP address and the mask are both 0.0.0.0, the configured route is a default route. If routing table searching fails, the router will use the default route for packet forwarding.
2. Different route management policies can be implemented for different route preference configurations. For example, specifying the same preference for different routes to the same destination address enables load sharing, while specifying different preferences for these routes enables route backup.

3 When configuring a static route, you can specify the output interface or the next hop address based on the actual requirement. Note that the next hop address must not be the IP address of the local interface; otherwise, the route configuration will not take effect. For interfaces that support network address to link layer address resolution or point-to-point interfaces, you can specify the output interface or next hop address. When specifying the output interface, note that:

- For a NULL0 or loopback interface, if the output interface has already been configured, there is no need to configure the next hop address.
- For point-to-point interfaces, you can specify the output interface if you do not know the peer address. Thus, there is no need to change the router's configuration even if the peer address is changed. A PPP interface obtains the peer's IP address through PPP negotiation. In this case, you need only specify the output interface.
- For NBMA and P2MP interfaces, which support point-to-multipoint networks, the IP address to link layer address mapping must be established in addition to IP route configuration. In general, it is recommended to configure the next hop IP address when you configure the output interface.
- It is not recommended to specify a broadcast interface as the output interface for a static route, because a broadcast interface may have multiple next hops. If you have to do so, you must specify the corresponding next hop at the same time.

Related commands: **display ip routing-table** and **ip route-static default-preference**.

If you specify the next hop of a static route and then configure the next hop as the IP address of a local interface such as a VLAN interface, the static route cannot take effect.

Examples # Configure a static route, whose destination address is 1.1.1.1/24, next hop address is 2.2.2.2, tag value is 45, and description information is "for internet & intranet".

```
<Sysname> system-view
[Sysname] ip route-static 1.1.1.1 24 2.2.2.2 tag 45 description for
internet & intranet
```

Configure a static route for a VPN instance named vpn1: the destination address is 1.1.1.1/16 and the next hop address is 1.1.1.2, which is the address of this VPN instance.

```
<Sysname> system-view
[Sysname] ip route-static vpn-instance vpn1 1.1.1.1 16 vpn-instance
vpn1 1.1.1.2
```

ip route-static default-preference

Syntax **ip route-static default-preference** *default-preference-value*

undo ip route-static default-preference

View System view

Parameters *default-preference-value*: Default preference for static routes.

Description Use the **ip route-static default-preference** command to configure the default preference for static routes.

Use the **undo ip route-static default-preference** command to restore the default.

By default, the default preference of static routes is 60.

Note that If no preference is specified when configuring a static route, the default preference is used.

Related commands: **display ip routing-table** and **ip route-static**.

Examples # Set the default preference of static routes to 120.

```
<Sysname> system-view
[Sysname] ip route-static default-preference 120
```

32 IPv6 Static Routing Configuration Commands

delete ipv6 static-routes all

Syntax **delete ipv6 static-routes all**

View System view

Parameters None

Description Use the **delete ipv6 static-routes all** command to delete all static routes including the default route.

When using this command, you will be prompted whether to continue the deletion and only after you confirm the deletion will the static routes be deleted.

Related commands: **display ipv6 routing-table**, **ipv6 route-static**.

Examples # Delete all IPv6 static routes.

```
<Sysname> system-view
[Sysname] delete ipv6 static-routes all
This will erase all ipv6 static routes and their configurations, you
 must reconfigure all static routes
Are you sure?[Y/N]
```

ipv6 route-static

Syntax For a broadcast interface, or NBMA interface:

ipv6 route-static *ipv6-address prefix-length* [*interface-type interface-number*] *nexthop-address* [**preference** *preference-value*]

undo ipv6 route-static *ipv6-address prefix-length* [*interface-type interface-number*] [*nexthop-address*] [**preference** *preference-value*]

For a point-to-point interface:

ipv6 route-static *ipv6-address prefix-length* { *interface-type interface-number* | *nexthop-address* } [**preference** *preference-value*]

undo ipv6 route-static *ipv6-address prefix-length* [*interface-type interface-number* | *nexthop-address*] [**preference** *preference-value*]

View

System view

Parameters *ipv6-address prefix-length*: IPv6 address and prefix length.

interface-type interface-number: Interface type and interface number of the output interface.

nexthop-address: Next hop IPv6 address.

preference-value: Route preference value. The default is 60.

Description Use the **ipv6 route-static** command to configure an IPv6 static route.

Use the **undo ipv6 route-static** command to remove an IPv6 static route.

An IPv6 static route that has the destination address configured as "::/0" (a prefix length of 0) is the default IPv6 route. If the destination address of an IPv6 packet does not match any entry in the routing table, this default route will be used to forward the packet.

While configuring static routes, you can configure either the output interface or the next-hop address depending on the situations:

- If the output interface is a broadcast interface or an NBMA interface, then the next hop address must be specified;
- If the output interface is a point-to-point interface, you can specify either the output interface or the next hop address, but not both.

Related commands: **display ipv6 routing-table**, **delete ipv6 static-routes all**.

Examples # Configure a static IPv6 route, with the destination address being 1:1:2::/24 and next hop being 1:1:3::1.

```
<Sysname> system-view
[Sysname] ipv6 route-static 1:1:2:: 24 1:1:3::1
```

reset ipv6 routing-table statistics (User view)

Syntax **reset ipv6 routing-table statistics protocol** { **all** | *protocol* }

View User view

Parameters **all**: Clears all route statistics in the routing table.

protocol: Clears route statistics of a specified protocol, **bgp4+**, **direct**, **isisv6**, **ospfv3**, **ripng**, or **static.**

Description Use the **reset ipv6 routing-table statistics** command to clear the routing table statistics.

Examples # Clear all routing statistics in the routing table.

```
<Sysname> reset ipv6 routing-table statistics protocol all
```

33 RIP CONFIGURATION COMMANDS

checkzero (RIP view)

Syntax **checkzero**

undo checkzero

View RIP view

Parameter None

Description Use the **checkzero** command to enable the zero field check on RIP-1 messages.

Use the **undo checkzero** command to disable the zero field check.

The zero field check is enabled by default.

After the zero field check is enabled, the router discards RIP-1 messages in which zero fields are non-zero. If all messages are trusty, you can disable this feature to spare the processing time of the CPU.

Examples # Disable the zero field check on RIP-1 messages for RIP process 100.

```
<Sysname> system-view
[Sysname] rip 100
[Sysname-rip-100] undo checkzero
```

debugging rip

Syntax **debugging rip** *process-id* [**brief** | **event** | **packet** [**interface** *interface-type interface-number*] | **receive** [**interface** *interface-type interface-number*] | **send** [**interface** *interface-type interface-number*] | **timer**]

undo debugging rip *process-id* [**brief** | **event** | **packet** [**interface** *interface-type interface-number*] | **receive** [**interface** *interface-type interface-number*] | **send** [**interface** *interface-type interface-number*] | **timer**]

View User view

Parameters *process-id*: RIP process ID. If no following parameter is specified, all debugging of the RIP process is enabled.

brief: Enables RIP brief debugging.

event: Enables RIP event debugging.

packet: Enables RIP packet debugging.

receive: Enables RIP debugging of received packets.

send: Enables RIP debugging of sent packets.

interface *interface-type interface-number*: Enables the specified debugging on the interface.

timer: Enables RIP timer debugging.

Description Use the **debugging rip** command to enable specified RIP debugging.

Use the **undo debugging** command to disable specified RIP debugging.

RIP debugging is disabled by default.

Examples # Enable RIP brief debugging on the RIP enabled device with RIP enabled on a specified interface.

```
<Sysname> debugging rip 1 brief
*Oct 23 14:13:20:808 2006 Sysname RM/6/RMDEBUG: RIP 1 : Sending v2 r
esponse on Vlan-interface11 from 12.0.0.1
```

// RIP process 1 sends a RIPv2 response via VLAN-interface11, and the source IP address is 12.0.0.1.

```
*Oct 23 14:17:40:320 2006 Sysname RM/6/RMDEBUG: RIP 1 : Receiving v2
 response on Vlan-interface11 from 12.0.0.1
```

// RIP process 1 receives a RIPv2 response from VLAN-interface11, and the source IP address is 12.0.0.1.

Enable RIP timer debugging.

```
<Sysname> debugging rip 1 timer
*Oct 23 14:21:01:382 2006 Sysname RM/6/RMDEBUG: RIP 1 : Periodic tim
er expired
```

// The update timer of RIP process 1 timed out.

Enable RIP debugging of sent packets on the RIP enabled device with RIP enabled on a specified interface.

```
<Sysname> debugging rip 1 send
*Oct 23 14:27:37:150 2006 Sysname RM/6/RMDEBUG: RIP 1 : Sending resp
onse on interface Vlan-interface11 from 12.0.0.1 to 224.0.0.9
*Oct 23 14:27:37:150 2006 Sysname RM/6/RMDEBUG:   Packet : vers 2, c
md response, length 108
*Oct 23 14:27:37:150 2006 Sysname RM/6/RMDEBUG:   authentication-mod
e: MD5 Digest: 4de038ea.69b217e7.2ca5a091.9f8e3bd9
*Oct 23 14:27:37:150 2006 Sysname RM/6/RMDEBUG:   Sequence: e717b269
```

```
 (11230)
*Oct 23 14:27:37:150 2006 Sysname RM/6/RMDEBUG:     AFI 2, dest 4.4.
4.4/255.255.255.255, nexthop 0.0.0.0, cost 1, tag 0
*Oct 23 14:27:37:150 2006 Sysname RM/6/RMDEBUG:     AFI 2, dest 12.0
.0.0/255.0.0.0, nexthop 0.0.0.0, cost 2, tag 0
*Oct 23 14:27:37:150 2006 Sysname RM/6/RMDEBUG:     AFI 2, dest 22.0
.0.0/255.0.0.0, nexthop 0.0.0.0, cost 1, tag 0
*Oct 23 14:27:37:150 2006 Sysname RM/6/RMDEBUG:     AFI 2, dest 55.4
.4.4/255.255.255.255, nexthop 0.0.0.0, cost 1, tag 0
```

// RIP process 1 sent a response to the multicast address 224.0.0.9 through VLAN-interface11, and the source IP address is 12.0.0.1.

// Packet version is RIPv2, and the length of the response is 108 bytes.

// The authentication mode is MD5. The MD5 digest is 4de038ea.69b217e7.2ca5a091.9f8e3bd9. The sequence number is e717b269, and timestamp is 11230.

// The packet contains 4 route entries with AFI field being 2: Destination 4.4.4.4/255.255.255.255, next hop 0.0.0.0, cost 1, tag 0; destination 12.0.0.0/255.0.0.0, next hop 0.0.0.0, cost 2, tag 0; destination 22.0.0.0/255.0.0.0, next hop 0.0.0.0, cost 1, tag 0; destination 55.4.4.4/255.255.255.255, next hop 0.0.0.0, cost 1, tag 0.

Enable RIP debugging of sent packets on the RIP enabled device with TRIP enabled on a specified interface.

```
<Sysname> debugging rip 1 send
*Oct 23 14:39:05:380 2006 Sysname RM/6/RMDEBUG: TRIP 1 : Sending ack
nowledgement on interface Serial0/2/0 to 22.0.0.2
*Oct 23 14:39:05:390 2006 Sysname RM/6/RMDEBUG:   Packet : vers 2, c
md acknowledgement (FLUSH), length 8, sequence num 0
```

// TRIP process 1 sent a TRIP acknowledgement to IP address 22.0.0.2 through Serial 0/2/0.

// The RIP version of the packet with FLUSH is 2. The packet length is 8 bytes, and sequence number is 0.

Enable RIP debugging of received packets on the RIP enabled device with RIP enabled on a specified interface.

```
<Sysname> debugging rip 1 receive
*Oct 23 14:44:44:610 2006 Sysname RM/6/RMDEBUG: RIP 1 : Receive resp
onse from 12.0.0.1 on Vlan-interface11
*Oct 23 14:44:44:620 2006 Sysname RM/6/RMDEBUG:   Packet : vers 2, c
md response, length 108
*Oct 23 14:44:44:630 2006 Sysname RM/6/RMDEBUG:   authentication-mod
e: MD5 Digest: e4429d25.d9251034.e5c0fc9e.25f7d9a1
*Oct 23 14:44:44:640 2006 Sysname RM/6/RMDEBUG:   Sequence: 341025d9
 (12252)
*Oct 23 14:44:44:650 2006 Sysname RM/6/RMDEBUG:     AFI 2, dest 4.4.
4.4/255.255.255.255, nexthop 0.0.0.0, cost 1, tag 0
*Oct 23 14:44:44:650 2006 Sysname RM/6/RMDEBUG:     AFI 2, dest 12.0
.0.0/255.0.0.0, nexthop 0.0.0.0, cost 2, tag 0
```

```
*Oct 23 14:44:44:660 2006 Sysname RM/6/RMDEBUG:     AFI 2, dest 22.0
.0.0/255.0.0.0, nexthop 0.0.0.0, cost 1, tag 0
*Oct 23 14:44:44:670 2006 Sysname RM/6/RMDEBUG:     AFI 2, dest 55.4
.4.4/255.255.255.255, nexthop 0.0.0.0, cost 1, tag 0
*Oct 23 14:44:44:680 2006 Sysname RM/3/RMDEBUG: RIP 1 : Ignoring thi
s packet. Authentication validation failed.
```

// RIP process 1 received a response from VLAN-interface11 at 12.0.0.1.

// Packet version is RIPv2, and the length is 108 bytes.

// The authentication mode is MD5. The MD5 digest is e4429d25.d9251034.e5c0fc9e.25f7d9a1. The sequence number is 341025d9, and timestamp is 12252.

// The packet contains 4 route entries with AFI field being 2: Destination 4.4.4.4/255.255.255.255, next hop 0.0.0.0, cost 1, tag 0; destination 12.0.0.0/255.0.0.0, next hop 0.0.0.0, cost 2, tag 0; destination 22.0.0.0/255.0.0.0, next hop 0.0.0.0, cost 1, tag 0; destination 55.4.4.4/255.255.255.255, next hop 0.0.0.0, cost 1, tag 0.

Enable RIP debugging of received packets on the RIP enabled device with TRIP enabled on a specified interface.

```
<Sysname> debugging rip 1 receive
*Oct 23 14:52:40:298 2006 Sysname RM/6/RMDEBUG: TRIP 1 : Receive res
ponse on Serial0/2/0 from 22.0.0.1
*Oct 23 14:52:40:298 2006 Sysname RM/6/RMDEBUG:   Packet : vers 2, c
md response, length 28, sequence num 1
*Oct 23 14:52:40:298 2006 Sysname RM/6/RMDEBUG:     AFI 2, dest 12.0
.0.0/255.0.0.0, nexthop 0.0.0.0, cost 16, tag 0
```

// TRIP process 1 received a TRIP response from Serial 0/2/0, and the receiving IP address is 22.0.0.1.

// The RIP version of the packet without FLUSH is 2. The packet length is 28 bytes, and sequence number is 1.

// The packet contains a route entry with the AFI field being 2: Destination 12.0.0.0/255.0.0.0, next hop 0.0.0.0, cost 16, tag 0.

Enable RIP event debugging on the RIP enabled device with RIP enabled on a specified interface.

```
<Sysname> debugging rip 1 event
*Oct 23 15:00:55:202 2006 Sysname RM/6/RMDEBUG: RIP 1 : Rebuilding o
f Database has started
*Oct 23 15:00:55:212 2006 Sysname RM/6/RMDEBUG: RIP 1 : Database has
 been rebuilt
```

// RIP process 1 started to rebuild the database.

```
*Oct 23 15:02:11:00 2006 Sysname RM/6/RMDEBUG: RIP 1 : Adding Vlan-i
nterface11 to Network List
```

// VLAN-interface11 is enabled with RIP process 1.

```
*Oct 23 15:02:01:633 2006 Sysname RM/6/RMDEBUG: RIP 1 : Removing Vla
n-interface11 from Network List
```

// VLAN-interface11 is disabled with RIP process 1.

```
*Oct 23 15:02:01:622 2006 Sysname RM/6/RMDEBUG: RIP 1 : Triggered up
date sent
```

// RIP process 1 sent a triggered update.

```
*Oct 23 15:06:09:306 2006 Sysname RM/6/RMDEBUG: RIP 1 : prefix list
used in filter-policy import has changed
```

// The IP prefix list referenced by the inbound filter policy has changed.

```
*Oct 23 15:07:41:590 2006 Sysname RM/6/RMDEBUG: RIP 1 : acl used in
filter-policy export has changed
```

// The ACL referenced by the outbound filter policy has changed.

```
*Oct 23 15:08:34:422 2006 Sysname RM/6/RMDEBUG: RIP 1 : route-policy
 used in import-route has changed
```

// The routing policy for route redistribution has changed.

```
*Oct 23 15:09:11:398 2006 Sysname RM/6/RMDEBUG: RIP 1 : route-policy
 used in preference has changed
```

// The routing policy for preference configuration has changed.

Enable RIP event debugging on the RIP enabled device with TRIP enabled on a specified interface.

```
<Sysname> debugging rip 1 event
*Oct 23 15:03:39:194 2006 Sysname RM/3/RMDEBUG: TRIP 1 : TRIP’s neig
hbour changes to DOWN status for neighbour deleted.
```

// The neighbor of TRIP process 1 is removed, and the neighbor’s state changed to DOWN.

```
*Oct 23 15:04:07:04 2006 Sysname RM/3/RMDEBUG: TRIP 1 : TRIP’s neigh
bour changes to NEW status.
```

// TRIP process 1 created a new neighbor, and the neighbor state changed to NEW.

```
*Oct 23 15:04:07:14 2006 Sysname RM/3/RMDEBUG: TRIP 1 : TRIP’s neigh
bour changes to UP status.
```

// The neighbor’s state changed to UP.

```
*Oct 23 15:04:07:34 2006 Sysname RM/3/RMDEBUG: TRIP 1 : TRIP’s neigh
bour changes from UP to FULL status.
```

// The neighbor’s state changed from UP to FULL.

default cost (RIP view)

Syntax **default cost** *value*

undo default cost

View RIP view

Parameters *value*: Default metric of redistributed routes.

Description Use the **default cost** command to configure the default metric for redistributed routes.

Use the **undo default cost** command to restore the default.

By default, the default metric of redistributed routes is 0.

When you use the **import-route** command to redistribute routes from other protocols without specifying a metric, the metric specified by the **default cost** command applies.

Related commands: **import-route**.

Examples # Set the default metric for redistributed routes to 3.

```
<Sysname> system-view
[Sysname] rip 100
[Sysname-rip-100] default cost 3
```

default-route originate

Syntax **default-route originate cost** *value*

undo default-route originate

View RIP view

Parameters *value*: Cost of the default route.

Description Use the **default-route originate cost** command to advertise a default route with the specified metric to RIP neighbors.

Use the **undo default-route originate** command to disable the sending of a default route.

By default, no default route is sent to RIP neighbors.

The RIP router with this feature configured will not receive any default routes from RIP neighbors.

Examples # Send a default route with a metric of 2 to RIP neighbors.

```
<Sysname> system-view
[Sysname] rip 100
[Sysname-rip-100] default-route originate cost 2
```

Disable default route sending.

```
[Sysname-rip-100] undo default-route originate
```

display rip

Syntax **display rip** [*process-id* | **vpn-instance** *vpn-instance-name*]

View Any view

Parameters *process-id*: RIP process ID.

vpn-instance *vpn-instance-name*: Specifies a VPN instance name.

Description Use the **display rip** command to display the current status and configuration information of the specified RIP process.

- If *process-id* is not specified, information about all configured RIP processes is displayed.
- If *vpn-instance-name* is specified, the RIP configuration of the specified VPN instance is displayed.

Examples # Display the current status and configuration information of all configured RIP processes.

```
<Sysname> display rip
  Public VPN-instance name :

    RIP process : 1
       RIP version : 1
       Preference : 100
       Checkzero : Enabled
       Default-cost : 0
       Summary : Enabled
       Hostroutes : Enabled
       Maximum number of balanced paths : 8
       Update time   :   30 sec(s)  Timeout time         :  180 sec(s)
       Suppress time :  120 sec(s)  Garbage-collect time :  120 sec(s)
       TRIP retransmit time :    5 sec(s)
       TRIP response packets retransmit count :   36
       Silent interfaces : None
       Default routes : Disabled
       Verify-source : Enabled
       Networks :
           192.168.1.0
       Configured peers : None
       Triggered updates sent : 0
       Number of routes changes : 0
       Number of replies to queries : 0
```

Table 100 Field descriptions of the display rip command

Field	Description
Public VPN-instance name (or Private VPN-instance name)	The RIP process runs under a public VPN instance/The RIP process runs under a private VPN instance
RIP process	RIP process ID
RIP version	RIP version 1 or 2
Preference	RIP route priority
Checkzero	Indicates whether the zero field check is enabled for RIP-1 messages.
Default-cost	Default cost of the redistributed routes
Summary	Indicates whether the routing summarization is enabled
Hostroutes	Indicates whether to receive host routes
Maximum number of balanced paths	Maximum number of load balanced routes
Update time	RIP update interval
Timeout time	RIP timeout time
Suppress time	RIP suppress interval
Garbage-collect time	RIP garbage collection interval
TRIP retransmit time	Interval for retransmitting TRIP update requests and responses
TRIP response packets retransmit count	Maximum retransmission count for update requests and responses
Silent interfaces	Number of silent interfaces, which do not periodically send updates
Default routes	Indicates whether a default route is sent to RIP neighbors
Verify-source	Indicates whether the source IP address is checked on the received RIP routing updates
Networks	Networks enabled with RIP
Configured peers	Configured neighbors
Triggered updates sent	Number of sent triggered updates
Number of routes changes	Number of changed routes in the database
Number of replies to queries	Number of RIP responses

display rip database

Syntax **display rip** *process-id* **database**

View Any view

Parameters *process-id*: RIP process ID.

Description Use the **display rip database** command to display the active routes in the RIP database, which are sent in normal RIP routing updates.

Examples # Display the active routes in the database of RIP process 100.

```
<Sysname> display rip 100 database
  10.0.0.0/8, cost 1, ClassfulSumm
  10.0.0.0/24, cost 1, nexthop 10.0.0.1, Rip-interface
  11.0.0.0/8, cost 1, ClassfulSumm
  11.0.0.0/24, cost 1, nexthop 10.0.0.1, Imported
```

Table 101 Description on fields of the display rip database command

Field	Description
X.X.X.X/X	Destination address and subnet mask
cost	Cost of the route
classful-summ	Indicates the route is a RIP summary route.
Nexthop	Address of the next hop
Rip-interface	Routes learnt from a RIP-enabled interface
imported	Routes redistributed from other routing protocols

display rip interface

Syntax **display rip** *process-id* **interface** [*interface-type interface-number*]

View Any view

Parameters *process-id*: RIP process ID, in the range of 1 to 65535.

interface-type interface-number: Specifies an interface.

Description Use the **display rip interface** command to display the RIP interface information of the RIP process.

If no interface is specified, information about all RIP interfaces of the RIP process is displayed.

Examples # Display all the interface information of RIP process 1.

```
<Sysname> display rip 1 interface

 Interface-name: vlan-interface12
        Address/Mask:1.1.1.1/24                MetricIn/Out:0/1   Version: RIPv1
        Split-horizon/Poison-reverse:on/off     Input/Output:on/on
        Current packets number/Maximum packets number: 234/2000
```

Table 102 Field descriptions of the display rip interface command

Field	Description
Interface-name	The name of an interface running RIP.
Address/Mask	The IP address and Mask of the interface.
MetricIn/Out	Additional routing metric added to the incoming and outgoing routes
Version	RIP version running on the interface
Split-horizon	Indicates whether the split-horizon is enabled (ON: enabled, OFF: disabled).
Poison-reverse	Indicates whether the poison-reverse is enabled (ON: enabled, OFF: disabled)

Table 102 Field descriptions of the display rip interface command

Input/Output	Indicates if the interface is allowed to receiving (Input) or sending (Output) RIP messages (on is allowed, off is not allowed).
Current packets number/Maximum packets number	Packets to be sent/Maximum packets that can be sent on the interface

display rip route

Syntax **display rip** *process-id* **route** [**statistics** | *ip-address* { *mask* | *mask-length* } | **peer** *ip-address*]

View Any view

Parameters *process-id*: RIP process ID.

statistics: Displays the route statistics, including total number of routes and number of routes of each neighbor.

ip-address { *mask* | *mask-length* }: Displays route information about a specified IP address.

peer *ip-address*: Displays all routing information learned from a specified neighbor.

Description Use the **display rip route** command to display the routing information of a specified RIP process.

Examples # Display all routing information of RIP process 1.

```
<Sysname> display rip 1 route
 Route Flags: R-RIP, T-TRIP
              P-Permanent, A-Aging, S-Suppressed, G-Garbage-collect
Peer 21.0.0.23 on Ethernet1/0
Destination/Mask    NextHop      Cost     Tag    Flags     Sec
56.0.0.0/8         21.0.0.23      1         0       RA     102
34.0.0.0/8         21.0.0.23      1         0       RA      23
Peer 21.0.0.12 on Ethernet1/0
Destination/Mask    NextHop      Cost     Tag    Flags     Sec
56.0.0.0/8         21.0.0.12      1         0       RA      34
12.0.0.0/8         21.0.0.12      1         0       RA      12
```

Display routing information for network 56.0.0.0/8 of RIP process 1.

```
<Sysname> display rip 1 route 56.0.0.0 8
Route Flags: R-RIP, T-TRIP
             P-Permanent, A-Aging, S-Suppressed, G-Garbage-collect
Peer 21.0.0.23 on vlan-interface 12
Destination/Mask    NextHop      Cost     Tag    Flags     Sec
56.0.0.0/8         21.0.0.23      1         0       RA     102
Peer 21.0.0.12 on vlan-interface 12
Destination/Mask    NextHop      Cost     Tag    Flags     Sec
56.0.0.0/8         21.0.0.12      1         0       RA      34
```

Display RIP process1 routing information learned from the specified neighbor.

```
<Sysname> display rip 1 route peer 21.0.0.23
Route Flags: R-RIP, T-TRIP
             P-Permanent, A-Aging, S-Suppressed, G-Garbage-collect
Peer 21.0.0.23 on vlan-interface 12
Destination/Mask    NextHop      Cost     Tag    Flags     Sec
56.0.0.0/8          21.0.0.23      1        0       RA        102
34.0.0.0/8          21.0.0.23      1        0       RA        23
```

Table 103 Field descriptions of the display rip route command

Field	Description
Route Flags	R - RIP route
	T - TRIP route
	P - The route never expires
	A - The route is aging
	S - The route is suppressed
	G - The route is in Garbage-collect state
Peer 21.0.0.23 on vlan-interface12	Routing information learned on a RIP interface from the specified neighbor
Destination/Mask	Destination IP address and subnet mask
Nexthop	Next hop of the route
Cost	Cost of the route
Tag	Route tag
Flags	The first character indicates the route is generated by RIP or TRIP, and the second character indicates the route state.
Sec	Elapsed time of the timer corresponding to the route state

Display the routing statistics of RIP process 1.

```
<Sysname> display rip 1 route statistics
Peer         Aging     Permanent    Garbage
21.0.0.23      2          0             3
21.0.0.12      2          0             4
Total          4          0             7
```

Table 104 Field descriptions of the display rip route statistics command

Field	Description
Peer	IP address of a neighbor
Aging	Total number of aging routes learned from the specified neighbor
Permanent	Total number of permanent routes learned from the specified neighbor
Garbage	Total number of routes in the garbage-collection state learned from the specified neighbor
Total	Total number of routes learned from all RIP neighbors

filter-policy export (RIP view)

Syntax **filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [*protocol* [*process-id*] | *interface-type interface-number*]

undo filter-policy export [*protocol* [*process-id*] | *interface-type interface-number*]

View RIP view

Parameters *acl-number*: Number of the Access Control List (ACL) used for filtering outbound routes.

ip-prefix *ip-prefix-name*: Name of the IP prefix list used for filtering outbound routes.

protocol: Filters outbound routes redistributed from a specified routing protocol, which can be **bgp**, **direct**, **isis**, **ospf**, **rip**, and **static**.

process-id: Process ID of the specified routing protocol. You need to specify a process ID when the routing protocol is **rip**, **ospf**, or **isis**.

interface-type interface-number: Specifies an interface.

Description Use the **filter-policy export** command to define a RIP route outbound filtering policy. Only routes not filtered out can be advertised.

Use the **undo filter-policy export** command to remove the configured filtering policy.

By default, RIP does not filter outbound routes.

Note that:

- If *protocol* is specified, RIP filters only the routes redistributed from the specified routing protocol. Otherwise, RIP filters all routes to be advertised.
- If *interface-type interface-number* is specified, RIP filters only the routes advertised by the specified interface. Otherwise, RIP filters routes advertised by all RIP interfaces.

Related commands: **acl**, **import-route**, and **ip ip-prefix**.

Examples # Reference ACL 2000 to filter outbound routes.

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] filter-policy 2000 export
```

Reference IP prefix list abc to filter outbound routes on Vlan-interface 100.

```
[Sysname-rip-1] filter-policy ip-prefix abc export static Vlan-interface 100
```

filter-policy import (RIP view)

Syntax **filter-policy** { *acl-number* | **gateway** *ip-prefix-name* | **ip-prefix** *ip-prefix-name* [**gateway** *ip-prefix-name*] } **import** [*interface-type interface-number*]

undo filter-policy import [*interface-type interface-number*]

View RIP view

Parameters *acl-number*: Number of the Access Control List (ACL) used for filtering incoming routes.

ip-prefix *ip-prefix-name*: References an IP prefix list to filter incoming routes.

gateway *ip-prefix-name*: References an IP prefix list to filter routes from the gateway.

interface-type interface-number: Specifies an interface.

Description Use the **filter-policy import** command to filter the incoming routes.

Use the **undo filter-policy import** command to restore the default.

By default, RIP does not filter incoming routes.

Related commands: **acl** and **ip ip-prefix**.

Examples # Reference ACL 2000 to filter incoming routes.

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] filter-policy 2000 import
```

host-route

Syntax **host-route**

undo host-route

View RIP view

Parameters None

Description Use the **host-route** command to enable host route reception.

Use the **undo host-route** command to disable host route reception.

By default, receiving host routes is enabled.

In some cases, a routing device may receive many host routes from the same network segment. These routes are not helpful for routing and occupy a large amount of network resources. You can use the **undo host-route** command to disable receiving of host routes.

Examples # Disable RIP from receiving host routes.

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] undo host-route
```

import-route (RIP view)

Syntax **import-route** *protocol* [*process-id*] [**allow-jbgp**] [**cost** *cost* | **route-policy** *route-policy-name* | **tag** *tag*]*

undo import-route *protocol* [*process-id*]

View RIP view

Parameters *protocol*: Specify a routing protocol from which to redistribute routes, currently including **bgp**, **direct**, **isis**, **ospf**, **rip**, **rip** and **static**.

process-id: Process ID of the routing protocol, used for **isis**, **rip**, and **ospf**.

cost: Cost for redistributed routes. If *cost* is not specified, the default cost specified by the **default cost** command applies.

tag: Tag marking redistributed routes. The default is 0.

route-policy *route-policy-name*: Specifies a routing policy with 1 to 19 characters.

allow-ibgp: When the *protocol* argument is set to **bgp**, **allow-ibgp** is an optional keyword. The **import-route bgp** command only redistributes EBGP routes, while the **import-route bgp allow-ibgp** command additionally redistributes IBGP routes, which may cause routing loops. Be cautious when using it.

Description Use the **import-route** command to redistribute routes from other routing protocols.

Use the **undo import-route** command to cancel route redistribution.

By default, RIP does not redistribute routes from other routing protocols.

- You can specify a routing policy using keyword **route-policy** to redistribute only the specified routes.
- You can configure a cost for redistributed routes using keyword **cost**.
- You can configure a tag value for redistributed routes using keyword **tag**.

Related commands: **default cost**.

Examples # Redistribute static routes, and set the cost to 4.

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] import-route static cost 4
```

Set the default cost for redistributed OSPF routes to 3.

```
[Sysname-rip-1] default cost 3
[Sysname-rip-1] import-route ospf
```

maximum load-balancing (RIP view)

Syntax **maximum load-balancing** *number*

undo maximum load-balancing

View RIP view

Parameters *number*: Maximum number of equal cost routes for load balancing.

Description Use the **maximum load-balancing** command to specify the maximum number of equal cost routes for load balancing.

Use the **undo maximum load-balancing** command to restore the default.

Examples # Specify the maximum number of equal cost routes for load balancing as 2.

```
<Sysname> system-view
[Sysname] rip
[Sysname-rip-1] maximum load-balancing 2
```

network (RIP view)

Syntax **network** *network-address*

undo network *network-address*

View RIP view

Parameters *network-address*: IP address of a network segment, which can be the IP network address of any interface.

Description Use the **network** command to enable RIP on the interface attached to the specified network.

Use the **undo network** command to disable RIP on the interface attached to the specified network.

Use the **network** 0.0.0.0 command to enable RIP on all interfaces.

RIP is disabled on an interface by default.

Examples # Enable RIP on the interface attached to the network 129.102.0.0.

```
<Sysname> system-view
[Sysname] rip 100
[Sysname-rip-100] network 129.102.0.0
```

peer (RIP view)

Syntax **peer** *ip-address*

undo peer *ip-address*

View RIP view

Parameters *ip-address*: IP address of a peer device, in dotted decimal format.

Description Use the **peer** command to specify the IP address of a neighbor in the non-broadcast multi-access (NBMA) network, where routing updates destined to the peer are unicast, rather than multicast or broadcast.

Use the **undo peer** command to remove the IP address of a neighbor.

By default, no neighbor is specified.

you need not use the **peer** *ip-address* command when the neighbor is directly connected; otherwise the neighbor may receive both the unicast and multicast (or broadcast) of the same routing information.

Examples # Specify to send unicast updates to peer 202.38.165.1.

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] peer 202.38.165.1
```

preference (RIP view)

Syntax **preference** [**route-policy** *route-policy-name*] *value*

undo preference [**route-policy**]

View RIP view

Parameters *route-policy-name*: Routing policy name.

value: Priority for RIP routes. The smaller the value, the higher the priority.

Description Use the **preference** command to specify the RIP route priority.

Use the **undo preference route-policy** command to restore the default.

By default, the priority of RIP route is 100.

You can specify a routing policy using keyword **route-policy** to set the specified priority to routes matching the routing policy.

- If a priority is set for matched routes in the routing policy, the priority applies to these routes. The priority of other routes is the one set by the **preference** command.
- If no priority is set for matched routes in the routing policy, the priority of all routes is the one set by the **preference** command.

Examples # Set the priority of RIP routes to 120.

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] preference 120
```

reset rip statistics

Syntax **reset rip** *process-id* **statistics**

View User view

Parameters *process-id*: RIP process ID.

Description Use the **reset rip statistics** command to clear the statistics of the specified RIP process.

Examples # Clear statistics of RIP process 100.

```
<Sysname> reset rip 100 statistics
```

rip

Syntax **rip** [*process-id*] [**vpn-instance** *vpn-instance-name*]

undo rip [*process-id*] [**vpn-instance** *vpn-instance-name*]

View System view

Parameters *process-id*: RIP process ID. The default is 1.

vpn-instance *vpn-instance-name*: Specifies a VPN instance name.

Description Use the **rip** command to enable a RIP process and enter RIP view.

Use the **undo rip** command to disable a RIP process.

By default, no RIP process runs.

Note that:

- If no VPN instance is specified, the RIP process will run under public network instance.
- You must create a VPN instance before you apply a RIP process to it. For related configuration, refer to the **ip vpn-instance** command.
- You must enable the RIP process before configuring the global parameters. This limitation is not for configuration of interface parameters.
- The configured interface parameters become invalid after you disable the RIP process.

Examples # Enable a RIP process and enter its view.

```
<Sysname> system-view
[Sysname] rip
[Sysname-rip-1]
```

rip authentication-mode

Syntax **rip authentication-mode** { **md5** { **rfc2082** *key-string key-id* | **rfc2453** *key-string* } | **simple** *password* }

undo rip authentication-mode

View Interface view

Parameters **md5**: MD5 authentication mode.

rfc2453: Uses the message format defined in RFC 2453 (IETF standard).

rfc2082: Uses the message format defined in RFC 2082.

key-id: MD5 key number, in the range of 1 to 255.

key-string: MD5 key string with 1 to 16 characters in plain text format, or 1 to 24 characters in cipher text format. When the **display current-configuration** command is used to display system information, a 24-character cipher string is displayed as the MD5 key string.

simple: Plain text authentication mode.

password: Plain text authentication string with 1 to 16 characters.

Description Use the **rip authentication-mode** command to configure RIP-2 authentication mode and parameters.

Use the **undo rip authentication-mode** command to cancel authentication.

Note that the key string you configured can overwrite the old one if there is any.

Related commands: **rip version**.

Examples # Configure MD5 authentication on Vlan-interface10 with the key string being rose in the format defined in RFC 2453.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rip version 2
[Sysname-Vlan-interface10] rip authentication-mode md5 rfc2453 rose
```

rip input

Syntax **rip input**

undo rip input

View Interface view

Parameters None

Description Use the **rip input** command to enable the interface to receive RIP messages.

Use the **undo rip input** command to disable the interface from receiving RIP messages.

By default, an interface is enabled to receive RIP messages.

Related commands: **rip output**.

Examples # Disable Vlan-interface10 from receiving RIP messages.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] undo rip input
```

rip metricin

Syntax **rip metricin** *value*

undo rip metricin

View Interface view

Parameters *value*: Additional metric added to received routes. The default is 0.

Description Use the **rip metricin** command to add a metric to the received routes.

Use the **undo rip metricin** command to restore the default.

When a valid RIP route is received, the system will add a metric to it and then put it into the routing table. Therefore, the metric of routes received on the configured interface is increased.

Related commands: **rip metricout**.

Examples # Configure an additional metric of 2 for routes received on Vlan-interface10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rip metricin 2
```

rip metricout

Syntax **rip metricout** *value*

undo rip metricout

View Interface view

Parameters *value*: Additional metric of sent routes. The default is 1.

Description Use the **rip metricout** command to add a metric to a sent route.

Use the **undo rip metricout** command to restore the default.

Before a RIP route is sent, a metric will be added to it. Therefore, when the metric is configured on an interface, the metric of RIP routes sent on the interface will be increased.

Related commands: **rip metricin**.

Examples # Configure an additional metric of 12 for RIP routes sent on Vlan-interface10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rip metricout 12
```

rip mib-binding

Syntax **rip mib-binding** *process-id*

undo rip mib-binding

View System view

Parameters *process-id*: RIP process ID.

Description Use the **rip mib-binding** command to bind MIB operations with a specified RIP process.

Use the **undo rip mib-binding** command to restore the default.

By default, MIB operations are bound to the RIP process with the smallest process ID.

Examples # Configure RIP 100 to accept SNMP requests.

```
<Sysname> system-view
[Sysname] rip mib-binding 100
```

Restore the default.

```
[Sysname] undo rip mib-binding
```

rip output

Syntax **rip output**

undo rip output

View Interface view

Parameters None

Description Use the **rip output** command to enable the interface to send RIP messages.

Use the **undo rip output** command to disable the interface from sending RIP messages.

Sending RIP messages is enabled on an interface by default.

Related commands: **rip input**.

Examples # Disable Vlan-interface10 from receiving RIP messages.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] undo rip output
```

rip poison-reverse

Syntax **rip poison-reverse**

undo rip poison-reverse

View Interface view

Parameters **None**

Description Use the **rip poison-reverse** command to enable the poison reverse function.

Use the **undo rip poison-reverse** command to disable the poison reverse function.

By default, the poison reverse function is disabled.

Examples # Enable the poison reverse function for RIP routing updates on Vlan-interface10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rip poison-reverse
```

rip split-horizon

Syntax **rip split-horizon**

undo rip split-horizon

View Interface view

Parameters None

Description Use the **rip split-horizon** command to enable the split horizon function.

Use the **undo rip split-horizon** command to disable the split horizon function.

The split horizon function is enabled by default.

- The split horizon function is necessary for preventing routing loops. Therefore, you are not recommended to disable it.
- In special cases, make sure it is necessary to disable the split horizon function.

Only the poison reverse function takes effect if both the split horizon and poison reverse functions are enabled.

Examples # Enable the split horizon function on Vlan-interface10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rip split-horizon
```

rip summary-address

Syntax **rip summary-address** *ip-address* { *mask* | *mask-length* }

undo rip summary-address *ip-address* { *mask* | *mask-length* }

View Interface view

Parameters *ip-address*: Summary IP address.

mask: Subnet mask in dotted decimal format.

mask-length: Subnet mask length.

Description Use the **rip summary-address** command to configure RIP-2 to advertise a summary route via the interface.

Use the **undo rip summary-address** command to remove the configuration.

Note that the summary address is valid only when the automatic summarization is disabled.

Related commands: **summary**.

Examples # Advertise a local summary IP address on Vlan-interface10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rip summary-address 10.0.0.0 255.255.255.0
```

rip triggered

Syntax **rip triggered**

undo rip triggered

View Interface view

Parameters None

Description Use the **rip triggered** command to enable triggered RIP.

Use the **undo rip triggered** command to disable triggered RIP.

By default, the triggered RIP is disabled.

Note that triggered RIP can only run on link layer protocols PPP, Frame Relay, and X.25.

Examples # Enable triggered RIP.

```
<Sysname> system-view
[Sysname] interface pos 6/1/1
[Sysname-pos 6/1/1] rip triggered
```

rip version

Syntax **rip version** { **1** | **2** [**broadcast** | **multicast**] }

undo rip version

View Interface view

Parameters **1**: RIP version 1.

2: RIP version 2.

broadcast: Sends RIP-2 messages in broadcast mode.

multicast: Sends RIP-2 messages in multicast mode.

Description Use the **rip version** command to specify a RIP version for the interface.

Use the **undo rip version** command to remove the specified RIP version.

By default, no RIP version is configured for an interface, which uses the global RIP version. If the global RIP version is not configured, the interface can only send RIP-1 broadcasts and can receive RIP-1 broadcasts and unicasts, and RIP-2 broadcasts, multicasts and unicasts.

If RIP-2 is specified with no sending mode configured, RIP-2 messages will be sent in multicast mode.

When RIP-1 runs on an interface, the interface will:

- Send RIP-1 broadcast messages
- Receive RIP-1 broadcast messages
- Receive RIP-1 unicast messages

When RIP-2 runs on the interface in broadcast mode, the interface will:

- Send RIP-2 broadcast messages
- Receive RIP-1 broadcast messages
- Receive RIP-1 unicast messages
- Receive RIP-2 broadcast messages
- Receive RIP-2 multicast messages
- Receive RIP-2 unicast messages

When RIP-2 runs on the interface in multicast mode, the interface will:

- Send RIP-2 multicast messages
- Receive RIP-2 broadcast messages
- Receive RIP-2 multicast messages
- Receive RIP-2 unicast messages

Examples # Configure Vlan-interface10 to broadcast RIP-2 messages.

```
<Sysname> system-view
[Sysname] interface Vlan-interface 10
[Sysname-Vlan-interface10] rip version 2 broadcast
```

silent-interface (RIP view)

Syntax **silent-interface** { **all** | *interface-type interface-number* }

undo silent-interface { **all** | *interface-type interface-number* }

View RIP view

Parameters **all**: Silents all interfaces.

interface-type interface-number: Specifies an interface.

Description Use the **silent-interface** command to disable an interface or all interfaces from sending routing updates. That is, the interface only receives but does not send RIP messages.

Use the **undo silent-interface** command to restore the default.

By default, all interfaces are allowed to send routing updates.

Examples # Configure all Vlan interfaces to work in the silent state, and activate Vlan-interface10.

```
<Sysname> system-view
[Sysname] rip 100
[Sysname-rip-100] silent-interface all
[Sysname-rip-100] undo silent-interface vlan-interface 10
[Sysname-rip-100] network 131.108.0.0
```

summary

Syntax **summary**

undo summary

View RIP view

Parameters None

Description Use the **summary** command to enable automatic RIP-2 summarization. Natural masks are used to advertise summary routes so as to reduce the size of routing tables.

Use the **undo summary** command to disable automatic RIP-2 summarization so that all subnet routes can be broadcasted.

By default, automatic RIP-2 summarization is enabled.

Enabling automatic RIP-2 summarization can reduce the size of the routing table to enhance the scalability and efficiency of large networks.

Related commands: **rip version**.

Examples # Enable RIP-2 automatic summarization.

```
<Sysname> system-view
[Sysname] rip
[Sysname-rip-1] summary
```

timers (RIP view)

Syntax **timers** { **garbage-collect** *garbage-collect-value* | **suppress** *suppress-value* | **timeout** *timeout-value* | **update** *update-value* }*

undo timers { **garbage-collect** | **suppress** | **timeout** | **update** } *

View RIP view

Parameters *garbage-collect-value*: Garbage-collect timer time in seconds.

suppress-value: Suppress timer time in seconds.

timeout-value: Timeout timer time in seconds. The value should be at least three times the update timer value.

update-value: Update timer time in seconds.

Description Use the **timers** command to configure RIP timers. By adjusting RIP timers, you can improve network performance.

Use the **undo timers** command to restore the default.

By default, the garbage-collect timer is 120 seconds, the suppress timer 120 seconds, the timeout timer 180 seconds, and the update timer 30 seconds.

RIP is controlled by the above four timers.

- The update timer defines the interval between routing updates.
- The timeout timer defines the route aging time. If no routing update related to a route is received after the aging time, the metric of the route is set to 16 in the routing table.
- The suppress timer defines how long a RIP route stays in the suppressed state. When the metric of a route is 16, the route enters the suppressed state. In the suppressed state, only routes which come from the same neighbor and whose metric is less than 16 will be received by the device to replace unreachable routes.
- The garbage-collect timer defines the interval from when the metric of a route becomes 16 to when it is deleted from the routing table. During the Garbage-Collect timer length, RIP advertises the route with the routing metric set to 16. If no routing update is announced for that route after the Garbage-Collect timer expires, the route will be deleted from the routing table.

Note that:

- Generally, you are not recommended to change the default values of these timers.
- The time lengths of these timers must be kept consistent on all routing devices and access servers in the network.

Examples # Specifies the update, timeout, suppress, and garbage-collect timers as 5, 15, 15 and 30 respectively.

```
<Sysname> system-view
[Sysname] rip 100
[Sysname-rip-100] timers update 5
[Sysname-rip-100] timers timeout 15
[Sysname-rip-100] timers suppress 15
[Sysname-rip-100] timers garbage-collect 30
```

trip retransmit count

Syntax **trip retransmit count** *retransmit-count-value*

undo trip retransmit count

View RIP view

Parameters ***retransmit-count-value:*** **Upper limit for retransmitting an Update Request or Update Response.**

Description Use the **trip retransmit count** command to configure the upper limit for retransmitting an Update Request or Update Response.

Use the **undo validate-source-address** command to restore the default.

The default upper limit is 36.

Examples # Configure an upper limit of 20 for retransmitting an Update Request or Update Response.

```
<Sysname> system-view
[Sysname] rip 100
[Sysname-rip-100] trip retransmit count 20
```

trip retransmit timer

Syntax **trip retransmit timer** *retransmit-time-value*

undo trip retransmit timer

View RIP view

Parameters ***retransmit-time-value:*** **Interval in seconds for retransmitting an Update Request or Update Response.**

Description Use the **trip retransmit timer** command to configure the interval for retransmitting an Update Request or Update Response.

Use the **undo validate-source-address** command to restore the default.

The default interval is 5 seconds.

For two routers on an analog dial-up link, the difference between retransmission intervals on the two ends must be bigger than 50 seconds; otherwise, they can not become TRIP neighbors.

Examples # Configure an interval of 80 seconds for retransmitting an Update Request or Update Response.

```
<Sysname> system-view
[Sysname] rip 100
[Sysname-rip-100] trip retransmit timer 80
```

validate-source-address

Syntax **validate-source-address**

undo validate-source-address

View RIP view

Parameters **None**

Description Use the **validate-source-address** command to enable the source IP address validation on incoming RIP routing updates.

Use the **undo validate-source-address** command to disable the source IP address validation.

The source IP address validation is enabled by default.

Generally, disabling the validation is not recommended.

Examples # Enable the source IP address validation on incoming messages.

```
<Sysname> system-view
[Sysname-rip] rip 100
[Sysname-rip-100] validate-source-address
```

version (RIP view)

Syntax **version** { **1** | **2** }

undo version

View RIP view

Parameters **1**: Specifies the RIP version as RIP-1.

2: Specifies the RIP version as RIP-2. RIP-2 messages are multicast.

Description Use the **version** command to specify a global RIP version.

Use the **undo version** command to remove the configured global RIP version.

By default, the global RIP version is RIP-1.

Note that:

- If an interface has an RIP version specified, the RIP version takes precedence over the global one.
- If no RIP version is specified for the interface and the global version is RIP-1, the interface inherits RIP-1, and then it can send RIP-1 broadcasts, and receive RIP-1 broadcasts and unicasts.
- If no RIP version is specified for the interface and the global version is RIP-2, the interface inherits RIP-2, and then it can send RIP-2 multicasts, and receive RIP-2 broadcasts, multicasts and unicasts

Note that the global RIP version takes effect on RIP interfaces only when no interface RIP version is configured.

Examples # Specify RIP-2 as the global RIP version.

```
<Sysname> system-view
[Sysname] rip 100
[Sysname-rip-100] version 2
```

34 IPv6 RIPng Configuration Commands

checkzero (RIPng view)

Syntax **checkzero**

undo checkzero

View RIPng view

Parameter None

Description Use the **checkzero** command to enable the zero field check on RIPng packets.

Use the **undo checkzero** command to disable the zero field check.

The zero field check is enabled by default.

Some fields in RIPng packet headers must be zero. These fields are called zero fields. You can enable the zero field check on RIPng packet headers. If any such field contains a non-zero value, the RIPng packet will be discarded.

Example # Disable the zero field check on RIPng packet headers of RIPng 100.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] undo checkzero
```

debugging ripng

Syntax **debugging ripng** *process-id* [**brief** | **event** | **packet** | **receive** | **send** | **timer**]

undo debugging ripng *process-id* { **brief** | **event** | **packet** | **receive** | **send** | **timer** }

debugging ripng *process-id* { **packet** | **receive** | **send** } [**interface** *interface-type interface-number*]

undo debugging ripng *process-id* { **packet** | **receive** | **send** } [**interface** *interface-type interface-number*]

View User view

Parameter *process-id*: RIPng process ID.

brief: Displays brief RIPng debugging information.

event: RIPng event debugging.

packet: RIPng packet debugging.

receive: Debugging of received RIPng packets.

send: Debugging of sent RIPng packets.

timer: RIPng timer debugging.

interface *interface-type interface-number*: Displays the specified RIPng debugging information of an interface.

Description Use the **debugging ripng** command to enable specified RIPng debugging.

Use the **undo debugging ripng** command to disable specified RIPng debugging.

The keyword **interface** is usable only when the keyword **packet**, **receive** or **send** is included.

The **debugging ripng** command with the keyword **interface** not specified displays the debugging information of RIPng packets sent and received by all interfaces. With the keyword **interface** included, the command displays the debugging information of RIPng packets sent and received by the interface.

Example # Display the debugging information of sent RIPng packets.

```
<Sysname> debugging ripng 1 send
*0.84520 RTA RM/7/RMDEBUG:RIPng 1 : Sending response message on vlan
-interface 12 to FF02::9
*0.84520 RTA RM/7/RMDEBUG: Packet : vers 1, cmd response, length 84
*0.84520 RTA RM/7/RMDEBUG: Dest 1:12::/120, cost 5, tag 0
*0.84520 RTA RM/7/RMDEBUG: Dest 1:13::/120, cost 5, tag 0
*0.84520 RTA RM/7/RMDEBUG: Dest 1:32::/120, cost 5, tag 0
*0.84520 RTA RM/7/RMDEBUG: Dest 1:33::/120, cost 5, tag 0
```

Display the debugging information of received RIPng packets.

```
<Sysname> debugging ripng 1 receive
*0.85450 RTA RM/7/RMDEBUG:RIPng 1 : Receiving response message from
FE80::200:5E
FF:FE04:3302 on vlan-interface 12
*0.85450 RTA RM/7/RMDEBUG: Packet : vers 1, cmd response, length 504
*0.85450 RTA RM/7/RMDEBUG: Dest 100::/32, metric 2, tag 0
*0.85450 RTA RM/7/RMDEBUG: Dest 4000:1::/64, cost 2, tag 0
*0.85450 RTA RM/7/RMDEBUG: Dest 4000:2::/64, cost 2, tag 0
*0.85450 RTA RM/7/RMDEBUG: Dest 4000:3::/64, cost 2, tag 0
*0.85450 RTA RM/7/RMDEBUG: Dest 4000:4::/64, cost 2, tag 0
*0.85450 RTA RM/7/RMDEBUG: Dest 4000:5::/64, cost 2, tag 0
*0.85450 RTA RM/7/RMDEBUG: Dest 4000:6::/64, cost 2, tag 0
*0.85450 RTA RM/7/RMDEBUG: Dest 4000:7::/64, cost 2, tag 0
*0.85450 RTA RM/7/RMDEBUG: Dest 4000:8::/64, cost 2, tag 0
```

Display the debugging information of RIPng packets received by Vlan-interface12..

```
<Sysname> debugging ripng 1 receive interface vlan-interface 12
*0.718490 RTB RM/7/RMDEBUG:RIPng 100 : Receiving response message from FE80:
C00:C18:5:: on vlan-interface 12
*0.718500 RTB RM/7/RMDEBUG: Packet : version 1, command response, length 104
*0.718510 RTB RM/7/RMDEBUG: Dest 3FFE:C00:C18:1::/64, metric 3, tag 0
*0.718520 RTB RM/7/RMDEBUG: Dest 3FFE:C00:C18:2::/64, metric 3, tag 0
*0.718530 RTB RM/7/RMDEBUG: Dest 3FFE:C00:C18:3::/64, metric 3, tag 0
*0.718540 RTB RM/7/RMDEBUG: Dest 3FFE:C00:C18:4::/64, metric 3, tag 0
*0.718560 RTB RM/7/RMDEBUG: Dest 3FFE:C00:C18:5::/64, metric 8, tag 0
```

Display the RIPng event debugging information.

```
<Sysname> debugging ripng 1 event
*0.125140  Sysname RM/7/RMDEBUG:RIPng 1 : Adding LoopBack0 to Network List
*0.131510  Sysname RM/7/RMDEBUG:RIPng 1 : Removing LoopBack0 from Network List
```

Display the RIPng timer debugging information.

```
<Sysname> debugging ripng 1 timer
*0.605600  Sysname RM/7/RMDEBUG:RIPng 1 : Periodic timer expired
```

Table 105 Field descriptions of the debugging ripng command

Field	Description
Dest	Destination IPv6 address
cost/metric	Cost of RIPng
tag	Route tag

default cost (RIPng view)

Syntax **default cost** *cost*

undo default cost

View RIPng view

Parameter *cost*: Default metric of redistributed routes. The default is 0.

Description Use the **default cost** command to specify the default metric of redistributed routes.

Use the **undo default cost** command to restore the default.

By default, the default metric of redistributed routes is 0.

The specified default metric applies to routes redistributed by the **import-route** command that has no metric specified.

Related commands: import-route.

Examples # Set the default metric of redistributed routes to 2.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] default cost 2
```

display ripng

Syntax **display ripng** [*process-id*]

View Any view

Parameters *process-id*: RIPng process ID.

Description Use the **display ripng** command to display the running status and configuration information of a RIPng process. If *process-id* is not specified, information of all RIPng processes will be displayed.

Examples # Display the running status and configuration information of all configured RIPng processes.

```
<Sysname> display ripng
    RIPng process : 1
       Preference : 100
       Checkzero : Enabled
       Default Cost : 0
       Maximum number of balanced paths : 3
       Update time  :   30 sec(s)  Timeout time           :  180 sec(s)
       Suppress time    :  120 sec(s)  Garbage-Collect time :  120 sec(s)
       Number of periodic updates sent : 0
       Number of trigger updates sent : 0
```

Table 106 Field descriptions of the display ripng command

Field	Description
RIPng Process	RIPng process ID
Preference	RIPng route priority
Checkzero	Whether zero field check for RIPng packet headers is enabled
Default Cost	Default metric of redistributed routes
Maximum number of balanced paths	Maximum number of load balanced routes
Update time	RIPng updating interval, in seconds
Timeout time	RIPng timeout interval, in seconds
Suppress time	RIPng suppress interval, in seconds
Garbage-Collect time	RIPng garbage collection interval, in seconds
Number of periodic updates sent	Number of periodic updates sent
Number of trigger updates sent	Number of triggered updates sent

display ripng database

Syntax **display ripng *process-id* database**

View Any view

Parameters *process-id*: RIPng process ID.

Description Use the **display ripng database** command to display all active routes in the RIPng advertising database, which are sent in normal RIPng update messages.

Examples # Display the active routes in the database of RIPng process 100.

```
<Sysname> display ripng 100 database
   2001:7B::2:2A1:5DE/64,
        cost 4, Imported
   1:13::/120,
        cost 4, Imported
   1:32::/120,
        cost 4, Imported
   1:33::/120,
        cost 4, Imported
   100::/32,
       via FE80::200:5EFF:FE04:3302, cost 2
   3FFE:C00:C18:1::/64,
       via FE80::200:5EFF:FE04:B602, cost 2
   3FFE:C00:C18:1::/64,
       via FE80::200:5EFF:FE04:B601, cost 2
   3FFE:C00:C18:2::/64,
       via FE80::200:5EFF:FE04:B602, cost 2
   3FFE:C00:C18:3::/64,
       via FE80::200:5EFF:FE04:B601, cost 2
   4000:1::/64,
       via FE80::200:5EFF:FE04:3302, cost 2
   4000:2::/64,
       via FE80::200:5EFF:FE04:3302, cost 2
```

Table 107 Description on fields of the display ripng database command

Field	Description
2001:7B::2:2A1:5DE/64	IPv6 destination address/prefix length
via	Next hop IPv6 address
cost	Route metric value
Imported	Routes learnt from other routing protocols

display ripng interface

Syntax **display ripng** *process-id* **interface** [*interface-type interface-number*]

View Any view

Parameters *process-id*: RIPng process ID.

interface-type interface-number: Specified an interface.

Description Use the **display ripng interface** command to display the interface information of the RIPng process.

Examples # Display the interface information of RIPng process 1.

```
<Sysname> display ripng 1 interface

    Interface-name: vlan-interface 12

     Link Local Address: FE80::200:5EFF:FE19:3E00

     Split-horizon: on Poison-reverse: off

     MetricIn: 0 MetricOut: 1

     Default route: off
```

Table 108 Field descriptions of the display ripng interface command

Field	Description
Interface-name	Name of an interface running RIPng.
Link Local Address	Link-local address of an interface running RIPng
Split-horizon	Indicates whether the split horizon function is enabled (on: Enabled off: Disabled).
Poison-reverse	Indicates whether the poison reverse function is enabled (on: Enabled off: Disabled).
MetricIn/MetricOut	Additional metric to incoming and outgoing routes
Default route	■ Only/Originate: Only means that the interface advertises only the default route. Originate means that the default route and other RIPng routes are advertised. ■ Off, indicates that no default route is advertised or the garbage-collect time expires after the default route advertisement was disabled. ■ In garbage-collect status: With default route advertisement disabled, the interface advertises the default route with metric 16 during the garbage-collect time.

display ripng route

Syntax **display ripng** *process-id* **route**

View Any view

Parameters *process-id*: RIPng process ID.

Description Use the **display ripng route** command to display all RIPng routes and timers associated to each route of a RIPng process.

Examples # Display the routing information of RIPng process 100.

```
<Sysname> display ripng 100 route
   Route Flags: A - Aging, S - Suppressed, G - Garbage-collect
 ----------------------------------------------------------------
 Peer FE80::200:5EFF:FE04:B602  on vlan-interface 12
 Dest 3FFE:C00:C18:1::/64,
```

```
    via FE80::200:5EFF:FE04:B602, cost  2, tag 0, A, 34 Sec
Dest 3FFE:C00:C18:2::/64,
    via FE80::200:5EFF:FE04:B602, cost  2, tag 0, A, 34 Sec

Peer FE80::200:5EFF:FE04:B601 on vlan-interface 12
Dest 3FFE:C00:C18:1::/64,
    via FE80::200:5EFF:FE04:B601, cost  2, tag 0, A, 13 Sec
Dest 3FFE:C00:C18:3::/64,
    via FE80::200:5EFF:FE04:B601, cost  2, tag 0, A, 13 Sec

Peer FE80::200:5EFF:FE04:3302  on vlan-interface 12
Dest 100::/32,
    via FE80::200:5EFF:FE04:3302, cost  2, tag 0, A, 6 Sec
Dest 4000:1::/64,
    via FE80::200:5EFF:FE04:3302, cost  2, tag 0, A, 6 Sec
Dest 4000:2::/64,
    via FE80::200:5EFF:FE04:3302, cost  2, tag 0, A, 6 Sec
Dest 4000:3::/64,
    via FE80::200:5EFF:FE04:3302, cost  2, tag 0, A, 6 Sec
Dest 4000:4::/64,
```

Table 109 Field descriptions of the display ripng route command

Field	Description
Peer	Neighbor connected to the interface
Dest	IPv6 destination address
via	Next hop IPv6 address
cost	Routing metric value
tag	Route tag
Sec	Time that a route entry stays in a particular state
A"	The route is in the aging state
S"	The route is in the suppressed state
G"	The route is in the Garbage-collect state

filter-policy export (RIPng view)

Syntax **filter-policy** { *acl6-number* | **ipv6-prefix** *ipv6-prefix-name* } **export** [*protocol* [*process-id*]]

undo filter-policy export [*protocol* [*process-id*]]

View RIPng view

Parameters *acl6-number*: Specifies the number of an ACL to filter outgoing routing information, in the range of 2000 to 3999.

ipv6-prefix *ipv6-prefix-name*: Specifies the name of an IPv6 prefix list used to filter outgoing routing information.

protocol: Filter routes redistributed from a routing protocol, currently including **bgp4+**, **direct**, **isisv6**, **ospfv3**, **ripng**, and **static**.

process-id: Process ID of the specified routing protocol. This argument is specified only when the routing protocol is **rip**, **ospf**, or **isis**.

Description Use the **filter-policy export** command to define an outbound route filtering policy. Only routes passing the filter can be advertised in the update messages.

Use the **undo filter-policy export** command to disable the filtering.

By default, RIPng does not filter any outbound routing information.

With the *protocol* argument specified, only routing information redistributed from the specified routing protocol will be filtered. Otherwise, all outgoing routing information will be filtered.

Examples # Use IPv6 prefix list Filter 2 to filter outgoing RIPng updates.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] filter-policy ipv6-prefix Filter2 export
```

filter-policy import (RIPng view)

Syntax **filter-policy** { *acl6-number* | **ipv6-prefix** *ipv6-prefix-name* } **import**

undo filter-policy import

View RIPng view

Parameters *acl6-number*: Specifies the number of an ACL to filter incoming routing information.

ipv6-prefix *ipv6-prefix-name*: Specifies the name of an IPv6 Prefix list to filter incoming routes.

Description Use the **filter-policy import** command to define an inbound route filtering policy. Only routes which match the filtering policy can be received.

Use the **undo filter-policy import** command to disable incoming route filtering.

By default, RIPng does not filter incoming routing information.

Examples # Reference IPv6 prefix list Filter1 to filter incoming RIPng updates.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] filter-policy ipv6-prefix Filter1 import
```

import-route (RIPng view)

Syntax **import-route** *protocol* [*process-id*] [**allow-ibgp**] [**cost** *cost* | **route-policy** *route-policy-name*] *

undo import-route *protocol* [*process-id*]

View RIPng view

Parameters *protocol*: Specifies a routing protocol from which to redistribute routes, currently including **bgp4+, direct, isisv6, ospfv3, ripng,** and **static**.

process-id: Process ID of the specified routing protocol, available for **isisv6**, **ospfv3**, and **ripng**.

cost: Routing metric of redistributed routes. If *cost value* is not specified, the metric is the default metric specified with the **default cost** command.

route-policy *route-policy-name*: Specifies a routing policy by its name.

allow-ibgp: Optional keyword when the specified *protocol* is **bgp4+**. The **import-route bgp4+** command redistributes only EBGP routes. The **import-route bgp4+ allow-ibgp** command redistributes additionally IBGP routes, thus be cautious when using it.

Description Use the **import-route** command to redistribute routes from another routing protocol.

Use the **undo import-route** command to disable redistributing routes from another routing protocol.

By default, RIPng does not redistribute routes from other routing protocols.

- You can configure a routing policy to redistribute only needed routes.
- You can specify a cost for redistributed routes using keyword **cost**.

Related commands: **default cost**.

Examples # Redistribute routes from IPv6-IS-IS process 7 and specify the metric as 7.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] import-route isisv6 7 cost 7
```

maximum load-balancing (RIPng view)

Syntax **maximum load-balancing** *number*

undo maximum load-balancing

View RIPng view

Parameters *number*: Maximum number of equal-cost load-balanced routes.

Description Use the **maximum load-balancing** command to specify the maximum number of equal cost routes for load balancing.

Use the **undo maximum load-balancing** command to restore the default.

Examples # Set the maximum number of equal cost load balanced routes to 2.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] maximum load-balancing 2
```

Restore the default.

```
[Sysname-ripng-100] undo maximum load-balancing
```

preference (RIPng view)

Syntax **preference** [**route-policy** *route-policy-name*] *preference*

undo preference [**route-policy**]

View RIPng view

Parameters *preference*: RIPng route priority. The default is 100. The smaller the value, the higher the priority.

route-policy-name: Name of a routing policy.

Description Use the **preference** command to specify the RIPng route priority.

Use the **undo preference route-policy** command to restore the default.

By default, the priority of a RIPng route is 100.

Using the **route-policy** keyword can set a priority for routes filtered in by the routing policy:

- If a priority is set in the routing policy, the priority applies to matched routes, and the priority set by the **preference** command applies to routes not matched.

- If no priority is set in the routing policy, the one set by the **preference** command applies to all routes.

Examples # Set the RIPng route priority to 120.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] preference 120
```

Restore the default RIPng route priority.

```
[Sysname-ripng-100] undo preference
```

ripng

Syntax **ripng** [*process-id*]

undo ripng [*process-id*]

View System view

Parameters *process-id*: RIPng process ID.

Description Use the **ripng** command to create a RIPng process and enter RIPng view.

Use the **undo ripng** command to disable a RIPng process.

By default, no RIPng process is enabled.

Examples # Create RIPng process 100 and enter its view.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100]
```

Disable RIPng process 100.

```
[Sysname] undo ripng 100
```

ripng default-route

Syntax **ripng default-route** { **only** | **originate** } [**cost** *cost*]

undo ripng default-route

View Interface view

Parameters **only**: Indicates that only the IPv6 default route is advertised via the interface.

originate: Indicates that the IPv6 default route is advertised without suppressing other routes.

cost: Metric of the advertised default route. The default value is 1.

Description Use the **ripng default-route** command to advertise a default route with the specified routing metric to a RIPng neighbor.

Use the **undo ripng default-route** command to stop advertising and forwarding the default route.

By default, a RIP process does not advertise any default route.

After you execute this command, the generated RIPng default route is advertised in a route update over the specified interface. This IPv6 default route is advertised without considering whether it already exists in local IPv6 routing table.

Examples # Advertise only the default route via Vlan-interface100.

<Sysname> system-view

```
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ripng default-route only
```

Advertise the default route together with other routes via Vlan-interface101.

```
[Sysname] interface vlan-interface 101
[Sysname-Vlan-interface101] ripng default-route originate
```

ripng enable

Syntax **ripng** *process-id* **enable**

undo ripng

View Interface view

Parameters *process-id*: RIPng process ID.

Description Use the **ripng enable** command to enable RIPng on the specified interface.

Use the **undo ripng enable** command to disable RIPng on the specified interface.

Examples # Enable RIPng100 on Vlan-interface100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ripng 100 enable
```

ripng metricin

Syntax **ripng metricin** *value*

undo ripng metricin

View Interface view

Parameters *value*: Additional metric for received routes.

Description Use the **ripng metricin** command to specify an additional metric for received RIPng routes.

Use the **undo ripng metricin** command to restore the default.

By default, the additional metric to received routes is 0.

Related commands: **ripng metricout**.

Examples # Specify the additional routing metric as 12 for RIPng routes received by Vlan-interface100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ripng metricin 12
```

ripng metricout

Syntax **ripng metricout** *value*

undo ripng metricout

View Interface view

Parameters *value*: Additional metric for advertised routes. The default is 1.

Description Use the **ripng metricout** command to configure an additional metric for RIPng routes advertised by an interface.

Use the **undo rip metricout** command to restore the default.

The default additional routing metric is 1.

Related commands: **ripng metricin**.

Examples # Set the additional metric to 12 for routes advertised by Vlan-interface100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ripng metricout 12
```

ripng poison-reverse

Syntax **ripng poison-reverse**

undo ripng poison-reverse

View Interface view

Parameters None

Description Use the **rip poison-reverse** command to enable the poison reverse function.

Use the **undo rip poison-reverse** command to disable the poison reverse function.

By default, the poison reverse function is disabled.

Examples # Enable the poison reverse function on Vlan-interface100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ripng poison-reverse
```

ripng split-horizon

Syntax **ripng split-horizon**

undo ripng split-horizon

View Interface view

Parameters **None**

Description Use the **rip split-horizon** command to enable the split horizon function.

Use the **undo rip split-horizon** command to disable the split horizon function.

By default, the split horizon function is enabled.

Note that:

- The split horizon function is necessary for preventing routing loops. Therefore, you are not recommended to disable it.
- In special cases, make sure that it is necessary to disable the split horizon function before doing so.

If both the poison reverse and split horizon functions are enabled, only the poison reverse function takes effect.

Examples # Enable the split horizon function on Van-interface100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ripng split-horizon
```

ripng summary-address

Syntax **ripng summary-address** *ipv6-address prefix-length*

undo ripng summary-address ***ipv6-address prefix-length***

View Interface view

Parameters *ipv6-address*: IPv6 network address of the summary route.

prefix-length: IPv6 prefix length. It indicates the number of consecutive ones of the prefix, which represents the network ID.

Description Use the **ripng summary-address** command to configure a summary advertised through the interface.

Use the **undo ripng summary-address** command to remove the summary.

If the prefix and the prefix length of a route match the specified IPv6 prefix, the IPv6 prefix will be advertised instead. Thus, one route can be advertised on behalf of many routes. After summarization, the summary route cost is the lowest cost among summarized routes.

Examples # Assign an IPv6 address with the 64-bit prefix to Vlan-interface100 and configure a summary with the 35-bit prefix.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address 2001:200::3EFF:FE11:6770/64
[Sysname-Vlan-interface100] ripng summary-address 2001:200:: 35
```

timers (RIPng view)

Syntax **timers** { **garbage-collect** *garbage-collect-value* | **suppress** *suppress-value* | **timeout** *timeout-value* | **update** *update-value* }*

undo timers { **garbage-collect** | **suppress** | **timeout** | **update** }*

View RIPng view

Parameters *garbage-collect-value*: Interval of the garbage-collect timer in seconds.

suppress-value: Interval of the suppress timer in seconds.

timeout-value: Interval of the timeout timer in seconds.

update-value: Interval of the update timer in seconds.

Description Use the **timers** command to configure RIPng timers.

Use the **undo timers** command to restore the default.

By default, the garbage-collect timer is 120 seconds, the suppress timer 120 seconds, the timeout timer 180 seconds, and the update timer 30 seconds.

RIPng is controlled by the above four timers.

- The update timer defines the interval between update messages.
- The timeout timer defines the route aging time. If no update message related to a route is received within the aging time, the metric of the route is set to 16 in the routing table.
- The suppress timer defines how long a RIPng route stays in the suppressed state. When the metric of a route is 16, the route enters the suppressed state. In the suppressed state, only routes which come from the same neighbor and whose metric is less than 16 will be received by the device to replace unreachable routes.
- The garbage-collect timer defines the interval from when the metric of a route becomes 16 to when it is deleted from the routing table. During the garbage-collect timer length, RIPng advertises the route with the routing metric set to 16. If no update message is announced for that route before the garbage-collect timer expires, the route will completely be deleted from the routing table.

Note that:

- You are not recommended to change the default values of these timers under normal circumstances.
- The lengths of these timers must be kept consistent on all devices and access servers in the network

Examples # Configure the update, timeout, suppress, and garbage-collect timers as 5s, 15s, 15s and 30s.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] timers update 5
[Sysname-ripng-100] timers timeout 15
[Sysname-ripng-100] timers suppress 15
[Sysname-ripng-100] timers garbage-collect 30
```

35 OSPF CONFIGURATION COMMANDS

- *Refer to "graceful-restart (OSPF view)" on page 974 for OSPF GR related commands.*

abr-summary (OSPF area view)

Syntax **abr-summary** *ip-address* { *mask* | *mask-length* } [**advertise** | **not-advertise**] [**cost** *cost*]

undo abr-summary *ip-address* { *mask* | *mask-length* }

View OSPF area view

Parameters *ip-address*: IP address of the summary route, in dotted decimal format.

mask: Mask of the IP address in dotted decimal format.

mask-length: Mask length, in the range 0 to 32 bits.

advertise | **not-advertise**: Advertises or not to advertise the summary route. By default, the summary route is advertised.

cost *cost*: Specifies the cost of the summary route. The default cost is the biggest cost value among routes that are summarized.

Description Use the **abr-summary** command to configure a summary route on the Area Border Router.

Use the **undo abr-summary** command to remove a summary route.

By default, no route summarization is available on an ABR.

You can configure to advertise or not to advertise the summary route, and specify a route cost.

This command is usable only on an ABR. Multiple contiguous networks may be available in an area, where you can summarize them with one network on the ABR for advertisement. The ABR advertises only the summary route to other areas.

With the **undo abr-summary** command used, summarized routes will be advertised.

Examples # Summarize networks 36.42.10.0/24 and 36.42.110.0/24 in Area1 with 36.42.0.0/16 for advertisement to other areas.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] network 36.42.10.0 0.0.0.255
[Sysname-ospf-100-area-0.0.0.1] network 36.42.110.0 0.0.0.255
[Sysname-ospf-100-area-0.0.0.1] abr-summary 36.42.0.0 255.255.0.0
```

area (OSPF view)

Syntax **area** *area-id*

undo area *area-id*

View OSPF view

Parameters *area-id*: ID of an area, a decimal integer, or an IP address.

Description Use the **area** command to create an area and enter area view.

Use the **undo area** command to remove a specified area.

Examples # Create Area0 and enter Area 0 view

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 0
[Sysname-ospf-100-area-0.0.0.0]
```

asbr-summary

Syntax **asbr-summary** *ip-address* { *mask* | *mask-length* } [**tag** *tag* | **not-advertise** | **cost** *cost*]*

undo asbr-summary *ip-address* { *mask* | *mask-length* }

View OSPF view

Parameters *ip-address*: IP address of the summary route in dotted decimal notation.

mask: IP address mask in dotted decimal notation.

mask-length: Mask length.

not-advertise: Specifies not to advertise the summary route. If the keyword is not specified, the route is advertised.

tag *tag*: Specifies a tag value for the summary route, used by a route policy to control route advertisement. The value defaults to 1.

cost *cost*: Specifies the cost of the summary route. For Type-1 external routes, the cost defaults to the biggest cost among routes that are summarized. For Type-2 external routes, the cost defaults to the value of the biggest cost among routes that are summarized plus 1.

Description Use the **asbr-summary** command to configure a summary route.

Use the **undo asbr-summary** command to remove a summary route.

No route summarization is configured by default.

With the **asbr-summary** command configured on an ASBR, it summarizes redistributed routes that fall into the specified address range with a single route. If the ASBR resides in an NSSA area, it advertises the summary route in a Type-7 LSA into the area.

With the **asbr-summary** command configured on an NSSA ABR, it summarizes routes in Type-5 LSAs translated from Type-7 LSAs with a single route and advertises the summary route to other areas. This command does not take effect on non NSSA ABRs.

With the **undo asbr-summary** command used, summarized routes will be advertised.

Related commands: **display ospf asbr-summary**.

Examples # Summarize redistributed routes with a single route.

```
<Sysname> system-view
[Sysname] ip route-static 10.2.1.0 24 null 0
[Sysname] ip route-static 10.2.2.0 24 null 0
[Sysname] ospf 100
[Sysname-ospf-100] import-route static
[Sysname-ospf-100] asbr-summary 10.2.0.0 255.255.0.0 tag 2 cost 100
```

authentication-mode (OSPF area view)

Syntax **authentication-mode** { **simple** | **md5** }

undo authentication-mode

View OSPF area view

Parameters **simple**: Specifies the simple authentication mode.

md5: Specifies the MD5 ciphertext authentication mode.

Description Use the **authentication-mode** command to specify an authentication mode for the OSPF area.

Use the **undo authentication-mode** command to cancel a specified authentication mode.

By default, no authentication mode is configured for an OSPF area.

Devices that reside in the same area must have the same authentication mode: non-authentication, simple, or MD5.

Related commands: **ospf authentication-mode**.

Examples # Specify the MD5 ciphertext authentication mode for OSPF area0.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 0
[Sysname-ospf-100-area-0.0.0.0] authentication-mode md5
```

bandwidth-reference (OSPF view)

Syntax **bandwidth-reference** *value*

undo bandwidth-reference

View OSPF view

Parameters *value*: Bandwidth reference value for link cost calculation, in Mbps.

Description Use the **bandwidth-reference** command to specify a reference bandwidth value for link cost calculation.

Use the **undo bandwidth-reference** command to restore the default.

The default value is 100 Mbps.

When links have no cost values configured, OSPF calculates their cost values: Cost=Reference bandwidth value / Link bandwidth. If the calculated cost is greater than 65535, the value of 65535 is used.

Examples # Specify the reference bandwidth value as 1000 Mbps.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] bandwidth-reference 1000
```

default

Syntax **default** { **cost** *cost* | **limit** *limit* | **tag** *tag* | **type** *type* } *

undo default { **cost** | **limit** | **tag** | **type** } *

View OSPF view

Parameters *cost*: Default cost for redistributed routes.

limit: Default upper limit of routes to be redistributed per time.

tag: Default tag for redistributed routes.

type: Default type for redistributed routes.

Description Use the **default** command to configure default parameters for redistributed routes: cost, route type (Type1 or Type2), tag, and the upper limit.

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

The cost, route type, tag, and the upper limit are 1, 2, 1 and 1000 by default.

Related commands: **import-route**.

Examples # Configure default parameters cost as 10, upper limit as 20000, tag as 100 and type as 2 for redistributed external routes.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] default cost 10 limit 20000 tag 100 type 2
```

default-cost (OSPF area view)

Syntax **default-cost** *cost*

undo default-cost

View OSPF area view

Parameters *cost*: Cost for the default route advertised to the Stub or NSSA area.

Description Use the **default-cost** command to specify a cost for the default route advertised to the stub or NSSA area.

Use the **undo default-cost** command to restore the default.

This command is only applicable to the ABR of a stub area or the ABR/ASBR of an NSSA area.

Related commands: **stub**, **nssa**.

Examples # Configure Area1 as a stub area, and specify the cost of the default route advertised to the stub area as 20.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] stub
[Sysname-ospf-100-area-0.0.0.1] default-cost 20
```

default-route-advertise (OSPF view)

Syntax **default-route-advertise** [[**always** | **cost** *cost* | **type** *type* | **route-policy** *route-policy-name*] * | **summary cost** *cost*]

undo default-route-advertise

View OSPF view

Parameters **always**: Generates a default external route in an ASE LSA into the OSPF routing domain, if the router has no default route configured. With this keyword not included, you have to configure a default route to distribute an ASE LSA into the OSPF routing domain.

cost *cost*: Specifies a cost for the default route. The default is 1.

type *type*: Specifies a type for the ASE LSA. The default is 2.

route-policy *route-policy-name*: Specifies a route policy name. If the default route matches the specified route policy, the route policy affects some value in the ASE LSA.

summary: Advertises the Type-3 summary LSA of the specified default route.

Description Use the **default-route-advertise** command to generate a default route into the OSPF routing domain.

Use the **undo default-route-advertise** command to disable OSPF from distributing a default external route.

By default, no default route is distributed.

Using the **import-route** command cannot redistribute a default route. To do so, use the **default-route-advertise** command. If the default route is not configured, to generate the ASE LSA for a default route, use the **default-route-advertise always** command.

The **default-route-advertise summary cost** command is applicable only to VPNs, and the default route is redistributed in a Type-3 LSA. The PE device advertises the redistributed default route to the CE device.

Related commands: **import-route**.

Examples # Generate a default route in an ASE LSA into the OSPF routing domain.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] default-route-advertise always
```

description (OSPF/OSPF area view)

Syntax **description** *description*

undo description

View OSPF view/OSPF area view

Parameters *description*: Describes the OSPF process in OSPF view, or describes the OSPF area in OSPF area view.

Description Use the **description** command to configure a description for an OSPF process or area.

Use the **undo description** command to remove the description.

No description is configured by default.

Use of this command is only for identification of an OSPF process or area. The description has no special meaning.

Examples # Configure a description for the OSPF process 100 as "abc".

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] description abc
```

Configure a description for the OSPF area0 as "bone area".

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 0
[Sysname-ospf-100-area-0.0.0.0] description bone area
```

display ospf abr-asbr

Syntax **display ospf** [*process-id*] **abr-asbr**

View Any view

Parameters *process-id*: OSPF process ID.

Description Use the **display ospf abr-asbr** command to display information about ABR/ASBR.

If no process ID is specified, ABR/ASBR information of all OSPF processes is displayed.

If you use this command on devices in a stub area, no ASBR information is displayed.

If you use this command on devices in an NSSA area, only information about ASBR is displayed.

Examples # Display information about ABR/ASBR.

```
<Sysname> display ospf abr-asbr

          OSPF Process 1 with Router ID 192.168.1.2
                  Routing Table to ABR and ASBR

 Type        Destination       Area       Cost  Nexthop         RtType
 Intra         192.168.1.1       0.0.0.0    1562  192.168.1.1     ABR
```

Table 110 Field descriptions of the display ospf abr-asbr command

Field	Description
Type	Intra-area router or Inter-area router
Destination	Router ID of an ABR/ASBR
Area	ID of the area of the next hop
Cost	Cost from the device to the ABR/ASBR
Nexthop	Next hop address
RtType	Device type: ABR, ASBR

display ospf asbr-summary

Syntax **display ospf** [*process-id*] **asbr-summary** [*ip-address* { *mask* | *mask-length* }]

View Any view

Parameters *process-id*: OSPF process ID.

ip-address: Matched IP address, in dotted decimal format.

mask: IP address mask, in dotted decimal format.

mask-length: Mask length, in the range 0 to 32 bits.

Description Use the **display ospf asbr-summary** command to display information about the redistributed routes that are summarized.

If no OSPF process is specified, related information of all OSPF processes is displayed.

If no IP address is specified, information about all summarized redistributed routes will be displayed.

Related commands: **asbr-summary**.

Examples # Display information about all summarized redistributed routes.

```
<Sysname> display ospf asbr-summary

          OSPF Process 1 with Router ID 2.2.2.2
```

```
                Summary Addresses

Total Summary Address Count: 1

                Summary Address

Net          : 30.1.0.0
Mask         : 255.255.0.0
Tag          : 20
Status       : Advertise
Cost         : 10 (Configured)
The Count of Route is : 2

Destination     Net Mask        Proto      Process   Type     Metric

30.1.2.0        255.255.255.0   OSPF       1         2        1
30.1.1.0        255.255.255.0   OSPF       1         2        1
```

Table 111 Field descriptions of the display ospf asbr-summary command

Field	Description
Total Summary Address Count	Total summary route number
Net	The address of the summary route
Mask	The mask of the summary route address
Tag	The tag of the summary route
Status	The advertisement status of the summary route
Cost	The cost to the summary route
The Count of Route	The count of routes that are summarized
Destination	Destination address of a summarized route
Net Mask	Network mask of a summarized route
Proto	Routing protocol
Process	Process ID of routing protocol
Type	Type of a summarized route
Metric	Metric of a summarized route

display ospf brief

Syntax **display ospf** [*process-id*] **brief**

View Any view

Parameters *process-id*: OSPF process ID.

Description Use the **display ospf brief** command to display OSPF brief information. If no OSPF process is specified, brief information of all OSPF processes is displayed.

Examples # Display OSPF brief information.

```
<Sysname> display ospf brief

          OSPF Process 1 with Router ID 192.168.1.2
                  OSPF Protocol Information

 RouterID: 192.168.1.2      Border Router:  NSSA
```

```
Route Tag: 0
Multi-VPN-Instance is not enabled
Applications Supported: MPLS Traffic-Engineering
SPF-schedule-interval: 5 0 5000
LSA generation interval: 5 0 5000
LSA arrival interval: 1000
Default ASE Parameter: Metric: 1 Tag: 1 Type: 2
Route Preference: 10
ASE Route Preference: 150
SPF Computation Count: 22
RFC 1583 Compatible
Area Count: 1   Nssa Area Count: 1
ExChange/Loading Neighbors: 0


Area: 0.0.0.1          (MPLS TE  not enabled)
Authtype: None Area flag: NSSA
SPF Scheduled Count: 5
ExChange/Loading Neighbors: 0

Interface: 192.168.1.2 (vlan-interface 12)
Cost: 1       State: DR        Type: Broadcast    MTU: 1500
Priority: 1
Designated Router: 192.168.1.2
Backup Designated Router: 192.168.1.1
Timers: Hello 10 , Dead 40 , Poll  40 , Retransmit 5 , Transmit Delay 1
```

Table 112 Field descriptions of the display ospf brief command

Field	Description
RouterID	The current router ID
Border Router	An ABR, ASBR or NSSA ABR
Route Tag	The tag of redistributed routes
Multi-VPN-Instance is not enabled	The current OSPF process supports no multi-VPN-instance
Applications Supported	Applications supported
SPF-schedule-interval	Interval for SPF calculation
LSA generation interval	LSA generation interval
LSA arrival interval	The minimum LSA repeat arrival interval
Default ASE Parameter	Default ASE Parameter: metric, tag, route type.
Route Preference	Internal route priority
ASE Route Preference	External route priority
SPF Computation count	The total number of routes calculated by SPF
RFC1583 Compatible	Compatible with routing rules defined in RFC1583
Area Count	Area number of the current process
Nssa Area Count	NSSA area number of the current process
ExChange/Loading Neighbors	Neighbors in ExChange/Loading state
Area	Area ID in the IP address format
Authtype	Authentication type of the area: Non-authentication, simple authentication, or MD5 authentication
Area flag	The type of the area
SPF scheduled Count	SPF calculation count
Interface	IP address of the interface

Table 112 Field descriptions of the display ospf brief command

Field	Description
Cost	Interface cost
State	Interface state
Type	Interface network type
MTU	Interface MTU
Priority	Device priority
Designated Router	The Designated Router
Backup Designated Router	The Backup Designated Router
Timers	Intervals of timers: hello, dead, poll, retransmit, and transmit delay

display ospf cumulative

Syntax **display ospf** [*process-id*] **cumulative**

View Any view

Parameters *process-id*: OSPF process ID.

Description Use the **display ospf cumulative** command to display OSPF statistics.

Use of this command is helpful for troubleshooting.

Examples # Display OSPF statistics.

```
<Sysname> display ospf cumulative
          OSPF Process 1 with Router ID 192.168.1.2
                  Cumulations

  IO Statistics
             Type        Input     Output
            Hello          808        809
   DB Description            4          3
   Link-State Req            1          1
Link-State Update           12         18
   Link-State Ack           18         11

  LSAs originated by this router
  Router:  6
  Network: 0
  Sum-Net: 0
  Sum-Asbr: 0
  External: 1
  NSSA: 0
  Opq-Link: 0
  Opq-Area: 0
  Opq-As: 0

  LSAs Originated: 7  LSAs Received: 15
```

```
Routing Table:
  Intra Area: 1  Inter Area: 1  ASE: 0
```

Table 113 Field descriptions of the display ospf cumulative command

Field	Description
IO statistics	Statistics about inbound/outbound packets and LSAs
Type	OSPF packet type
Input	Packets received
Output	Packets sent
Hello	Hell packet
DB Description	Database Description packet
Link-State Req	Link-State Request packet
Link-State Update	Link-State Update packet
Link-State Ack	Link-State Acknowledge packet
LSAs originated by this router	LSAs originated by this device
Router	Type-1 LSA
Network	Type-2 LSA
Sum-Net	Type-3 LSA
Sum-Asbr	Type-4 LSA
External	Type-5 LSA
NSSA	Type-7 LSA
Opq-Link	Type-9 LSA
Opq-Area	Type-10 LSA
Opq-As	Type-11 LSA
LSA originated	LSA originated
LSA Received	LSA received
Routing Table	Routing table
Intra Area	Intraarea route number
Inter Area	Interarea route number
ASE/NSSA	ASE/NSSA route number

display ospf error

Syntax **display ospf** [*process-id*] **error**

View Anyview

Parameters *process-id*: OSPF process ID.

Description Use the **display ospf error** command to display OSPF error information.

If no process is specified, OSPF error information of all OSPF processes is displayed.

Examples # Display OSPF error information.

```
<Sysname> display ospf error

          OSPF Process 1 with Router ID 192.168.80.100
                  OSPF Packet Error Statistics

0    : OSPF Router ID confusion     0    : OSPF bad packet
0    : OSPF bad version             0    : OSPF bad checksum
0    : OSPF bad area ID             0    : OSPF drop on unnumber interface
0    : OSPF bad virtual link        0    : OSPF bad authentication type
0    : OSPF bad authentication key  0    : OSPF packet too small
0    : OSPF Neighbor state low      0    : OSPF transmit error
0    : OSPF interface down          0    : OSPF unknown neighbor
0    : HELLO: Netmask mismatch      0    : HELLO: Hello timer mismatch
0    : HELLO: Dead timer mismatch   0    : HELLO: Extern option mismatch
0    : HELLO: NBMA neighbor unknown 0    : DD: MTU option mismatch
0    : DD: Unknown LSA type         0    : DD: Extern option mismatch
0    : LS ACK: Bad ack              0    : LS ACK: Unknown LSA type
0    : LS REQ: Empty request        0    : LS REQ: Bad request
0    : LS UPD: LSA checksum bad     0    : LS UPD: Received less recent LSA
0    : LS UPD: Unknown LSA type
```

Table 114 Field descriptions of the display ospf error command

Field	Description
OSPF Router ID confusion	Packets with duplicate route ID
OSPF bad packet	Packets illegal
OSPF bad version	Packets with wrong version
OSPF bad checksum	Packets with wrong checksum
OSPF bad area ID	Packets with invalid area ID
OSPF drop on unnumber interface	Packets dropped on the unnumbered interface
OSPF bad virtual link	Packets on wrong virtual links
OSPF bad authentication type	Packets with invalid authentication type
OSPF bad authentication key	Packets with invalid authentication key
OSPF packet too small	Packets too small in length
OSPF Neighbor state low	Packets received in low neighbor state
OSPF transmit error	Packets with error occurred when being transmitted
OSPF interface down	Shutdown times of the interface
OSPF unknown neighbor	Packets received from unknown neighbors
HELLO: Netmask mismatch	Hello packets with mask mismatch
HELLO: Hello timer mismatch	Hello packets with hello timer mismatch
HELLO: Dead timer mismatch	Hello packets with dead timer mismatch
HELLO: Extern option mismatch	Hello packets with option field mismatch
HELLO: NBMA neighbor unknown	Hello packets received from unknown NBMA neighbors
DD: MTU option mismatch	DD packets with MTU mismatch
DD: Unknown LSA type	DD packets with unknown LSA type
DD: Extern option mismatch	DD packets with option field mismatch
LS ACK: Bad ack	LSAck packets for LSU packets error acknowledgement
LS ACK: Unknown LSA type	LSAck packets with unknown LSA type
LS REQ: Empty request	LSR packets with no request information
LS REQ: Bad request	LSR packets with wrong request

Table 114 Field descriptions of the display ospf error command

Field	Description
LS UPD: LSA checksum bad	LSU packets with wrong LSA checksum
LS UPD: Received less recent LSA	LSU packets without latest LSA
LS UPD: Unknown LSA type	LSU packets with unknown LSA type

display ospf interface

Syntax **display ospf** [*process-id*] **interface** [**all** | *interface-type interface-number*]

View Any view

Parameters *process-id*: OSPF process ID.

all: Display OSPF information of all interfaces.

interface-type interface-number: Interface type and interface number.

Description Use the **display ospf interface** command to display OSPF interface information.

If no OSPF process is specified, OSPF interface information of all OSPF processes is displayed.

Examples # Display OSPF interface information.

```
<Sysname> display ospf interface

          OSPF Process 1 with Router ID 192.168.1.1
                  Interfaces

 Area: 0.0.0.0
 IP Address      Type         State    Cost  Pri   DR              BDR
 192.168.1.1     PTP          P-2-P    1562  1     0.0.0.0         0.0.0.0

 Area: 0.0.0.1
 IP Address      Type         State    Cost  Pri   DR              BDR
 172.16.0.1      Broadcast    DR       1     1     172.16.0.1      0.0.0.0
```

Table 115 Field descriptions of the display ospf interface command

Field	Description
Area	The ID of the area the interface attached to
IP address	Interface IP address (regardless of TE enabled or not)
Type	Interface network type: PTP, PTMP, Broadcast, or NBMA
State	Interface state defined by interface state machine: DOWN, Waiting, p-2-p, DR, BDR, or DROther
Cost	Interface cost
Pri	DR priority
DR	The DR on the interface's network segment
BDR	The BDR on the interface's network segment

display ospf lsdb

Syntax **display ospf** [*process-id*] **lsdb** [**brief** | [{ **ase** | **router** | **network** | **summary** | **asbr** | **nssa** | **opaque-link** | **opaque-area** | **opaque-as** } [*link-state-id*]] [**originate-router** *advertising-router-id* | **self-originate**]]

View Any view

Parameters *process-id*: OSPF process ID.

brief: Displays brief LSDB information.

ase: Displays Type5 LSA (AS External LSA) information in the LSDB.

router: Displays Type1 LSA (Router LSA) information in the LSDB.

network: Displays Type2 LSA (Network LSA) information in the LSDB.

summary: Displays Type3 LSA (Network Summary LSA) information in the LSDB.

asbr: Displays Type4 LSA (ASBR Summary LSA) information in the LSDB.

nssa: Displays Type7 LSA (NSSA External LSA) information in the LSDB.

opaque-link: Displays Type9 LSA (Opaque-link LSA) information in the LSDB.

opaque-area: Displays Type10 LSA (Opaque-area LSA) information in the LSDB.

opaque-as: Displays Type11 LSA (Opaque-AS LSA) information in the LSDB.

link-state-id: Link state ID, in the IP address format.

originate-router *advertising-router-id*: Displays information about LSAs originated by the router.

self-originate: Displays information about self-originated LSAs.

Description Use the **display ospf lsdb** command to display LSDB information.

If no OSPF process is specified, LSDB information of all OSPF processes is displayed.

Examples # Display OSPF LSDB information.

```
<Sysname> display ospf lsdb
         OSPF Process 1 with Router ID 192.168.0.1
                 Link State Database

                         Area: 0.0.0.0
 Type      LinkState ID    AdvRouter         Age  Len   Sequence   Metric
 Router    192.168.0.2     192.168.0.2       474  36    80000004       0
 Router    192.168.0.1     192.168.0.1        21  36    80000009       0
 Network   192.168.0.1     192.168.0.1       321  32    80000003       0
 Sum-Net   192.168.1.0     192.168.0.1       321  28    80000002       1
 Sum-Net   192.168.2.0     192.168.0.2       474  28    80000002       1
                         Area: 0.0.0.1
```

```
Type      LinkState ID    AdvRouter          Age  Len   Sequence   Metric
Router    192.168.0.1     192.168.0.1         21  36    80000005       0
Sum-Net   192.168.2.0     192.168.0.1        321  28    80000002       2
Sum-Net   192.168.0.0     192.168.0.1        321  28    80000002       1
```

Table 116 Field descriptions of the display ospf lsdb command

Field	Description
Area	Area
Type	LSA type
LinkState ID	Linkstate ID
AdvRouter	The router that advertised the LSA
Age	Aging time of the LSA
Len	Length of the LSA
Sequence	Sequence number of the LSA
Metric	Cost of the LSA

Display Type2 LSA (Network LSA) information in the LSDB.

```
[Sysname] display ospf 1 lsdb network

         OSPF Process 1 with Router ID 192.168.1.1
                        Area: 0.0.0.0
                Link State Database


    Type      : Network
    LS ID     : 192.168.0.2
    Adv Rtr   : 192.168.2.1
    LS Age    : 922
    Len       : 32
    Options   :  E
    Seq#      : 80000003
    Chksum    : 0x8d1b
    Net Mask  : 255.255.255.0
       Attached Router    192.168.1.1
       Attached Router    192.168.2.1
                          Area: 0.0.0.1
                  Link State Database
    Type      : Network
    LS ID     : 192.168.1.2
    Adv Rtr   : 192.168.1.2
    LS Age    : 782
    Len       : 32
    Options   :  NP
    Seq#      : 80000003
    Chksum    : 0x2a77
    Net Mask  : 255.255.255.0
       Attached Router    192.168.1.1
       Attached Router    192.168.1.2
```

Table 117 Field descriptions of the display ospf 1 lsdb network command

Field	Description
Type	LSA type
LS ID	DR IP address

Table 117 Field descriptions of the display ospf 1 lsdb network command

Field	Description
Adv Rtr	Router that advertised the LSA
LS Age	LSA age time
Len	LSA length
Options	LSA options
Seq#	LSA sequence number
Chksum	LSA checksum
Net Mask	Network mask
Attached Router	Router ID of the device that established adjacency with the DR, and ID of the DR itself

display ospf nexthop

Syntax **display ospf** [*process-id*] **nexthop**

View Any view

Parameters *process-id*: OSPF process ID.

Description Use the **display ospf nexthop** command to display OSPF next hop information.

If no OSPF process is specified, next hop information of all OSPF processes is displayed.

Examples # Display OSPF next hop information.

```
<Sysname> display ospf nexthop
         OSPF Process 1 with Router ID 192.168.0.1
                 Routing Nexthop Information

  Next Hops:
  Address          Refcount  IntfAddr        Intf Name
 ----------------------------------------------------------------
  192.168.0.1      1         192.168.0.1     vlan-interface12
  192.168.0.2      1         192.168.0.1     vlan-interface12
  192.168.1.1      1         192.168.1.1     vlan-interface14
```

Table 118 Field descriptions of the display ospf nexthop command

Field	Description
Next hops	Information about Next hops
Address	Next hop address
Refcount	Reference count
IntfAddr	Outbound interface address
Intf Name	Outbound interface name

display ospf peer

Syntax **display ospf** [*process-id*] **peer** [**verbose |** [*interface-type interface-number*] [*neighbor-id*]]

View Any view

Parameters *process-id*: OSPF process ID.

interface-type interface-number: Interface type and number

verbose: Displays detailed neighbor information.

neighbor-id: Neighbor router ID.

Description Use the **display ospf peer** command to display information about OSPF neighbors.

Note that:

If no OSPF process is specified, OSPF neighbor information of all OSPF processes is displayed.

If an interface is specified, the neighbor on the interface is displayed.

If a neighbor ID is specified, detailed information about the neighbor is displayed,

If neither interface nor neighbor ID is specified, brief information about neighbors of the specified OSPF process or all OSPF processes is displayed.

Examples # Display detailed OSPF neighbor information.

```
<Sysname> display ospf peer verbose

          OSPF Process 1 with Router ID 2.2.2.2
 Router ID: 47.47.47.47      Address: 1.1.5.5          GR State: Normal
   State: Full  Mode: Nbr is Master  Priority: 1
   DR: 1.1.5.5  BDR: 1.1.5.6  MTU: 0
   Dead timer due in 33  sec
   Neighbor is up for 93:12:38
   Authentication Sequence: [ 0 ]
   Neighbor state change count: 6

 Router ID: 192.168.1.48     Address: 1.1.3.2          GR State: Normal
   State: Full  Mode: Nbr is Master  Priority: 1
   DR: 1.1.3.1  BDR: 1.1.3.2  MTU: 0
   Dead timer due in 31  sec
   Neighbor is up for 93:10:45
   Authentication Sequence: [ 0 ]
   Neighbor state change count: 5
```

Table 119 Field descriptions of the display ospf peer verbose command

Field	Description
Area	Area neighbors attached to
Interface	Interface connected to neighbor

Table 119 Field descriptions of the display ospf peer verbose command

Field	Description
Router ID	Neighbor router ID
Address	Neighbor router address
GR State	GR state
State	Neighbor state: Down, Init, Attempt, 2-Way, Exstart, Exchange, Loading or Full
Mode	Neighbor mode for DD exchange: Master or Slave
Priority	Router priority
DR	The DR on the interface's network segment
BDR	The BDR on the interface's network segment
MTU	Interface MTU
Dead timer due in 33 sec	Dead timer times out in 33 seconds
Neighbor is up for 93:12:38	The neighbor has been up for 93:12:38
Authentication Sequence	Authentication sequence number
Neighbor state change count	Counts of neighbor state changes

Display brief OSPF neighbor information.

```
<Sysname> display ospf peer

                  OSPF Process 1 with Router ID 2.2.2.2
                       Neighbor Brief Information

 Area: 0.0.0.0
 Router ID       Address         Pri Dead-Time Interface       State
 47.47.47.47     1.1.5.5         1   40        Vlan600         Full/BDR

 Area: 0.0.0.2
 Router ID       Address         Pri Dead-Time Interface       State
 192.168.1.48    1.1.3.2         1   38        Vlan900         Full/DR
```

Table 120 Field descriptions of the display ospf peer command

Field	Description
Area	Area of neighbors
Router ID	Neighbor router ID
Address	Neighbor interface address
Pri	Router priority
Dead time(s)	Dead interval remained
Interface	The Interface connected to neighbors
State	Neighbor state: Down, Init, Attempt, 2-Way, Exstart, Exchange, Loading or Full

display ospf peer statistics

Syntax **display ospf** [*process-id*] **peer statistics**

View Any view

Parameters *process-id*: OSPF process ID.

Description Use the **display ospf peer statistics** command to display OSPF neighbor statistics.

If no OSPF process is specified, OSPF neighbor statistics of all OSPF processes is displayed.

Examples # Display OSPF neighbor statistics.

```
<Sysname> display ospf peer statistics
                 OSPF Process 1 with Router ID 1.1.1.1
                          Neighbor Statistics

Area ID       Down  Attempt Init 2-Way ExStart Exchange Loading Full Total
0.0.0.1       0      0         0     0     0        0          0        1     1
Total         0      0         0     0     0        0          0        1     1
```

Table 121 Field descriptions of the display ospf peer statistics command

Field	Description
Area ID	Area ID
Down	Under this state, neighbor initial state, the router has not received any information from a neighboring router for a period of time.
Attempt	Available only in an NBMA network, such as Frame Relay, X.25 or ATM. Under this state, the OSPF router has not received any information from a neighbor for a period but can send Hello packets with a longer interval to keep neighbor relationship.
Init	Under this state, the router received a Hello packet from a neighbor but the packet contains no IP address of itself, so mutual communication is not established.
2-Way	Indicates mutual communication between the router and its neighbor is available. DR/BDR election is finished under this state (or higher).
ExStart	Under this state, the router decides on sequence numbers of DD packets, to guarantee the neighbor always gets the latest link state information.
Exchange	Under this state, the router exchanges routing information with the neighbor.
Loading	Under this state, the router requests the neighbor for needed LSAs.
Full	Indicates LSDB synchronization has been accomplished between neighbors.
Total	Total number of neighbors under the same state

display ospf request-queue

Syntax **display ospf** [*process-id*] **request-queue** [*interface-type interface-number*] [*neighbor-id*]

View Any view

Parameters *process-id*: OSPF process ID.

interface-type interface-number: Interface type and number.

neighbor-id: Neighbor's router ID.

Description Use the **display ospf request-queue** command to display OSPF request queue information.

If no OSPF process is specified, the OSPF request queue information of all OSPF processes is displayed.

Examples # Display OSPF request queue information.

```
<Sysname> display ospf request-queue

         OSPF Process 1 with Router ID 1.1.1.1
                OSPF Request List

  The Router's Neighbor is Router ID 2.2.2.2         Address 10.1.1.2
  Interface 10.1.1.1         Area 0.0.0.0
  Request list:
       Type       LinkState ID      AdvRouter         Sequence   Age
       Router     2.2.2.2           1.1.1.1           80000004   1
       Network    192.168.0.1       1.1.1.1            80000003   1
       Sum-Net    192.168.1.0       1.1.1.1            80000002   2
```

Table 122 Field descriptions of the display ospf request queue command

Field	Description
The Router's Neighbor is Router ID	Neighbor router ID
Address	Neighbor interface IP address
Interface	Local interface IP address
Area	Area ID
Request list	Request list information
Type	LSA type
LinkState ID	Link state ID
AdvRouter	Advertising router
Sequence	LSA sequence number
Age	LSA age time

display ospf retrans-queue

Syntax **display ospf** [*process-id*] **retrans-queue** [*interface-type interface-number*] [*neighbor-id*]

View Any view

Parameters *process-id*: OSPF process ID.

interface-type interface-number: Specifies an interface.

neighbor-id: Neighbor's router ID.

Description Use the **display ospf retrans-queue** command to display retransmission queue information.

If no OSPF process is specified, the retransmission queue information of all OSPF processes is displayed.

Examples # Display OSPF retransmission queue information.

```
<Sysname> display ospf retrans-queue

         OSPF Process 1 with Router ID 1.1.1.1
                 OSPF Retransmit List

  The Router's Neighbor is Router ID 2.2.2.2         Address 10.1.1.2
  Interface 10.1.1.1         Area 0.0.0.0
  Retransmit list:
       Type       LinkState ID      AdvRouter         Sequence   Age
       Router     2.2.2.2           2.2.2.2           80000004   1
       Network    12.18.0.1         2.2.2.2            80000003   1
       Sum-Net    12.18.1.0         2.2.2.2            80000002   2
```

Table 123 Field descriptions of the display ospf retrans-queue command

Field	Description
The Router's Neighbor is Router ID	Neighbor router ID
Address	Neighbor interface IP address
Interface	Interface address of the router
Area	Area ID
Retrans List	Retransmit list
Type	LSA type
LinkState ID	Link state ID
AdvRouter	Advertising router
Sequence	LSA sequence number
Age	LSA age time

display ospf routing

Syntax **display ospf** [*process-id*] **routing** [**interface** *interface-type interface-number*] [**nexthop** *nexthop-address*]

View Any view

Parameters *process-id*: OSPF process ID, in the range 1 to 65535.

interface *interface-type interface-number*: Displays OSPF routing information advertised via the interface.

nexthop *nexthop-address*: Displays OSPF routing information with the specified next hop.

Description Use the **display ospf routing** command to display the OSPF routing information.

If no OSPF process is specified, routing information of all OSPF processes is displayed.

Examples # Display OSPF routing information.

```
<Sysname> display ospf routing

         OSPF Process 1 with Router ID 192.168.1.2
                 Routing Tables
```

```
Routing for Network
Destination        Cost  Type       NextHop         AdvRouter     Area
192.168.1.0/24     1562  stub       192.168.1.2     192.168.1.2   0.0.0.0
172.16.0.0/16      1563  Inter      192.168.1.1     192.168.1.1   0.0.0.0

Total Nets: 2
Intra Area: 1  Inter Area: 1  ASE: 0  NSSA: 0
```

Table 124 Field descriptions of the display ospf routing command

Field	Description
Destination	Destination network
Cost	Cost to destination
Type	Route type: intra-area, Transit, stub, Inter-area, Type1 External, Type2 External.
NextHop	Next hop address
AdvRouter	Advertising router
Area	Area ID
Total Nets	Total routes
Intra Area	Total intraarea routes
Inter Area	Total interarea routes
ASE	Total ASE routes
NSSA	Total NSSA routes

display ospf vlink

Syntax **display ospf** [*process-id*] **vlink**

View Any view

Parameters *process-id*: OSPF process ID.

Description Use the **display ospf vlink** command to display OSPF virtual link information.

If no OSPF process is specified, the OSPF virtual link information of all OSPF processes is displayed.

Examples # Display OSPF virtual link information.

```
<Sysname> display ospf vlink
          OSPF Process 1 with Router ID 3.3.3.3
                  Virtual Links

 Virtual-link Neighbor-ID  -> 2.2.2.2, Neighbor-State: Full
 Interface: 10.1.2.1 (vlan-interface763)
 Cost: 1562  State: P-2-P  Type: Virtual
 Transit Area: 0.0.0.1
 Timers: Hello 10 , Dead 40 , Retransmit 5 , Transmit Delay 1
```

Table 125 Field descriptions of the display ospf vlink command

Field	Description
Virtual-link Neighbor-id	ID of neighbor connected to the router via the virtual link

Table 125 Field descriptions of the display ospf vlink command

Field	Description
Neighbor-State	Neighbor State: Down, Attempt, Init, 2-Way, ExStart, Exchange, Loading, Full.
Interface	Local interface's IP address and name of the virtual link
Cost	Interface route cost
State	Interface state
Type	Type: virtual link
Transit Area	Transit area ID if the interface attached to a virtual link
Timers	Values of timers: Hello, Dead, Poll (NBMA), Retransmit, and Interface transmit delay

Enable log

Syntax **enable log** [**config** | **error** | **state**]

undo enable log [**config** | **error** | **state**]

View OSPF view

Parameters **config**: Enables configuration logging.

error: Enables error logging.

state: Enables state logging.

Description Use the **enable** command to enable specified OSPF logging.

Use the **undo enable** command to disable specified logging.

OSPF logging is disabled by default.

If no keyword is specified, all logging is enabled.

Examples # Enable OSPF logging.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] enable log
```

filter import/export

Syntax **filter** { *acl-number* | **ip-prefix** *ip-prefix-name* } { **import** | **export** }

undo filter { **import** | **export** }

View OSPF area view

Parameters *acl-number*: ACL number.

ip-prefix-name: IP prefix list name.

import: Filters incoming LSAs.

export: Filters outgoing LSAs.

Description Use the **filter** command to configure incoming/outgoing Summary LSAs filtering on an ABR.

Use the **undo filter** command to disable Summary LSA filtering.

By default, Summary LSAs filtering is disabled.

This command is only available on an ABR.

Examples # Apply IP prefix list "my-prefix-list" to filter inbound Type-3 LSAs, and ACL2000 to filter outbound Type-3 LSAs in OSPF area 1.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] filter ip-prefix my-prefix-list import
[Sysname-ospf-100-area-0.0.0.1] filter 2000 export
```

filter-policy export (OSPF view)

Syntax **filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [*protocol* [*process-id*]]

undo filter-policy export [*protocol* [*process-id*]]

View OSPF view

Parameters *acl-number*: ACL number.

ip-prefix-name: IP prefix list name.

protocol: Filters redistributed routes from the protocol. Protocols include **direct**, **static**, **rip**, **ospf**, **isis** or **bgp**. If no protocol is specified, all redistributed routes are filtered.

process-id: Process ID, which is required when the *protocol* is **rip**, **ospf** or **isis**.

Description Use the **filter-policy export** command to configure the filtering of redistributed routes.

Use the **undo filter-policy export** command to disable such filtering.

By default, filtering of redistributed routes is not configured.

You can use this command to filter redistributed routes as needed.

Related commands: **import-route**.

Examples # Filter redistributed routes using ACL2000.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] filter-policy 2000 export
```

filter-policy import (OSPF view)

Syntax **filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* | **gateway** *ip-prefix-name* } **import**

undo filter-policy import

View OSPF view

Parameters *acl-number*: Number of an ACL used to filter incoming routes.

ip-prefix-name: Name of an IP address prefix list used to filter incoming routes.

gateway *ip-prefix-name*: Name of an IP address prefix list used to filter routes received from the specified neighbor.

Description Use the **filter-policy import** command to configure the filtering of incoming routes.

Use the **undo filter-policy import** command to disable such filtering.

By default, no filtering of incoming routes is configured.

You can use the command to filter incoming routes as needed.

Examples # Filter incoming routes using ACL2000.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 192.168.10.0 0.0.0.255
[Sysname-acl-basic-2000] quit
[Sysname] ospf 100
[Sysname-ospf-100] filter-policy 2000 import
```

host-advertise

Syntax **host-advertise** *ip-address cost*

undo host-advertise *ip-address*

View OSPF area view

Parameters *ip-address*: IP address of a host

cost: Cost of the host route.

Description Use the **host-advertise** command to advertise a host route.

Use the **undo host-advertise** command to remove a host route.

No host route is configured by default.

Examples # Configure host route 1.1.1.1 and specify cost 100 for it.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname] area 0
[Sysname-ospf-100-area-0.0.0.0] host-advertise 1.1.1.1 100
```

import-route (OSPF view)

Syntax **import-route** *protocol* [*process-id* | **allow-ibgp**] [**cost** *cost* | **type** *type* | **tag** *tag* | **route-policy** *route-policy-name*]*

undo import-route *protocol* [*process-id*]

View OSPF view

Parameters *protocol*: Redistributes routes from the protocol, which can be **direct**, **static**, **rip**, **ospf**, **isis** or **bgp**.

process-id: Process ID, which is optional when the *protocol* is **rip**, **ospf** or **isis**, in the range 1 to 65535.

allow-ibgp: Allows to redistribute IBGP routes; optional only when the *protocol* is **bgp**.

cost *cost*: Specifies a route cost. The default is 1.

type *type*: Specifies a cost type. The default is 2.

tag *tag* : Specifies a tag for external LSAs. The default is 1.

route-policy: Specifies a route policy to redistribute qualified routes only.

route-policy-name: Route policy name, a string of 1 to 19 characters.

Description Use the **import-route** command to redistribute routes from another protocol.

Use the **undo import-route** command to disable route redistribution from a protocol.

Route redistribution from another protocol is not configured by default.

OSPF prioritize routes as follows:

- Intra-area route
- Inter-area route
- Type1 External route
- Type2 External route

An intraarea route is a route in an OSPF area. An interarea route is between any two OSPF areas. Both of them are internal routes.

An external route is a route to a destination outside the OSPF AS.

A Type1 external route is an IGP route, such as RIP or STATIC, which has high reliability and whose cost is comparable with the cost of OSPF internal routes: Cost from an OSPF router to a Type1 external route's destination= Cost from the device to the corresponding ASBR+ Cost from the ASBR to the external route's destination.

A Type2 external route is an EGP route, which has low credibility, so OSPF considers the cost from ASBR to a Type2 external route is much bigger than the cost from the ASBR to an OSPF internal router. Therefore, Cost from an internal router to a Type2 external route=Cost from the ASBR to the Type2 external route.

Examples # Redistribute routes from RIP process 40 and specify the type as type2, tag as 33, and cost as 50 for redistributed routes.

```
<Sysname> system-view
[Sysname> ospf 100
[Sysname-ospf-100] import-route rip 40 type 2 tag 33 cost 50
```

log-peer-change (OSPF view)

Syntax **log-peer-change**

undo log-peer-change

View OSPF view

Parameters None

Description Use the **log-peer-change** command to enable the logging on OSPF neighbor state changes.

Use the **undo log-peer-change** command to disable the logging.

The logging is enabled by default.

With this feature enabled, information about neighbor state changes is display on the terminal until the feature is disabled.

Examples # Disable the logging on neighbor state changes of OSPF process 100.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] undo log-peer-change
```

lsa-arrival-interval

Syntax **lsa-arrival-interval** *interval*

undo lsa-arrival-interval

View OSPF view

Parameters *interval*: Minimum interval between two received identical LSAs in milliseconds.

Description Use the **lsa-arrival-interval** command to specify the minimum interval between two identical received LSAs.

Use the **undo lsa-arrival-interval** command to restore the default.

The interval defaults to 1000 milliseconds.

If an LSA that has the same LSA type, LS ID, originating router ID with the previous LSA is received within the interval, the LSA will be discarded. This feature helps you protect routers and bandwidth from being over-consumed due to frequent network changes.

It is recommended the interval set by the **lsa-arrival-interval** command is smaller or equal to the *minimum-interval* set by the **lsa-generation-interval** command.

Related commands: **lsa-generation-interval**.

Examples # Set the LSA minimum repeat arrival interval to 200 milliseconds.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] lsa-arrival-interval 200
```

lsa-generation-interval

Syntax **lsa-generation-interval** *maximum-interval* [*initial-interval* [*incremental-interval*]]

undo lsa-generation-interval

View OSPF view

Parameters *maximum-interval*: Maximum LSA generation interval in seconds.

initial-interval: Minimum LSA generation interval in milliseconds. The default is 0.

incremental-interval: LSA generation incremental interval in milliseconds. The default is 5000 milliseconds.

Description Use the **lsa-generation-interval** command to configure the OSPF LSA generation interval.

Use the **undo lsa-generation-interval** command to restore the default.

The LSA generation interval defaults to 5 seconds.

With this command configured, when network changes are not frequent, an LSA is generated at the *initial-interval.* If network changes become frequent, LSA generation interval is incremented by a specified value each time a generation happens, up to the *maximum-interval*.

Related commands: **lsa-arrival-interval**.

Examples # Configure the LSA generation maximum interval as 2 seconds, minimum interval as 100 milliseconds and incremental interval as 100 milliseconds.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] lsa-generation-interval 2 100 100
```

lsdb-overflow-limit

Syntax **lsdb-overflow-limit** *number*

undo lsdb-overflow-limit

View OSPF view

Parameters *number*: Upper limit of external LSAs in the LSDB.

Description Use the **lsdb-overflow-limit** command to specify the upper limit of external LSAs in the LSDB.

Use the **undo lsdb-overflow-limit** command to restore the default.

The upper limit is unlimited by default.

Examples # Specify the upper limit of external LSAs as 400000.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] lsdb-overflow-limit 400000
```

maximum load-balancing (OSPF view)

Syntax **maximum load-balancing** *maximum*

undo maximum load-balancing

View OSPF view

Parameters *maximum*: Maximum number of equal cost routes for load balancing.

Description Use the **maximum load-balancing** command to specify the maximum number of equal cost routes for load balancing.

Use the **undo maximum load-balancing** command to restore the default.

The default number is 8.

Examples # Specify the maximum number of equal cost routes for load balancing as 2.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] maximum load-balancing 2
```

maximum-routes

Syntax **maximum-routes** { **external** | **inter** | **intra** } *number*

undo maximum-routes { **external** | **inter** | **intra** }

View OSPF view

Parameters *number*: Maximum route number.

external: Specifies the maximum number of external routes.

inter: Specifies the maximum number of interarea routes.

intra: Specifies the maximum number of intraarea routes.

Description Use the **maximum-routes** command to specify the maximum route number of a specified type: interarea, intraarea, external.

Use the **undo maximum-routes** command to restore the default route maximum value of a specified type.

Examples # Specify the maximum number of intraarea routes as 500.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] maximum-routes intra 500
```

network (OSPF area view)

Syntax **network** *ip-address wildcard-mask*

undo network *ip-address wildcard-mask*

View OSPF area view

Parameters *ip-address*: IP address of a network

wildcard-mask: Wildcard mask of the IP address

Description Use the **network** command to specify a network to belong to the area and enable OSPF on the interface attached to the network.

Use the **undo network** command to remove an OSPF interface.

By default, an interface neither belongs to any area nor runs OSPF.

You can configure in an area one or multiple interfaces to run OSPF. Note that the interface's primary IP address must fall into the specified network segment to make the interface run OSPF. If only the interface's secondary IP address falls into the segment, the interface cannot run OSPF.

Related commands: **ospf**.

Examples # Specify the interface whose primary IP address falls into 131.108.20.0/24 to run OSPF, and specify the interface to belong to area2.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 2
[Sysname-ospf-100-area-0.0.0.2] network 131.108.20.0 0.0.0.255
```

nssa

Syntax **nssa** [**default-route-advertise** | **no-import-route** | **no-summary**]*

undo nssa

View OSPF area view

Parameters **default-route-advertise**: Used on an NSSA ABR or an ASBR only. If configured on an NSSA ABR, the ABR generates a default route in a Type7 LSA into the NSSA regardless of whether the default route is available. If configured on an ASBR, only a default route is available on the ASBR can it generates a Type7 LSA into the attached area.

no-import-route: Used only on the NSSA ABR that is also the ASBR of the OSPF routing domain to disable redistributing any route in Type7 LSA into the NSSA area, making sure routes can be redistributed correctly.

no-summary: Used only on an NSSA ABR to advertise only a default route in a Type3 summary LSA into the NSSA area, and all other summary LSAs are not advertised into the area. Area of this kind is known as NSSA Totally Stub area.

Description Use the **nssa** command to configure the current area as an NSSA area.

Use the **undo nssa** command to restore the default.

By default, no NSSA area is configured.

All routers attached to an NSSA area must be configured with the **nssa** command in area view.

Related commands: **default-cost**.

Examples # Configure area1 as an NSSA area.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] nssa
```

opaque-capability enable

Syntax **opaque-capability enable**

undo opaque-capability

View OSPF view

Parameters None

Description Use the **opaque-capability enable** command to enable Opaque LSA advertisement and reception. With the command configured, the OSPF device can receive and advertise the Type 9, Type 10 and Type 11 opaque LSAs.

Use the **undo opaque-capability** command to restore the default.

The feature is disabled by default.

Examples # Enable advertising and receiving opaque LSAs.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100]opaque-capability enable
```

ospf

Syntax **ospf** [*process-id* | **router-id** *router-id* | **vpn-instance** *instance-name*]*

undo ospf *process-id*

View System view

Parameters *process-id*: OSPF process ID. The default is 1.

router-id: OSPF router ID, in dotted decimal format.

instance-name: VPN instance name, case insensitive.

Description Use the **ospf** command to enable an OSPF process.

Use the **undo ospf** command to disable an OSPF process.

OSPF is not enabled by default.

You can specify multiple OSPF processes on a device and different Router IDs for these processes.

When using OSPF as the VPN internal routing protocol for MPLS VPN implementation, you need to bind the OSPF process with a VPN instance.

Enabling OSPF first is required before performing other tasks.

Examples # Enable OSPF process 100 and specify Router ID as 10.10.10.1.

```
<Sysname> system-view
[Sysname] ospf 100 router-id 10.10.10.1
[Sysname-ospf-100]
```

ospf authentication-mode

Syntax For MD5/HMAC-MD5 authentication:

ospf authentication-mode { **md5** | **hmac-md5** } *key-id* [**plain** | **cipher**] *password*

undo ospf authentication-mode { **md5** | **hmac-md5** } *key-id*

For simple authentication:

ospf authentication-mode simple [**plain** | **cipher**] *password*

undo ospf authentication-mode simple

View Interface view

Parameters **md5**: MD5 authentication.

hmac-md5: HMAC-MD5 authentication.

simple: Simple authentication.

key-id: Authentication key ID.

plain | **cipher** : Plain or cipher password. If **plain** is specified, only plain password is supported and displayed upon displaying the configuration file. If **cipher** is specified, both plain and cipher are supported, but only cipher password is displayed when displaying the configuration file. If no keyword is specified, the cipher type is the default for the MD5/HMAC-MD5 authentication mode, and the plain type is the default for the simple authentication mode.

password: Password of plain or cipher. Simple authentication: For plain type password, a plain password is a string of up to 8 characters. For cipher type password, a plain password is a string of up to 8 characters, and a cipher password is a string of up to 24 characters. MD5/HMAC-MD5 authentication: For plain type password, a plain password is a string of up to 16 characters. For cipher type password, a plain password is a string of up to 16 characters, and a cipher password is a string of up to 24 characters.

Description Use the **ospf authentication-mode** command to set the authentication mode and key ID on an interface.

Use the **undo ospf authentication-mode** command to remove specified configuration.

By default, no authentication is available on an interface.

Interfaces attached to the same network segment must have the same authentication password and mode.

This configuration is not supported on the NULL interface.

Related commands: **authentication-mode**.

Examples # Configure the network 131.119.0.0/16 in area1 to support MD5 cipher authentication, and set the interface key ID to 15, authentication password to "password", and password type to cipher.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] network 131.119.0.0 0.0.255.255
[Sysname-ospf-100-area-0.0.0.1] authentication-mode md5
[Sysname-ospf-100-area-0.0.0.1] quit
[Sysname-ospf-100] quit
[Sysname] interface Vlan-interface 12
[Sysname-Vlan-interface12] ospf authentication-mode md5 15 cipher password
```

Configure the network 131.119.0.0/16 in area1 to support simple authentication, and set for the interface the authentication password to "password", and password type to cipher.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] network 131.119.0.0 0.0.255.255
[Sysname-ospf-100-area-0.0.0.1] authentication-mode simple
[Sysname-ospf-100-area-0.0.0.1] quit
[Sysname-ospf-100] quit
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf authentication-mode simple cipher password
```

ospf cost

Syntax **ospf cost** *value*

undo ospf cost

View Interface view

Parameters *value*: OSPF cost, in the range 1 to 65535.

Description Use the **ospf cost** command to set the OSPF cost of the interface.

Use the **undo ospf cost** command to restore the default OSPF cost of the interface.

By default, an OSPF interface calculates its cost automatically: Interface default cost=100 Mbps /Interface bandwidth(Mbps), default costs of some interfaces are:

- 1785 for the 56kbps serial interface
- 1562 for the 64kbps serial interface
- 48 for the E1 (2.048Mbps) interface
- 1 for the Ethernet interface

You can use the **ospf cost** command to set an interface's OSPF cost manually.

This configuration is not supported on the NULL interface.

Examples # Set the OSPF cost of VLAN-interface 12 to 65.

```
<Sysname> system-view
[Sysname] interface vlan-interface 12
[Sysname-Vlan-interface12] ospf cost 65
```

ospf dr-priority

Syntax **ospf dr-priority** *priority*

undo ospf dr-priority

View Interface view

Parameters *priority*: DR Priority of the interface.

Description Use the **ospf dr-priority** command to set the priority for DR/BDR election on an interface.

Use the **undo ospf dr-priority** command to restore the default value.

By default, the priority is 1.

The bigger the value, the higher the priority.

This configuration is not supported on the NULL interface.

Examples # Set the DR priority of VLAN-interface12 to 8.

```
<Sysname> system-view
[Sysname] interface vlan-interface 12
[Sysname-Vlan-interface12] ospf dr-priority 8
```

ospf mib-binding

Syntax **ospf mib-binding** *process-id*

undo ospf mib-binding

View System view

Parameters *process-id*: OSPF process ID.

Description Use the **ospf mib-binding** command to bind an OSPF process to MIB operation.

Use the **undo ospf mib-binding** command to restore the default.

By default, MIB operation is bound to the first enabled OSPF process.

Examples # Bind OSPF process 100 to MIB operation.

```
<Sysname> system-view
[Sysname] ospf mib-binding 100
```

Restore the default, that is, bind the first enabled OSPF process to MIB operation

```
<Sysname> system-view
[Sysname] undo ospf mib-binding
```

ospf mtu-enable

Syntax **ospf mtu-enable**

undo ospf mtu-enable

View Interface view

Parameters None

Description Use the **ospf mtu-enable** command to enable an interface to add the real MTU into DD packets.

Use the **undo ospf mtu-enable** command to restore the default.

By default, an interface adds the MTU value of 0 into DD packets, that is, no real MTU is added.

Note that:

- After a virtual link is established via the Virtual-Template or Tunnel, two devices on the link from different vendors may have different default MTU values. To make them consistent, set the attached interfaces' default MTU to 0 for sending DD packets.
- This configuration is not supported on the NULL interface.

Examples # Enable the VLAN-interface12 to add the real MTU value into DD packets.

```
<Sysname> system-view
[Sysname] interface vlan-interface 12
[Sysname-Vlan-interface12] ospf mtu-enable
```

ospf network-type

Syntax **ospf network-type** { **broadcast** | **nbma** | **p2mp** | **p2p** }

undo ospf network-type

View Interface view

Parameters **broadcast**: Specifies the network type as Broadcast.

nbma: Specifies the network type as NBMA.

p2mp: Specifies the network type as P2MP.

p2p: Specifies the network type as P2P.

Description Use the **ospf network-type** command to set the network type of an interface.

Use the **undo ospf network-type** command to restore the default network type for an interface.

By default, the network type of an interface depends on its physical media. The network type for Ethernet interfaces is Broadcast, for serial interfaces is P2P, and for ATM interfaces is NBMA.

If a router attached to a broadcast network does not support multicast, you can configure the interface's network type as NBMA or change NBMA to Broadcast.

The requirements for changing the network type from NBMA to Broadcast on an interface: Any two routers in the network are directly connected via a virtual link, or the network is fully meshed. If a network cannot meets the requirements, you have to change the network type of an attached interface to P2MP, thus two routers having no direct link can exchange routing information via another router. After changing the network type to P2MP, you do not need to configure any neighbor.

If only two routers run OSPF on a network segment, you can configure associated interfaces' network type as P2P.

This configuration is not supported on the NULL interface.

Related commands: **ospf dr-priority**.

*When changing an interface's network type to NBMA or the interface's network type is NBMA, you need to use the **peer** command to configure adjacencies.*

Examples # Configure the network type of VLAN-interface12 as NBMA.

```
<Sysname> system-view
[Sysname] interface vlan-interface 12
[Sysname-Vlan-interface12] ospf network-type nbma
```

ospf timer dead

Syntax **ospf timer dead** *seconds*

undo ospf timer dead

View Interface view

Parameters *seconds*: Dead interval in seconds.

Description Use the **ospf timer dead** command to set the dead interval.

Use the **undo ospf timer dead** command to restore the default.

The dead interval defaults to 40s for Broadcast, P2P interfaces and defaults to 120s for P2MP and NBMA interfaces

If an interface receives no Hello packet from the neighbor after the dead interval elapsed, the interface considers the neighbor as dead. The dead interval on an interface is at least four times the hello interval. Any two routers attached to the same segment must have the same dead interval.

This configuration is not supported on the NULL interface.

Related commands: **ospf timer hello**.

Examples # Configure the dead interval on VLAN-interface12 as 60 seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 12
[Sysname-Vlan-interface12] ospf timer dead 60
```

ospf timer hello

Syntax **ospf timer hello** *seconds*

undo ospf timer hello

View Interface view

Parameters *seconds*: Hello interval in seconds.

Description Use the **ospf timer hello** command to set the hello interval on an interface.

Use the **undo ospf timer hello** command to restore the default hello interval on an interface.

The hello interval defaults to 10s for P2P and Broadcast interfaces, and defaults to 30s for P2MP and NBMA interfaces

The shorter the hello interval, the faster the topology convergence speed and the more resources consumed. Make sure the hello interval on two neighboring interfaces is the same.

This configuration is not supported on the NULL interface.

Related commands: **ospf timer dead**.

Examples # Configure the hello interval on VLAN-interface12 as 20 seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 12
[Sysname-Vlan-interface12] ospf timer hello 20
```

ospf timer poll

Syntax **ospf timer poll** *seconds*

undo ospf timer poll

View Interface view

Parameters *seconds*: Poll interval in seconds.

Description Use the **ospf timer poll** command to set the poll interval on an NBMA interface.

Use the **undo ospf timer poll** command to restore the default value.

By default, the poll interval is 120s.

When an NBMA or P2MP interface finds its neighbor is dead, it will send hello packets at the poll interval. The poll interval is at least four times the hello interval.

This configuration is not supported on the NULL interface.

Related commands: **ospf timer hello**.

Examples # Set the poll interval on VLAN-interface12 to 130 seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 12
[Sysname-Vlan-interface12] ospf timer poll 130
```

ospf timer retransmit

Syntax **ospf timer retransmit** *interval*

undo ospf timer retransmit

View Interface view

Parameters *interval*: LSA retransmission interval in seconds, in the range 1 to 3600.

Description Use the **ospf timer retransmit** command to set the LSA retransmission interval on an interface.

Use the **undo ospf timer retransmit** command to restore the default.

The interval defaults to 5s.

After sending an LSA, an interface waits for an acknowledgement packet. If the interface receives no acknowledgement when the retransmission interval elapses, it will retransmit the LSA.

The retransmission interval should not be so small to avoid unnecessary retransmissions.

This configuration is not supported on the NULL interface.

Examples # Set the LSA retransmission interval of VLAN-interface12 to 8 seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 12
[Sysname-Vlan-interface12] ospf timer retransmit 8
```

ospf trans-delay

Syntax **ospf trans-delay** *seconds*

undo ospf trans-delay

View Interface view

Parameters *seconds*: LSA transmission delay in seconds.

Description Use the **ospf trans-delay** command to set the LSA transmission delay of an interface.

Use the **undo ospf trans-delay** command to restore the default.

The default LSA transmission delay is 1 second.

Each LSA in the LSDB has an age that incremented by 1 every second, but the age does not change during transmission. It is necessary to add a transmit delay into its age time, which is important for transmission on low speed networks.

This configuration is not supported on the NULL interface.

Examples # Set the LSA transmission delay to 3 seconds on VLAN-interface12.

```
<Sysname> system-view
[Sysname] interface vlan-interface 12
[Sysname-Vlan-interface12] ospf trans-delay 3
```

peer

Syntax **peer** *ip-address* [**dr-priority** *dr-priority*]

undo peer *ip-address*

View OSPF view

Parameters *ip-address*: Neighbor IP address.

dr-priority: Neighbor DR priority; The bigger the value, the higher the priority.

Description Use the **peer** command to specify the IP address and DR priority of a neighbor.

Use the **undo peer** command to remove the configuration.

After startup, a router sends a Hello packet to routers with DR priorities higher than 0. When the DR and BDR are elected, they will send Hello packets to all neighbors for adjacency establishment.

A router uses the priority set with the **peer** command to determine whether to send a Hello packet to the neighbor rather than for DR election. The DR priority set with the **ospf dr-priority** command is used for DR election.

Related commands: **ospf dr-priority**.

Examples # Specify the neighbor IP address 1.1.1.1.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] peer 1.1.1.1
```

preference (OSPF view)

Syntax **preference** [**ase** [**route-policy** *route-policy-name*]] *value*

undo preference [**ase**]

View OSPF view

Parameters **ase**: Sets a priority for ASE routes. If the keyword is not specified, using the command sets a priority for internal routes.

route-policy: Applies a route policy to set priorities for specified routes.

route-policy-name: Routing policy name.

value: Priority for OSPF routes. A smaller value represents a higher priority.

Description Use the **preference** command to set the priority of OSPF routes.

Use the **undo preference** command to restore the default.

The priority of OSPF internal routes defaults to 10, and the priority of OSPF external routes defaults to 150.

If a route-policy is applied, priorities defined by the route-policy will apply, and priorities not defined by the policy will still use values set by the **preference** command.

Since a device may run multiple routing protocols, it has to decide on routes found by these protocols. Every protocol has a priority to help the router determine which route to use especially when multiple routes to the same destination are found by several routing protocols. The route found by the protocol with the highest priority will be used.

Examples # Set OSPF priority to 150.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] preference 150
```

reset ospf counters

Syntax **reset ospf** [*process-id*] **counters** [**neighbor** [*interface-type interface-number*] [*router-id*]]

View User view

Parameters *process-id*: OSPF process ID.

neighbor: Clears neighbor statistics on an interface.

interface-type interface-number: Interface type and interface number.

router-id: Neighbor router ID.

Description Use the **reset ospf counters** command to reset OSPF counters. If no OSPF process is specified, counters of all OSPF processes are reset.

Examples # Clear OSPF counters.

```
<Sysname> reset ospf counters
```

reset ospf process

Syntax **reset ospf** [*process-id*] **process**

View User view

Parameters *process-id*: OSPF process ID.

Description Use the **reset ospf process** command to reset all OSPF processes or a specified process.

Using the **reset ospf process** command will:

- Clear all invalid LSAs without waiting for their timeouts
- Make a newly configured Router ID take effect
- Start a new round of DR/BDR election
- Not remove any previous OSPF configurations.

The system prompts whether to reset OSPF process upon execution of this command.

Examples # Reset all OSPF processes.

```
<Sysname> reset ospf process
```

reset ospf redistribution

Syntax **reset ospf** [*process-id*] **redistribution**

View User view

Parameters *process-id*: OSPF process ID.

Description Use the **reset ospf redistribution** command to restart route redistribution. If no process ID is specified, using the command restarts route redistribution for all OSPF processes.

Examples # Restart route redistribution.

```
<Sysname> reset ospf redistribution
```

rfc1583 compatible

Syntax **rfc1583 compatible**

undo rfc1583 compatible

View OSPF view

Parameters None

Description Use the **rfc1583 compatible** command to make routing rules defined in RFC1583 compatible.

Use the **undo rfc1583 compatible** command to disable the function.

By default, RFC1583 routing rules are compatible.

On selecting the best route when multiple AS external LSAs describe routes to the same destination, RFC1583 and RFC2328 have different routing rules.

Examples # Make RFC1583 routing rules compatible.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] rfc1583 compatible
```

silent-interface (OSPF view)

Syntax **silent-interface** { **all** | *interface-type interface-number* }

undo silent-interface { **all** | *interface-type interface-number* }

View OSPF view

Parameters **all**: Disables all interfaces from sending OSPF packet.

interface-type interface-number: Interface type and interface number.

Description Use the **silent-interface** command to disable specified interfaces from sending any OSPF packet.

Use the **undo silent-interface** command to restore the default.

By default, an interface sends OSPF packets.

A disabled interface is a Passive Interface, which cannot send any Hello packet.

To make no routing information obtained by other routers on a network segment, you can use this command to disable the interface from sending OSPF packets.

Examples # Disable VLAN-interface12 from sending OSPF packets.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] silent-interface vlan-interface 10
```

snmp-agent trap enable ospf

Syntax **snmp-agent trap enable ospf** [*process-id*] [**ifauthfail** | **ifcfgerror** | **ifrxbadpkt** | **ifstatechange** | **lsdbapproachoverflow** | **lsdboverflow** | **maxagelsa** | **nbrstatechange** | **originatelsa** | **txretransmit** | **vifauthfail** | **vifcfgerror** | **virifrxbadpkt** | **virifstatechange** | **viriftxretransmit** | **virnbrstatechange**] *

undo snmp-agent trap enable ospf [*process-id*] [**ifauthfail** | **ifcfgerror** | **ifrxbadpkt** | **ifstatechange** | **lsdbapproachoverflow** | **lsdboverflow** | **maxagelsa** | **nbrstatechange** | **originatelsa** | **txretransmit** | **vifauthfail** | **vifcfgerror** | **virifrxbadpkt** | **virifstatechange** | **viriftxretransmit** | **virnbrstatechange**] *

View System view

Parameters *process-id*: OSPF process ID.

ifauthfail: Interface authentication failure information.

ifcfgerror: Interface configuration error information.

ifrxbadpkt: Information about error packets received.

ifstatechange: Interface state change information.

lsdbapproachoverflow: Information about cases approaching LSDB overflow

lsdboverflow: LSDB overflow information.

maxagelsa: LSA max age information.

nbrstatechange: Neighbor state change information.

originatelsa: Information about LSAs originated locally.

txretransmit: Packet receiving and forwarding information.

vifauthfail: Virtual interface authentication failure information.

vifcfgerror: Virtual interface configuration error information.

virifrxbadpkt: Information about error packets received by virtual interfaces.

virifstatechange: Virtual interface state change information.

viriftxretransmit: Virtual interface packet retransmit information.

virnbrstatechange: Virtual interface neighbor state change information.

Description Use the **snmp-agent trap enable ospf** command to enable TRAP function for a specified OSPF process. If no process is specified, TRAP function for all processes is enabled.

Use the **undo snmp-agent trap enable ospf** command to disable the function.

By default, this function is enabled.

Refer to "SNMP Configuration Commands" on page 1347 for related information.

Examples # Enable trap packet transmission for all OSPF processes.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable ospf
```

spf-schedule-interval

Syntax **spf-schedule-interval** *maximum-interval* [*minimum-interval* [*incremental-interval*]]

undo spf-schedule-interval

View OSPF view

Parameters *maximum-interval*: Maximum SPF calculation interval in seconds. The default is 5 seconds.

minimum-interval: Minimum SPF calculation interval in milliseconds. The default is 0.

incremental-interval: Incremental value for increasing SPF calculation interval in milliseconds. The default is 5000.

Description Use the **spf-schedule-interval** command to set intervals for OSPF SPF calculation.

Use the **undo spf-schedule-interval** command to restore the default.

By default, SPF calculation interval is 5 seconds.

Based on its LSDB, an OSPF router calculates the shortest path tree with itself being the root, using which to determine the next hop to a destination. Through adjusting SPF calculation interval, you can protect bandwidth and router resources from being over-consumed due to frequent network changes.

With this command configured, when network changes are not frequent, SPF calculation applies at the *minimum-interval*. If network changes become frequent, SPF calculation interval is incremented each time a calculation happens, up to the *maximum-interval*.

Examples # Configure the SPF calculation interval as 6 seconds.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] spf-schedule-interval 6
```

stub (OSPF area view)

Syntax **stub** [**no-summary**]

undo stub

View OSPF area view

Parameters **no-summary**: Used only on a stub ABR. With it configured, the ABR advertises only a default route in a Summary LSA into the stub area (Stub area of this kind is known as totally stub area).

Description Use the **stub** command to configure an area as a stub area.

Use the **undo stub** command to remove the configuration.

No area is stub area by default. To configure an area as a stub area, all routers attached to it must be configured with this command.

Related commands: **default-cost**.

Examples # Configure area1 as a stub area.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] stub
```

stub-router

Syntax **stub-router**

undo stub-router

View OSPF view

Parameters None

Description Use the **stub-router** command to configure the router as a stub router.

Use the **undo stub-router** command to restore the default.

By default, no router is configured as a stub router.

The router LSAs from the stub router may contain different link type values. A value of 3 means a link to the stub network, so the cost of the link remains unchanged. A value of 1, 2 or 4 means a point-to-point link, a link to a transit network or a virtual link, in such cases, a maximum cost value of 65535 is used. Thus, other neighbors find the links to the stub router have such big costs, they will not send packets to the stub router for forwarding as long as there is a route with a smaller cost.

Examples # Enable a stub-router.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] stub-router
```

vlink-peer (OSPF area view)

Syntax **vlink-peer** *router-id* [**hello** *seconds* | **retransmit** *seconds* | **trans-delay** *seconds* | **dead** *seconds* | **simple** [**plain** | **cipher**] *password* | { **md5** | **hmac-md5** } *key-id* [**plain** | **cipher**] *password*]*

undo vlink-peer *router-id* [**hello** | **retransmit** | **trans-delay** | **dead** | [**simple** | { **md5** | **hmac-md5** } *key-id*]]*

View OSPF area view

Parameters *router-id*: Router ID of the neighbor on the virtual link.

hello *seconds*: Hello interval in seconds. The default is 10. It must be identical to the hello interval of the neighbor on the virtual link.

retransmit *seconds*: LSA retransmission interval in seconds. The default is 5.

trans-delay *seconds*: Transmission delay in seconds. The default is 1.

dead *seconds*: Dead interval in seconds. The default is 40. It must be identical to the dead interval on its virtual link neighbor. The dead interval is at least four times the hello interval.

md5: MD5 authentication.

hmac-md5: HMAC-MD5 authentication.

simple: Simple authentication.

key-id: Key ID for MD5 or HMAC-MD5 authentication.

plain | **cipher**: Plain or cipher type. If **plain** is specified, only plain password is supported. If **cipher** is specified, both plain and cipher password are supported, but only cipher password is displayed when displaying the configuration file. If no keword is specified, MD5 and HMAC-MD5 use cipher password, and the simple authentication mode uses plain password.

password: Plain or cipher password. Simple authentication: For plain type, a plain password is a string of up to 8 characters. For cipher type, a plain password is a string of up to 8 characters, and a cipher password is a string of up to 24 characters. MD5/HMAC-MD5 authentication: For plain type, a plain password is a string of up to 16 characters. For cipher type, a plain password is a string of up to 16 characters, and a cipher password is a string of up to 24 characters.

Description Use the **vlink-peer** command to create and configure a virtual link.

Use the **undo vlink-peer** command to remove a virtual link.

As defined in RFC2328, all non-backbone areas must maintain connectivity to the backbone. You can use the **vlink-peer** command to configure a virtual link to connect an area to the backbone.

Considerations on parameters:

- The smaller the hello interval is, the faster the network changes are found and the more network resources are consumed.
- A so small retransmission interval will lead to unnecessary retransmissions. A bigger value is appropriate for a low speed link.
- You need to consider the interface transmission delay when specifying the **trans-delay** value.

The authentication mode (MD5 or Simple) at the non-backbone virtual link end follows the one at the backbone virtual link end. The two authentication modes are independent. You can specify neither of them.

Related commands: **authentication-mode**, **display ospf**.

Examples # Configure a virtual link to the neighbor with router ID 1.1.1.1.

```
<Sysname> system-view
[Sysname] ospf 100
```

```
[Sysname-ospf-100] area 2
[Sysname-ospf-100-area-0.0.0.2] vlink-peer 1.1.1.1
```

36 IPv6 OSPFv3 Configuration Commands

abr-summary(OSPFv3 area view)

Syntax **abr-summary** *ipv6-address prefix-length* [**not-advertise**]

undo abr-summary *ipv6-address prefix-length*

View OSPFv3 area view

Parameters *ipv6-address*: Destination IPv6 address prefix of the summary route.

prefix-length: Length of the prefix.

not-advertise: Specifies not to advertise the summary IPv6 route.

Description Use the **abr-summary** command to configure an IPv6 summary route on an area border router.

Use the **undo abr-summary** command to remove an IPv6 summary route. Then the summarized routes are advertised.

By default, no route summarization is configured on an ABR.

You can use this command only on an ABR to configure a summary route for the area. The ABR advertises only the summary route to other areas. Multiple contiguous networks may be available in an area, where you can summarize them with one route for advertisement.

Examples # Summarize networks 2000:1:1:1::/64 and 2000:1:1:2::/64 in Area 1 with 2000:1:1::/48.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] area 1
[Sysname-ospfv3-1-area-0.0.0.1] abr-summary 2000:1:1:: 48
```

area (OSPFv3 view)

Syntax **area** *area-id*

View OSPFv3 view

Parameters *area-id*: ID of an area, a decimal integer or an IPv4 address.

Description Use the **area** command to enter OSPFv3 area view.

The undo form of the command is not available. An area is removed automatically if there is no configuration and no interface is up in the area.

Examples # Enter OSPFv3 Area 0 view.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] area 0
[Sysname-ospfv3-1-area-0.0.0.0]
```

debugging ospfv3 event

Syntax **debugging ospfv3 event** { **abr** | **asbr** | **vlink** | **all** }

undo debugging ospfv3 event { **abr** | **asbr** | **vlink** | **all** }

View User view

Parameters **abr**: ABR event debugging.

Asbr: ASBR event debugging.

Vlink: Virtual link event debugging.

all: All event debugging.

Description Use the **debugging ospfv3 event** command to enable specified OSPFv3 event debugging, such as ABR, ASBR, or virtual link event debugging.

Use the **undo debugging ospfv3 event** command to disable specified OSPFv3 event debugging.

By default, no OSPFv3 event debugging is enabled.

Examples # Enable OSPFv3 virtual link event debugging.

```
<Sysname> debugging ospfv3 event vlink
```

debugging ospfv3 ifsm

Syntax **debugging ospfv3 ifsm** [**status** | **event** | **timer**]

undo debugging ospfv3 ifsm [**status** | **event** | **timer**]

View User view

Parameters **status**: Status debugging of the interface state machine.

event: Event debugging of the interface state machine.

timer: Timer debugging of the interface state machine.

Description Use the **debugging ospfv3 ifsm** command to enable specified debugging of the OSPFv3 interface state machine.

Use the **undo debugging ospfv3 ifsm** command to disable specified debugging of the OSPFv3 interface state machine.

By default, no debugging of the OSPFv3 interface state machine is enabled.

Related commands: **display debugging ospfv3**.

Examples # Enable status debugging of the interface state machine.

```
<Sysname> debugging ospfv3 ifsm status
```

debugging ospfv3 lsa

Syntax **debugging ospfv3 lsa** { **all** | **flooding** | **generate** | **install** | **maxage** | **refresh | verbose** }

undo debugging ospfv3 lsa { **all** | **flooding** | **generate** | **install** | **maxage** | **refresh | verbose** }

View User view

Parameters **all**: All LSA debugging.

flooding: LSA flooding debugging.

generate: LSA generation debugging.

install: Debugging of LSAs installed into the LSDB.

maxage: LSA maxage debugging.

refresh: LSA refresh debugging.

verbose: LSA detailed debugging.

Description Use the **debugging ospfv3 lsa** command to enable specified OSPFv3 LSA debugging.

Use the **undo debugging ospfv3 lsa** command to disable specified OSPFv3 LSA debugging.

No LSA debugging is enabled by default.

Examples # Enable OSPFv3 LSA flooding debugging.

```
<Sysname> debugging ospfv3 lsa flooding
```

debugging ospfv3 nfsm

Syntax **debugging ospfv3 nfsm** [**status** | **event** | **timer**]

undo debugging ospfv3 nfsm [**status** | **event** | **timer**]

View User view

Parameters **status**: Status debugging of neighbor state machine.

event: Event debugging of neighbor state machine.

timer: Timer debugging of neighbor state machine.

Description Use the **debugging ospfv3 nfsm** command to enable specified debugging of OSPF neighbor state machine.

Use the **undo debugging ospfv3 nfsm** command to disable specified debugging of OSPF neighbor state machine.

No debugging of OSPF neighbor state machine is enabled by default.

Examples # Enable status debugging of OSPF neighbor state machine.

```
<Sysname> debugging ospfv3 nfsm status
```

debugging ospfv3 packet

Syntax **debugging ospfv3 packet** { **all** [**verbose**] | { **hello** | **dd** | **request** | **update** | **ack** | **verbose** }* }

undo debugging ospfv3 packet { **all** [**verbose**] | { **hello** | **dd** | **request** | **update** | **ack | verbose** }* }

View User view

Parameters **ack**: LSAck packet debugging.

dd: DD packet debugging.

hello: Hello packet debugging.

request: LSR packet debugging.

update: LSA packet debugging.

all: All packet debugging.

verbose: Packet detailed debugging.

Description Use the **debugging ospfv3 packet** command to enable specified OSPFv3 packet debugging.

Use the **undo debugging ospfv3 packet** command to disable specified OSPFv3 packet debugging.

No OSPFv3 packet debugging is enabled by default.

Examples # Enable detailed debugging for all OSPFv3 packets.

```
<Sysname> debugging ospfv3 packet all verbose
```

debugging ospfv3 route

Syntax **debugging ospfv3 route** [**ase** | **install** | **spf** | **ia**]

undo debugging ospfv3 route [**ase** | **install** | **spf** | **ia**]

View User view

Parameters **ase**: OSPFv3 ASE route debugging.

install: Debugging of OSPFv3 routes installed into the routing table..

spf: OSPFv3 SPF route calculation debugging.

ia: OSPFv3 inter-area route debugging.

Description Use the **debugging ospfv3 route** command to enable specified OSPFv3 route debugging.

Use the **undo debugging ospfv3 route** command to disable specified OSPFv3 route debugging.

No OSPFv3 route debugging is enabled by default.

Examples # Enable OSPFv3 ASE route debugging.

```
<Sysname> debugging ospfv3 route ase
```

default cost (OSPFv3 view)

Syntax **default cost** *value*

undo default cost

View OSPFv3 view

Parameters *value*: Default cost for redistributed routes.

Description Use the **default cost** command to configure a default cost for redistributed routes.

Use the **undo default cost** command to restore the default.

By default, the default cost is 1.

You need to configure the default cost value for redistributed routes to advertise them throughout the whole AS.

If multiple OSPFv3 processes are enabled, use of this command takes effect for the current process only.

Examples # Specify the default cost for redistributed routes as 10.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] default cost 10
```

default-cost (OSPFv3 area view)

Syntax **default-cost** *value*

undo default-cost

View OSPFv3 area view

Parameters *value*: Specifies a cost for the default route advertised to the stub area. The default is 1.

Description Use the **default-cost** command to specify the cost of the default route to be advertised to the stub area.

Use the **undo-default-cost** command to restore the default value.

This command is only available on the ABR that is connected to a stub area.

You have two commands to configure a stub area: **stub**, **defaulted-cost**. You need to use the **stub** command on routers connected to a stub area to configure the area as stub.

If multiple OSPFv3 processes are running, use of this command takes effect only for the current process.

Related commands: **stub**.

Examples # Configure Area1 as a stub area, and specify the cost of the default route advertised to the stub area as 60.

```
<Sysname> system-view
[Sysname] ospfv3
[Sysname-ospfv3-1] area 1
[Sysname-ospfv3-1-area-0.0.0.1] stub
[Sysname-ospfv3-1-area-0.0.0.1] default-cost 60
```

display debugging ospfv3

Syntax **display debugging ospfv3**

View Any view

Parameters None

Description Use the **display debugging ospfv3** command to display global OSPFv3 debugging state information.

Examples # Display the global OSPFv3 debugging state information.

```
<Sysname> display debugging ospfv3
OSPFv3 External route calculation debugging is on
```

display ospfv3

Syntax **display ospfv3** [*process-id*]

View Any view

Parameters *process-id*: OSPFv3 process ID.

Description Use the **display ospfv3** command to display the brief information of an OSPFv3 process. If no process ID is specified, brief information about all OSPFv3 processes will be displayed.

Examples # Display brief information about all OSPFv3 processes.

```
<Sysname> display ospfv3
Routing Process "OSPFv3 (1)" with ID 1.1.1.1
 SPF schedule delay 5 secs, Hold time between SPFs 10 secs
 Minimum LSA interval 5 secs, Minimum LSA arrival 1 secs
 Number of external LSA 0. These external LSAs' checksum Sum 0x0000
 Number of AS-Scoped Unknown LSA 0
 Number of LSA originated 3
 Number of LSA received 0
 Number of areas in this router is 1
  Area 0.0.0.1
       Number of interfaces in this area is 1
       SPF algorithm executed 1 times
       Number of LSA 2. These LSAs' checksum Sum 0x20C8
       Number of Unknown LSA 0
```

Table 126 Field descriptions of the display isofv3 command

Field	Description
Routing Process "OSPFv3 (1)" with ID 1.1.1.1	OSPFv3 process is 1, and router ID is 1.1.1.1.
SPF schedule delay	Delay interval of SPF calculation
Hold time between SPFs	Hold time between SPF calculations
Minimum LSA interval	Minimum interval for generating LSAs
Minimum LSA arrival	Minimum LSA repeat arrival interval
Number of external LSA	Number of ASEs
These external LSAs' checksum Sum	Sum of all the ASEs' checksum
Number of AS-Scoped Unknown LSA	Number of LSAs with unknown flooding scope
Number of LSA originated	Number of LSAs originated
Number of LSA received	Number of LSAs received
Number of areas in this router	Number of areas this device is attached to
Area	Area ID
Number of interfaces in this area	Number of interfaces attached to this area
SPF algorithm executed 1 times	SPF algorithm is executed 1 time
Number of LSA	Number of LSAs
These LSAs' checksum Sum	Sum of all LSAs' checksum
Number of Unknown LSA	Number of unknown LSAs

display ospfv3 interface

Syntax **display ospfv3 interface** [*interface-type interface-number* | **statistic**]

View Any view

Parameters *interface-type interface-number*: Interface type and interface number.

statistic: Displays the interface statistics.

Description Use the **display ospfv3 interface** command to display OSPFv3 interface information.

Examples # Display information about OSPFv3 Vlan-interface10.

```
<Sysname> display ospfv3 interface vlan-interface 10
Vlan-interface 10 is up, line protocol is up
  Interface ID 518
  IPv6 Prefixes
    FE80::1441:0:E213:1 (Link-Local Address)
    2000:1::1
  OSPFv3 Process (1), Area 0.0.0.1, Instance ID 0
    Router ID 2.2.2.2, Network Type POINTOPOINT, Cost: 1562
    Transmit Delay is 1 sec, State Point-To-Point, Priority 1
    No designated router on this link
     No backup designated router on this link
    Timer interval configured, Hello: 10, Dead: 40, Wait: 40, Retransmit: 5
       Hello due in 00:00:02
Neighbor Count is 1, Adjacent neighbor count is 1
```

Table 127 Field descriptions of the display ospfv3 interface command

Field	Description
Interface ID	Interface ID
IPv6 Prefixes	IPv6 Prefix
OSPFv3 Process	OSPFv3 Process
Area	Area ID
Instance ID	Instance ID
Router ID	Router ID
Network Type	Network type of the interface
Cost	Cost value of the interface
Transmit Delay	Transmission delay of the interface
State	Interface state
Priority	DR priority of the interface
No designated router on this link	No designated router on this link
No backup designated router on this link	No backup designated router on this link
Timer interval configured, Hello: 10, Dead: 40, Wait: 40, Retransmit: 5	Time intervals in seconds configured on the interface, Hello: 10, Dead: 40, Wait: 40, Retransmit: 5
Hello due in 00:00:02	Hello packet will be sent in 2 seconds
Neighbor Count	Number of Neighbors on the interface
Adjacent neighbor count	Number of Adjacencies on the interface

display ospfv3 lsdb

Syntax **display ospfv3** [*process-id*] **lsdb** [[**external** | **inter-prefix** | **inter-router** | **intra-prefix** | **link** | **network** | **router**] [*link-state-id*] [**originate-router** *router-id*] | **total**]

View Any view

Parameters *process-id*: ID of an OSPFv3 process.

external: Specifies to display information about AS-external LSAs.

inter-prefix: Specifies to display information about Inter-area-prefix LSAs.

inter-router: Specifies to display information about Inter-area-router LSAs.

intra-prefix: Specifies to display information about Intra-area-prefix LSAs.

link: Specifies to display information about Link-LSAs.

network: Specifies to display information about Network-LSAs.

router: Specifies to display information about Router-LSAs.

link-state-id: Link state ID, an IPv4 address.

originate-router *router-id*: ID of the advertising routing device .

total: Specifies to display all information in the LSDB.

Description Use the **display ospfv3 lsdb** command to display OSPFv3 LSDB information.

Examples # Display OSPFv3 LSDB information.

```
<Sysname> display ospfv3 lsdb

            OSPFv3 Router with ID (5.5.5.5) (Process 1)
               Link-LSA (Interface vlan-interface 12)
 ----------------------------------------------------------------
Link State ID   Origin Router    Age   SeqNum     CkSum  Prefix
0.15.0.9        5.5.5.5          0304  0x80000001 0x5b6a      1
0.15.0.9        6.6.6.6          0311  0x80000001 0x6956      1

               Router-LSA (Area 0.0.0.0)
 ----------------------------------------------------------------
Link State ID   Origin Router    Age   SeqNum     CkSum    Link
0.0.0.0         5.5.5.5          0263  0x80000002 0x823f      1
0.0.0.0         6.6.6.6          0264  0x80000003 0x625a      1

               Network-LSA (Area 0.0.0.0)
 ----------------------------------------------------------------
Link State ID   Origin Router    Age   SeqNum     CkSum
0.15.0.9        6.6.6.6          0264  0x80000001 0x3498

               Intra-Area-Prefix-LSA (Area 0.0.0.0)
 ----------------------------------------------------------------
Link State ID  Origin Router   Age   SeqNum     CkSum  Prefix  Reference
0.0.0.2        6.6.6.6         0263  0x80000001 0x95c4      1  Network-LSA
```

Table 128 Field descriptions of the display isofv3 lsdb command

Field	Description
Link-LSA	Type 8 LSA
Link State ID	Link State ID
Origin Router	Originating device
Age	Age of LSAs
SeqNum	LSA sequence number
CkSum	LSA Checksum
Prefix	Number of Prefixes
Router-LSA	Router-LSA
Link	Number of links
Network-LSA	Network-LSA
Intra-Area-Prefix-LSA	Type 9 LSA
Reference	Type of referenced LSA

Display Link-local LSA information in the LSDB.

```
<Sysname> display ospfv3 lsdb link
            OSPFv3 Router with ID (2.2.2.2) (Process 1)

                Link-LSA (Interface vlan-interface 10)

  LS age: 11
```

```
  LS Type: Link-LSA
  Link State ID: 0.0.2.6
  Originating Router: 2.2.2.2
  LS Seq Number: 0x80000002
  Checksum: 0xEFFA
  Length: 56
  Priority: 1
  Options: 0x000013 (-|R|-|-|E|V6)
  Link-Local Address: FE80::1441:0:E213:1
  Number of Prefixes: 1
    Prefix: 2000:1::/64
    Prefix Options: 0 (-|-|-|-)
```

Table 129 Field descriptions of the display ospfv3 lsdb command

Field	Description
LS age	Age of LSA
LS Type	Type of LSA
Originating Router	Originating device
LS Seq Number	LSA Sequence Number
Checksum	LSA Checksum
Length	LSA Length
Priority	Device Priority
Options	Options
Link-Local Address	Link-Local Address
Number of Prefixes	Number of Prefixes
Prefix	Address prefix
Prefix Options	Prefix options

display ospfv3 lsdb statistic

Syntax **display ospfv3 lsdb statistic**

View Any view

Parameters None

Description Use the **display ospfv3 lsdb statistic** command to display LSA statistics in the OSPFv3 LSDB.

Examples # Display OSPFv3 LSDB statistics.

```
<System> display ospfv3 lsdb statistic

            OSPFv3 Router with ID (1.1.1.1) (Process 1)
                        LSA Statistics
 ----------------------------------------------------------------------
Area ID         Router   Network  InterPre InterRou IntraPre Link     ASE
0.0.0.0         2        1        1        0        1
0.0.0.1         1        0        1        0        1
Total           3        1        2        0        2        3        0
```

Table 130 Descriptions on the fields of the display ospfv3 lsdb statistic command

Field	Description
Area ID	Area ID
Router	Router-LSA number
Network	Network-LSA number
InterPre	Inter-Area-Prefix-LSA number
InterRou	Inter-Area-Router-LSA number
IntraPre	Intra-Area-Prefix-LSA number
Link	Link-LSA number
ASE	AS-external-LSA number
Total	Total LSA number

display ospfv3 next-hop

Syntax **display ospfv3** [*process-id*] **next-hop**

View Any view

Parameters *process-id*: OSPFv3 process ID.

Description Use the **display ospfv3 next-hop** command to display OSPFv3 next hop information.

If no process is specified, next hop information of all OSPFv3 processes is displayed.

Examples # Display OSPFv3 next hop information.

```
<Sysname> display ospfv3 next-hop

            OSPFv3 Router with ID (2.2.2.2) (Process 1)
Neighbor-Id     Next-Hop                                Interface   RefCount
1.1.1.1         FE80::20F:E2FF:FE00:1                   Vlan 10      1
```

Table 131 Field descriptions of the display ospfv3 next-hop command

Field	Description
Neighbor-Id	Neighboring router ID
Next-hop	Next-hop address
Interface	Outbound interface
RefCount	Reference count

display ospfv3 peer

Syntax **display ospfv3** [*process-id*] [**area** *area-id*] **peer** [[*interface-type interface-number*] [**verbose**] | *peer-router-id*]

View Any view

Parameters *process-id*: OSPFv3 process ID.

area: Displays neighbor information of the specified area.

area-id: The ID of an area, a decimal integer or an IPv4 address.

interface-type interface-number: interface type and number.

verbose: Displays detailed neighbor information.

peer-router-id: Router ID of the specified neighbor.

Description Use the **display ospfv3 peer** command to display OSPFv3 neighbor information.

- If no *area-id* is specified, the neighbor information of all areas is displayed.
- If no *process-id* is specified, the information of all processes is displayed.
- If no interface or neighbor Router-ID is specified, the neighbor information of all interfaces is displayed.

Examples # Display the neighbor information of OSPFv3 process 1 of an interface.

```
<Sysname> display ospfv3 1 peer vlan-interface 10
OSPFv3 Process (1)
Neighbor ID     Pri   State            Dead Time   Interface  Instance ID
1.1.1.1         1     Full/ -          00:00:30    vlan10     0
```

Table 132 Field descriptions of the display isofv3 peer command

Field	Description
Neighbor ID	Neighbor ID
Pri	Priority of the neighbor
State	Neighbor state
Dead Time	Dead time remained
Interface	Interface connected to the neighbor
Instance ID	Instance ID

Display detailed neighbor information of OSPFv3 process 100 of an interface.

```
<Sysname> display ospfv3 100 peer vlan-interface 10 verbose
OSPFv3 Process (100)
 Neighbor: 1.1.1.1, interface address: FE80::3D43:0:8C14:1
    In the area 0.0.0.1 via vlan-interface 10
    DR is 0.0.0.0 BDR is 0.0.0.0
    Options is 0x000013 (-|R|-|-|E|V6)
    Dead timer due in 00:00:29
    Neighbor is up for 00:06:28
    Database Summary List 0
    Link State Request List 0
    Link State Retransmission List 0
```

Table 133 Field descriptions of the display isofv3 peer verbose command

Field	Description
Neighbor	Neighbor ID
interface address	Interface address

Table 133 Field descriptions of the display isofv3 peer verbose command

Field	Description
In the area 0.0.0.1 via interface vlan-interface 10	Interface Serial 2/0 belongs to area 1
DR is 0.0.0.0 BDR is 0.0.0.0	Neither DR nor BDR is elected
Options is 0x000013 (-|R|-|-|E|V6)	The option is 0x000013 (-|R|-|-|E|V6)
Dead timer due in 00:00:29	Dead timer due in 00:00:29
Neighbor is up for 00:06:28	Neighbor is up for 6 minutes and 28 seconds
Database Summary List	Number of LSAs sent in DD packet
Link State Request List	Number of LSAs in the link state request list
Link State Retransmission List	Number of LSAs in the link state retransmission list

display ospfv3 peer statistic

Syntax **display ospfv3 peer statistic**

View Any view

Parameters None

Description Use the **display ospfv3 peer statistic** command to display information about all OSPFv3 neighbors on the device, that is, numbers of neighbors in different states.

Examples # Display information about all OSPFv3 neighbors.

```
<Sysname> display ospfv3 peer statistic

            OSPFv3 Router with ID (1.1.1.1) (Process 1)
                          Neighbor Statistics
 ------------------------------------------------------------------------
Area ID          Down     Init     2-way    ExStar   Exchange Loading  Full
0.0.0.0          0        0        0        0        0        0        1
Total            0        0        0        0        0        0        1
```

Table 134 Field descriptions of the display ospfv3 peer statistic command

Field	Description
Area ID	Area ID
Down	In this state, neighbor initial state, the device has not received any information from a neighboring device for a period of time.
Init	In this state, the device received a Hello packet from the neighbor but the packet contains no Router ID of the neighbor. Mutual communication is not setup.
2-Way	Indicates mutual communication between the device and its neighbor is setup. DR/BDR election is finished under this state (or higher).
ExStart	In this state, the device decides on the initial DD sequence number and master/slave relationship of the two parties.
Exchange	In this state, the device exchanges DD packets with the neighbor.
Loading	In this state, the device sends LSRs to request the neighbor for needed LSAs.
Full	Indicates LSDB synchronization has been accomplished between neighbors.
Total	Total number of neighbors under the same state

display ospfv3 request-list

Syntax **display ospfv3** [*process-id*] **request-list** [**statistic**]

View Any view

Parameters *process-id*: OSPFv3 process ID.

statistic: Statistics of link state request list.

Description Use the **display ospfv3 request-list** command to display OSPFv3 link state request list information.

If no process is specified, link state request list information of all OSPFv3 processes is displayed.

Examples # Display the information of OSPFv3 link state request list.

<Sysname> display ospfv3 request-list

OSPFv3 Router with ID (1.1.1.1) (Process 1)

Interface vlan10 Area-ID 0.0.0.1

Nbr-ID 2.2.2.2

```
LS-Type              LS-ID          AdvRouter       SeqNum       Age
AS-External-LSA      0.0.16.66      2.2.2.2         0x80000001   98
AS-External-LSA      0.0.16.67      2.2.2.2         0x80000001   98
AS-External-LSA      0.0.16.68      2.2.2.2         0x80000001   98
```

Table 135 Field descriptions of the display ospfv3 request-list command

Field	Description
Interface	Interface name
Area-ID	Area ID
Nbr-ID	Neighbor's router ID
LS-Type	Type of LSA
LS-ID	Link state ID
AdvRouter	Advertising router
SeqNum	LSA sequence number
Age	Age of LSA

Display the statistics of OSPFv3 link state request list.

```
<Sysname> display ospfv3 request-list statistics

            OSPFv3 Router with ID (1.1.1.1) (Process 1)
Interface   Neighbor        LSA-Count
Vlan10          2.2.2.2         0
```

Table 136 Field descriptions of the display ospfv3 request-list statistics command

Field	Description
Interface	Interface name
Neighbor	Neighbor's router ID
LSA-Count	Number of LSAs in the request list

display ospfv3 retrans-list

Syntax **display ospfv3** [*process-id*] **retrans-list** [**statistic**]

View Any view

Parameters *process-id*: OSPFv3 process ID, in the range 1 to 65535.

statistic: Displays link state retransmission list statistics.

Description Use the **display ospfv3 retrans-list** command to display OSPFv3 link state retransmission list information.

If no process is specified, link state retransmission list information of all OSPFv3 processes is displayed.

Examples # Display the information of OSPFv3 link state retransmission list.

<Sysname> display ospfv3 retrans-list

OSPFv3 Router with ID (2.2.2.2) (Process 1)

Interface Eth1/0 Area-ID 0.0.0.1

Nbr-ID 2.2.2.2

```
LS-Type                LS-ID           AdvRouter       SeqNum       Age
Router-LSA             0.0.0.0         2.2.2.2         0x80000006   0
Network-LSA            0.15.0.8        2.2.2.2         0x80000001   0
Intra-Area-Prefix-LSA  0.0.0.1         2.2.2.2         0x80000006   0
```

Table 137 Field descriptions of the display ospfv3 retrans-list command

Field	Description
Interface	Interface name
Area-ID	Area ID
Nbr-ID	Neighbor's Router ID
LS-Type	Type of LSA
LS-ID	Link state ID
AdvRouter	Advertising Router
SeqNum	LSA sequence Number
Age	Age of LSA

Display the statistics of OSPFv3 link state retransmission list.

```
<Sysname>display ospfv3 retrans-list statistics

            OSPFv3 Router with ID (3.3.3.3) (Process 1)
Interface  Neighbor        LSA-Count
vlan 1     1.1.1.1           0
```

Table 138 Field descriptions of the display ospfv3 retrans-list statistics command

Field	Description
Interface	Interface name
Neighbor	Neighbor ID
LSA-Count	Number of LSAs in the retransmission request list

display ospfv3 routing

Syntax **display ospfv3** [*process-id*] **routing** [*ipv6-address prefix-length* **|** *ipv6-address/prefix-length* | **abr-routes** | **asbr-routes** | **all | statistics**]

View Any view

Parameters *process-id*: OSPFv3 process ID.

ipv6-address: IPv6 address.

prefix-length: Prefix length.

abr-routes: Displays routes to ABR.

asbr-routes: Displays routes to ASBR.

all: Displays all routes.

statistics: Displays the OSPFv3 routing table statistics .

Description Use the **display ospfv3 routing** command to display OSPFv3 routing table information.

If no process is specified, routing table information of all OSPFv3 processes is displayed.

Examples # Display OSPFv3 routing table information.

```
<Sysname> display ospfv3 routing

 E1 - Type 1 external route,    IA - Inter area route,    I  - Intra area route
 E2 - Type 2 external route,    *  - Seleted route

            OSPFv3 Router with ID (1.1.1.1) (Process 1)
 ------------------------------------------------------------------------
 *Destination: 2001::/64
  Type       : I                                    Cost     : 1
  NextHop    : directly-connected                   Interface: vlan12
```

Table 139 Field descriptions of the display ospfv3 routing command

Field	Description
Destination	Destination network segment
Type	Route type
Cost	Route cost value
Next-hop	Next hop address
Interface	Outbound interface

Display the statistics of OSPFv3 routing table.

```
<Sysname> display ospfv3 routing statistics
            OSPFv3 Router with ID (1.1.1.1) (Process 1)
                          OSPFv3 Routing Statistics
 Intra-area-routes    :   1
 Inter-area-routes    :   0
 External-routes      :   0
```

Table 140 Field descriptions of the display ospfv3 routing statistics command

Field	Description
Intra-area-routes	Number of Intra-area-routes
Inter-area-routes	Number of inter-area routes
External-routes	Number of external routes

display ospfv3 statistic

Syntax **display ospfv3 statistic**

View Any view

Parameters None

Description Use the **display ospfv3 statistic** command to display outbound/inbound OSPFv3 packet statistics on associated interface(s).

Examples # Display outbound/inbound OSPFv3 packet statistics on associated interfaces.

```
<Sysname> display ospfv3 statistic

                      OSPFv3 Statistics
Interface vlan-interface 14 Instance 0
 Type              Input       Output
 Hello             189         63
 DB Description    10          8
 Ls Req            2           1
 Ls Upd            16          6
 Ls Ack            10          6
```

Table 141 Field descriptions of the display ospfv3 statistics command

Field	Description
Interface	Interface name

Table 141 Field descriptions of the display ospfv3 statistics command

Field	Description
Instance	Instance number
Type	Type of packet
Input	Number of packets received by the interface
Output	Number of packets sent by the interface
Hello	Hello packet
DB Description	Database description packet
Ls Req	Link state request packet
Ls Upd	Link state update packet
Ls Ack	Link state acknowledgement packet

display ospfv3 topology

Syntax **display ospfv3** [*process-id*] **topology** [**area** *area-id*]

View Any view

Parameters *process-id*: OSPFv3 process ID.

area: Displays the topology information of the specified area.

area-id: Area ID, a decimal integer or an IPv4 address.

Description Use the **display ospfv3 topology** command to display OSPFv3 topology information.

Examples # Display OSPFv3 area 1 topology information.

```
<Sysname> display ospfv3 topology area 1

                      OSPFv3 Process (1)
OSPFv3 Area (0.0.0.1) topology
Type  ID(If-Index)       Bits      Metric    Next-Hop        Interface
Rtr   1.1.1.1                      --
Rtr   2.2.2.2                      1         2.2.2.2         Eth1/0
Rtr   3.3.3.3                      1         3.3.3.3         Eth1/0
Rtr   4.4.4.4                      1         4.4.4.4         Eth1/0
Net   4.4.4.4(983049)              1         0.0.0.0         Eth1/0
```

Table 142 Field descriptions of the display ospfv3 topology command

Field	Description
Type	Type of node
ID(If-Index)	Router ID
Bits	Flag bit
Metric	Cost value
Next-Hop	Next hop
Interface	Outbound interface

display ospfv3 vlink

Syntax **display ospfv3** [*process-id*] **vlink**

View Any view

Parameters *process-id*: OSPFv3 process ID.

Description Use the **display ospfv3 vlink** command to display OSPFv3 virtual link information. If no process is specified, virtual link information of all OSPFv3 processes is displayed.

Examples # Display OSPFv3 virtual link information.

```
<Sysname> display ospfv3 vlink
Virtual Link VLINK1 to router 1.1.1.1 is up
  Transit area :0.0.0.1 via interface Vlan-interface 10, instance ID: 0
  Local address: 2000:1::1
  Remote address: 2001:1:1::1
  Transmit Delay is 1 sec, State: P-To-P,
  Timer intervals configured, Hello: 10, Dead: 40, Wait: 40, Retransmit: 5
    Hello due in 00:00:02
    Adjacency state :Full
```

Table 143 Field descriptions of the display ospfv3 vlink command

Field	Description
Virtual Link VLINK1 to router 1.1.1.1 is up	The virtual link VLINK1 to switch 1.1.1.1 is up
Transit area 0.0.0.1 via interface Vlan-interface 10	Interface Vlan-interface 10 in transit area 0.0.0.1.
instance ID	Instance ID
Local address	Local IPv6 address
Remote address	Remote IPv6 address
Transmit Delay	Transmit delay of sending LSAs
State	Interface state
Timer intervals configured, Hello: 10, Dead: 40, Wait: 40, Retransmit: 5	Timer intervals in seconds, Hello: 10, Dead: 40, Wait: 40, Retransmit: 5
Hello due in 00:00:02	Send hello packets in 2 seconds.
Adjacency state	Adjacency state

filter-policy export (OSPFv3 view)

Syntax **filter-policy** { *acl6-number* | **ipv6-prefix** *ipv6-prefix-name* } **export** [**isisv6** *process-id* | **ospfv3** *process-id* | **ripng** *process-id* | **bgp4+** | **direct** | **static**]

undo filter-policy export [**isisv6** *process-id* | **ospfv3** *process-id* | **ripng** *process-id* | **bgp4+** | **direct** | **static**]

View OSPFv3 view

Parameters *acl-number*: ACL6 number.

ipv6-prefix *ipv6-prefix-name*: Specifies the name of an IPv6 prefix list.

isisv6 *process-id*: Filters the routes of an IPv6-IS-IS process.

ospfv3 *process-id*: Filters the routes of an OSPFv3 process.

ripng *process-id*: Filters the routes of a RIPng process.

bgp4+: Filters BGP4+ routes.

direct: Filters direct routes.

static: Filters static routes.

Description Use the **filter-policy export** command to filter redistributed routes.

Use the **undo filter-policy export** command to remove the configuration.

If no protocol is specified, all redistributed routes will be filtered.

By default, IPv6 OSPFv3 does not filter redistributed routes.

*Using the **filter-policy export** command filters only routes redistributed by the **import-route** command. If the **import-route** command is not configured to redistribute routes from other protocols and other OSPFv3 processes, use of the **filter-policy export** command does not take effect.*

Examples # Filter all redistributed routes using IPv6 ACL 2001.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2001
[Sysname-acl6-basic-2000] rule permit source 2002:1:: 64
[Sysname-acl6-basic-2000] quit
[Sysname] ospfv3
[Sysname-ospfv3-1] filter-policy 2001 export
```

filter-policy import (OSPFv3 view)

Syntax **filter-policy** { *acl6-number* | **ipv6-prefix** *ipv6-prefix-name* } **import**

undo filter-policy import

View OSPFv3 view

Parameters *acl6-number*: ACL6 number.

ipv6-prefix *ipv6-prefix-name*: Specifies the name of an IPv6 prefix list.

Description Use the **filter-policy import** command to filter received routes.

Use the **undo filter-policy import** command to remove the configuration.

No received routes are filtered by default.

*Using the **filter-policy import** command only filters routes computed by OSPFv3. The routes that fail to pass are not added to the routing table.*

Examples # Filter received routes using the IPv6 prefix list abc.

```
<Sysname> system-view
[Sysname] ip ipv6-prefix abc permit 2002:1:: 64
[Sysname] ospfv3 1
[Sysname-ospfv3-1] filter-policy ipv6-prefix abc import
```

import-route (OSPFv3 view)

Syntax **import-route** { **isisv6** *process-id* | **ospfv3** *process-id* | **ripng** *process-id* | **bgp4+** [**allow-ibgp**] | **direct** | **static** } [**cost** *value* | **type** *type* | **route-policy** *route-policy-name*]*

undo import-route { **isis** *process-id* | **ospfv3** *process-id* | **ripng** *process-id* | **bgp4+** | **direct** | **static** }

View OSPFv3 view

Parameters **isisv6** *process-id*: Redistributes IPv6 ISIS routes from an IPv6 IS-IS process.

ospfv3 *process-id*: Redistributes OSPFv3 routes from an OSPFv3 process.

ripng *process-id*: Redistributes RIPng routes from a RIPng process.

bgp4+: Redistributes BGP4+ routes.

allow-ibgp: Allows redistributing IBGP routes.

direct: Redistributes direct routes.

static: Redistributes static routes.

cost *value*: Cost for redistributed routes. The default is 1.

type *type*: Specifies the type of redistributed routes, 1 or 2. It defaults to 2.

route-policy *route-policy-name*: Specifies to redistribute only the routes that match the specified route-policy.

CAUTION: *Using the* ***import-route bgp4+*** *command redistributes only EBGP routes, while using the* ***import-route bgp4+ allow-ibgp*** *command redistributes both EBGP and IBGP routes.*

Description Use the **import-route** command to redistribute routes.

Use the **undo import-route** command to disable routes redistribution.

IPv6 OSPFv3 does not redistribute routes from other protocols by default.

Examples # Configure to redistribute routes from RIPng and specify the type as type 2 and cost as 50.

```
<Sysname> system-view
[Sysname] ospfv3
[Sysname-ospfv3-1] import-route ripng 10 type 2 cost 50
```

Configure OSPFv3 process 100 to redistribute the routes found by OSPFv3 process 160.

```
<Sysname> system-view
[Sysname] ospfv3 100
[Sysname-ospfv3-100] import-route ospfv3 160
```

log-peer-change (OSPFv3 view)

Syntax **log-peer-change**

undo log-peer-change

View OSPFv3 view

Parameters None

Description Use the **log-peer-change** command to enable the logging on neighbor state changes.

Use the **undo maximum load-balancing** command to disable the logging.

With this feature enabled, information about neighbor state changes of the current OSPFv3 process will display on the configuration terminal.

Examples # Disable the logging of neighbor state changes of OSPFv3 process 100.

```
<Sysname> system-view
[Sysname] ospfv3 100
[Sysname-ospfv3-100] undo log-peer-change
```

maximum load-balancing (OSPFv3 view)

Syntax **maximum load-balancing** *maximum*

undo maximum load-balancing

View OSPFv3 view

Parameters *maximum*: Maximum number of equal-cost routes for load-balancing.

Description Use the **maximum load-balancing** command to configure the maximum number of equal-cost routes for load-balancing.

Use the **undo maximum load-balancing** command to restore the default.

The default number is 8.

Examples # Configure the maximum number of equal-cost routes for load-balancing as 6.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] maximum load-balancing 6
```

ospfv3

Syntax **ospfv3** [*process-id*]

undo ospfv3 [*process-id*]

View System view

Parameters *process-id*: OSPFv3 process ID. The process ID defaults to 1.

Description Use the **ospfv3** command to enable an OSPFv3 process and enter OSPFv3 view.

Use the **undo ospfv3** command to disable an OSPFv3 process.

The system runs no OSPFv3 process by default.

An OSPFv3 process can run normally only when Router ID is configured in OSPFv3 view. Otherwise, you can find the process, but which cannot generate any LSA.

Examples # Enable the OSPFv3 process with process ID as 120 and configure the Router ID as 1.1.1.1.

```
<Sysname> system-view
[Sysname] ospfv3 120
[Sysname-ospfv3-120] router-id 1.1.1.1
```

ospfv3 area

Syntax **ospfv3** *process-id* **area** *area-id* [**instance** *instance-id*]

undo ospfv3 *process-id* **area** *area-id* [**instance** *instance-id*]

View Interface view

Parameters *process-id*: OSPFv3 process ID.

area-id: Area ID, a decimal integer or an IPv4 address.

instance-id: Instance ID of an interface. The default is 0.

Description Use the **ospfv3 area** command to enable an OSPFv3 process on the interface and specify the area for the process.

Use the **undo ospfv3 area** command to disable an OSPFv3 process.

OSPFv3 is not enabled on an interface by default.

Examples # Enable OSPFv3 process 1 on an interface that belongs to instance 1 and specify area 1 for the process.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 1 area 1 instance 1
```

ospfv3 cost

Syntax **ospfv3 cost** *value* [**instance** *instance-id*]

undo ospfv3 cost [**instance** *instance-id*]

View Interface view

Parameters *value*: OSPFv3 cost of the interface.

instance-id: Instance ID of the interface. The default is 0.

Description Use the **ospfv3 cost** command to configure the OSPFv3 cost of the interface in an instance.

Use the **undo ospfv3 cost** command to restore the default OSPFv3 cost of the interface in an instance.

By default, the interface automatically calculates the OSPFv3 cost based on its bandwidth. For a VLAN interface of a switch, the cost value defaults to 1.

Examples # Specifies the OSPFv3 cost of the interface in instance 1 as 33 .

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 cost 33 instance 1
```

ospfv3 dr-priority

Syntax **ospfv3 dr-priority** *priority* [**instance** *instance-id*]

undo ospfv3 dr-priority [**instance** *instance-id*]

View Interface view

Parameters *priority*: DR priority. The default is 1.

instance-id: ID of the instance the interface belongs to. The default is 0.

Description Use the **ospfv3 dr-priority** command to set the DR priority for an interface in an instance.

Use the **undo ospfv3 dr-priority** command to restore the default value.

An interface's DR priority determines its privilege in DR/BDR selection, and the interface with the highest priority is preferred.

Examples # Set the DR priority for Vlan-interface10 in instance 1 to 8.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 dr-priority 8 instance 1
```

ospfv3 mtu-ignore

Syntax **ospfv3 mtu-ignore** [**instance** *instance-id*]

undo ospfv3 mtu-ignore [**instance** *instance-id*]

View Interface view

Parameters *instance-id*: Instance ID, which defaults to 0.

Description Use the **ospfv3 mtu-ignore** command to configure the interface to ignore MTU when sending DD packets.

Use the **undo ospfv3 mtu-ignore** command to restore the default configuration.

MTU is not ignored by default.

Examples # Configure the interface that belongs to instance 1 to ignore MTU.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 mtu-ignore instance 1
```

ospfv3 timer dead

Syntax **ospfv3 timer dead** *seconds* [**instance** *instance-id*]

undo ospfv3 timer dead [**instance** *instance-id*]

View Interface view

Parameters *seconds*: Dead time in seconds.

instance-id: Instance ID of an interface, which defaults to 0.

Description Use the **ospfv3 timer dead** command to configure the OSPFv3 neighbor dead time for an interface that belongs to a specified instance.

Use the **undo ospfv3 timer dead** command to restore the default.

By default, the OSPFv3 neighbor dead time is 40 seconds for P2P and Broadcast interfaces, and is not supported on P2MP and NBMA interfaces at present.

OSPFv3 neighbor dead time: If an interface receives no hello packet from a neighbor after dead time elapses, the interface will consider the neighbor dead.

The **dead** *seconds* value is at least four times the **Hello** *seconds* value and must be identical on interfaces attached to the same network segment.

Related commands: **ospfv3 timer hello**.

Examples # Configure the OSPFv3 neighbor dead time as 80 seconds for Vlan-interface10 in instance 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 timer dead 80 instance 1
```

ospfv3 timer hello

Syntax **ospfv3 timer hello** *seconds* [**instance** *instance-id*]

undo ospfv3 timer hello [**instance** *instance-id*]

View Interface view

Parameters *seconds*: Interval between hello packets in seconds.

instance-id: Instance ID of an interface, which defaults to 0.

Description Use the **ospfv3 timer hello** command to configure the hello interval for an interface that belongs to an instance.

Use the **undo ospfv3 timer hello** command to restore the default .

By default, the hello interval is 10 seconds for P2P and Broadcast interfaces, and is not supported on the P2MP or NBMA interfaces at present.

Related commands: **ospfv3 timer dead**.

Examples # Configure the hello interval as 20 seconds for Vlan-interface10 in instance 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 timer hello 20 instance 1
```

ospfv3 timer retransmit

Syntax **ospfv3 timer retransmit** *interval* [**instance** *instance-id*]

undo ospfv3 timer retransmit [**instance** *instance-id*]

View Interface view

Parameters *interval*: LSA retransmission interval in seconds.

instance-id: Instance ID of an interface, which defaults to 0.

Description Use the **ospfv3 timer retransmit** command to configure the LSA retransmission interval for an interface in an instance.

Use the **undo ospfv3 timer retransmit** command to restore the default.

The interval defaults to 5 seconds.

After sending a LSA to its neighbor, the device waits for an acknowledgement. If receiving no acknowledgement after the LSA retransmission interval elapses, it will retransmit the LSA.

The LSA retransmission interval should not be too small for avoidance of unnecessary retransmissions.

Examples # Configure the LSA retransmission interval on Vlan-interface in instance 1 as 12 seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 timer retransmit 12 instance 1
```

ospfv3 trans-delay

Syntax **ospfv3 trans-delay** *seconds* [**instance** *instance-id*]

undo ospfv3 trans-delay [**instance** *instance-id*]

View Interface view

Parameters *seconds*: Transmission delay in seconds.

instance-id: Instance ID of the interface. The default is 0.

Description Use the **ospfv3 trans-delay** command to configure the transmission delay for an interface with an instance ID.

Use the **undo ospfv3 trans-delay** command to restore the default.

The transmission delay defaults to 1s.

As LSAs are aged in the LSDB (incremented by 1 every second) but not aged on transmission, it is necessary to add a delay time to the age time before sending a LSA. This configuration is important for low-speed networks.

Examples # Configure the transmission delay as 3 seconds for Vlan-interface10 in instance 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospfv3 trans-delay 3 instance 1
```

preference (OSPFv3 view)

Syntax **preference** [**ase**] [**route-policy** *route-policy-name*] *preference*

undo preference [**ase**]

View OSPFv3 view

Parameters **ase**: Applies the preference to OSPFv3 external routes. If the keyword is not specified, the preference applies to OSPFv3 internal routes.

route-policy *route-policy-name*: References a routing policy to set the preference for specific routes.

Preference: Preference for OSPFv3 routes.

Description Use the **preference** command to specify a preference for OSPFv3 routes.

Use the **undo preference** command to restore the default.

By default, the preference for OSPFv3 internal routes is 10, and that for OSPFv3 external routes is 150.

The smaller the value is, the higher the preference is.

A device may run multiple routing protocols. Each protocol has a preference. When several routing protocols find multiple routes to the same destination, the route found by the protocol with the highest preference is selected.

Examples # Set a preference of 150 for OSPFv3 routes.

```
<Sysname> system-view
[Sysname] OSPFv3
[Sysname-OSPFv3-1] preference 150
```

router-id (OSPFv3 view)

Syntax **router-id** *router-id*

undo router-id

View OSPFv3 view

Parameters *router-id*: 32-bit router ID, in dotted decimal format.

Description Use the **router-id** command to configure the OSPFv3 router ID.

Use the **undo router-id** command to remove a configured router ID.

Router ID is the unique identifier of a device running an OSPFv3 process in the autonomous system. The OSPFv3 process cannot run without a Router ID.

Make sure that different processes have different Router IDs.

Related commands: **ospfv3**.

By configuring different router IDs for different processes, you can run multiple OSPFv3 processes on a device.

Examples # Configure the Router ID as 10.1.1.3 for OSPFv3 process 1.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] router-id 10.1.1.3
```

silent-interface (OSPFv3 view)

Syntax **silent-interface** { *interface-type interface-number* | **all** }

undo silent-interface { *interface-type interface-number* | **all** }

View OSPFv3 view

Parameters *interface-type interface-number*: Interface type and number

all: Specifies all interfaces.

Description Use the **silent-interface** command to disable the specified interface from sending OSPFv3 packets.

Use the **undo silent-interface** command to restore the default.

An interface is able to send OSPFv3 packets by default.

Multiple processes can disable the same interface from sending OSPFv3 packets, but use of the **silent-interface** command takes effect only on interfaces enabled with the current process.

Examples # Disable Vlan-interface from sending OSPFv3 packets in OSPFv3 processes 100 and 200.

```
<Sysname> system-view
[Sysname] ospfv3 100
[Sysname-ospfv3-100] router-id 10.110.1.9
[Sysname-ospfv3-100] silent-interface vlan-interface 10
[Sysname-ospfv3-100] quit
[Sysname] ospfv3 200
[Sysname-ospfv3-200] router-id 20.18.0.7
[Sysname-ospfv3-200] silent-interface vlan-interface 10
```

spf timers

Syntax **spf timers** *delay-interval hold-interval*

undo spf timers

View OSPFv3 view

Parameters *delay-interval*: Interval in seconds between when OSPFv3 receives a topology change and when it starts SPF calculation.

hold-interval: Hold interval in seconds between two consecutive SPF calculations.

Description Use the **spf timers** command to configure the delay interval and hold interval for OSPFv3 SPF calculation.

Use the **undo spf timers** command to restore the default.

The delay interval and hold interval default to 5s and 10s.

An OSPFv3 device works out a shortest path tree with itself as root based on the LSDB, and decides on the next hop to a destination network according the tree.

Adjusting the SPF calculation interval can restrain bandwidth and router resource from over consumption due to frequent network changes.

Examples # Configure the delay interval and hold interval as 6 seconds for SPF calculation.

```
<Sysname> system-view
[Sysname]ospfv3 1
[Sysname-ospfv3-1] spf timers 6 6
```

stub(OSPFv3 area view)

Syntax **stub** [**no-summary**]

undo stub

View OSPFv3 area view

Parameters **no-summary**: This argument is only applicable to the ABR of a stub area. With it configured, the ABR advertises only a default route in a Summary-LSA to the stub area (such an area is called a totally stub area).

Description Use the **stub** command to configure an area as a stub area.

Use the **undo stub** command to remove the configuration.

By default, an area is not configured as a stub area.

When an area is configured as a stub area, all the devices attached to the area must be configured with the **stub** command.

Related commands: **default-cost**.

Examples # Configure OSPFv3 area 1 as a stub area.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] area 1
[Sysname-ospfv3-1-area-0.0.0.1] stub
```

vlink-peer(OSPFv3 area view)

Syntax **vlink-peer** *router-id* [**hello** *seconds* | **retransmit** *seconds* | **trans-delay** *seconds* | **dead** *seconds* | **instance** *instance-id*] *

undo vlink-peer *router-id* [**hello** | **retransmit** | **trans-delay** | **dead**]*

View OSPFv3 area view

Parameters *router-id*: Router ID for a virtual link neighbor.

hello *seconds*: Specifies the interval in seconds for sending Hello packets. The default is 10. This value must be equal to the **hello** *seconds* configured on the virtual link peer.

retransmit *seconds*: Specifies the interval in seconds for retransmitting LSA packets. The default is 5.

trans-delay *seconds*: Specifies the delay interval in seconds for sending LSA packets. The default is 1.

dead *seconds*: Specifies the neighbor dead time in seconds. The default is 40. This value must be equal to the **dead** *seconds* configured on the virtual link peer, and at least four times the value of **hello** *seconds*.

instance *Instance-id*: Instance ID of an virtual link. The default is 0.

Description

Use the **vlink-peer** command to create and configure a virtual link.

Use the **undo vlink-peer** command to remove a virtual link.

For a non-backbone area without direct connection with the backbone area or for a backbone area that cannot maintain connectivity, you can use the **vlink-peer** command to create logical connectivity. A virtual link can be considered as an interface with OSPFv3 enabled, because parameters such as **hello**, **retransmit** and **trans-delay** are configured in the similar way.

Examples

Create a virtual link to 10.110.0.3.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] area 10.0.0.0
[Sysname-ospfv3-1-area-10.0.0.0] vlink-peer 10.110.0.3
```

37 DUAL STACK CONFIGURATION COMMANDS

ipv6 (System view)

Syntax **ipv6**

undo ipv6

View System view

Parameters None

Description Use the **ipv6** command to enable the IPv6 packet forwarding function.

Use the **undo ipv6** command to disable the IPv6 packet forwarding function.

By default, the function is disabled.

Examples # Enable the IPv6 packet forwarding function.

```
<Sysname> system-view
[Sysname] ipv6
```

ipv6 address (Interface view)

Syntax **ipv6 address** { *ipv6-address prefix-length* | *ipv6-address***/***prefix-length* }

undo ipv6 address [*ipv6-address prefix-length* | *ipv6-address***/***prefix-length*]

View Interface view

Parameters *ipv6-address*: IPv6 address for the interface.

prefix-length: Length of the prefix.

Description Use the **ipv6 address** command to configure a site-local address or global unicast address for an interface.

Use the **undo ipv6 address** command to remove the configuration.

By default, neither site-local addresses nor global unicast addresses are configured.

Note that:

- The total number of global unicast addresses and site-local addresses that can be configured on an interface is 20.
- The **undo ipv6 address** command without parameters removes all IPv6 addresses manually configured, except link-local addresses automatically configured on the interface.

Examples # Specify the global unicast address of the interface VLAN-interface 1 as 2001::1/64.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ipv6 address 2001::1/64
```

ipv6 address auto link-local (Interface view)

Syntax **ipv6 address auto link-local**

undo ipv6 address auto link-local

View Interface view

Parameters None

Description Use the **ipv6 address auto link-local** command to enable the device to automatically generate a link-local address for an interface.

Use the **undo ipv6 address auto link-local** command to remove the automatically generated link-local address.

By default, a link-local address will automatically be generated when an IPv6 site-local address or IPv6 global unicast address is configured for an interface.

Examples # Enable the interface VLAN-interface 1 to generate a link-local address automatically.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ipv6 address auto link-local
```

ipv6 address eui-64 (Ethernet interface view)

Syntax **ipv6 address** *ipv6-address*/*prefix-length* **eui-64**

undo ipv6 address *ipv6-address*/*prefix-length* **eui-64**

View Ethernet interface view

Parameters *ipv6-address*/*prefix-length*: IPv6 address and prefix length. They together specify the prefix length of an IPv6 address in the EUI-64 format. The prefix length of an EUI-64 address cannot exceed 64.

Description Use the **ipv6 address eui-64** command to configure a site-local address or global unicast address in the EUI-64 format on an interface.

Use the **undo ipv6 address eui-64** command to delete the site-local address or global unicast address in the EUI-64 format on an interface.

By default, no site-local or global unicast address in the EUI-64 format is configured for an interface.

Examples # Configure the interface VLAN-interface 1 to generate an IPv6 address in the EUI-64 format.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ipv6 address 2001::1/64 eui-64
```

ipv6 address link-local (Interface view)

Syntax **ipv6 address** *ipv6-address* **link-local**

undo ipv6 address *ipv6-address* **link-local**

View Interface view

Parameters *ipv6-address*: IPv6 link-local address. The high-order ten bits of an IPv6 link-local address must be 1111111010 (binary), that is to say, the first group of the IPv6 link-local address must range from FE80 to FEBF (hexadecimal).

Description Use the **ipv6 address link-local** command to configure manually a link-local address for an interface.

Use the **undo ipv6 address link-local** command to remove the link-local address of an interface.

By default, a link-local address will automatically be generated when an IPv6 site-local address or global unicast address is configured for an interface.

Examples # Configure a link-local address for the interface VLAN-interface 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ipv6 address fe80::1 link-local
```

38 GRE CONFIGURATION COMMANDS

aggregation-group (Tunnel interface view)

Syntax **aggregation-group** *aggregation-group-ID*

undo aggregation-group

View Tunnel interface view

Parameters *aggregation-group-ID*: Service loop group ID.

Description Use the **aggregation-group** command to specify the service loop group to be applied to a tunnel.

Use the **undo aggregation-group** command to remove the configuration.

By default, no service loop group is applied to a tunnel.

Before applying a service loop group to a tunnel in tunnel interface view, you need to configure the service loop group in system view and set its service type to tunnel.

Related commands: **link-aggregation group**.

Examples # Create service loop group 1. Then, set the configuration mode to manual and the service type to tunnel.

```
<Sysname> system-view
[Sysname] link-aggregation group 1 mode manual
[Sysname] link-aggregation group 1 service-type tunnel
```

Add the interface GigabitEthernet 4/2/1 to service loop group 1.

```
[Sysname] interface GigabitEthernet 4/2/1
[Sysname-GigabitEthernet 4/2/1] stp disable
[Sysname-GigabitEthernet 4/2/1] port link-aggregation group 1
[Sysname-GigabitEthernet 4/2/1] quit
```

Apply service loop group 1 to the tunnel in tunnel interface view.

```
[Sysname] interface tunnel 2/0/1
[Sysname-Tunnel2/0/1] aggregation-group 1
```

Remove the application of service loop group 1.

```
[Sysname-Tunnel2/0/1] undo aggregation-group
```

debugging gre

Syntax **debugging gre** { **all** | **error** | **packet** }

undo debugging gre { **all** | **error** | **packet** }

View User view

Parameters **all**: Turns on all the debugging switches of the GRE module.

error: Turns on the error information debugging switch of the GRE module.

error: Turns on the packet information debugging switch of the GRE module.

Description Use the **debugging gre** command to enable the GRE debugging switch.

Use the **undo debugging gre** command to disable the GRE debugging switch.

By default, the GRE debugging switch is disabled.

Examples # Enable GRE debugging. Then, ping the destination address of a tunnel to view the output information.

```
<Sysname> debugging gre all
<Sysname> terminal debugging
<Sysname>ping ipv6 -c 1 2004::2
  PING 2004::2 : 56  data bytes, press CTRL_C to break
*0.576797 Sysname-wvrp GRE/8/debug:
 Tunnel0/0/1 packet: Encapsulation protocol is IPV6.
*0.576828 Sysname-wvrp GRE/8/debug:
 gre packet: Decapsulate tunnel packet
        Outer packet header 2003::0002->2003::0001(length = 148)
*0.576828 Sysname-wvrp GRE/8/debug:
 Tunnel0/0/1 packet: After decapsulation,
        Outgoing packet header 2004::0002->2004::0001(length = 104)
    Reply from 2004::2
    bytes=56 Sequence=1 hop limit=255  time = 46 ms

  --- 2004::2 ping statistics ---
    1 packet(s) transmitted
    1 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 46/46/46 ms
```

Table 144 Field descriptions of the debugging gre command

Field	Description
Sysname -wvrp GRE/8/debug	GRE handling starts on the Sysname switch.
Tunnel0/0/1 packet: Encapsulation protocol is IPV6	On the interface Tunnel0/0/1, IPv6 is encapsulated.

Table 144 Field descriptions of the debugging gre command

Field	Description
gre packet: Decapsulate tunnel packet Outer packet header 2003::0002->2003::0001(length = 148).	The packet is being decapsulated. Before that, the source and destination addresses in the packet header are 2003::0002 and 2003::0001 respectively, and the packet size is 148 bytes.
Tunnel0/0/1 packet: After decapsulation, Outgoing packet header 2004::0002->2004::0001(length = 104)	After the decapsulation, the source and destination addresses in the packet header are 2004::0002 and 2004::0001 respectively, and the packet size is 104 bytes.

debugging tunnel (User view)

Syntax **debugging tunnel** { **all** | **error** | **event** | **packet** }

undo debugging tunnel { **all** | **error** | **event** | **packet** }

View User view

Parameters **all**: Turns on all the debugging switches of the tunnel module.

error: Turns on the error information debugging switch of tunnel module.

packet: Turns on the packet information debugging switch of the tunnel module.

event: Turns on the event information debugging switch of the tunnel module.

Description Use the **debugging tunnel** command to enable the tunnel debugging switch.

Use the **undo debugging tunnel** command to disable the tunnel debugging switch.

By default, the tunnel debugging switch is disabled.

Examples # Enable the tunnel debugging switch.

```
<Sysname> debugging tunnel all
<Sysname> terminal debugging
% Current terminal debugging is on
<Sysname>
*0.4445125 Sysname-wvrp TUNNEL/8/debug:
Tunnel0/0/0 link state is DOWN, no change.
```

When the tunnel source address is required yet not configured, the information below is given.

```
*0.4450125 Sysname-wvrp TUNNEL/8/debug:
Tunnel0/0/0 down, because the source ip is not set.
```

When the tunnel destination address is required yet not configured, the information below is given.

```
*0.4920140 Sysname-wvrp TUNNEL/8/debug:
Tunnel0/0/0 down, because the dest address is required.
```

When the service loop group ID applied is required yet not configured, the information below is given.

```
*0.9505431 3Com Switch 8807 (7-Slot Chassis) TUNNEL/8/debug:
 Tunnel0/0/0 down, because the aggregation group is required.
*0.9505560 3Com Switch 8807 (7-Slot Chassis) TUNNEL/8/debug:
Tunnel0/0/0 link state is DOWN, no change.
```

When the service loop group ID applied is configured but that group is down, the information below is given.

```
*0.8565431 3Com Switch 8807 (7-Slot Chassis) TUNNEL/8/debug:
 Tunnel0/0/0 down, because the status of aggregation group 1 is down
.
*0.8565570 3Com Switch 8807 (7-Slot Chassis) TUNNEL/8/debug:
Tunnel0/0/0 link state is DOWN, no change.
```

Table 145 Field descriptions of the debugging tunnel command

Field	Description
Sysname TUNNEL/8/debug	Tunnel debug information is shown on the Sysname switch.
Tunnel0/0/0 link state is DOWN, no change.	Tunnel 0/0/0 link state is DOWN, and it does not change.
Tunnel0/0/0 down, because the source ip is not set.	Tunnel 0/0/0 is down, because the source ip is not set.
Tunnel0/0/0 down, because the dest address is required.	Tunnel 0/0/0 is down, because the destination ip is not set.
Tunnel0/0/0 down, because the aggregation group is required.	Tunnel 0/0/0 is down, because the aggregation group applied to that tunnel is not configured. (This check is performed only when the service loop group ID is a mandatory parameter.)
Tunnel0/0/0 down, because the status of aggregation group 1 is down.	Tunnel 0/0/0 is down, because the status of aggregation group 1 applied to that tunnel is down. (This check is performed only when the service loop group ID is a mandatory parameter.)

destination (Tunnel interface view)

Syntax **destination** { *Ip-address* | *Ipv6-address* }

undo destination

View Tunnel interface view

Parameters *Ip-address*: Destination IPv4 address for the tunnel interface.

Ipv6-address: Destination IPv6 address for the tunnel interface.

Description Use the **destination** command to specify the destination address for a tunnel interface.

Use the **undo destination** command to remove the configuration.

By default, no destination address is configured for a tunnel interface.

Note that:

- The destination address of a tunnel interface is the address of the peer interface receiving packets. It is usually set to the source address of the peer tunnel interface.
- Two or more tunnel interfaces using the same encapsulation protocol must have different source addresses and destination addresses.

Related commands: **interface tunnel** and **source**.

Examples # Set Vlan interface 10 (193.101.1.1) of Switch 1 and Vlan interface 20 (192.100.1.1) of Switch 2 as the source (destination) interface and destination (source) interface of the tunnel between the two devices, mutually.

- Configure Switch 1.

```
<Sysname1> system-view
[Sysname1] interface Tunnel 3/0/1
[Sysname1-Tunnel3/0/1] source 193.101.1.1
[Sysname1-Tunnel3/0/1] destination 192.100.1.1
```

- Configure Switch 2.

```
<Sysname2> system-view
[Sysname2] interface Tunnel 4/0/1
[Sysname2-Tunnel4/0/1] source 192.100.1.1
[Sysname2-Tunnel4/0/1] destination 193.101.1.1
```

display interface tunnel (Any view)

Syntax **display interface tunnel** [*number*]

View Any view

Parameters *number*: Tunnel interface number.

Description Use the **display interface tunnel** command to display information about a specified or all tunnel interfaces.

With the *number* argument not specified, the command displays information about all tunnel interfaces.

Related commands: **source**, **destination**, **tunnel-protocol**.

Examples # Display information about interface Tunnel 3/0/0.

```
<Sysname> display interface tunnel 3/0/0
Tunnel3/0/0 current state: UP
Line protocol current state: UP
Description: Tunnel3/0/0 Interface
The Maximum Transmit Unit is 1500
Internet protocol processing : disabled
Encapsulation is TUNNEL, aggregation ID is 10.
Tunnel source 10.0.0.1 (Vlan-interface10), destination 10.0.0.2
Tunnel protocol/transport GRE/IP
    GRE key disabled
    Checksumming of GRE packets disabled
    Last 300 seconds input:  0 bytes/sec, 0 packets/sec
    Last 300 seconds output:  0 bytes/sec, 0 packets/sec
    0 packets input,  0 bytes
    0 input error
    0 packets output,  0 bytes
    0 output error
```

Table 146 Field descriptions of the display interface tunnel command

Field	Description
Tunnel3/0/0 current state: UP	Status of the physical layer of the tunnel interface is UP
Line protocol current state: UP	Status of the link layer of the tunnel interface is UP
Description	Descriptive information of the tunnel interface
Tunnel3/0/0 Interface	Number of the tunnel interface
Maximum Transmit Unit	Maximum transmission unit of the tunnel, 1500 bytes in this example
Encapsulation is TUNNEL	The encapsulation protocol is TUNNEL.
aggregation ID	ID of the service loop group applied to the tunnel.
Tunnel source	Source address of the tunnel interface
destination	Destination address of the tunnel interface
Tunnel protocol/transport	The Tunnel protocol/transport protocol that is in operation
GRE key	Keyword verification
Checksumming of GRE packets	End-to-end verification
Last 300 seconds input	Amount of inbound traffic per second in the last five minutes, in bytes and in packets respectively
Last 300 seconds output	Amount of outbound traffic per second in the last five minutes, in bytes and in packets respectively
packets input	Total number of bytes input
input error	Number of inbound packets in error
packets output	Total number of bytes output
output error	Number of outbound packets in error

display ipv6 interface tunnel (Any view)

Syntax **display ipv6 interface tunnel** *number*

View Any view

Parameters *number*: Tunnel interface number, in the format of module slot number/0/Tunnel interface number.

Description Use the **display ipv6 interface tunnel** command to display IPv6 information about a tunnel interface, including the Tunnel interface link status, IPv6 status, IPv6 addresses of the Tunnel interfaces, etc.

Examples # Display IPv6 information about interface Tunnel 3/0/0.

```
<Sysname> display ipv6 interface tunnel 3/0/0
Tunnel3/0/0 current state :UP
Line protocol current state :UP
IPv6 is enabled, link-local address is FE80::101:101
  Global unicast address(es):
    2002:101:101::1, subnet is 2002::/16
  Joined group address(es):
    FF02::1:FF01:101
    FF02::1:FF00:1
    FF02::2
    FF02::1
  MTU is 1500 bytes
  ND reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  Hosts use stateless autoconfig for addresses
```

Table 147 Field descriptions of the display ipv6 interface tunnel command

Field	Description
Tunnel3/0/0 current state: UP	Status of the physical layer of the tunnel interface is UP
Line protocol current state: UP	Status of the link layer of the tunnel interface is UP
IPv6 is enabled	IPv6 is enabled on the tunnel interface
link-local address	Link-local address of the tunnel interface
Global unicast address(es)	Global unicast addresses of the tunnel interface
Joined group address(es)	Multicast addresses of the tunnel interface
MTU is 1500 bytes	Maximum transmission unit of the tunnel, 1500 bytes in this example
ND reachable time	Interval during which the neighbor is considered reachable
ND retransmit interval	Neighbor discovery packet retransmission interval
Hosts use stateless autoconfig for addresses	Hosts use the stateless auto-configuration mode to acquire an IPv6 addresses.

expediting enable (Tunnel interface view)

Syntax **expediting enable**

undo expediting enable

View Tunnel interface view

Parameters None

Description Use the **expediting enable** command to enable the expediting function.

Use the **undo expediting enable** command to disable the expediting function.

By default, the expediting function is disabled.

Examples # Enable the expediting function

```
<Sysname> system-view
[Sysname] interface tunnel 2/0/0
[Sysname-Tunnel2/0/0] expediting enable
```

interface tunnel

Syntax **interface tunnel** *number*

undo interface tunnel *number*

View System view

Parameters *number*: Tunnel interface number, in the format of module slot number/0/Tunnel interface number.

Description Use the **interface tunnel** command to create a tunnel interface and enter tunnel interface view.

Use the **undo interface tunnel** command to remove a tunnel interface.

By default, there is no tunnel interface on the device.

- Executing the **interface tunnel** command, you enter tunnel interface view if the tunnel interface exists.
- A tunnel interface number has only local significance. Therefore, the same or different interface numbers can be set at both ends of a tunnel.

Related commands: **source**, **destination**, **tunnel-protocol**.

Examples # Create Tunnel 3/0/0.

```
<Sysname> system-view
[Sysname] interface tunnel 3/0/0.
```

ipv6 mtu (tunnel Interface view)

Syntax **ipv6 mtu** *mtu-size*

undo ipv6 mtu

View Tunnel interface view

Parameters *mtu-size*: Size of the interface MTU, in bytes.

Description Use the **ipv6 mtu** command to set the MTU for IPv6 packets on an interface.

Use the **undo ipv6 mtu** command to restore the default.

Examples # Set the MTU on a tunnel interface to 1400 bytes.

```
<Sysname> system-view
[Sysname] interface tunnel 4/0/1
[Sysname-tunnel4/0/1] ipv6 mtu 1400
```

mtu (tunnel Interface view)

Syntax **mtu** *mtu*

undo mtu

View Tunnel interface view

Parameters *mtu*: Specifies the MTU on a tunnel interface. The default value is 1500 bytes.

Description Use the **mtu** command to set the MTU on a tunnel interface.

Use the **undo mtu** command to restore the default.

Examples # Set the MTU on a tunnel interface to 1400 bytes.

```
<Sysname> system-view
[Sysname] interface tunnel 4/0/1
[Sysname-tunnel4/0/1] mtu 1400
```

source (Tunnel interface view)

Syntax **source** { *ip-address* | *ipv6-address* | *interface-type interface-number* }

undo source

View Tunnel interface view

Parameters *ip-address*: Specifies the source IPv4 address for the tunnel interface.

Ipv6-address: Specifies the source IPv6 address for the tunnel interface.

interface-type interface-num: Type and number of an interface.

Description Use the **source** command to specify the source address for a tunnel interface.

Use the **undo source** command to remove the configuration.

By default, no source address is configured for a tunnel interface.

Note that:

- The source address of a tunnel interface is the address of the interface sending GRE packets and is usually the destination address of the peer tunnel interface.
- Two or more tunnel interfaces using the same encapsulation protocol must have different source addresses and destination addresses.

Related commands: **interface tunnel** and **destination**.

Examples # Create interface Tunnel 5/0/0 and configure the IP address 192.100.1.1 as the source address of packets leaving that interface.

```
<Sysname> system-view
[Sysname] interface Tunnel 5/0/0
[Sysname-Tunnel5/0/0] source 192.100.1.1
```

tunnel-protocol (Tunnel interface view)

Syntax **tunnel-protocol gre**

undo tunnel-protocol

View Tunnel interface view

Parameters **gre**: Sets the tunnel mode to GRE.

Description Use the **tunnel-protocol gre** command to set the GRE tunnel mode.

Use the **undo tunnel-protocol** to restore the default.

By default, the GRE tunnel mode is adopted.

Select a tunnel mode according to the network topology and application. Note that both ends of a tunnel must be configured with the same tunnel mode. Otherwise, packet delivery will fail.

Related commands: **interface tunnel**.

Examples # Create a tunnel between Switch 1 and Switch 2. Then, configure the encapsulation protocol as GRE and the transport protocol as IP.

- Configure Switch 1.

```
<Sysname> system-view
[Sysname] interface Tunnel 5/0/0
[Sysname1-Tunnel5/0/0] tunnel-protocol gre
```

- Configure Switch 2.

```
<Sysname> system-view
[Sysname] interface Tunnel 2/0/0
[Sysname2-Tunnel2/0/0] tunnel-protocol gre
```

39 BGP CONFIGURATION COMMANDS

For routing policy configuration commands, refer to "Routing Policy Configuration Commands" on page 351.

aggregate

Syntax **aggregate** *ip-address* { *mask* | *mask-length* } [**as-set** | **attribute-policy** *route-policy-name* | **detail-suppressed** | **origin-policy** *route-policy-name* | **suppress-policy** *route-policy-name*] *

undo aggregate *ip-address* { *mask* | *mask-length* }

View BGP view/BGP-VPN instance view

Parameters *ip-address*: Summary address.

mask: Summary address mask, in dotted decimal notation.

mask-length: Summary address mask length.

as-set: Creates a summary with AS set.

detail-suppressed: Only advertises the summary route.

suppress-policy *route-policy-name*: Suppresses specific routes defined in the routing policy.

origin-policy *route-policy-name*: References the routing policy to specify routes for summarization.

attribute-policy *route-policy-name:* References a routing policy to set the attributes of the summary route. Note that the **apply as-path** clause of the routing policy cannot set the AS_PATH attribute of the summary route.

Description Use the **aggregate** command to create a summary route in the BGP routing table.

Use the **undo aggregate** command to remove a summary route.

By default, no summary route is configured.

The keywords of the command are described as follows:

Table 148 Functions of the keywords

Keywords	Function
as-set	Used to create a summary route, whose AS path contains the AS path information of summarized routes. Use this keyword carefully when many AS paths need to be summarized, because the frequent changes of routes may lead to route oscillation.
detail-suppressed	This keyword does not suppress the summary route, but it suppresses the advertisement of all the more specific routes. To summarize only some specific routes, use the **peer filter-policy** command.
suppress-policy	Used to create a summary route and suppress the advertisement of some summarized routes. If you want to suppress some routes selectively and leave other routes still advertised, use the **if-match** clause of the **route-policy** command.
origin-policy	Selects only routes satisfying the routing policy for route summarization
attribute-policy	Sets attributes except the AS-PATH attribute for the summary route. The same work can be done by using the **peer route-policy** command.

*The **suppress-policy** keyword takes priority over the keyword **detail-suppressed**.*

Examples # In BGP view, create a summary of 192.213.0.0/16 in the BGP routing table.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] aggregate 192.213.0.0 255.255.0.0
```

In BGP-VPN instance view, create a summary of 192.213.0.0/16 in BGP routing table (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] aggregate 192.213.0.0 255.255.0.0
```

balance (BGP/BGP-VPN instance view)

Syntax **balance** *number*

undo balance

View BGP view/VPN instance view

Parameters *number*: Number of BGP routes for load balancing. When it is set to 1, load balancing is disabled.

Description Use the **balance** command to configure the number of BGP routes for load balancing.

Use the **undo balance** command to disable load balancing.

By default, no load balancing is configured.

Unlike IGP, BGP has no explicit metric for making load balancing decision. Instead, it implements load balancing using route selection rules.

Related commands: **display ip routing-table**.

Examples # In BGP view, set the number of routes participating in BGP load balancing to 2.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] balance 2
```

In BGP-VPN instance view, set the number of routes participating in BGP load balancing to 2 (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] balance 2
```

bestroute as-path-neglect (BGP/BGP-VPN instance view)

Syntax **bestroute as-path-neglect**

undo bestroute as-path-neglect

View BGP view/BGP-VPN instance view

Parameters None

Description Use the **bestroute as-path-neglect** command to ignore the AS_PATH attribute during best route selection.

Use the **undo bestroute as-path-neglect** command to take the AS_PATH as a factor during best route selection.

By default, the device takes AS_PATH as a factor when selecting the best route.

Examples # In BGP view, ignore AS_PATH in route selection.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] bestroute as-path-neglect
```

In BGP-VPN instance view, ignore AS_PATH in route selection (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] bestroute as-path-neglect
```

bestroute compare-med (BGP/BGP-VPN instance view)

Syntax **bestroute compare-med**

undo bestroute compare-med

View BGP view/BGP-VPN instance view

Parameters None

Description Use the **bestroute compare-med** command to enable the comparison of the MED for paths from each AS.

Use the **undo bestroute compare-med** command to disable this comparison.

This comparison is not enabled by default.

Examples # In BGP view, enable the comparison of MEDs for paths from each AS when selecting the best route.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] bestroute compare-med
```

In BGP-VPN instance view, enable the comparison of MED for paths from each AS when selecting the best route. (The VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] bestroute compare-med
```

bestroute med-confederation (BGP/BGP-VPN instance view)

Syntax **bestroute med-confederation**

undo bestroute med-confederation

View BGP view/BGP-VPN instance view

Parameters None

Description Use the **bestroute med-confederation** command to enable the comparison of the MED for paths from confederation peers to select the optimal route.

Use the **undo bestroute med-confederation** command to disable the comparison.

The comparison is not enabled by default.

The system only compares MED values for paths from peers within the confederation. Paths from external ASs are advertised throughout the confederation without MED comparison.

Examples # In BGP view, enable the comparison of the MED for paths from peers within the confederation.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] bestroute med-confederation
```

In BGP-VPN instance view, enable the comparison of the MED for paths from peers within the confederation. (The VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] bestroute med-confederation
```

bgp

Syntax **bgp** *as-number*

undo bgp [*as-number*]

View System view

Parameters *as-number*: Local AS number.

Description Use the **bgp** command to enable BGP and enter the BGP view.

Use the **undo bgp** command to disable BGP.

By default, BGP is not enabled.

Examples # Enable BGP and set local AS number to 100.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp]
```

compare-different-as-med (BGP/BGP-VPN instance view)

Syntax **compare-different-as-med**

undo compare-different-as-med

View BGP view/BGP-VPN instance view

Parameters None

Description Use the **compare-different-as-med** command to enable the comparison of the MED for paths from peers in different ASs.

Use the **undo compare-different-as-med** command to disable the comparison.

The comparison is disabled by default.

If there are several paths for one destination available, the path with the smallest MED is selected.

Do not use this command unless associated ASs adopt the same IGP protocol and routing selection method.

Examples # In BGP view, enable to compare the MED for paths from peers in different ASs.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] compare-different-as-med
```

In BGP-VPN instance view, enable to compare the MED for paths from peers in different ASs (The VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] compare-different-as-med
```

confederation id

Syntax **confederation id** *as-number*

undo confederation id

View BGP view

Parameters *as-number*: Number of the AS that contains multiple sub-ASs.

Description Use the **confederation id** command to configure a confederation ID.

Use the **undo confederation id** command to remove a specified confederation.

By default, no confederation ID is configured.

Configuring a confederation can reduce IBGP connections in a large AS. You can split the AS into several sub-ASs, and each sub-AS remains fully meshed. These sub-ASs form a confederation. Key IGP attributes of a route, such as the next hop, MED, local preference, are not discarded when crossing each sub-AS. The sub-ASs still look like a whole from the perspective of other ASs. This can ensure the

integrity of the former AS, and solve the problem of too many IBGP connections in the AS.

Related commands: **confederation nonstandard** and **confederation peer-as**.

Examples # Confederation 9 consists of four sub-ASs, namely, 38, 39, 40 and 41. The peer 10.1.1.1 is a member of the confederation while the peer 200.1.1.1 is outside of the confederation. Take sub AS 41 as an example.

```
<Sysname> system-view
[Sysname] bgp 41
[Sysname-bgp] confederation id 9
[Sysname-bgp] confederation peer-as 38 39 40
[Sysname-bgp] group Confed38 external
[Sysname-bgp] peer Confed38 as-number 38
[Sysname-bgp] peer 10.1.1.1 group Confed38
[Sysname-bgp] group Remote98 external
[Sysname-bgp] peer Remote98 as-number 98
[Sysname-bgp] peer 200.1.1.1 group Remote98
```

confederation nonstandard

Syntax **confederation nonstandard**

undo confederation nonstandard

View BGP view

Parameters None

Description Use the **confederation nonstandard** command to make the device compatible with devices not compliant with RFC3065 in the confederation.

Use the **undo confederation nonstandard** command to restore the default.

By default, all devices in the confederation comply with RFC3065.

All devices should be configured with this command to interact with those nonstandard devices in the confederation.

Related commands: **confederation id** and **confederation peer-as**.

Examples # AS100 contains devices not compliant with RFC3065 and comprises two sub-ASs, 64000 and 65000.

```
<Sysname> system-view
[Sysname] bgp 64000
[Sysname-bgp] confederation id 100
[Sysname-bgp] confederation peer-as 65000
[Sysname-bgp] confederation nonstandard
```

confederation peer-as

Syntax **confederation peer-as** *as-number-list*

undo confederation peer-as [*as-number-list*]

View BGP view

Parameters *as-number-list*: Sub-AS number list. Up to 32 sub-ASs can be configured in one command line. The expression is *as-number-list* = a*s-number* &<1-32>, in which a*s-number* specifies a sub-AS number, and &<1-32> indicates up to 32 numbers can be specified.

Description Use the **confederation peer-as** command to specify confederation peer sub-ASs.

Use the **undo confederation peer-as** command to remove specified confederation peer sub-ASs.

By default, no confederation peer sub-ASs are configured.

Before this configuration, the **confederation id** command must be used to specify the confederation for the sub-ASs.

If the **undo confederation peer-as** command without the *as-number-list* argument is used, all confederation peer sub-ASs are removed.

Related commands: **confederation nonstandard** and **confederation id**.

Examples # Specify confederation peer sub ASs 2000 and 2001.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] confederation id 10
[Sysname-bgp] confederation peer-as 2000 2001
```

dampening (BGP/BGP-VPN instance view)

Syntax **dampening** [*half-life-reachable half-life-unreachable reuse suppress ceiling* | **route-policy** *route-policy-name*] *

undo dampening

View BGP view/BGP-VPN instance view

Parameters *half-life-reachable*: Half-life for reachable routes in minutes. By default, the value is 15 minutes.

half-life-unreachable: Half-life for unreachable routes in minutes. By default, the value is 15 minutes.

reuse: Reuse threshold value for suppressed routes. A suppressed route whose penalty value decreases under the value is reused. By default, the reuse value is 750.

suppress: Suppression threshold. The route with a penalty value higher than the threshold is suppressed. The default value is 2000.

ceiling: Ceiling penalty value, which must be bigger than the *suppress* value. By default, the value is 16000.

route-policy-name: Routing policy name.

*half-life-reachable, half-life-unreachable, reuse, suppres*s and *ceiling* are mutually dependent. Once any one is configured, all the others should also be specified accordingly.

Description Use the **dampening** command to enable BGP route dampening and/or configure dampening parameters.

Use the **undo dampening** command to disable route dampening.

By default, no route dampening is configured.

The command dampens only EBGP routes rather than IBGP routes.

Related commands: **reset bgp dampening**, **reset bgp flap-info**, **display bgp routing-table dampened**, **display bgp routing-table dampening parameter** and **display bgp routing-table flap-info**.

Examples # In BGP view, enable BGP route dampening and configure dampening parameters.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] dampening 15 15 1000 2000 10000
```

In BGP-VPN instance view, enable BGP route dampening and configure dampening parameters. (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] dampening 15 15 1000 2000 10000
```

debugging bgp

Syntax **debugging bgp** [*ip-address*] { **all** | **detail** | **event** | **graceful-restart** | **timer** | { **keepalive** | **open** | **packet** | **raw-packet** | **route-refresh** } [**receive** | **send**] [**verbose**] }

debugging bgp update [**acl** *acl-number* | **ip-prefix** *ip-prefix-name* | **ipv4** | **l2vpn** | **label-route** | **vpn-instance** *vpn-instance-name* | **vpnv4**] [**peer** { *ip-address* | *group-name* }] [**receive** | **send**] [**verbose**]

undo debugging bgp [*ip-address*] { **all** | **detail** | **event** | **graceful-restart** | **timer** | { **keepalive** | **open** | **packet** | **raw-packet** | **route-refresh** } [**receive** | **send**] [**verbose**] }

undo debugging bgp update [**acl** *acl-number* | **ip-prefix** *ip-prefix-name* | **ipv4** | **l2vpn** | **label-route** | **vpn-instance** *vpn-instance-name* | **vpnv4**] [**peer** { *ip-address* | *group-name* }] [**receive** | **send**] [**verbose**]

View User view

Parameters *ip-address*: IP address of a peer.

all: Enables all BGP debugging.

detail: Enables BGP detailed information debugging.

event: Enables BGP event debugging.

graceful-restart: Enables BGP GR debugging.

timer: Enables BGP timer debugging.

keepalive: Enables BGP keepalive packets debugging.

open: Enables BGP open packets debugging.

packet: Enables BGP packets debugging.

raw-packet: Enables BGP raw packets debugging.

route-refresh: Enables BGP route-refresh packets debugging.

receive: Received BGP packets.

send: Sent BGP packets.

Verbose: Displays detailed debugging information.

update: Enables BGP update packets debugging.

acl *acl-number*: Uses an ACL to filter output packet debugging information.

ip-prefix *ip-prefix-name*: Uses an IP prefix list to filter output packet debugging information.

ipv4: Enables IPv4 packet debugging.

l2vpn: Enables L2VPN packet debugging.

lable-route: Enables labeled BGP route debugging.

vpnv4: Enables VPNv4 packet debugging.

vpn-instance *vpn-instance-name*: Enables packet debugging for the VPN instance.

peer *ip-address/group-name*: Enables BGP packet debugging with the BGP peer or peer group.

Description Use the **debugging bgp** command to enable specified BGP debugging.

Use the **undo debugging bgp** command to disable specified BGP debugging.

Enabling any debugging will decrease system performance, so disable the debugging timely after debugging.

Examples # Enable BGP packet debugging.

```
<Sysname> debugging bgp packet
```

default ipv4-unicast

Syntax **default ipv4-unicast**

undo default ipv4-unicast

View BGP view

Parameters None

Description Use the **default ipv4-unicast** command to enable the use of IPv4 unicast address family for all peers.

Use the **undo default ipv4-unicast** command to disable the use of IPv4 unicast address family for all peers.

The use of IPv4 unicast address family is enabled by default.

Examples # Enable IPv4 unicast address family for all neighbors.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] default ipv4-unicast
```

default local-preference (BGP/BGP-VPN instance view)

Syntax **default local-preference** *value*

undo default local-preference

View BGP view/BGP-VPN instance view

Parameters *value*: Default local preference. The larger the value, the higher the preference.

Description Use the **default local-preference** command to configure the default local preference.

Use the **undo default local-preference** command to restore the default value.

Using this command can affect BGP route selection.

Examples # In BGP view, set the default local preference to 180.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] default local-preference 180
```

In BGP-VPN instance view, set the default local preference to 180 (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] default local-preference 180
```

default med (BGP/BGP-VPN instance view)

Syntax **default med** *med-value*

undo default med

View BGP view/BGP-VPN instance view

Parameters *med-value*: Default MED value.

Description Use the **default med** command to specify a default MED value.

Use the **undo default med** command to restore the default.

By default, the default *med-value* is 0.

Multi-exit discriminator (MED) is an external metric for routes. Different from local preference, MED is exchanged between ASs and will stay in the AS once it enters the AS. The route with a lower MED is preferred. When a device running BGP obtains several routes with an identical destination but different next-hops from various external peers, it will select the best route depending on the MED value. In the case that all other conditions are the same, the system first selects the route with the smallest MED as the best external route.

Examples # In BGP view, configure the default MED as 25.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] default med 25
```

In BGP-VPN instance view, configure the default MED as 25 (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] default med 25
```

default-route imported (BGP/BGP-VPN instance view)

Syntax **default-route imported**

undo default-route imported

View BGP view/BGP-VPN instance view

Parameters None

Description Use the **default-route imported** command to allow default route redistribution into the BGP routing table.

Use the **undo default-route imported** command to disallow the redistribution.

By default, default route redistribution is not allowed.

Using the **default-route imported** command cannot redistribute default routes. To do so, use the **import-route** command.

Related commands: import-route.

Examples # In BGP view, allow default route redistribution from OSPF into BGP.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] default-route imported
[Sysname-bgp] import-route ospf 1
```

In BGP-VPN instance view, enable redistributing default route from OSPF into BGP (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] default-route imported
[Sysname-bgp-vpn1] import-route ospf 1
```

display bgp group

Syntax **display bgp group** [*group-name*]

View Any view

Parameters *group-name*: Peer group name.

Description Use the **display bgp group** command to display the information of the peer group.

Examples # Display the information of the peer group "aaa".

```
<Sysname> display bgp group aaa

 BGP peer-group is aaa
 remote AS 200
 Type : external
 Maximum allowed prefix number: 4294967295
 Threshold: 75%
 Configured hold timer value: 180
 Keepalive timer value: 60
 Minimum time between advertisement runs is 30 seconds
 Peer Preferred Value: 0
 No routing policy is configured
  Members:
  Peer            V    AS  MsgRcvd  MsgSent  OutQ PrefRcv Up/Down  State

  2.2.2.1         4   200        0        0     0       0 00:00:35 Active
```

Table 149 Field descriptions of the display bgp group command

Field	Description
BGP peer-group	Name of the BGP peer group
remote AS	AS number of peer group
type	Type of the BGP peer group: IBGP or EBGP
Maximum allowed prefix number	Maximum allowed prefix number
Threshold	Threshold value
hold timer value	Holdtime interval
Keepalive timer value	Keepalive interval
Minimum time between advertisement runs	Minimum time between advertisement runs
Peer Preferred Value	Preferred value of the routes from the peer
No routing policy is configured	No routing policy is configured for the peer
Members	Detailed information of the members in the peer group
Peer	IPv4 address of the peer
V	BGP version running on peers
AS	AS number of the peers
MsgRcvd	Number of messages received
MsgSent	Number of messages sent
OutQ	Number of messages to be sent
PrefRcv	Number of prefixes received
Up/Down	The lasting time of a session/the lasting time of present state (when no session is established)
State	State machine of peer

display bgp network

Syntax **display bgp network**

View Any view

Parameters None

Description Use the **display bgp network** command to display routing information that has been advertised.

Examples # Display routing information that has been advertised.

```
<Sysname> display bgp network

  BGP Local Router ID is 10.1.4.2.
  Local AS Number is 400.
  Network          Mask            Route-policy        Short-cut

  100.1.2.0        255.255.255.0
  100.1.1.0        255.255.255.0                       Short-cut
```

Table 150 Field descriptions of the display bgp network command

Field	Description
BGP Local Router ID	BGP Local Router ID
Local AS Number	Local AS Number
Network	Network address
Mask	Mask
Route-policy	Routing policy
Short-cut	Short-cut route

display bgp paths

Syntax **display bgp paths** [*as-regular-expression*]

View Any view

Parameters *as-regular-expression*: AS path regular expression.

Description Use the **display bgp paths** command to display information about BGP paths.

Examples # Display information about BGP paths matching the AS path regular expression.

```
<Sysname> display bgp paths ^200

    Address       Hash    Refcount  MED         Path/Origin
    0x5917100     11      1                     200 300i
```

Table 151 Field descriptions of the display bgp paths command

Field	Description
Address	Route address in local database, in dotted hexadecimal notation
Hash	Hash index
Refcount	Count of routes that referenced the path

Table 151 Field descriptions of the display bgp paths command

Field	Description	
MED	MED of the path	
Path	AS_PATH attribute of the path, recording the ASs it has passed, for avoiding routing loops	
Origin	Origin attribute of the route:	
	i	Indicates the route is interior to the AS. Summary routes and routes defined using the **network** command are considered IGP routes.
	e	Indicates that a route is learned from the exterior gateway protocol (EGP).
	?	Short for INCOMPLETE. It indicates that the origin of a route is unknown and the route is learned by other means.

display bgp peer

Syntax **display bgp peer** [*ip-address* { **log-info** | **verbose** } | *group-name* **log-info** | **verbose**]

View Any view

Parameters *ip-address*: IP address of an peer to be displayed, in dotted decimal notation.

group-name: Name of a peer group to be displayed.

log-info: Displays the log information of the specified peer.

verbose: Displays the detailed information of the peer/peer group.

Description Use the **display bgp peer** command to display peer/peer group information.

Examples # Display the detailed information of the peer 10.110.25.20.

```
<Sysname> display bgp peer 10.110.25.20 verbose

         Peer: 10.110.25.20 Local: 2.2.2.2
         Type: EBGP link
         BGP version 4, remote router ID 1.1.1.1
         BGP current state: Established, Up for 00h01m51s
         BGP current event: RecvKeepalive
         BGP last state: OpenConfirm
         Port:  Local - 1029     Remote - 179
         Configured: Active Hold Time: 180 sec   Keepalive Time: 60 sec
         Received  : Active Hold Time: 180 sec
         Negotiated: Active Hold Time: 180 sec
         Peer optional capabilities:
         Peer support bgp multi-protocol extended
         Peer support bgp route refresh capability
         Address family IPv4 Unicast: advertised and received

 Received: Total 5 messages, Update messages 1
 Sent: Total 4 messages, Update messages 0
 Maximum allowed prefix number: 4294967295
 Threshold: 75%
```

```
Minimum time between advertisement runs is 30 seconds
Optional capabilities:
Route refresh capability has been enabled
Peer Preferred Value: 0

Routing policy configured:
No routing policy is configured
```

Table 152 Field descriptions of the display bgp peer command

Field	Description
Peer	IP address of the peer
Local	Local router ID
Type	Peer type: Internal as IBGP peers and External as EBGP peers.
BGP version	BGP protocol version
remote router ID	Router ID of the peer
BGP current state	Current state of the peer
BGP current event	Current event of the peer
BGP last state	Last state of the peer
Port	Port number of local router and its peer
Configured: Active Hold Time	Local holdtime interval
Configured: Keepalive Time	Local keepalive interval
Received: Active Hold Time	Remote holdtime interval
Negotiated: Active Hold Time	Negotiated holdtime interval
Peer optional capabilities	Optional capabilities supported by the peer, including BGP multiple extension and routing refresh.
Address family IPv4 Unicast	Routes are advertised and received in the form of IPv4 unicast
Received	Total numbers of received packets and updates
Sent	Total numbers of sent packets and updates
Maximum allowed prefix number	Maximum allowed prefix number
Threshold	Threshold value
Minimum time between advertisement runs	Minimum time between route advertisements
Optional capabilities	Optional capabilities enabled by the peer
Peer Preferred Value	Preferred value specified for the routes from the peer
Routing policy configured	Local routing policy

display bgp routing-table

Syntax **display bgp routing-table** [*ip-address* [{ *mask* | *mask-length* } [**longer-prefixes**]]]

View Any view

Parameters *ip-address*: Destination IP address.

mask: Network mask, in dotted decimal notation.

mask-length: Mask length, in the range 0 to 32.

longer-prefixes: Matches the longest prefix.

Description Use the **display bgp routing-table** command to display specified BGP routing information in the BGP routing table.

Examples # Display BGP routing table information.

```
<Sysname> display bgp routing-table

 Total Number of Routes: 1

 BGP Local router ID is 10.10.10.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

 *>  40.40.40.0/24     20.20.20.1                              0       200 300i
```

Table 153 Field descriptions of the display bgp routing command

Field	Description
Total Number of Routes	Total Number of Routes
BGP Local router ID	BGP Local router ID
Status codes	Status codes: * - valid > - best d - damped h - history i - internal (IGP) s - summary suppressed (suppressed) S - Stale
Origin	i - IGP (originated in the AS) e - EGP (learned through EGP) ? - incomplete (learned by other means)
Network	Destination network address
Next Hop	Next hop IP address
MED	MULTI_EXIT_DISC attribute
LocPrf	Local preference value
PrefVal	Preferred value of the route
Path	AS_PATH attribute, recording the ASs the packet has passed to avoid routing loops
PrefVal	Preferred value

Table 153 Field descriptions of the display bgp routing command

Field	Description	
Ogn	Origin attribute of the route, one of the following values:	
	i	Indicates that the route is interior to the AS. Summary routes and the routes configured using the **network** command are considered IGP routes.
	e	Indicates that the route is learned via the exterior gateway protocol (EGP).
	?	Short for INCOMPLETE. It indicates that the origin of the route is unknown and the route is learned by other means.

display bgp routing-table as-path-acl

Syntax **display bgp routing-table as-path-acl** *as-path-acl-number*

View Any view

Parameters *as-path-acl-number*: Displays routing information permitted by the AS path ACL.

Description Use the **display bgp routing as-path-acl** command to display BGP routes permitted by an as-path ACL.

Examples # Display BGP routes permitted by AS path ACL 1.

```
<Sysname> display bgp routing-table as-path-acl 1

 BGP Local router ID is 20.20.20.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
     Network            NextHop        MED        LocPrf      PrefVal Path/Ogn

*>  40.40.40.0/24     30.30.30.1     0                     0       300i
```

Refer to Table 153 for description on the fields above.

display bgp routing-table cidr

Syntax **display bgp routing-table cidr**

View Any view

Parameters None

Description Use the **display bgp routing-table cidr** command to display BGP CIDR (Classless Inter-Domain Routing) routing information.

Examples # Display BGP CIDR routing information.

```
<Sysname> display bgp routing-table cidr

 BGP Local router ID is 20.20.20.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
     Network          NextHop         MED        LocPrf     PrefVal Path/Ogn

*>  40.40.40.0/24    30.30.30.1      0                     0       300i
```

Refer to Table 153 for description on the above fields.

display bgp routing-table community

Syntax **display bgp routing-table community** [*aa:nn*&<1-13>] [**no-advertise** | **no-export | no-export-subconfed**]* [**whole-match**]

View Any view

Parameters *aa:nn*: Community number.

&<1-13>: Argument before it can be entered up to 13 times.

no-advertise: Displays BGP routes that are not advertised to any peer.

no-export: Displays routes that are not advertised out the AS. If a confederation is configured, it displays routes that are not advertised out the confederation, but can be advertised to other sub ASs in the confederation.

no-export-subconfed: Displays routes that are neither advertised out the AS nor to other sub ASs in a configured confederation.

whole-match: Displays the exactly matched routes.

Description Use the **display bgp routing community** command to display BGP routing information with the specified BGP community.

Examples # Display routing information with the specified BGP community.

```
<Sysname> display bgp routing-table community 11:22

 BGP Local router ID is 10.10.10.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

 *>  10.10.10.0/24     0.0.0.0         0                     0      i
 *>  40.40.40.0/24      20.20.20.1                                0       200 300i
```

Refer to Table 153 for description on the fields above.

display bgp routing-table community-list

Syntax **display bgp routing-table community-list** { *basic-community-list-number* [**whole-match**] | *adv-community-list-number* }&<1-16>

View Any view

Parameters *basic-community-list-number*: Basic community-list number.

adv-community-list-number: Advanced community-list number.

whole-match: Displays routes exactly matching the specified *basic-community-list*.

&<1-16>: Specifies the argument before it can be entered up to 16 times.

Description Use the **display bgp routing-table community-list** command to display BGP routing information matching the specified BGP community list.

Examples # Display BGP routing information matching BGP community list 100.

```
<Sysname> display bgp routing-table community-list 100
 BGP Local router ID is 1.2.3.4
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed,
 Origin codes: i - IGP, e - EGP, ? - incomplete
      Network            NextHop        Metric     LocPrf    PrefVal Path

 *>   3.3.3.0/30         1.2.3.4                             0       ?
 *>   4.4.0.0/20         1.2.3.4                             0       ?
 *>   4.5.6.0/26         1.2.3.4                             0       ?
```

Refer to Table 153 for description on the fields above.

display bgp routing-table dampened

Syntax **display bgp routing-table dampened**

View Any view

Parameters None

Description Use the **display bgp routing-table dampened** command to display dampened BGP routes.

Examples # Display dampened BGP routes.

```
<Sysname> display bgp routing-table dampened
 BGP Local router ID is 2.2.2.2
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
```

```
     Network            From              Reuse      Path/Origin
 *d  77.0.0.0           12.1.1.1          00:29:20   100?
```

Table 154 Field descriptions of the display bgp routing-table dampened command

Field	Description
From	IP address from which the route was received
Reuse	Reuse time of the route

Refer to Table 153 for description on the other fields above.

display bgp routing-table dampening parameter

Syntax **display bgp routing-table dampening parameter**

View Any view

Parameters None

Description Use the **display bgp routing-table dampening parameter** command to display BGP route dampening parameters.

Related commands: **dampening**.

Examples # Display BGP route dampening parameters.

```
<Sysname> display bgp routing-table dampening parameter
 Maximum Suppress Time(in second) : 3069
 Ceiling Value                    : 16000
 Reuse Value                      : 750
 HalfLife Time(in  second)        : 900
 Suppress-Limit                   : 2000
```

Table 155 Field descriptions of the display bgp routing-table dampening parameter command

Field	Description
Maximum Suppress Time	Maximum Suppress Time
Ceiling Value	Upper limit of penalty value
Reuse Value	Limit for a route to be desuppressed
HalfLife Time	Half-life time of active routes
Suppress-Limit	Limit for a route to be suppressed

display bgp routing-table different-origin-as

Syntax **display bgp routing-table different-origin-as**

View Any view

Parameters None

Description Use the **display bgp routing-table different-origin-as** command to display BGP routes originating from different autonomous systems.

Examples # Display BGP routes originating from different ASs.

```
<Sysname> display bgp routing-table different-origin-as
 BGP Local router ID is 2.2.2.2
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
     Network           NextHop         MED        LocPrf     PrefVal Path/Ogn

 *>  55.0.0.0         12.1.1.1       0                   0       100?
 *                    14.1.1.2       0                   0       300?
```

Refer to Table 153 for description on the fields above.

display bgp routing-table flap-info

Syntax **display bgp routing-table flap-info** [**regular-expression** *as-regular-expression* | **as-path-acl** *as-path-acl-number* | *ip-address* [{ *mask* | *mask-length* } [**longer-match**]]]

View Any view

Parameters *as-regular-expression*: Displays route flap information that matches the AS path regular expression.

as-path-acl-number: Displays route flap information matching the AS path ACL.

ip-address: Destination IP address.

mask: Mask, in dotted decimal notation.

mask-length: Mask length.

longer-match: Matches the longest prefix.

Description Use the **display bgp routing-table flap-info** command to display BGP route flap statistics. If no parameter is specified, this command displays all BGP route flap statistics.

Examples # Display BGP route flap statistics.

```
<Sysname> display bgp routing-table flap-info

 BGP Local router ID is 2.2.2.2
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
     Network        From        Flaps  Duration   Reuse     Path/Origin

 *>  55.0.0.0       12.1.1.1    2      00:00:16             100?
 *d  77.0.0.0       12.1.1.1    5      00:34:02   00:27:08  100?
```

Table 156 Field descriptions of the display bgp routing flap-info command

Field	Description
From	Source IP address of the route
Flaps	Number of routing flaps
Duration	Duration time of the flap route
Reuse	Reuse time of the flap route

Refer to Table 153 for description on the other fields above.

display bgp routing-table peer

Syntax **display bgp routing-table peer** *ip-address* { **advertised-routes** | **received-routes** } [*network-address* [*mask* | *mask-length*] | **statistic**]

View Any view

Parameters *ip-address*: IP address of a peer.

advertised-routes: Displays routing information advertised to the specified peer.

received-routes: Displays routing information received from the specified peer.

network-address: IP address of the destination network.

mask: Mask of the destination network, in dotted decimal notation.

mask-length: Mask length.

statistic: Displays route statistics.

Description Use the **display bgp routing-table peer** command to display BGP routing information advertised to or received from the specified BGP peer.

Related commands: **display bgp peer**.

Examples # Display BGP routing information advertised to BGP peer 20.20.20.1.

```
<Sysname> display bgp routing table peer 20.20.20.1 advertised-routes

 Total Number of Routes: 2

 BGP Local router ID is 30.30.30.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

 *>  30.30.30.0/24     0.0.0.0        0                    0       i
 *>  40.40.40.0/24     0.0.0.0        0                    0       i
```

Refer to Table 153 for description on the fields above.

display bgp routing-table regular-expression

Syntax **display bgp routing-table regular-expression** *as-regular-expression*

View Any view

Parameters *as-regular-expression*: AS regular expression.

Description Use the **display bgp routing-table regular-expression** command to display BGP routing information matching the specified AS regular expression.

Examples # Display BGP routing information matching AS regular expression 300$.

```
<Sysname> display bgp routing-table regular-expression 300$

 BGP Local router ID is 20.20.20.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
     Network           NextHop       MED        LocPrf    PrefVal Path/Ogn

 *>  40.40.40.0/24     30.30.30.1    0                    0       300i
```

Refer to Table 153 for description on the fields above.

display bgp routing-table statistic

Syntax **display bgp routing-table statistic**

View Any view

Parameters None

Description Use the **display bgp routing-table statistic** command to display BGP routing statistics.

Examples # Display BGP routing statistics.

```
<Sysname> display bgp routing-table statistic

 Total Number of Routes: 4
```

Table 157 Field descriptions of the display bgp routing-table statistic command

Field	Description
Total number of routes	Total number of routes

ebgp-interface-sensitive

Syntax **ebgp-interface-sensitive**

undo ebgp-interface-sensitive

View BGP view/BGP-VPN instance view

Parameters None

Description Use the **ebgp-interface-sensitive** command to enable the clearing of EBGP session on any interface that becomes down.

Use the undo **ebgp-interface-sensitive** command to disable the function.

This function is enabled by default.

Examples # In BGP view, enable the clearing of EBGP session on any interface that becomes down.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ebgp-interface-sensitive
```

In BGP-VPN instance view, enable the clearing of EBGP session on any interface that becomes down (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] ebgp-interface-sensitive
```

filter-policy export (BGP/BGP-VPN instance view)

Syntax **filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [**direct** | **isis** *process-id* | **ospf** *process-id* | **rip** *process-id* | **static**]

undo filter-policy export [**direct** | **isis** *process-id* | **ospf** *process-id* | **rip** *process-id* | **static**]

View BGP view/BGP-VPN instance view

Parameters *acl-number*: Number of an ACL used to filter outgoing redistributed routing information.

ip-prefix-name: Name of an IP prefix list used to filter outgoing redistributed routing information.

direct: Filters direct routes.

isis *process-id*: Filters outgoing routes redistributed from an ISIS process.

ospf *process-id*: Filters outgoing routes redistributed from the OSPF process.

rip *process-id*: Filters outgoing routes redistributed from a RIP process.

static: Filters static routes.

If no routing protocol is specified, all outgoing routes are filtered.

Description Use the **filter-policy export** command to filter outgoing redistributed routes and only the routes permitted by the specified filter can be advertised.

Use the **undo filter-policy export** command to remove the filtering.

If no routing protocol is specified, the filtering applies to all outgoing redistributed routes.

By default, the filtering is not configured.

Examples # In BGP view, reference ACL 2000 to filter all outgoing redistributed routes.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] filter-policy 2000 export
```

In BGP-VPN instance view, reference ACL 2000 to filter all outgoing redistributed routes (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] filter-policy 2000 export
```

filter-policy import (BGP/BGP-VPN instance view)

Syntax **filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* } **import**

undo filter-policy import

View BGP view/BGP-VPN instance view

Parameters *acl-number*: Number of an ACL used to filter incoming routing information.

ip-prefix-name: Name of an IP prefix list used to filter incoming routing information.

Description Use the **filter-policy import** command to configure the filtering of incoming routing information.

Use the **undo filter-policy import** command to disable the filtering.

By default, incoming routing information is not filtered.

Examples # In BGP view, reference ACL 2000 to filter incoming routing information.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] filter-policy 2000 import
```

In BGP-VPN instance view, reference ACL 2000 to filter incoming routing information (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] filter-policy 2000 import
```

group (BGP/BGP-VPN instance view)

Syntax **group** *group-name* [**external** | **internal**]

undo group *group-name*

View BGP view/BGP-VPN instance view

Parameters *group-name*: Name of a peer group.

external: Creates an EBGP peer group, which can be the group of another sub AS in a confederation.

internal: Creates an IBGP peer group; not supported in BGP-VPN instance view.

Description Use the **group** command to create a peer group.

Use the **undo group** command to delete a peer group.

An IBGP peer group is created if neither **internal** nor **external** is specified.

Examples # In BGP view, create an EBGP peer group "test" with AS number 200, and add EBGP peers 10.1.1.1 and 10.1.2.1 into the group.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] group test external
[Sysname-bgp] peer test as-number 200
[Sysname-bgp] peer 10.1.1.1 group test
[Sysname-bgp] peer 10.1.2.1 group test
```

In BGP-VPN instance view, create an EBGP peer group "test" with AS number 200, and add EBGP peers 10.1.1.1 and 10.1.2.1 into the group (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] group test external
[Sysname-bgp-vpn1] peer test as-number 200
[Sysname-bgp-vpn1] peer 10.1.1.1 group test
[Sysname-bgp-vpn1] peer 10.1.2.1 group test
```

import-route (BGP/BGP-VPN instance view)

Syntax **import-route** *protocol* [*process-id* [**med** *med-value* | **route-policy** *route-policy-name*] *]

undo import-route *protocol* [*process-id*]

View BGP view/BGP-VPN instance view

Parameters *protocol*: Redistributes routes from the routing protocol, which can be **direct**, **isis**, **ospf**, **rip** and **static** at present.

process-id: Process ID, in the range 1 to 65535. It is available only when the protocol is **isis**, **ospf** or **rip**.

med-value: Specifies the MED value to be applied to redistributed routes, ranging from 0 to 4294967295. If the argument is not specified, the cost of the redistributed route is used as its MED in the BGP routing domain.

route-policy-name: Name of a routing policy used to filter redistributed routes, a string of 1 to 19 characters.

Description Use the **import-route** command to configure BGP to redistribute routes from a specified routing protocol and advertise redistributed routes.

Use the **undo import-route** command to disable route redistribution from a routing protocol.

By default, BGP does not redistribute routes from other protocols.

The ORIGIN attribute of routes redistributed with the **import-route** command is incomplete.

Examples # In BGP view, redistribute routes from RIP.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] import-route rip
```

In BGP-VPN instance view, redistribute routes from RIP (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] import-route rip
```

log-peer-change (BGP view)

Syntax **log-peer-change**

undo log-peer-change

View BGP view

Parameters None

Description Use the **log-peer-change** command to enable the global BGP logging on peers going up and down.

Use the **undo log-peer-change** command to disable the function.

By default, the function is enabled.

Examples # Enable BGP logging on peers going up and down.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] log-peer-change
```

network (BGP/BGP-VPN instance view)

Syntax **network** *ip-address* [*mask* | *mask-length*] [**short-cut** | **route-policy** *route-policy-name*]

undo network *ip-address* [*mask* | *mask-length*] [**short-cut**]

View BGP view/BGP-VPN instance view

Parameters *ip-address*: Destination IP address.

mask: Mask of the network address, in dotted decimal notation.

mask-length: Mask length.

short-cut: Specifies the route to use the local preference. If the route is an EBGP route whose preference is higher than the local one, using this keyword can configure the EBGP route to use the local preference, so the route is hard to become the optimal route.

route-policy-name: Routing policy applied to the route.

Description Use the **network** command to advertise a network to the BGP routing table.

Use the **undo network** command to remove a network from the routing table.

By default, no network route is advertised.

Note that:

- The network route must be in the local IP routing table, and using a routing policy makes route management more flexible.
- The route advertised to the BGP routing table using the **network** command has the ORIGIN attribute as IGP.

Examples # In BGP view, advertise the network segment 10.0.0.0/16.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] network 10.0.0.0 255.255.0.0
```

In BGP-VPN instance view, advertise the network segment 10.0.0.0/16 (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] network 10.0.0.0 255.255.0.0
```

peer advertise-community (BGP/BGP-VPN instance view)

Syntax **peer** { *group-name* | *ip-address* } **advertise-community**

undo peer { *group-name* | *ip-address* } **advertise-community**

View BGP view/BGP-VPN instance view

Parameters *group-name*: Name of a peer group.

ip-address: IP address of a peer.

Description Use the **peer advertise-community** command to advertise the community attribute to a peer/peer group.

Use the **undo peer advertise-community** command to disable the community attribute advertisement to a peer/peer group.

By default, no community attribute is advertised to any peer group/peer.

Related commands: **ip community-list**, **if-match community**, **apply community** in "Routing Policy Configuration Commands" on page 351.

Examples # In BGP view, advertise the community attribute to peer group "test".

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test advertise-community
```

In BGP-VPN instance view, advertise the community attribute to peer group "test" (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test advertise-community
```

peer advertise-ext-community (BGP/BGP-VPN instance view)

Syntax **peer** { *group-name* | *ip-address* } **advertise-ext-community**

undo peer { *group-name* | *ip-address* } **advertise-ext-community**

View BGP view/BGP-VPN instance view

Parameters *group-name*: Name of a peer group.

ip-address: IP address of a peer.

Description Use the **peer advertise-ext-community** command to advertise the extended community attribute to a peer/peer group.

Use the **undo peer advertise-ext-community** command to disable the advertisement.

By default, no extended community attribute is advertised to a peer/peer group.

For related information, refer to the **ip extcommunity-list**, **if-match extcommunity** and **apply extcommunity** commands in "Routing Policy Configuration Commands" on page 351.

Examples # In BGP view, advertise the extended community attribute to the peer group "test".

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test advertise-ext-community
```

In BGP-VPN view, advertise the extended community attribute to the peer group "test" (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test advertise-community
```

peer allow-as-loop (BGP/BGP-VPN instance view)

Syntax **peer** { *group-name* | *ip-address* } **allow-as-loop** [*number*]

undo peer { *group-name* | *ip-address* } **allow-as-loop**

View BGP view/BGP-VPN instance view

Parameters *group-name*: Name of a peer group.

ip-address: IP address of a peer.

number: Specifies the repeating times of the local AS number. The default number is 1.

Description Use the **peer allow-as-loop** command to allow the local AS number to exist in the AS_PATH attribute of routes from a peer/peer group, and to configure the repeating times of the local AS number.

Use the **undo peer allow-as-loop** command to disable the feature.

By default, the local AS number is not allowed.

Related commands: **display bgp routing-table peer**.

Examples # In BGP view, configure the repeating times of the local AS number as 2 for routes from peer 1.1.1.1.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 1.1.1.1 allow-as-loop 2
```

In BGP-VPN instance view, configure the repeating times of the local AS number as 2 for routes from peer 1.1.1.1 (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer 1.1.1.1 allow-as-loop 2
```

peer as-number (BGP/BGP-VPN instance view)

Syntax **peer** { *group-name* | *ip-address* } **as-number** *as-number*

undo peer *group-name* **as-number**

undo peer *ip-address*

View BGP view/BGP-VPN instance view

Parameters *group-name*: Name of a peer group.

ip-address: IP address of a peer.

as-number: AS number of the peer or peer group.

Description Use the **peer as-number** command to specify the AS number for a peer/peer group.

Use the **undo peer as-number** command to delete the AS number of a peer group.

Use the **undo peer** command to delete a peer.

By default, no AS number is configured for a peer/peer group.

Examples # In BGP view, specify the AS number of the peer group "test" as 100.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test as-number 100
```

In BGP-VPN instance view, specify the AS number of the peer group "test" as 100 (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test as-number 100
```

peer as-path-acl (BGP/BGP-VPN instance view)

Syntax **peer** { *group-name* | *ip-address* } **as-path-acl** *as-path-acl-number* { **export** | **import** }

undo peer { *group-name* | *ip-address* } **as-path-acl** *as-path-acl-number* { **export** | **import** }

View BGP view/BGP-VPN instance view

Parameters *group-name*: Name of a peer group.

ip-address: IP address of a peer.

as-path-acl-number: AS path ACL number.

export: Filters outgoing routes.

import: Filters incoming routes.

Description Use the **peer as-path-acl** command to configure the filtering of routes incoming from or outgoing to a peer/peer group based on a specified AS path ACL.

Use the **undo peer as-path-acl** command to remove the configuration.

By default, no AS path ACL filtering is configured.

Related commands: **ip as-path-acl**, **if-match as-path** and **apply as-path** (refer to "Routing Policy Configuration Commands" on page 351).

Examples # In BGP view, reference the AS path ACL 1 to filter routes outgoing to the peer group "test".

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test as-path-acl 1 export
```

In BGP-VPN instance view, reference the AS path ACL 1 to filter routes outgoing to the peer group "test" (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test as-path-acl 1 export
```

peer capability-advertise conventional

Syntax **peer** { *group-name* | *ip-address* } **capability-advertise conventional**

undo peer { *group-name* | *ip-address* } **capability-advertise conventional**

View BGP view

Parameters *group-name*: Name of a peer group.

ip-address: IP address of a peer.

Description Use the **peer capability-advertise conventional** command to disable BGP multi-protocol extension and route refresh for a peer/peer group.

Use the **undo peer capability-advertise** command to enable BGP multi-protocol extension and route refresh for a peer/peer group.

By default, BGP multi-protocol extension and route refresh are enabled.

Examples # In BGP view, disable multi-protocol extension and route refresh for peer 160.89.2.33.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 160.89.2.33 as-number 100
[Sysname-bgp] peer 160.89.2.33 capability-advertise conventional
```

peer capability-advertise route-refresh

Syntax **peer** { *group-name* | *ip-address* } **capability-advertise route-refresh**

undo peer { *group-name* | *ip-address* } **capability-advertise route-refresh**

View BGP view/BGP-VPN instance view

Parameters *group-name*: Name of a peer group.

ip-address: IP address of a peer.

Description Use the **peer capability-advertise route-refresh** command to enable the BGP route refresh capability.

Use the **undo peer capability-advertise route-refresh** command to disable the capability.

The capability is enabled by default.

Examples # In BGP view, enable BGP route refresh for peer 160.89.2.33.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 160.89.2.33 as-number 100
[Sysname-bgp] peer 160.89.2.33 capability-advertise route-refresh
```

In BGP-VPN instance view, enable BGP route refresh for peer 160.89.2.33 (The VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer 160.89.2.33 as-number 100
[Sysname-bgp-vpn1] peer 160.89.2.33 capability-advertise route-refresh
```

peer connect-interface (BGP/BGP-VPN instance view)

Syntax **peer** { *group-name* | *ip-address* } **connect-interface** *interface-type interface-number*

undo peer { *group-name* | *ip-address* } **connect-interface**

View BGP view/BGP-VPN instance view

Parameters *group-name*: Name of a peer group.

ip-address: IP address of a peer.

interface-type interface-number: Specifies the type and number of the interface.

Description Use the **peer connect-interface** command to specify the source interface of updates to a peer/peer group.

Use the **undo peer connect-interface** command to restore the source interface of best routing updates.

By default, BGP uses the source interface of best routing updates.

For updates to be forwarded in case the interface experiences a failure, you can use a Loopback interface to forward route updates.

Examples # In BGP view, specify loopback0 as the source interface for routing updates to the peer group "test".

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test connect-interface loopback 0
```

In BGP-VPN instance view, specify loopback0 as the source interface for routing updates to the peer group "test" (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test connect-interface loopback 0
```

peer default-route-advertise (BGP/BGP-VPN instance view)

Syntax **peer** { *group-name* | *ip-address* } **default-route-advertise** [**route-policy** *route-policy-name*]

undo peer { *group-name* | *ip-address* } **default-route-advertise**

View BGP view/BGP-VPN instance view

Parameters *group-name*: Name of a peer group.

ip-address: IP address of a peer.

route-policy-name: Routing policy name.

Description Use the **peer default-route-advertise** command to advertise a default route to a peer/peer group.

Use the **undo peer default-route-advertise** command to disable default route advertisement to a peer/peer group.

By default, no default route is advertised to a peer/peer group.

With this command used, the router unconditionally sends a default route with the next hop being itself to the peer/peer group regardless of whether the default route is available in the routing table.

Examples # In BGP view, advertise a default route to peer group "test".

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test default-route-advertise
```

In BGP-VPN instance view, advertise a default route to peer group "test" (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
```

```
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test default-route-advertise
```

peer description (BGP/BGP-VPN instance view)

Syntax **peer** { *group-name* | *ip-address* } **description** *description-text*

undo peer { *group-name* | *ip-address* } **description**

View BGP view/BGP-VPN instance view

Parameters *group-name*: Name of a peer group.

ip-address: IP address of a peer.

description-text: Description information for the peer/peer group.

Description Use the **peer description** command to configure the description information for a peer/peer group.

Use the **undo peer description** command to remove the description information of a peer/peer group.

By default, no description information is configured for a peer/peer group.

Create a peer/peer group before configuring a description for it.

Related commands: **display bgp peer**.

Examples # In BGP view, configure the description information of the peer group test as ISP1.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test description ISP1
```

In BGP-VPN instance view, configure the description information of the peer group test as ISP1(the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test description ISP1
```

peer ebgp-max-hop (BGP/BGP-VPN instance view)

Syntax **peer** { *group-name* | *ip-address* } **ebgp-max-hop** [*hop-count*]

undo peer { *group-name* | *ip-address* } **ebgp-max-hop**

View BGP view/BGP-VPN instance view

Parameters *group-name*: Name of a peer group.

ip-address: IP address of a peer.

hop-count: Maximum hop count. The default is 64.

Description Use the **peer ebgp-max-hop** command to allow establishing an EBGP connection with a peer/peer group that is on an indirectly connected network.

Use the **undo peer ebgp-max-hop** command to restore the default.

By default, this feature is disabled.

You can use the argument *hop-count* to specify the maximum route hop count of the EBGP connection.

Examples # In BGP view, allow establishing the EBGP connection with the peer group "test" that is on an indirectly connected network.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test ebgp-max-hop
```

In BGP-VPN instance view, allow establishing the EBGP connection with the peer group "test" that is on an indirectly connected network (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test ebgp-max-hop
```

peer enable (BGP view)

Syntax **peer** *ip-address* **enable**

undo peer *ip-address* **enable**

View BGP view

Parameters *ip-address*: IP address of a peer.

Description Use the **peer enable** command to enable the specified peer.

Use the **undo peer enable** command to disable the specified peer.

By default, the BGP peer is enabled.

If a peer is disabled, the device will not exchange routing information with the peer.

Examples # Disable peer 18.10.0.9.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 18.10.0.9 group group1
[Sysname-bgp] undo peer 18.10.0.9 enable
```

peer fake-as (BGP/BGP-VPN instance view)

Syntax **peer** { *group-name* | *ip-address* } **fake-as** *as-number*

undo peer { *group-name* | *ip-address* } **fake-as**

View BGP view/BGP-VPN instance view

Parameters *group-name*: Name of a peer group.

ip-address: IP address of a peer.

as-number: Local autonomous system number.

Description Use the **peer fake-as** command to configure a fake local AS number for a peer or peer group.

Use the **undo peer fake-as** command to remove the configuration.

By default, no fake local AS number is configured for a peer or peer group.

*The **peer fake-as** command is only applicable to an EBGP peer or peer group.*

Examples # In BGP view, configure a fake AS number of 200 for the peer group "test".

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test fake-as 200
```

In BGP-VPN instance view, configure a fake AS number of 200 for the peer group "test" (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test fake-as 200
```

peer filter-policy (BGP/BGP-VPN instance view)

Syntax **peer** { *group-name* | *ip-address* } **filter-policy** *acl-number* { **export** | **import** }

undo peer { *group-name* | *ip-address* } **filter-policy** [*acl-number*] { **export** | **import** }

View BGP view/BGP-VPN instance view

Parameters *group-name*: Name of a peer group.

ip-address: IP address of a peer.

acl-number: ACL number.

export: Applies the filter-policy to routes advertised to the peer/peer group.

import: Applies the filter-policy to routes received from the peer/peer group.

Description Use the **peer filter-policy** command to configure an ACL-based filter policy for a peer or peer group.

Use the **undo peer filter-policy** command to remove the configuration.

By default, no ACL-based filter policy is configured for a peer or peer group.

Related commands: **peer as-path-acl**.

Examples # In BGP view, apply the ACL 2000 to filter routes advertised to the peer group test.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test filter-policy 2000 export
```

In BGP-VPN instance view, apply the ACL 2000 to filter routes advertised to the peer group test (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test filter-policy 2000 export
```

peer group (BGP/BGP-VPN instance view)

Syntax **peer** *ip-address* **group** *group-name* [**as-number** *as-number*]

undo peer *ip-address* **group** *group-name*

View BGP view/BGP-VPN instance view

Parameters *group-name*: Name of a peer group.

ip-address: IP address of a peer.

as-number: AS number of the peer.

Description Use the **peer group** command to add a peer to a peer group.

Use the **undo peer group** command to delete a specified peer from a peer group.

By default, no peer is added into a peer group.

Examples # In BGP view, add the peer 10.1.1.1 to the EBGP peer group test.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] group test external
[Sysname-bgp] peer test as-number 2004
[Sysname-bgp] peer 10.1.1.1 group test
```

In BGP-VPN view, add the peer 10.1.1.1 to the EBGP peer group test (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] group test external
[Sysname-bgp-vpn1] peer test as-number 2004
[Sysname-bgp-vpn1] peer 10.1.1.1 group test
```

peer ignore (BGP/BGP-VPN instance view)

Syntax **peer** { *group-name* | *ip-address* } **ignore**

undo peer { *group-name* | *ip-address* } **ignore**

View BGP view/BGP-VPN instance view

Parameters *group-name*: Name of a peer group.

ip-address: IP address of a peer.

Description Use the **peer ignore** command to disable session establishment with a peer or peer group.

Use the **undo peer ignore** command to remove the configuration.

By default, session establishment with a peer or peer group is allowed.

After the **peer ignore** command is executed, the system disables the session with the specified peer or peer group and clears all the related routing information. For a peer group, this means all sessions with the peer group will be tore down.

Examples # In BGP view, disable session establishment with peer 10.10.10.10.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 10.10.10.10 ignore
```

In BGP-VPN instance view, disable session establishment with peer 10.10.10.10 (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer 10.10.10.10 ignore
```

peer ip-prefix

Syntax **peer** { *group-name* | *ip-address* } **ip-prefix** *ip-prefix-name* { **export** | **import** }

undo peer { *group-name* | *ip-address* } **ip-prefix** { **export** | **import** }

View BGP view/BGP-VPN instance view

Parameters *group-name*: Name of a peer group.

ip-address: IP address of a peer.

ip-prefix-name: IP prefix list name.

export: Applies the filter to routes advertised to the specified peer/peer group.

import: Applies the filter to routes received from the specified peer/peer group.

Description Use the **peer ip-prefix** command to reference an IP prefix list to filter routes received from or advertised to a peer or peer group.

Use the **undo peer ip-prefix** command to remove the configuration.

By default, no IP prefix list is specified.

Examples # In BGP view, use the IP prefix list "list 1" to filter routes advertised to the peer group "test".

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test ip-prefix list1 export
```

In BGP-VPN view, use the IP prefix list "list 1" to filter routes advertised to the peer group "test" (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test ip-prefix list1 export
```

peer keep-all-routes (BGP/BGP-VPN instance view)

Syntax **peer** { *group-name* | *ip-address* } **keep-all-routes**

undo peer { *group-name* | *ip-address* } **keep-all-routes**

View BGP view/BGP-VPN instance view

Parameters *group-name*: Name of a peer group.

ip-address: IP address of a peer.

Description Use the **peer keep-all-routes** command to save original routing information from a peer or peer group, even routes that failed to pass the inbound policy (if configured).

Use the **undo peer keep-all-routes** command to disable this function.

By default, the function is not enabled.

Examples # In BGP view, save routing information from peer 131.100.1.1.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 131.100.1.1 as-number 200
[Sysname-bgp] peer 131.100.1.1 keep-all-routes
```

In BGP-VPN instance view, save routing information from peer 131.100.1.1(the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer 131.100.1.1 as-number 200
[Sysname-bgp-vpn1] peer 131.100.1.1 keep-all-routes
```

peer log-change (BGP/BGP-VPN instance view)

Syntax **peer** { *group-name* | *ip-address* } **log-change**

undo peer { *group-name* | *ip-address* } **log-change**

View BGP view/BGP-VPN instance view

Parameters *group-name*: Name of a peer group.

ip-address: IP address of a peer.

Description Use the **peer log-change** command to enable the logging of session state and event information for a specified peer or peer group.

Use the **undo peer log-change** command to remove the configuration.

The logging is enabled by default.

Examples # In BGP view, enable the logging of session state and event information for peer group "test".

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test log-change
```

In BGP-VPN instance view, enable the logging of session state and event information for peer group "test" (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test log-change
```

peer next-hop-local (BGP/BGP-VPN instance view)

Syntax **peer** { *group-name* | *ip-address* } **next-hop-local**

undo peer { *group-name* | *ip-address* } **next-hop-local**

View BGP view /BGP-VPN instance view

Parameters *group-name*: Name of a peer group.

ip-address: IP address of a peer.

Description Use the **peer next-hop-local** command to specify the router as the next hop for routes to a peer/peer group.

Use the **undo peer next-hop-local** command to remove the configuration.

By default, routes advertised to an EBGP peer/peer group take the local router as the next hop, while routes to an IBGP peer/peer group do not take the local router as the next hop.

Examples # In BGP view, set the next hop of routes advertised to peer group "test" to the router itself.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test next-hop-local
```

In BGP-VPN instance view, set the next hop of routes advertised to peer group "test" to the router itself (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test next-hop-local
```

peer password

Syntax **peer** { *group-name* | *ip-address* } **password** { **cipher** | **simple** } *password*

undo peer { *group-name* | *ip-address* } **password**

View BGP view/BGP-VPN instance view

Parameters *group-name*: Name of a peer group.

ip-address: IP address of a peer.

cipher: Displays the configured password in cipher text format.

simple: Displays the configured password in plain text format.

password: Password, a string of 1 to 80 characters when the keyword **simple** is used, or when keyword **cipher** is included and plain text password is input; a string of 24 to 108 characters when cipher text password and the keyword **cipher** are used.

Description Use the **peer password** command to configure BGP to perform MD5 authentication when a TCP connection is being established with a peer/peer group.

Use the **undo peer password** command to disable the function.

By default, no MD5 authentication is performed for TCP connection establishment.

Once MD5 authentication is enabled, both parties must be configured with the same authentication mode and password. Otherwise, the TCP connection will not be set up.

Examples # In BGP view, perform MD5 authentication on the TCP connection between the local device 10.1.100.1 and the peer device 10.1.100.2.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 10.1.100.2 password simple aabbcc
```

Perform the similar configuration on the peer.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 10.1.100.1 password simple aabbcc
```

In BGP-VPN instance view, perform MD5 authentication on the TCP connection between the local device 10.1.100.1 and the peer device 10.1.100.2 (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer 10.1.100.2 password simple aabbcc
```

Perform the similar configuration on the peer.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer 10.1.100.1 password simple aabbcc
```

peer preferred-value (BGP/BGP-VPN instance view)

Syntax **peer** { *group-name* | *ip-address* } **preferred-value** *value*

undo peer { *group-name* | *ip-address* } **preferred-value**

View BGP view/BGP-VPN instance view

Parameters *group-name*: Name of a peer group.

ip-address: IP address of a peer.

value: Preferred value.

Description Use the **peer preferred-value** command to assign a preferred value to routes received from a peer or peer group.

Use the **undo peer preferred-value** command to restore the default value.

The default preferred value is 0.

Routes learned from a peer have an initial preferred value.

Among multiple routes that have the same destination/mask and are learned from different peers, the one with the biggest preferred value is selected as the route to the network.

Examples # In BGP view, configure the preferred value as 50 for routes from peer 131.108.1.1.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 131.108.1.1 preferred-value 50
```

In BGP-VPN instance view, configure the preferred value as 50 for routes from peer 131.108.1.1 (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer 131.108.1.1 preferred-value 50
```

peer public-as-only (BGP/BGP-VPN instance view)

Syntax **peer** { *group-name* | *ip-address* } **public-as-only**

undo peer { *group-name* | *ip-address* } **public-as-only**

View BGP view/BGP-VPN instance view

Parameters *group-name*: Name of a peer group.

ip-address: IP address of a peer.

Description Use the **peer public-as-only** command to not keep private AS numbers in BGP updates sent to a peer/peer group.

Use the **undo peer public-as-only** command to keep private AS numbers in BGP updates sent to a peer/peer group.

By default, BGP updates carry private AS numbers.

The command does not take effect if the BGP update has both public and private AS numbers. The range of private AS number is from 64512 to 65535.

Examples # In BGP view, carry no private AS number in BGP updates sent to the peer "test".

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test public-as-only
```

In BGP-VPN instance view, carry no private AS number in BGP updates sent to the peer "test" (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test public-as-only
```

peer reflect-client (BGP/BGP-VPN instance view)

Syntax **peer** { *group-name* | *ip-address* } **reflect-client**

undo peer { *group-name* | *ip-address* } **reflect-client**

View BGP view/BGP-VPN instance view

Parameters *group-name*: Name of a peer group.

ip-address: IP address of a peer.

Description Use the **peer reflect-client** command to configure the router as a route reflector and specify a peer/peer group as a client.

Use the **undo peer reflect-client** command to remove the configuration.

By default, neither route reflector nor client is configured.

Related commands: **reflect between-clients** and **reflect cluster-id**.

Examples # In BGP view, configure the local device as a route reflector and specify the peer group "test" as a client.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test reflect-client
```

In BGP-VPN instance view, configure the local device as a route reflector and specify the peer group "test" as a client (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test reflect-client
```

peer route-limit (BGP/BGP-VPN instance view)

Syntax **peer** { *group-name* | *ip-address* } **route-limit** *limit* [*percentage*]

undo peer { *group-name* | *ip-address* } **route-limit**

View BGP view/BGP-VPN instance view

Parameters *group-name*: Name of a peer group.

ip-address: IP address of a peer.

limit: Upper limit of IP prefixes that can be received from the peer or peer group.

percentage: If the number of received routes reaches the specified percentage of the upper limit, the system will generate alarm information. The default percentage is 75.

Description Use the **peer route-limit** command to set the maximum number of routes that can be received from a peer/peer group.

Use the **undo peer route-limit** command to restore the default.

The number is unlimited by default.

Examples # In BGP view, set the number of routes that can be received from peer 129.140.6.6 to 10000.

```
<Sysname> system-view
[Sysname] bgp 109
[Sysname-bgp] peer 129.140.6.6 as-number 110
[Sysname-bgp] peer 129.140.6.6 route-limit 10000
```

In BGP-VPN instance view, set the maximum number of routes that can be received from peer 129.140.6.6 to 10000 (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 109
[Sysname-bgp] ipv4-family vpn-instance vpn1
```

```
[Sysname-bgp-vpn1] peer 129.140.6.6 as-number 110
[Sysname-bgp-vpn1] peer 129.140.6.6 route-limit 10000
```

peer route-policy (BGP/BGP-VPN instance view)

Syntax **peer** { *group-name* | *ip-address* } **route-policy** *route-policy-name* { **export** | **import** }

undo peer { *group-name* | *ip-address* } **route-policy** *route-policy-name* { **export** | **import** }

View BGP view/BGP-VPN instance view

Parameters *group-name*: Name of a peer group.

ip-address: IP address of a peer.

route-policy-name: Routing policy name.

export: Applies the routing policy to routes outgoing to the peer (or peer group).

import: Applies the routing policy to routes incoming from the peer (or peer group).

Description Use the **peer route-policy** command to apply a routing policy to routes incoming from or outgoing to a peer or peer group.

Use the **undo peer route-policy** command to remove the configuration.

By default, no inbound/outbound routing policy is configured for the peer/peer group.

The **peer route-policy** command does not apply the **if-match interface** clause in the referenced routing policy. Refer to "Routing Policy Configuration Commands" on page 351 for related commands.

Examples # In BGP view, apply routing policy "test-policy" to routes outgoing to peer group "test".

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test route-policy test-policy export
```

In BGP-VPN instance view, apply routing policy "test-policy" to routes outgoing to the peer group "test" (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test route-policy test-policy export
```

peer route-update-interval (BGP/BGP-VPN instance view)

Syntax **peer** { *group-name* | *ip-address* } **route-update-interval** *seconds*

undo peer { *group-name* | *ip-address* } **route-update-interval**

View BGP view/BGP-VPN instance view

Parameters *group-name*: Name of a peer group.

ip-address: IP address of a peer.

seconds: Minimum interval for sending the same update message.

Description Use the **peer route-update-interval** command to specify the interval for sending the same update to a peer/peer group.

Use the **undo peer route-update-interval** command to restore the default value.

By default, the interval is 5 seconds for IBGP peers, and 30 seconds for EBGP peers.

Examples # In BGP view, specify the interval for sending the same update to peer group "test" as 10 seconds.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test as-number 100
[Sysname-bgp] peer test route-update-interval 10
```

In BGP-VPN instance view, specify the interval for sending the same update to peer group "test" as 10 seconds (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test as-number 100
[Sysname-bgp-vpn1] peer test route-update-interval 10
```

peer substitute-as (BGP/BGP-VPN instance view)

Syntax **peer** { *group-name* | *ip-address* } **substitute-as**

undo peer { *group-name* | *ip-address* } **substitute-as**

View BGP view/BGP-VPN instance view

Parameters *group-name*: Name of a peer group.

ip-address: IP address of a peer.

Description Use the **peer substitute-as** command to replace the AS number of a peer/peer group in the AS_PATH attribute with the local AS number.

Use the **undo peer substitute-as** command to remove the configuration.

No AS number is replaced by default.

Examples # In BGP view, substitute local AS number for AS number of peer 1.1.1.1.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 1.1.1.1 substitute-as
```

In BGP-VPN instance view, substitute local AS number for AS number of peer 1.1.1.1 (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer 1.1.1.1 substitute-as
```

peer timer (BGP/BGP-VPN instance view)

Syntax **peer** { *group-name* | *ip-address* } **timer keepalive** *keepalive* **hold** *holdtime*

undo peer { *group-name* | *ip-address* } **timer**

View BGP view/BGP-VPN instance view

Parameters *group-name*: Name of a peer group.

ip-address: IP address of a peer.

keepalive: Keepalive interval in seconds.

holdtime: Holdtime interval in seconds.

Description Use the **peer timer** command to configure the keepalive interval and holdtime interval for a peer or peer group.

Use the **undo peer timer** command to restore the default.

By default, the *keepalive* and *holdtime* are 60s and 180s respectively.

Note that:

- The timer configured with this command is preferred to the timer configured with the **timer** command.
- The holdtime interval must be at least three times the keepalive interval.

Related commands: **timer**.

Examples # In BGP view, configure the keepalive interval and holdtime interval for peer group "test" as 60s and 180s.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test timer keepalive 60 hold 180
```

In BGP-VPN instance view, configure the keepalive interval and holdtime interval for peer group "test" as 60s and 180s (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test timer keepalive 60 hold 180
```

preference (BGP/BGP-VPN instance view)

Syntax **preference** { *external-preference internal-preference local-preference* | **route-policy** *route-policy-name* }

undo preference

View BGP view/BGP-VPN instance view

Parameters *external-preference*: Preference of EBGP routes.

internal-preference: Preference of IBGP routes.

local-preference: Preference of local routes.

route-policy-name: Routing policy name. Using the routing policy can set a preference for routes passing through it. The default value applies to the routes filtered out.

Description Use the **preference** command to configure preferences for external, internal, and local routes.

Use the **undo preference** command to restore the default.

For *external-preference*, *internal-preference* and *local-preference*, the bigger the preference value is, the lower the preference is. The default values are 255, 255, 130 respectively.

Examples # In BGP view, configure preferences for EBGP, IBGP and local routes as 20, 20 and 200.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] preference 20 20 200
```

In BGP-VPN instance view, configure preferences for EBGP, IBGP and local routes as 20, 20 and 200 (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] preference 20 20 200
```

reflect between-clients (BGP view)

Syntax **reflect between-clients**

undo reflect between-clients

View BGP view

Parameters None

Description Use the **reflect between-clients** command to enable route reflection between clients.

Use the **undo reflect between-clients** command to disable this function.

By default, route reflection between clients is enabled.

After a route reflector is configured, it reflects the routes of a client to other clients. If the clients of a route reflector are fully meshed, you need disable route reflection between clients to reduce routing costs.

Related commands: **reflector cluster-id** and **peer reflect-client**.

Examples # Disable route reflection between clients.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] undo reflect between-clients
```

reflector cluster-id (BGP view)

Syntax **reflector cluster-id** *cluster-id*

undo reflector cluster-id

View BGP view

Parameters *cluster-id*: Cluster ID of the route reflector, a decimal integer or an IP address.

Description Use the **reflector cluster-id** command to configure the cluster ID of the route reflector.

Use the **undo reflector cluster-id** command to remove the configured cluster ID.

By default, each route reflector uses its router ID as the cluster ID.

Usually, there is only one route reflector in a cluster. The router ID of the route reflector is the ID of the cluster. You can configure multiple route reflectors to improve the stability of the network. In this case, using this command can configure the identical cluster ID for all the route reflectors to avoid routing loops.

Related commands: **reflect between-clients** and **peer reflect-client**.

Examples # Set the cluster ID to 80.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] reflector cluster-id 80
```

refresh bgp

Syntax **refresh bgp** { **all** | *ip-address* | **group** *group-name* | **external** | **internal** } { **export** | **import** }

View User view

Parameters **all**: Soft-resets all BGP connections.

ip-address: Soft-resets the BGP connection to a peer.

group-name: Soft-resets connections to a peer group.

external: EBGP connection.

internal: IBGP connection.

export: Outbound soft reset.

import: Inbound soft reset.

Description Use the **refresh bgp** command to perform soft reset on specified BGP connections. Using this function can refresh the BGP routing table without tearing down BGP connections and apply a newly configured routing policy.

To perform BGP soft reset, all devices in the network must support route-refresh. If a device not supporting route-refresh exists in the network, you need to configure the **peer keep-all-routes** command to save all routing updates before performing soft reset.

Examples # Perform inbound BGP soft reset.

```
<Sysname> refresh bgp all import
```

reset bgp

Syntax **reset bgp** { **all** | *as-number* | *ip-address* [**flap-info**] | **group** *group-name* | **external** | **internal** }

View User view

Parameters **all**: Resets all BGP connections.

as-number: Resets BGP connections to peers in the AS.

ip-address: Specifies the IP address of a peer with which to reset the connection.

flap-info: Clears history information of routing flap.

group *group-name*: Specifies to reset connections with the specified BGP peer group.

external: Resets all the EBGP connections.

internal: Resets all the IBGP connections.

Description Use the **reset bgp** command to reset specified BGP connections.

Examples # Reset all the BGP connections.

```
<Sysname> reset bgp all
```

reset bgp dampening

Syntax **reset bgp dampening** [*ip-address* [*mask* | *mask-length*]]

View User view

Parameters *ip-address*: Destination IP address of a route.

mask: Mask, in dotted decimal notation.

mask-length: Mask length.

Description Use the **reset bgp dampening** command to clear route dampening information and release suppressed routes.

Related commands: **dampening**, **display bgp routing-table dampened**.

Examples # Clear damping information of route 20.1.0.0/16 and release suppressed route.

```
<Sysname> reset bgp dampening 20.1.0.0 255.255.0.0
```

reset bgp flap-info

Syntax **reset bgp flap-info** [**regexp** *as-path-regexp* | **as-path-acl** *as-path-acl-number* | *ip-address* [*mask* | *mask-length*]]

View User view

Parameters *as-path-regexp*: Clears the flap statistics of routes matching the AS path regular expression.

as-path-acl-number: Clears the flap statistics of routes matching an AS path ACL, number of which is in the range 1 to 256.

ip-address: Clears the flap statistics of a route.

mask: Network mask, in dotted decimal notation.

mask-length: Mask length.

Description Use the **reset bgp flap-info** command to clear the flap statistics of routes matching the specified filter.

The flap statistics of all the routes will be cleared if no parameter is specified.

Examples # Clear the flap statistics of all routes matching AS path ACL 10.

```
<Sysname> reset bgp flap-info as-path-acl 10
```

reset bgp ipv4 all

Syntax **reset bgp ipv4 all**

View User view

Parameters None

Description Use the **reset bgp ipv4 all** command to reset all the BGP connections of IPv4 unicast address family.

Examples # Reset all the BGP connections of IPv4 unicast address family.

```
<Sysname> reset bgp ipv4 all
```

router-id (BGP view)

Syntax **router-id** *router-id*

undo router-id

View BGP view

Parameters *router-id*: Router ID in IP address format.

Description Use the **router-id** command to specify a router ID.

Use the **undo router-id** command to remove the router ID.

To run BGP, the device must have a router ID, which is an unsigned 32-bit integer, the unique ID of the device in the AS.

You can specify a router ID manually. If not, the system selects an IP address as the router ID. The selection sequence is the highest IP address among loopback interface addresses; if not available, then the highest IP address of interfaces. It is recommended to specify a loopback interface address as the router ID to enhance network reliability.

Only when the interface with the selected Router ID or the manual Router ID is deleted will the system select another ID for the device.

Examples # Specifies the Router ID as 10.18.4.221.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] router-id 10.18.4.221
```

summary automatic

Syntax **summary automatic**

undo summary automatic

View BGP view/BGP-VPN instance view

Parameters None

Description Use the **summary automatic** command to enable automatic summarization for redistributed subnets.

Use the **undo summary automatic** command to disable automatic summarization.

By default, automatic summarization is disabled.

Note that:

- Neither the default route nor the routes imported using the **network** command can be summarized automatically.
- With this feature enabled, BGP limits the subnets redistribution from IGP to reduce the size of routing table.

Examples # In BGP view, enable automatic summarization.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] summary automatic
```

In BGP-VPN instance view, enable automatic summarization (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] summary automatic
```

synchronization (BGP view)

Syntax **synchronization**

undo synchronization

View BGP view

Parameters None

Description Use the **synchronization** command to enable the synchronization between BGP and IGP.

Use the **undo synchronization** command to disable the synchronization.

The feature is disabled by default.

With this feature enabled and when a non-BGP router is responsible for forwarding packets in an AS, BGP speakers in the AS cannot advertise routing information to other ASs unless all routers in the AS know the latest routing information.

When a BGP device receives an IBGP route, it checks only whether the next hop is reachable by default. If the synchronization is enabled, the IBGP route is synchronized and advertised to EBGP peers only when the route is also advertised by IGP. Otherwise, the IBGP route cannot be advertised to EBGP peers.

Examples # Enable the synchronization between BGP and IGP routes.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] synchronization
```

timer (BGP/BGP-VPN instance view)

Syntax **timer keepalive** *keepalive* **hold** *holdtime*

undo timer

View BGP view/BGP-VPN instance view

Parameters *keepalive*: Keepalive interval in seconds, ranging from 1 to 21845.

holdtime: Holdtime interval in seconds, ranging from 3 to 65535.

Description Use the **timer** command to configure BGP keepalive interval and holdtime interval.

Use the **undo timer** command to restore the default.

By default, BGP keepalive and holdtime intervals are 60s and 180s.

Note that:

- Timer configured using the **peer timer** command is preferred to the timer configured using this command.
- The holdtime interval must be at least three times the keepalive interval.
- The configured timer applies to all the BGP peers, while it becomes valid only after the corresponding BGP connections are reset.

Related commands: **peer timer**.

Examples # Configure keepalive interval and holdtime interval as 60s and 180s.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] timer keepalive 60 hold 180
```

In BGP-VPN instance view, configure keepalive interval and holdtime interval as 60s and 180s (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] timer keepalive 60 hold 180
```

40 IPv6 BGP CONFIGURATION COMMANDS

This chapter describes only configuration commands specific to IPv6 BGP. For BGP related information, refer to "BGP Configuration Commands" on page 537.

balance (IPv6 address family view)

Syntax **balance** *number*

undo balance

View IPv6 address family view

Parameters *number*: Number of BGP routes participating in load balancing. Its range varies with devices. When it is set to 1, load balancing is disabled.

Description Use the **balance** command to configure the number of routes participating in IPv6 BGP load balancing.

Use the **undo balance** command to restore the default.

The feature is not available by default.

Unlike IGP, BGP has no explicit metric for making load balancing decision. Instead, it implements load balancing by defining its routing rule.

Related commands: **display ipv6 routing-table**.

Examples # Set the number of routes participating in IPv6 BGP load balancing to 2.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] balance 2
```

bestroute as-path-neglect (IPv6 address family view)

Syntax **bestroute as-path-neglect**

undo bestroute as-path-neglect

View IPv6 address family view

Parameters None

Description Use the **bestroute as-path-neglect** command to configure the IPv6 BGP router to ignore AS_PATH during best route selection.

Use the **undo bestroute as-path-neglect** command to configure the IPv6 BGP router to use AS_PATH during best route selection.

By default, the router takes AS_PATH as a factor when selecting the best route.

Examples # Ignore AS_PATH in route selection.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] bestroute as-path-neglect
```

bestroute compare-med (IPv6 address family view)

Syntax **bestroute compare-med**

undo bestroute compare-med

View IPv6 address family view

Parameters None

Description Use the **bestroute compare-med** command to enable the comparison of the MED for paths from each AS.

Use the **undo bestroute compare-med** command to disable this comparison.

This comparison is not enabled by default.

Examples # Compare the MED for paths from an AS for selecting the best route.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] bestroute compare-med
```

bestroute med-confederation (IPv6 address family view)

Syntax **bestroute med-confederation**

undo bestroute med-confederation

View IPv6 address family view

Parameters None

Description Use the **bestroute med-confederation** command to enable the comparison of the MED for paths from confederation peers for best route selection.

Use the **undo bestroute med-confederation** command to disable the comparison.

By default, this comparison is not enabled.

With this feature enabled, the system can only compare the MED for paths from peers within the confederation. Paths from external ASs are advertised throughout the confederation without MED comparison.

Examples # Compare the MED for paths from peers within the confederation.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] bestroute med-confederation
```

compare-different-as-med (IPv6 address family view)

Syntax **compare-different-as-med**

undo compare-different-as-med

View IPv6 address family view

Parameters None

Description Use the **compare-different-as-med** command to enable the comparison of the MED for paths from peers in different ASs.

Use the **undo compare-different-as-med** command to disable the comparison.

The comparison is disabled by default.

If there are several paths available for one destination, the path with the smallest MED value is selected.

Do not use this command unless associated ASs adopt the same IGP protocol and routing selection method.

Examples # Enable to compare the MED for paths from peers in different ASs.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] compare-different-as-med
```

dampening (IPv6 address family view)

Syntax **dampening** [*half-life-reachable half-life-unreachable reuse suppress ceiling* | **route-policy** *route-policy-name*] *

undo dampening

View IPv6 address family view

Parameters *half-life-reachable*: Half-life for reachable routes in minutes. By default, the value is 15 minutes.

half-life-unreachable: Half-life for unreachable routes in minutes. By default, the value is 15 minutes.

reuse: Reuse threshold value for suppressed routes. Penalty value of a suppressed route decreasing under the value is reused. By default, the value is 750.

suppress: Suppression threshold, which should be bigger than the *reuse* value. Routes with a penalty value bigger than the threshold are suppressed. By default, it is 2000.

ceiling: Ceiling penalty value. The value must be bigger than the *suppress* value. By default, the value is 16000.

route-policy-name: Routing policy name.

*half-life-reachable, half-life-unreachable, reuse, suppres*s and *ceiling* are mutually dependent. Once any one is configured, all the others should also be specified accordingly.

Description Use the **dampening** command to enable IPv6 BGP route dampening or/and configure dampening parameters.

Use the **undo dampening** command to disable route dampening.

By default, no route dampening is configured.

Related commands: **reset bgp ipv6 dampening**, **reset bgp ipv6 flap-info**, **display bgp ipv6 routing-table dampened**, **display bgp ipv6 routing-table dampening parameter** and **display bgp ipv6 routing-table flap-info**.

Examples # Enable IPv6 BGP route dampening and configure route dampening parameters.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] dampening 10 10 1000 2000 3000
```

debugging bgp update ipv6

Syntax **debugging bgp update ipv6** [**peer** { *ipv6-address* | *group-name* } | **ip-prefix** *ipv6-prefix-name*] [**receive** | **send**] [**verbose**]

undo debugging bgp update ipv6 [**peer** { *ipv6-address* | *group-name* } | **ip-prefix** *ipv6-prefix-name*] [**receive** | **send**] [**verbose**]

View User view

Parameters **peer**: Debugs the IPv6 BGP updates of the peer or peer group.

ipv6-address: Debugs the IPv6 BGP updates of the peer.

group-name: Debugs the IPv6 BGP updates of the peer group.

ip-prefix *ipv6-prefix-name*: Debugging information passing the IPv6 prefix list.

receive: Debugs the received IPv6 BGP updates.

send: Debugs the sent IPv6 BGP updates.

verbose: Debugs the detailed IPv6 BGP updates.

Description Use the **debugging bgp update ipv6** command to debug received or sent IPv6 BGP updates.

Examples # Debug IPv6 BGP updates.

```
<Sysname> debugging bgp update ipv6
```

default local-preference (IPv6 address family view)

Syntax **default local-preference** *value*

undo default local-preference

View IPv6 address family view

Parameters *value*: Default local preference. The larger the value is, the higher the preference is. The default is 100.

Description Use the **default local-preference** command to configure the default local preference.

Use the **undo default local-preference** command to restore the default value.

Use this command to affect IPv6 BGP route selection.

Examples # Two devices A and B in the same AS are connected to another AS. Change the local preference of B from default value 100 to 180, making the route passing B preferred.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] default local-preference 180
```

default med (IPv6 address family view)

Syntax **default med** *med-value*

undo default med

View IPv6 address family view

Parameters *med-value*: MED value. The default is 0.

Description Use the **default med** command to specify the default MED value.

Use the **undo default med** command to restore the default.

By default, the default *med-value* is 0.

The multi-exit discriminator (MED) is an external metric of a route. Different from local preference, MED is exchanged between ASs and will stay in the AS once it enters the AS. The route with a lower MED is preferred. When a device running BGP obtains several routes with the identical destination and different next-hops from various external peers, it will select the best route depending on the MED value. In the case that all other conditions are the same, the system first selects the route with the smaller MED value as the best route for the autonomous system.

Examples # Devices A and B belong to AS100 and device C belongs to AS200. C is the peer of A and B. Configure the MED of A as 25 to make C select the path from B.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] default med 25
```

default-route imported

Syntax **default-route imported**

undo default-route imported

View IPv6 address family view

Parameters None

Description Use the **default-route imported** command to enable the redistribution of default route into the IPv6 BGP routing table.

Use the **undo default-route imported** command to disable the redistribution.

By default, the redistribution is not enabled.

Examples # Enable the redistribution of default route from OSPFv3 into IPv6 BGP.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] default-route imported
[Sysname-bgp-af-ipv6] import-route ospfv3 1
```

display bgp ipv6 group

Syntax **display bgp ipv6 group** [*ipv6-group-name*]

View Any view

Parameters *ipv6-group-name*: IPv6 peer group name.

Description Use the **display bgp ipv6 group** command to display IPv6 peer group information.

If no *ipv6-group-name* is specified, information about all peer groups is displayed.

Examples # Display the information of the IPv6 peer group "aaa".

```
<Sysname> display bgp ipv6 group aaa

 BGP peer-group is aaa
 remote AS number not specified
 Type : external
 Maximum allowed prefix number: 4294967295
 Threshold: 75%
 Configured hold timer value: 180
 Keepalive timer value: 60
 Minimum time between advertisement runs is 30 seconds
 Peer Preferred Value: 0
 No routing policy is configured
  Members:
  Peer        V    AS  MsgRcvd  MsgSent  OutQ PrefRcv Up/Down  State

  20:20::20:1  4   200       170       141      0        2 02:13:35 Established
```

Table 158 Field descriptions of the display bgp ipv6 group command

Field	Description
BGP peer-group	Name of the peer group
remote AS	AS number of the peer group
Type	Type of the peer group
Maximum allowed prefix number	Maximum allowed prefix number
Threshold	Threshold value

Table 158 Field descriptions of the display bgp ipv6 group command

Field	Description
hold timer value	Holdtime
Keepalive timer value	Keepalive interval
Minimum time between advertisement runs	Minimum interval between advertisements
Peer Preferred Value	Preferred value of the routes from the peer
No routing policy is configured	No routing policy is configured for the peer
Members	Group members
Peer	IPv6 address of the peer
V	Peer BGP version
AS	AS number
MsgRcvd	Number of messages received
MsgSent	Number of messages sent
OutQ	Number of messages to be sent
PrefRcv	Number of prefixes received
Up/Down	The lasting time of a session/the lasting time of present state (when no session is established)
State	State machine of peer

display bgp ipv6 network

Syntax **display bgp ipv6 network**

View Any view

Parameters None

Description Use the **display bgp ipv6 network** command to display IPv6 routes advertised with the **network** command.

Examples # Display IPv6 routes advertised with the **network** command.

```
<Sysname> display bgp ipv6 network
  BGP Local Router ID is 1.1.1.2.
  Local AS Number is 200.
  Network          Mask            Route-policy        Short-cut

  2002::           64
  2001::           64                                  Short-cut
```

Table 159 Field descriptions of the display bgp ipv6 network command

Field	Description
BGP Local Router ID	BGP Local Router ID
Local AS Number	Local AS Number

Table 159 Field descriptions of the display bgp ipv6 network command

Field	Description
Network	Network address
Prefix	Prefix length
Route-policy	Routing policy
Short-cut	Shortcut route

display bgp ipv6 paths

Syntax **display bgp ipv6 paths** [*as-regular-expression*]

View Any view

Parameters *as-regular-expression*: AS path regular expression.

Description Use the **display bgp ipv6 paths** command to display IPv6 BGP path information.

If no parameter is specified, all path information will be displayed.

Examples # Display IPv6 BGP path information.

```
<Sysname> display bgp ipv6 paths

    Address        Hash     Refcount  MED          Path/Origin
    0x5917098      1        1          0             i
    0x59171D0      9        2          0             100i
```

Table 160 Field descriptions of the display bgp ipv6 paths command

Field	Description	
Address	Route destination address in local database, in dotted hexadecimal notation	
Hash	Hash index	
Refcount	Count of routes that used the path	
MED	MED of the path	
Path	AS_PATH attribute of the path, recording the ASs it has passed, for avoiding routing loops	
Origin	Origin attribute of the route, which can take on one of the following values:	
	i	Indicates the route is interior to the AS. Summary routes and routes defined using the **network** command are considered IGP routes.
	e	Indicates that a route is learned from the exterior gateway protocol (EGP).
	?	Short for INCOMPLETE. It indicates that the origin of a route is unknown and the route is learned by other means. BGP sets Origin attribute of routes learned from other IGP protocols to INCOMPLETE.

display bgp ipv6 peer

Syntax **display bgp ipv6 peer** [*ipv6-address* { **log-info** | **verbose** } | *ipv6-group-name* **log-info** | **verbose**]

View Any view

Parameters *ipv6-address*: IPv6 address of a peer to be displayed.

ipv6-group-name: Name of an IPv4 or IPv6 peer group.

log-info: Displays log information of the specified peer.

verbose: Displays the detailed information of the peer.

Description Use the **display bgp ipv6 peer** command to display peer/peer group information.

If no parameter specified, information about all peers and peer groups is displayed.

Examples # Display all IPv6 peer information.

```
<Sysname> display bgp ipv6 peer

 BGP Local router ID : 20.0.0.1
 local AS number : 100
Total number of peers : 1                 Peers in established state : 1

Peer      V    AS  MsgRcvd  MsgSent  OutQ PrefRcv  Up/Down    State

20::21    4   200  17       19       0          3  00:09:59   Established
```

Table 161 Field descriptions of the display bgp ipv6 peer command

Field	Description
Peer	IPv6 address of the peer
V	Peer BGP version
AS	AS number
MsgRcvd	Messages received
MsgSent	Messages sent
OutQ	Messages to be sent
PrefRcv	Number of prefixes received
Up/Down	The lasting time of a session/the lasting time of present state (when no session is established)
State	Peer state

display bgp ipv6 routing-table

Syntax **display bgp ipv6 routing-table** [*ipv6-address prefix-length*]

View Any view

Parameters *ipv6-address*: Destination IPv6 address.

prefix-length: Prefix length of the IPv6 address.

Description Use the **display bgp ipv6 routing-table** command to display IPv6 BGP routing table information.

Examples # Display the IPv6 BGP routing table.

```
<Sysname> display bgp ipv6 routing-table

 Total Number of Routes: 2

 BGP Local router ID is 30.30.30.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 *>  Network : 30:30::                                  PrefixLen : 64
     NextHop : 30:30::30:1                              LocPrf    :
     PrefVal : 0                                        Label     : NULL
     MED      : 0
     Path/Ogn: i

 *>  Network : 40:40::                                  PrefixLen : 64
     NextHop : 40:40::40:1                              LocPrf    :
     PrefVal : 0                                        Label     : NULL
     MED     : 0
     Path/Ogn: i
```

Table 162 Field descriptions of the display bgp ipv6 routing-table command

Field	Description
Local router ID	Local router ID
Status codes	Status codes:
	* - valid
	> - best
	d - damped
	h - history
	i - internal (IGP)
	s - summary suppressed (suppressed)
	S - Stale
Origin	i - IGP (originated in the AS)
	e - EGP (learned through EGP)
	? - incomplete (learned by other means)
Network	Destination network address
PrefixLen	Prefix length
NextHop	Next Hop
MED	MULTI_EXIT_DISC attribute
LocPrf	Local preference value
Path	AS_PATH attribute, recording the ASs the packet has passed to avoid routing loops
PrefVal	Preferred value
Label	Label

Table 162 Field descriptions of the display bgp ipv6 routing-table command

Field	Description
Ogn	Origin attribute of the route, which can take on one of the following values: i Indicates that a route is interior to the AS. Summary routes and the routes configured using the **network** command are considered IGP routes. e Indicates that a route is learned from the exterior gateway protocol (EGP). ? Short for INCOMPLETE. It indicates that the origin of a route is unknown and the route is learned by other means. BGP sets Origin attribute of routes learned from other IGP protocols to INCOMPLETE.

display bgp ipv6 routing-table as-path-acl

Syntax **display bgp ipv6 routing-table as-path-acl** *as-path-acl-number*

View Any view

Parameters *as-path-acl-number*: Number of an AS path ACL.

Description Use the **display bgp ipv6 routing-table as-path-acl** command to display routes permitted by the specified AS path ACL.

Examples # Display routes passing through the AS path ACL 20.

```
<Sysname> display bgp ipv6 routing-table as-path-acl 20
 BGP Local router ID is 30.30.30.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 *>  Network : 30:30::                                  PrefixLen : 64
     NextHop : 30:30::30:1                              LocPrf    :
     PrefVal : 0                                        Label     : NULL
     MED     : 0
     Path/Ogn: i
```

Refer to Table 162 for description on the fields above.

display bgp ipv6 routing-table community

Syntax **display bgp ipv6 routing-table community** [*aa:nn*&<1-13>] [**no-advertise** | **no-export** | **no-export-subconfed**] * [**whole-match**]

View Any view

Parameters *aa:nn*: Community number.

&<1-13>: Indicates the argument before it can be entered up to 13 times.

no-advertise: Displays routes not advertised to any peer.

no-export: Displays routes advertised outside the AS; if there is a confederation, it displays routes not advertised outside the confederation, but to other sub ASs in the confederation.

no-export-subconfed: Displays routes neither advertised outside the AS nor to other sub ASs if the confederation is configured.

whole-match: Displays the exactly matched routes.

Description Use the **display bgp ipv6 routing-table community** command to display the routing information of the specified community.

Examples # Display the routing information of the community no-export.

```
<Sysname> display bgp ipv6 routing-table community no-export
BGP Local router ID is 30.30.30.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 *>  Network : 30:30::                                  PrefixLen : 64
     NextHop : 30:30::30:1                              LocPrf    :
     PrefVal : 0                                          Label     : NULL
     MED     : 0
     Path/Ogn: i
```

Refer to Table 162 for description on the fields above.

display bgp ipv6 routing-table community-list

Syntax **display bgp ipv6 routing-table community-list** { *basic-community-list-number* [**whole-match**] | *adv-community-list-number* }&<1-16>

View Any view

Parameters *basic-community-list-number*: Basic community-list number, in the range 1 to 99.

adv-community-list-number: Advanced community-list number, in the range 100 to 199.

whole-match: Displays routes exactly matching the specified *basic-community-list-number*.

&<1-16>: Specifies to allow entering the argument before it up to 16 times.

Description Use the **display bgp ipv6 routing-table community-list** command to view the routing information matching the specified IPv6 BGP community list.

Examples # Display the routing information matching the specified IPv6 BGP community list.

```
<Sysname> display bgp ipv6 routing-table community-list 99
BGP Local router ID is 30.30.30.1
```

```
Status codes: * - valid, > - best, d - damped,
              h - history,  i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete

*>  Network : 30:30::                                   PrefixLen : 64
    NextHop : 30:30::30:1                               LocPrf    :
    PrefVal : 0                                           Label     : NULL
    MED     : 0
    Path/Ogn: i
```

Refer to Table 162 for description on the fields above.

display bgp ipv6 routing-table dampened

Syntax **display bgp ipv6 routing-table dampened**

View Any view

Parameters None

Description Use the **display bgp ipv6 routing-table dampened** command to display the IPv6 BGP dampened routes.

Examples # Display IPv6 BGP dampened routes.

```
<Sysname> display bgp ipv6 routing-table dampened

BGP Local router ID is 1.1.1.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 *d  Network : 111::                                  PrefixLen : 64
     From    : 122::1                                   Reuse     : 00:29:34
     Path/Ogn: 200?
```

Table 163 Field descriptions of the display bgp ipv6 routing-table dampened command

Field	Description
From	Source IP address of a route
Reuse	Time for reuse

Refer to Table 162 for description on the fields above.

display bgp ipv6 routing-table dampening parameter

Syntax **display bgp ipv6 routing-table dampening parameter**

View Any view

Parameters None

Description Use the **display bgp ipv6 routing-table dampening parameter** command to display IPv6 BGP routing dampening parameters.

Related commands: **dampening**.

Examples # Display IPv6 BGP routing dampening parameters.

```
<Sysname> display bgp ipv6 routing-table dampening parameter
 Maximum Suppress Time(in second)     : 3069
 Ceiling Value                        : 16000
 Reuse Value                          : 750
 HalfLife Time(in  second)            : 900
 Suppress-Limit                       : 2000
```

Table 164 Description on the above fields

Field	Description
Maximum Suppress Time	Maximum Suppress Time
Ceiling Value	Upper limit of penalty value
Reuse Value	Reuse Value
HalfLife Time	Half life Time
Suppress-Limit	Suppress value

display bgp ipv6 routing-table different-origin-as

Syntax **display bgp ipv6 routing-table different-origin-as**

View Any view

Parameters None

Description Use the **display bgp ipv6 routing-table different-origin-as** command to display IPv6 BGP routes originating from different autonomous systems.

Examples # Display routes from different ASs.

```
<Sysname> display bgp ipv6 routing-table different-origin-as

BGP Local router ID is 2.2.2.2
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 *>  Network : 222::                                  PrefixLen : 64
     NextHop : 122::2                                 LocPrf    :
     PrefVal : 0                                      Label     : NULL
     MED     : 0
     Path/Ogn: 100 ?
```

Refer to Table 162 for description on the fields above.

display bgp ipv6 routing-table flap-info

Syntax **display bgp ipv6 routing-table flap-info** [**regular-expression** *as-regular-expression* | **as-path-acl** *as-path-acl-number* | *ipv6-address* [*prefix-length* [**longer-match**]]]

View Any view

Parameters *as-regular-expression*: AS path regular expression to be matched.

as-path-acl-number: Number of the specified AS path ACL to be matched.

ipv6-address: IPv6 address of a route to be displayed.

prefix-length: Prefix length of the IPv6 address.

longer-match: Matches the longest prefix.

Description Use the **display bgp ipv6 routing-table flap-info** command to display IPv6 BGP route flap statistics.

Examples # Display IPv6 BGP route flap statistics.

```
<Sysname> display bgp ipv6 routing-table flap-info

 BGP Local router ID is 1.1.1.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 *d  Network  : 111::                                PrefixLen : 64
     From     : 122::1                               Flaps     : 3
     Duration : 00:13:47                             Reuse     : 00:16:36
     Path/Ogn : 200?
```

Table 165 Field descriptions of the display bgp ipv6 routing-table flap-info command

Field	Description
Flaps	Number of flaps
Duration	Flap duration
Reuse	Reuse time of the route

Refer to Table 162 for description on the fields above.

display bgp ipv6 routing-table peer

Syntax **display bgp ipv6 routing-table peer** *ipv6-address* { **advertised-routes** | **received-routes** } [*network-address prefix-length* | **statistic**]

View Any view

Parameters *ipv6-address*: Specifies the IPv6 peer to be displayed.

advertised-routes: Routing information advertised to the specified peer.

received-routes: Routing information received from the specified peer.

network-address prefix-length: IPv6 address and prefix length.

statistic: Displays route statistics.

Description Use the **display bgp ipv6 routing-table peer** command to display the routing information advertised to or received from the specified IPv6 BGP peer.

Examples # Display the routing information advertised to the specified BGP peer.

```
<Sysname> display bgp ipv6 routing-table peer 10:10::10:1 advertised-routes
 Total Number of Routes: 2

 BGP Local router ID is 20.20.20.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 *>  Network : 20:20::                                  PrefixLen : 64
     NextHop : 20:20::20:1                              LocPrf    :
     PrefVal : 0                                        Label     : NULL
     MED     : 0
     Path/Ogn: i

 *>  Network : 40:40::                                  PrefixLen : 64
     NextHop : 30:30::30:1                              LocPrf    :
     PrefVal : 0                                        Label     : NULL
     MED     : 0
     Path/Ogn: 300 i
```

Refer to Table 162 for description on the fields above.

display bgp ipv6 routing-table regular-expression

Syntax **display bgp ipv6 routing-table regular-expression** *as-regular-expression*

View Any view

Parameters *as-regular-expression*: AS regular expression.

Description Use the **display bgp ipv6 routing-table regular-expression** command to display the routes permitted by the specified AS regular expression.

Examples # Display routing information matching the specified AS regular expression.

```
<Sysname> display bgp ipv6 routing-table regular-expression ^200

 BGP Local router ID is 20.20.20.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 *>  Network : 50:50::                                  PrefixLen : 64
     NextHop : 10:10::10:1                              LocPrf    :
     PrefVal : 0                                        Label     : NULL
     MED     : 0
     Path/Ogn: 100 i
```

Refer to Table 162 for description on the fields above.

display bgp ipv6 routing-table statistic

Syntax **display bgp ipv6 routing-table statistic**

View Any view

Parameters None

Description Use the **display bgp ipv6 routing-table statistic** command to display IPv6 BGP routing statistics.

Examples # Display IPv6 BGP routing statistics.

```
<Sysname> display bgp ipv6 routing-table statistic

 Total Number of Routes: 1
```

filter-policy export(IPv6 address family view)

Syntax **filter-policy** { *acl6-number* | **ipv6-prefix** *ipv6-prefix-name* } **export** [*protocol process-id*]

undo filter-policy export [*protocol process-id*]

View IPv6 address family view

Parameters *acl6-number*: Specifies the number of an ACL6 used to match against the destination of routing information.

ipv6-prefix-name: Specifies the name of an IPv6 prefix list used to match against the destination address field of routing information.

protocol: Filters routes redistributed from the routing protocol. It can be **direct**, **isisv6**, **ospfv3**, **ripng**, and **static** at present. If no protocol is specified, all routes will be filtered when advertised.

process-id: Process ID of the routing protocol. It is available only when the protocol is **isisv6**, **ospfv3** or **ripng**.

Description Use the **filter-policy export** command to filter outbound routes using a specified filter.

Use the **undo filter-policy export** command to cancel filtering outbound routes.

By default, no outbound routing information is filtered.

If a protocol is specified, only routes redistributed from the specified protocol are filtered. If no protocol is specified, all redistributed routes will be filtered.

Examples # Reference ACL6 2001 to filter all outbound IPv6 BGP routes.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] filter-policy 2001 export
```

filter-policy import (IPv6 address family view)

Syntax **filter-policy** { *acl6-number* | **ipv6-prefix** *ipv6-prefix-name* } **import**

undo filter-policy import

View IPv6 address family view

Parameters *acl6-number*: Number of an IPv6 ACL used to match against the destination address field of routing information.

ipv6-prefix-name: Name of an IPv6 prefix list used to match against the destination address field of routing information.

Description Use the **filter-policy import** command to configure the filtering of inbound IPv6 BGP routing information using a specified filter.

Use the **undo filter-policy import** command to remove the filtering of IPv6 BGP inbound routing information.

By default, no inbound IPv6 BGP routing information is filtered.

Examples # Reference ACL6 2001 to filter all inbound IPv6 BGP routes.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] filter-policy 2001 import
```

group (IPv6 address family view)

Syntax **group** *ipv6-group-name* [**internal** | **external**]

undo group *ipv6-group-name*

View IPv6 address family view

Parameters *ipv6-group-name*: Name of an IPv6 peer group.

internal: Creates an IBGP peer group.

external: Creates an EBGP peer group, which can be a group of another sub AS in the confederation.

Description Use the **group** command to create a peer group.

Use the **undo group** command to delete a peer group.

An IBGP peer group will be created if neither **internal** nor **external** is selected.

Examples # Create an IBGP peer group named "test".

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname] ipv6-family
[Sysname-bgp-af-ipv6] group test
```

import-route (IPv6 address family view)

Syntax **import-route** *protocol* [*process-id* [**med** *med-value* | **route-policy** *route-policy-name*] *]

undo import-route *protocol* [*process-id*]

View IPv6 address family view

Parameters *protocol*: Redistributes routes from the protocol, which can be **direct**, **isisv6**, **ospfv3**, **ripng** and **static** at present.

process-id: Process ID. It is available only when the protocol is **isisv6**, **ospfv3** or **ripng**.

med-value: Applies the MED value to redistributed routes. If not specified, the cost of the redistributed route is used as its MED in the IPv6 BGP routing domain.

route-policy-name: Name of a routing policy used to filter redistributed routes.

Description Use the **import-route** command to redistribute routes from another routing protocol.

Use the **undo import-route** command to remove the configuration.

By default, IPv6 BGP does not redistribute routes from any routing protocol.

The routes redistributed using the **import-route** command has the incomplete origin attribute.

Examples # Redistribute routes from RIPng 1.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] import-route ripng 1
```

ipv6-family

Syntax **ipv6-family**

undo ipv6-family

View BGP view

Parameters None

Description Use the **ipv6-family** command to enter BGP IPv6 address family view.

Use the **undo ipv6-family** command to exit BGP IPv6 address family view and remove all configurations from the view.

IPv4 BGP unicast view is the default.

Examples # Enter BGP IPv6 address family view.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6]
```

network (IPv6 address family view)

Syntax **network** *ipv6-address prefix-length* [**short-cut** | **route-policy** *route-policy-name*]

undo network *ipv6-address prefix-length* [**short-cut**]

View IPv6 address family view

Parameters *ipv6-address*: IPv6 address.

prefix-length: Prefix length.

short-cut: If the keyword is specified for an EBGP route, the route will use the local routing management value rather than that of EBGP routes, and the preference of the route is reduced to 130.

route-policy-name: Name of a routing policy.

Description Use the **network** command to advertise a network to the IPv6 BGP routing table.

Use the **undo network** command to remove an entry from the IPv6 BGP routing table.

By default, no route is advertised.

Note that:

- The route to be advertised must exist in the local IP routing table, and using a routing policy makes route management more flexible.
- The route advertised to the BGP routing table using the **network** command has the IGP origin attribute.

Examples # Advertise the network 2002::/16 into the IPv6 BGP routing table.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] network 2002:: 16
```

peer advertise-community (IPv6 address family view)

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **advertise-community**

undo peer { *ipv6-group-name* | *ipv6-address* } **advertise-community**

View IPv6 address family view

Parameters *ipv6-group-name*: Name of an IPv6 peer group.

ipv6-address: IPv6 address of a peer.

Description Use the **peer advertise-community** command to advertise the community attribute to a peer/peer group.

Use the **undo peer advertise-community** command to remove the configuration.

By default, no community attribute is advertised to any peer group/peer.

Examples # Advertise the community attribute to the peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 advertise-community
```

peer advertise-ext-community (IPv6 address family view)

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **advertise-ext-community**

undo peer { *ipv6-group-name* | *ipv6-address* } **advertise-ext-community**

View IPv6 address family view

Parameters *ipv6-group-name*: Name of an IPv6 peer group.

ipv6-address: IPv6 address of a peer.

Description Use the **peer advertise-ext-community** command to advertise the extended community attribute to a peer/peer group.

Use the **undo peer advertise-ext-community** command to remove the configuration.

By default, no extended community attribute is advertised to a peer/peer group.

Examples # Advertise the extended community attribute to the peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 advertise-ext-community
```

peer allow-as-loop (IPv6 address family view)

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **allow-as-loop** [*number*]

undo peer { *ipv6-group-name* | *ipv6-address* } **allow-as-loop**

View IPv6 address family view

Parameters *ipv6-group-name*: Name of an IPv6 peer group.

ipv6-address: IPv6 address of a peer.

number: Specifies the repeating times of the local AS number. The default number is 1.

Description Use the **peer allow-as-loop** command to configure IPv6 BGP to allow the local AS number to exist in the AS_PATH attribute of routes from a peer/peer group, and to configure the repeating times of the local AS number.

Use the **undo peer allow-as-loop** command to disable the function.

The local AS number is not allowed to exist in the AS PATH attribute of routes by default.

Examples # Configure the repeating times of the local AS number allowed in the AS PATH of routes from peer 1::1 as 2.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1::1 allow-as-loop 2
```

peer as-number (IPv6 address family view)

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **as-number** *as-number*

undo peer *ipv6-group-name* **as-number**

undo peer *ipv6-address*

View IPv6 address family view

Parameters *ipv6-group-name*: Name of an IPv6 peer group.

ipv6-address: IPv6 address of a peer.

as-number: AS number of the peer/peer group.

Description Use the **peer as-number** command to specify an AS number for an IPv6 peer/peer group.

Use the **undo peer as-number** command to delete the AS number of an IPv6 peer group.

Use the **undo peer** command to delete a peer.

By default, no AS number is configured for a peer/peer group.

Examples # Specify the AS number of the peer group test as 100.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-af-ipv6] peer test as-number 100
```

peer as-path-acl (IPv6 address family view)

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **as-path-acl** *as-path-acl-number* { **import** | **export** }

undo peer { *ipv6-group-name* | *ipv6-address* } **as-path-acl** *as-path-acl-number* { **import** | **export** }

View IPv6 address family view

Parameters *ipv6-group-name*: Name of an IPv6 peer group.

ipv4-address: IPv4 address of a peer.

ipv6-address: IPv6 address of a peer.

as-path-acl-number: Number of an AS path ACL.

import: Filters incoming routes.

export: Filters outgoing routes.

Description Use the **peer as-path-acl** command to specify an AS path ACL to filter routes incoming from or outgoing to a peer/peer group.

Use the **undo peer as-path-acl** command to remove the configuration.

By default, no AS path list is specified for filtering.

Examples # Specify the AS path ACL 3 to filter routes outgoing to the peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 as-path-acl 3 export
```

peer capability-advertise route-refresh

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **capability-advertise route-refresh**

undo peer { *ipv6-group-name* | *ipv6-address* } **capability-advertise route-refresh**

View IPv6 address family view

Parameters *ipv6-group-name*: Name of an IPv6 peer group.

ipv6-address: IPv6 address of a peer.

Description Use the **peer capability-advertise route-refresh** command to enable IPv6 BGP route-refresh.

Use the **undo peer capability-advertise route-refresh** command to disable the function.

By default, route-refresh is enabled.

Examples # Disable route-refresh of peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 as-number 100
[Sysname-bgp-af-ipv6] undo peer 1:2::3:4 capability-advertise route-refresh
```

peer connect-interface (IPv6 address family view)

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **connect-interface** *interface-type interface-number*

undo peer { *ipv6-group-name* | *ipv6-address* } **connect-interface**

View IPv6 address family view

Parameters *ipv6-group-name*: Name of an IPv6 peer group.

ipv6-address: IPv6 address of a peer.

interface-type interface-number: Specifies the type and name of the interface.

Description Use the **peer connect-interface** command to specify the source interface of updates to a peer/peer group.

Use the **undo peer connect-interface** command to restore the source interface of the best update.

By default, IPv6 BGP uses the source interface of the best update.

For updates to be forwarded in case the interface experiences a failure, you can configure a Loopback interface as the source to forward routing updates.

Examples # Specify loopback0 as the source interface for sending routing updates to peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-af-ipv6] peer 1:1::1:1 connect-interface loopback 0
```

peer default-route-advertise (IPv6 address family view)

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **default-route-advertise** [**route-policy** *route-policy-name*]

undo peer { *ipv6-group-name* | *ipv6-address* } **default-route-advertise**

View IPv6 address family view

Parameters *ipv6-group-name*: Name of an IPv6 peer group.

ipv6-address: IPv6 address of a peer.

route-policy-name: Routing policy name.

Description Use the **peer default-route-advertise** command to advertise a default route to a peer/peer group.

Use the **undo peer default-route-advertise** command to disable advertising a default route.

By default, no default route is advertised to a peer/peer group.

Using this command does not require the default route available in the routing table. With this command used, the router sends the default route unconditionally to the peer/peer group with the next hop being itself.

Examples # Advertise a default route to peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 default-route-advertise
```

peer description (IPv6 address family view)

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **description** *description-text*

undo peer { *ipv6-group-name* | *ipv6-address* } **description**

View IPv6 address family view

Parameters *ipv6-group-name*: Name of a IPv6 peer group.

ipv6-address: IPv6 address of a peer.

description-text: Description information for the peer/peer group.

Description Use the **peer description** command to configure the description information for a peer/peer group.

Use the **undo peer description** command to remove the description information of a peer/peer group.

By default, no description information is configured for a peer (group).

You need create a peer/peer group before configuring a description for it.

Examples # Configure the description for the peer group "test" as ISP1.

```
<Sysname] system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test external
[Sysname-bgp-af-ipv6] peer test description ISP1
```

peer ebgp-max-hop (IPv6 address family view)

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **ebgp-max-hop** [*hop-count*]

undo peer { *ipv6-group-name* | *ipv6-address* } **ebgp-max-hop**

View IPv6 address family view

Parameters *ipv6-group-name*: Name of an IPv6 peer group.

ipv6-address: IPv6 address of a peer.

hop-count: Maximum hop count. By default, the value is 64.

Description Use the **peer ebgp-max-hop** command to allow establishing the EBGP connection to a peer/peer group indirectly connected.

Use the **undo peer ebgp-max-hop** command to remove the configuration.

By default, this feature is disabled.

You can use the argument *hop-count* to specify the maximum router hops of the EBGP connection.

Examples # Allow establishing the EBGP connection with the peer group "test" on an indirectly connected network.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test external
[Sysname-bgp-af-ipv6] peer test ebgp-max-hop
```

peer fake-as (IPv6 address family view)

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **fake-as** *as-number*

undo peer { *ipv6-group-name* | *ipv6-address* } **fake-as**

View IPv6 address family view

Parameters *ipv6-group-name*: Name of an IPv6 peer group.

ipv6-address: IPv6 address of a peer.

as-number: Local autonomous system number.

Description Use the **peer fake-as** command to configure a fake local AS number for a peer or peer group.

Use the **undo peer fake-as** command to remove the configuration.

By default, no fake local AS number is configured for a peer or peer group.

Examples # Configure a fake AS number of 200 for the peer group test.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test external
[Sysname-bgp-af-ipv6] peer test fake-as 200
```

peer filter-policy (IPv6 address family view)

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **filter-policy** *acl6-number* { **import** | **export** }

undo peer { *ipv6-group-name* | *ipv6-address* } **filter-policy** [*acl6-number*] { **import** | **export** }

View IPv6 address family view

Parameters *ipv6-group-name*: Name of an IPv6 peer group.

ipv6-address: IPv6 address of a peer.

acl6-number: IPv6 ACL number.

import: Applies the filter-policy to routes received from the peer/peer group.

export: Applies the filter-policy to routes advertised to the peer/peer group.

Description Use the **peer filter-policy** command to configure an ACL-based filter policy for a peer or peer group.

Use the **undo peer filter-policy** command to remove the configuration.

By default, no ACL-based filter policy is configured for a peer or peer group.

Examples # Apply the ACL6 2000 to filter routes advertised to the peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule permit source 2001:1:: 64
[Sysname-acl6-basic-2000] quit
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 filter-policy 2000 export
```

peer group (IPv6 address family view)

Syntax **peer** *ipv6-address* **group** *ipv6-group-name* [**as-number** *as-number*]

undo peer *ipv6-address* **group** *ipv6-group-name*

View IPv6 address family view

Parameters *ipv6-group-name*: Name of an IPv6 peer group.

ipv6-address: IPv6 address of a peer.

as-number: AS number of the peer/peer group.

Description Use the **peer group** command to add a peer to a configured peer group.

Use the **undo peer group** command to delete a specified peer from a peer group.

By default, the peer does not belong to any peer group.

Examples # Create a peer group named "test" and add the peer 1:2::3:4 to the peer group.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test external
[Sysname-bgp-af-ipv6] peer 1:2::3:4 as-number 200
[Sysname-bgp-af-ipv6] peer 1:2::3:4 group test
```

peer ignore (IPv6 address family view)

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **ignore**

undo peer { *ipv6-group-name* | *ipv6-address* } **ignore**

View IPv6 address family view

Parameters *ipv6-group-name*: Name of an IPv6 peer group.

ipv6-address: IPv6 address of a peer.

Description Use the **peer ignore** command to terminate the session to a peer or peer group.

Use the **undo peer ignore** command to remove the configuration.

By default, a router can establish sessions with a peer or peer group.

After the **peer ignore** command is executed, the system terminates the active session(s) with the specified peer or peer group and clears all the related routing information. For a peer group, this means all the sessions with the peer group will be tore down.

Examples # Terminate the session with peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 ignore
```

peer ipv6-prefix

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **ipv6-prefix** *ipv6-prefix-name* { **import** | **export** }

undo peer { *ipv6-group-name* | *ipv6-address* } **ipv6-prefix** { **import** | **export** }

View IPv6 address family view

Parameters *ipv6-group-name*: Name of an IPv6 peer group.

ipv6-address: IPv6 address of a peer.

ipv6-prefix-name: IPv6 prefix list name.

import: Applies the filtering policy to routes received from the specified peer/peer group.

export: Applies the filtering policy to routes advertised to the specified peer/peer group.

Description Use the **peer ipv6-prefix** command to specify an IPv6 prefix list to filter routes incoming from or outgoing to a peer or peer group.

Use the **undo peer ipv6-prefix** command to remove the configuration.

By default, no IPv6 prefix list is specified for filtering.

Examples # Reference the IPv6 prefix list "list 1" to filter routes outgoing to peer 1:1::1:1.

```
<Sysname> system-view
[Sysname] ip ipv6-prefix list1 permit 2002:: 64
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:1::1:1 ipv6-prefix list1 export
```

peer keep-all-routes (IPv6 address family view)

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **keep-all-routes**

undo peer { *ipv6-group-name* | *ipv6-address* } **keep-all-routes**

View IPv6 address family view

Parameters *ipv6-group-name*: Name of an IPv6 peer group.

ipv6-address: IPv6 address of a peer.

Description Use the **peer keep-all-routes** command to save the original routing information from a peer or peer group, including even routes that failed to pass the inbound policy.

Use the **undo peer keep-all-routes** command to disable this function.

By default, the function is not enabled.

Examples # Save routing information from peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 keep-all-routes
```

peer log-change (IPv6 address family view)

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **log-change**

undo peer { *ipv6-group-name* | *ipv6-address* } **log-change**

View IPv6 address family view

Parameters *ipv6-group-name*: Name of an IPv6 peer group.

ipv6-address: IPv6 address of a peer.

Description Use the **peer log-change** command to enable the logging of session state and event information of a specified peer or peer group.

Use the **undo peer log-change** command to remove the configuration.

The logging is enabled by default.

Examples # Enable the logging of session state and event information of peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 log-change
```

peer next-hop-local (IPv6 address family view)

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **next-hop-local**

undo peer { *ipv6-group-name* | *ipv6-address* } **next-hop-local**

View IPv6 address family view

Parameters *ipv6-group-name*: Name of an IPv6 peer group.

ipv6-address: IPv6 address of a peer.

Description Use the **peer next-hop-local** command to configure the next hop of routes advertised to a peer/peer group as the local router.

Use the **undo peer next-hop-local** command to restore the default.

By default, the system sets the next hop of routes advertised to an EBGP peer/peer group to the local router, but does not set for routes outgoing to an IBGP peer/peer group.

Examples # Set the next hop of routes advertised to EBGP peer group "test" to the router itself.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test external
[Sysname-bgp-af-ipv6] peer test next-hop-local
```

peer preferred-value (IPv6 address family view)

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **preferred-value** *value*

undo peer { *ipv6-group-name* | *ipv6-address* } **preferred-value**

View IPv6 address family view

Parameters *ipv6-group-name*: Name of an IPv6 peer group.

ipv6-address: IPv6 address of a peer.

value: Preferred value.

Description Use the **peer preferred-value** command to assign a preferred value to routes received from a peer or peer group.

Use the **undo peer preferred-value** command to restore the default.

By default, routes received from a peer or peer group have a preferred value of 0.

Routes learned from peers each have an initial preferred value. Among multiple routes to the same destination, the route with the biggest value is selected.

Examples # Configure the preferred value as 50 for routes from peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 preferred-value 50
```

peer public-as-only (IPv6 address family view)

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **public-as-only**

undo peer { *ipv6-group-name* | *ipv6-address* } **public-as-only**

View IPv6 address family view

Parameters *ipv6-group-name*: Name of an IPv6 peer group.

ipv6-address: IPv6 address of a peer.

Description Use the **peer public-as-only** command to configure IPv6 BGP updates to a peer/peer group to not carry private AS numbers.

Use the **undo peer public-as-only** command to allow IPv6 BGP updates to a peer/peer group to carry private AS numbers.

By default, BGP updates carry the private AS number.

The command does not take effect if the BGP update has both the public AS number and private AS number. The range of private AS number is from 64512 to 65535.

Examples # Carry no private AS number in BGP updates sent to the peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 public-as-only
```

peer reflect-client (IPv6 address family view)

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **reflect-client**

undo peer { *ipv6-group-name* | *ipv6-address* } **reflect-client**

View IPv6 address family view

Parameters *ipv6-group-name*: Name of an IPv6 peer group.

ipv6-address: IPv6 address of a peer.

Description Use the **peer reflect-client** command to configure the router as a route reflector and specify a peer/peer group as a client.

Use the **undo peer reflect-client** command to remove the configuration.

By default, neither route reflector nor client is configured.

Related commands: **reflect between-clients** and **reflector cluster-id**.

Examples # Configure the local device as a route reflector and specify the peer group "test" as a client.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer test reflect-client
```

peer route-limit (IPv6 address family view)

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **route-limit** *limit* [*percentage*]

undo peer { *ipv6-group-name* | *ipv6-address* } **route-limit**

View IPv6 address family view

Parameters *group-name*: Name of an IPv6 peer group.

ipv6-address: IPv6 address of a peer.

limit: Upper limit of prefixes that can be received from the peer or peer group.

percentage: Percentage of routes to generate alarm information. The default is 75.

Description Use the **peer route-limit** command to set the maximum number of prefixes that can be received from a peer/peer group.

Use the **undo peer route-limit** command to restore the default.

By default, the router has no limit on prefixes from a peer/peer group.

If the received IPv6 prefixes exceed the upper limit, the neighbor is still maintained but the exceeding routes will be discarded.

Examples # Set the number of prefixes allowed to receive from the peer 1:2::3:4 to 10000.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 route-limit 10000
```

peer route-policy (IPv6 address family view)

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **route-policy** *route-policy-name* { **import** | **export** }

undo peer { *ipv6-group-name* | *ipv6-address* } **route-policy** *route-policy-name* { **import** | **export** }

View IPv6 address family view

Parameters *ipv6-group-name*: Name of an IPv6 peer group.

ipv6-address: IPv6 address of a peer.

route-policy-name: Routing policy name.

import: Applies the routing policy to routes from the peer (group).

export: Applies the routing policy to routes to the peer (group).

Description Use the **peer route-policy** command to apply a routing policy to routes incoming from or outgoing to a peer or peer group.

Use the **undo peer route-policy** command to remove the configuration.

By default, no routing policy is specified for the peer (group).

Use of the **peer route-policy** command does not apply the **if-match interface** clause defined in the routing policy. Refer to "Routing Policy Configuration Commands" on page 351 for related information.

Examples # Apply the routing policy test-policy to routes received from the peer group test.

```
<Sysname> system-view
[Sysname] route-policy test-policy permit node 10
[Sysname-route-policy] if-match cost 10
[Sysname-route-policy] apply cost 65535
[Sysname-route-policy] quit
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test external
[Sysname-bgp-af-ipv6] peer test route-policy test-policy import
```

peer route-update-interval (IPv6 address family view)

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **route-update-interval** *seconds*

undo peer { *ipv6-group-name* | *ipv6-address* } **route-update-interval**

View IPv6 address family view

Parameters *ipv6-group-name*: Name of an IPv6 peer group.

ipv6-address: IPv6 address of a peer.

seconds: Specifies the minimum interval in seconds for sending the same update to a peer (group) .

Description Use the **peer route-update-interval** command to specify the interval for sending the same update to a peer/peer group.

Use the **undo peer route-update-interval** command to restore the default.

By default, the interval is 15 seconds for the IBGP peer, and 30 seconds for the EBGP peer.

Examples # Specify the interval for sending the same update to the peer 1:2::3:4 as 10 seconds.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 as-number 100
[Sysname-bgp-af-ipv6] peer 1:2::3:4 route-update-interval 10
```

peer substitute-as (IPv6 address family view)

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **substitute-as**

undo peer { *ipv6-group-name* | *ipv6-address* } **substitute-as**

View IPv6 address family view

Parameters *ipv6-group-name*: Name of an IPv6 peer group.

ipv6-address: IPv6 address of a peer.

Description Use the **peer substitute-as** command to substitute the local AS number for the AS number of a peer/peer group in the AS_PATH attribute.

Use the **undo peer substitute-as** command to remove the configuration.

The substitution is not configured by default.

Examples # Substitute the local AS number for the AS number of peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 substitute-as
```

peer timer (IPv6 address family view)

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **timer keepalive** *keepalive* **hold** *holdtime*

undo peer { *ipv6-group-name* | *ipv6-address* } **timer**

View IPv6 address family view

Parameters *ipv6-group-name*: Name of an IPv6 peer group.

ipv6-address: IPv6 address of a peer.

keepalive: Specifies the keepalive interval in seconds.

holdtime: Specifies the holdtime in seconds.

Description Use the **peer timer** command to configure keepalive interval and holdtime interval for a peer or peer group.

Use the **undo peer timer** command to restore the default.

keepalive interval defaults to 60 seconds, and *holdtime* interval defaults to 180 seconds

Note that:

- The timer configured with this command is preferred to the timer configured with the **timer** command.
- The holdtime interval must be at least three times the keepalive interval.

Related commands: **timer**.

Examples # Configure the keepalive interval and holdtime interval for the peer group test as 60 seconds and 180 seconds.

```
<Sysname] system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test external
[Sysname-bgp-af-ipv6] peer test timer keep-alive 60 hold 180
```

preference (IPv6 address family view)

Syntax **preference** { *external-preference internal-preference local-preference* | **route-policy** *route-policy-name* }

undo preference

View IPv6 address family view

Parameters *external-preference*: Preference of the best EBGP routes learned from EBGP peers. The default is 255.

internal-preference: Preference of IBGP routes learned from IBGP peers.

local-preference: Preference of IPv6 BGP local routes.

route-policy-name: Routing policy name. The routing policy can set a preference for routes passing it. The default value applies to the routes filtered out.

Description Use the **preference** command to configure preferences for EBGP, IBGP, and local routes.

Use the **undo preference** command to restore the default.

The bigger the preference value is, the lower the preference is. The default values of *external-preference*, *internal-preference* and *local-preference* are 255, 255 and 130 respectively.

Examples # Configure preferences for EBGP, IBGP, and local routes as 20, 20 and 200.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] preference 20 20 200
```

reflect between-clients (IPv6 address family view)

Syntax **reflect between-clients**

undo reflect between-clients

View IPv6 address family view

Parameters None

Description Use the **reflect between-clients** command to enable route reflection between clients.

Use the **undo reflect between-clients** command to disable this function.

By default, route reflection between clients is enabled.

After a route reflector is configured, it reflects routes between clients. If the clients are fully meshed, it is recommended to disable route reflection on the route reflector to reduce costs.

Related commands: **reflector cluster-id** and **peer reflect-client**.

Examples # Enable route reflection between clients.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] reflect between-clients
```

reflector cluster-id (IPv6 address family view)

Syntax **reflector cluster-id** *cluster-id*

undo reflector cluster-id

View IPv6 address family view

Parameters *cluster-id*: Cluster ID of the route reflector, an integer or an IP address.

Description Use the **reflector cluster-id** command to configure the cluster ID of the route reflector.

Use the **undo reflector cluster-id** command to remove the configured cluster ID.

By default, a route reflector uses its router ID as the cluster ID.

Usually, there is only one route reflector in a cluster, so the router ID of the route reflector identifies the cluster. If multiple route reflectors are configured to improve the stability of the network, you should use this command to configure the identical cluster ID for all the reflectors to avoid routing loops.

Related commands: **reflect between-clients** and **peer reflect-client**.

Examples # Set 50 as the cluster ID for the route reflector, which is one of multiple route reflectors in the cluster.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] reflector cluster-id 50
```

refresh bgp ipv6

Syntax **refresh bgp ipv6** { **all** | *ipv6-address* | **group** *ipv6-group-name* | **external** | **internal** } { **export** | **import** }

View User view

Parameters **all**: Soft-resets all IPv6 BGP connections.

ipv6-address: Soft-resets the connection with an IPv6 BGP peer.

ipv6-group-name: Soft-resets connections with a peer group.

external: Soft-resets EBGP connections.

internal: Soft-resets IBGP connections.

export: Performs soft reset in outbound direction.

import: Performs soft reset in inbound direction.

Description Use the **refresh bgp ipv6** command to soft reset specified IPv4/IPv6 BGP connections. With this feature, you can refresh the IPv4/IPv6 BGP routing table and apply a new available policy without tearing down BGP connections.

To perform IPv4/IPv6 BGP soft reset, all routers in the network should support route-refresh. If a router not supporting route refresh exists in the network, you need to use the **peer keep-all-routes** command on the local router to save all route updates before performing soft reset.

Examples # Soft reset inbound IPv6 BGP connections.

```
<Sysname> refresh bgp ipv6 all import
```

reset bgp ipv6

Syntax **reset bgp ipv6** { **all** | *as-number* | *ipv6-address* [**flap-info**] | **group** *ipv6-group-name* | **external** | **internal** }

View User view

Parameters **all**: Resets all IPv6 BGP connections.

as-number: Resets the IPv6 BGP connections to peers in the specified AS.

ipv6-address: Resets the connection to the specified IPv6 BGP peer.

flap-info: Clears the history information of routing flaps.

group *ipv6-group-name*: Resets the connections to the specified IPv6 BGP peer group.

external: Resets all the EBGP connections.

internal: Resets all the IBGP connections.

Description Use the **reset bgp ipv6** command to reset specified IPv6 BGP connections.

Examples # Reset all the IPv6 BGP connections.

```
<Sysname> reset bgp ipv6 all
```

reset bgp ipv6 dampening

Syntax **reset bgp ipv6 dampening** [*ipv6-address prefix-length*]

View User view

Parameters *ipv6-address*: IPv6 address

prefix-length: Prefix length of the address.

Description Use the **reset bgp ipv6 dampening** command to clear dampened IPv6 BGP route information and release suppressed routes.

If no *ipv6-address prefix-length* is specified, all dampened IPv6 route information will be cleared.

Examples # Clear the damping information of routes to 2345::/64 and release suppressed routes.

```
<Sysname> reset bgp ipv6 dampening 2345:: 64
```

reset bgp ipv6 flap-info

Syntax **reset bgp ipv6 flap-info** [*ipv6-address/prefix-length* | **regexp** *as-path-regexp* | **as-path-acl** *as-path-acl-number*]

View User view

Parameters *ipv6-address*: Clears the flap statistics for the specified IPv6 address.

prefix-length: Prefix length of the address.

as-path-regexp: Clears the flap statistics for routes matching the AS path regular expression.

as-path-acl-number: Clears the flap statistics of routes matching the AS path ACL.

Description Use the **reset bgp ipv6 flap-info** command to clear IPv6 routing flap statistics.

If no parameters are specified, the flap statistics of all the routes will be cleared

Examples # Clear the flap statistics of the routes matching AS path ACL 10.

```
<Sysname> reset bgp ipv6 flap-info as-path-acl 10
```

router-id (BGP view)

Syntax **router-id** *router-id*

undo router-id

View BGP view

Parameters *router-id*: Router ID in IP address format.

Description Use the **router-id** command to specify a router ID for the router.

Use the **undo router-id** command to remove a router ID.

To run IPv6 BGP protocol, a router must have a router ID, an unsigned 32-bit integer and the unique ID of the router in the AS.

A router ID can be configured manually. If not, the system will select a router ID automatically from the current interfaces' IP addresses. The selection sequence is the highest IP address of Loopback interfaces' addresses, then the highest IP address of physical interfaces' addresses if no Loopback interfaces are configured.

Only when the interface of the router ID is removed or the manually configured router ID is removed, will the system select another Router ID. To improve network reliability, it is recommended to configure the IPv4 address of a loopback interface as the router ID.

Examples # Specify the router ID of the router as 10.18.4.221.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] router-id 10.18.4.221
```

synchronization (IPv6 address family view)

Syntax **synchronization**

undo synchronization

View IPv6 address family view

Parameters None

Description Use the **synchronization** command to enable the synchronization between IPv6 BGP and IGP.

Use the **undo synchronization** command to disable the synchronization.

The feature is disabled by default.

With this feature enabled and when a non-BGP router is responsible for forwarding packets in an AS, IPv6 BGP speakers in the AS cannot advertise routing information to other ASs unless all routers in the AS know the latest routing information.

By default, upon receiving an IPv6 IBGP route, the BGP router only checks whether the next hop is reachable before advertisement. If synchronization is enabled, the IBGP route can be advertised to EBGP peers only when the route is also advertised by the IGP.

Examples # Enable the route synchronization between IPv6 BGP and IGP.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] synchronization
```

41 MULTICAST VLAN CONFIGURATION COMMANDS

display multicast-vlan

Syntax **display multicast-vlan** [*vlan-id*]

View Any view

Parameters *vlan-id*: VLAN ID of a multicast VLAN. If this argument is not provided, the information about all multicast VLANs and their sub-VLANs will be displayed.

Description Use the **display multicast-vlan** command to view the information about the specified multicast VLAN and its sub-VLANs.

Examples # View the information about all multicast VLANs and their sub-VLANs.

```
<Sysname> display multicast-vlan
 multicast vlan 100's subvlan list:
   vlan 4-8
```

multicast-vlan enable

Syntax **multicast-vlan** *vlan-id* **enable**

undo multicast-vlan *vlan-id* **enable**

View System view

Parameters *vlan-id*: Specifies a VLAN by its ID.

Description Use the **multicast-vlan enable** command to configure the specified VLAN as a multicast VLAN.

Use the **undo multicast-vlan enable** command to remove the specified VLAN as a multicast VLAN.

No VLAN is a multicast VLAN by default.

Note that:

- The specified VLAN must exist.

- Currently, a Switch 8800 supports only one multicast VLAN. With the **multicast routing-enable** or the **multicast ipv6 routing-enable** command enabled, you cannot enable multicast VLAN on the device. For details about these two commands, see "Multicast Routing and Forwarding Configuration Commands" on page 645 and "IPv6 Multicast Routing and Forwarding Configuration Commands" on page 663.

Examples # Configure VLAN 10 as a multicast VLAN.

```
<Sysname> system-view
[Sysname] multicast-vlan 10 enable
```

multicast-vlan subvlan

Syntax **multicast-vlan** *vlan-id* **subvlan** *vlan-list*

undo multicast-vlan *vlan-id* **subvlan** *vlan-list*

View System view

Parameters *vlan-id*: VLAN ID of a multicast VLAN.

subvlan *vlan-list*: Defines one or multiple VLANs to be configured as sub-VLANs of the multicast VLAN. You can provide up to 10 VLAN lists, by each of which you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* **to** *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID.

Currently, the Switch 8800s supports up to 1024 sub-VLANs for a multicast VLAN.

Description Use the **multicast-vlan subvlan** command to configure sub-VLAN(s) for the specified multicast VLAN.

Use the **undo multicast-vlan subvlan** command to remove the specified sub-VLAN(s) from the specified multicast VLAN.

A multicast VLAN has no sub-VLANs by default.

Note that:

- The VLAN to be configured as the multicast VLAN and the VLANs to be configured as sub-VLANs of the multicast VLAN exist.
- The VLANs to be configured as sub-VLANs of the multicast VLAN must not be multicast VLANs.
- The VLANs to be configured as the sub-VLANs of the multicast VLAN must not be sub-VLANs of another multicast VLAN.
- The number of sub-VLANs of the multicast VLAN must not exceed the system-defined limit.

Examples # Configure VLANs 2 through 5 as sub-VLANs of multicast VLAN 10.

```
<Sysname> system-view
[Sysname] multicast-vlan 10 subvlan 2 to 5
```

42 MULTICAST ROUTING AND FORWARDING CONFIGURATION COMMANDS

debugging mfib

Syntax **debugging mfib** { **all** | { **driver** | **no-cache** | **packet** | **register** | **route** | **sync** | **upcall** | **wrong-iif** } [*advanced-acl-number*] } [**slot** *slot-id*]

undo debugging mfib { **all** | { **driver** | **no-cache** | **packet** | **register** | **route** | **sync** | **upcall** | **wrong-iif** } [*advanced-acl-number*] } [**slot** *slot-id*]

View User view

Parameters **all**: Specifies all types of MFIB debugging.

driver: Specifies MFIB interface driver debugging.

no-cache: Specifies MFIB unmatched packet debugging.

packet: Specifies MFIB packet debugging.

register: Specifies MFIB register message debugging.

route: Specifies MFIB route debugging.

sync: Specifies MFIB synchronization message debugging.

upcall: Enables/disables debugging for packets that MFIB reports to MRM.

wrong-iif: Enables/disables MFIB debugging for incoming interface errors. Currently, Switch 8800s do not support this option.

advanced-acl-number: Advanced ACL number.

slot *slot-id*: Specifies the slot where the interface module resides.

Description Use the **debugging mfib** command to enable MFIB debugging.

Use the **undo debugging mfib** command to disable MFIB debugging.

By default, MFIB debugging is disabled.

Table 166 Field descriptions of the debugging mfib command

Field	Description
MFIB packet debugging switch is on	MFIB packet debugging is enabled.

Table 166 Field descriptions of the debugging mfib command

Field	Description
MFIB route debugging switch is on	MFIB route debugging is enabled.
MFIB sync debugging switch is on	MFIB synchronization message debugging is enabled.
MFIB no-cache debugging switch is on	MFIB debugging for unmatched packets is enabled.
MFIB wrong-iif debugging switch is on	MFIB incoming interface error debugging is enabled.
MFIB register debugging switch is on	MFIB register message debugging is enabled.
MFIB upcall debugging switch is on	Debugging for packets that MFIB reports to MRM is enabled.
MFIB driver debugging switch is on	MFIB debugging for interface drivers is enabled.

Table 167 Field descriptions of the debugging mfib packet command

Field	Description
Receive packet	Received packets
Drop packet	Dropped packets
(*sadd, gadd*)	(S, G) entry
The TTL	TTL value of the packet
Forward multicast packet	Forwarded packets

Table 168 Field descriptions of the debugging mfib route command

Field	Description
receive Add entry message from MRM	An Add entry message is received from MRM.
receive Del entry message from MRM	A Del entry message is received from MRM.
receive Set IIF message from MRM	A Set IIF message is received from MRM.
receive Del OIF message from MRM	A Del OIF message is received from MRM.
receive Add OIF message from MRM	An Add OIF message is received from MRM.
The Following OIFs are added	The following OIFs are added.
(*sadd, gadd*)	(S, G) entry

Table 169 Field descriptions of the debugging mfib sync command

Field	Description
added to updated list	An entry is added into the updated list
deleted from updated list	An entry is deleted from the updated list.
Encoded the ADD message	The ADD message is encapsulated.
Encoded the DEL message	The DEL message is encapsulated.
Encoded the MOD message	The MOD message is encapsulated.
(*sadd, gadd*)	(S, G) entry

Table 170 Field descriptions of the debugging mfib no-cache command

Field	Description
Receive no cache report	An unmatched packet is received.
No MFIB entry matches	No matching entries

Table 170 Field descriptions of the debugging mfib no-cache command

Field	Description
(*sadd, gadd*)	(S, G) entry
Cache the packet	Packets are cached.

Table 171 Field descriptions of the debugging mfib register command

Field	Description
Send register	A register message is sent.
(*sadd, gadd*)	(S, G) entry
Dropping received register packet	An error register message is dropped.

Table 172 Field descriptions of the debugging mfib upcall command

Field	Description
Send No cache up call	The corresponding message is sent to MRM.
(*sadd, gadd*)	(S, G) entry

Table 173 Field descriptions of the debugging mfib driver command

Field	Description
call driver	The driver interface is called.
Do not add to driver	Not adding entries to driver
downloaded to driver Failed	Delivery to driver failed.
(*sadd, gadd*)	(S, G) entry

Examples # Enable PIM-DM on the corresponding interface and enable debugging for packets that MFIB reports to MRM.

```
<Sysname> debugging mfib upcall
*Sep  7 21:10:08:130 2006 Sysname MFIB/7/MFIB UPCALL:
Send No cache up call (3.4.5.6, 226.1.1.1) to MRM.(A14624)
```

// MFIB reports an unmatched packet to MRM.

Enable PIM-DM on the corresponding interface and enable MFIB route debugging.

```
<Sysname> debugging mfib route
*Sep  7 21:10:08:178 2006 Sysname MFIB/7/MFIB ROUTE:
Entry (3.4.5.6, 226.1.1.1) receive Add entry message from MRM, OIF n
um is 0.(A111928)
```

// An Add entry message is received from MRM.

Enable PIM-DM on the corresponding interface and enable MFIB synchronization message debugging.

```
<Sysname> debugging mfib sync
*Sep  7 21:10:08:156 2006 Sysname MFIB/7/MFIB SYNC:
Entry (3.4.5.6, 226.1.1.1) is added to updated list(A063552)
```

// The entry is added into the updated list.

debugging mrm

Syntax **debugging mrm** { **all** | **event** | **packet** [*advanced-acl-number*] | **route** [*advanced-acl-number*] }

undo debugging mrm { **all** | **event** | **packet** | **route** }

View User view

Parameters **all**: Specifies all types of debugging for multicast routing management (MRM).

event: Specifies MRM event debugging.

packet: Specifies MRM packet debugging.

route: Specifies MRM route debugging.

advanced-acl-number: Advanced ACL number.

Description Use the **debugging mrm** command to enable MRM debugging.

Use the **undo debugging mrm** command to disable MRM debugging.

By default, MRM debugging is disabled.

Table 174 Field descriptions of the debugging mrm command

Field	Description
MRM packet debugging switch is on	MRM packet debugging is enabled.
MRM route debugging switch is on	MRM route debugging is enabled.
MRM event debugging switch is on	MRM event debugging is enabled.

Table 175 Field descriptions of the debugging mrm packet command

Field	Description
Received	Received packets
MFIB information(NOCACHE)	Types of received packets
MFIB information(WRONGIF)	
MFIB information(ACTIVE)	
MFIB information(INACTIVE)	
MFIB information(SPT)	
MFIB information(CLEAR)	
MFIB information(REG-Timeout)	
Pim	
packet (protocol = 2)	
(*sadd, gadd*)	(S, G) entry

Table 176 Field descriptions of the debugging mrm route command

Field	Description
lost the route	A route is deleted.
a new route	A new route is added.
(*sadd, gadd*)	(S, G) entry

Table 177 Field descriptions of the debugging mrm event command

Field	Description
register interest/unregistered interest	Register/deregister
(*sadd, gadd*)	(S, G) entry
failed	Operation failed.

Examples # Enable PIM-SM on the corresponding interface and enable MRM packet debugging.

```
<Sysname> debugging mrm packet
*0.21838588 85 MRM/7/PACKET:
Received MFIB information(NOCACHE) for (1.1.1.108, 235.1.1.1) with i
ncoming interface index 0x30f0188(C22380)
```

// An unmatched packet is received from MFIB.

display multicast boundary

Syntax **display multicast boundary** [*group-address* [*mask* | *mask-length*]] [**interface** *interface-type interface-number*]

View Any view

Parameters *group-address*: Multicast group address.

mask: Mask of the multicast group address, 255.255.255.255 by default.

mask-length: Mask length of the multicast group address, 32 by default.

interface-type interface-number: Specifies an interface by its type and number.

Description Use the **display multicast boundary** command to view the multicast boundary information on the specified interface or all interfaces.

Related commands: **multicast boundary**.

Examples # View the multicast boundary information on all interfaces.

```
<Sysname> display multicast boundary
Multicast boundary information
```

Boundary Interface

224.1.1.0/24 Pos5/1/1

239.2.2.0/24 Pos5/1/2

Table 178 Field descriptions of the display multicast boundary command

Field	Description
Boundary	Multicast group corresponding to the multicast boundary
Interface:	Boundary interface corresponding to the multicast boundary

display multicast forwarding-table

Syntax **display multicast forwarding-table** [*group-address* [**mask** { *mask* | *mask-length* }] | *source-address* [**mask** { *mask* | *mask-length* }] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** } } | **statistics** | **slot** *slot-id*] * [**port-info**]

View Any view

Parameters *group-address*: Multicast group address.

mask: Mask of the multicast group/source address, 255.255.255.255 by default.

mask-length: Mask length of the multicast group/source address. For a multicast group address, this argument has an effective value range of 4 to 32; for a multicast source address, this argument has an effective value range of 0 to 32. The system default is 32 in both cases.

source-address: Multicast source address.

incoming-interface: Displays forwarding entries of which the incoming interface is the specified one.

interface-type interface-number: Specifies an interface by its type and number.

register: Specifies the register interface.

outgoing-interface: Displays forwarding entries of which the outgoing interface is the specified one.

include: Displays the routing entries of which the outgoing interface list includes the specified interface.

exclude: Displays the routing entries of which the outgoing interface list excludes the specified interface.

match: Specifies the routing entries of which the outgoing interface list includes and includes only the specified interface.

statistics: Specifies to display the statistics information of multicast forwarding table.

slot *slot-id*: Specifies the slot number of an interface module. If you do not specify this option, this command will display the multicast forwarding table information of all cards.

port-info: Specifies to display Layer 2 port information.

Description Use the **display multicast forwarding-table** command to view the multicast forwarding table information.

Related commands: **multicast forwarding-table downstream-limit**, **multicast forwarding-table route-limit** and **display multicast routing-table**.

Examples # View the multicast forwarding table information.

```
<Sysname> display multicast forwarding-table
Multicast Forwarding Table
```

Total 1 entry matched

00001. (10.1.1.3, 225.1.1.1)

MID: 0, Flags: 0x100000:0

Uptime: 00:00:27, Timeout in: 00:03:21

Incoming interface: Vlan-interface10

```
    List of 1 outgoing interfaces:
    1: Vlan-interface6
```

Matched 5 packets(140 bytes), Wrong If 0 packets

Forwarded 2 packets(58 bytes)

Table 179 Field descriptions of the display multicast forwarding-table command

Field	Description
00001	Sequence number the (S, G) entry
(10.1.1.3, 225.1.1.1)	An (S, G) entry of the multicast forwarding table
MID	(S, G) entry ID. Each (S, G) entry has an unique MID
Flags	Current state of the (S, G) entry. Different bits are used to indicate different states of (S, G) entries. Major values of this field are described in Table 180.
Uptime	Length of time for which the (S, G) entry has been up, in hours:minutes:seconds
Timeout in	Length of time in which the (S, G) entry will expire, in hours:minutes:seconds
Incoming interface	Incoming interface of the (S, G) entry
List of 1 outgoing interfaces	Outgoing interface list

Table 179 Field descriptions of the display multicast forwarding-table command

Field	Description
Matched 5 packets(140 bytes), Wrong If 0 packets	Number of (S, G)-matched packets (number of bytes), number of packets with incoming interface errors
	(The values are for reference only)
Forwarded 2 packets(58 bytes)	Number of (S, G)-forwarded IPv6 multicast packets (number of bytes)
	(The values are for reference only)

Table 180 Major values of the flags field

Value	Meaning
0x00000001	Indicates that a register-stop message must be sent
0x00000002	Indicates whether the multicast source corresponding to the (S, G) is active
0x00000004	Indicates a null forwarding entry
0x00000008	Indicates whether the RP is a PIM domain border router
0x00000010	Indicates that a register outgoing interface is available
0x00000400	Identifies a packet to be deleted
0x00008000	Indicates that the (S, G) entry is in the smoothening process after active/standby switchover
0x00010000	Indicates that the (S, G) has been updated during the smoothing process
0x00080000	Indicates that the (S, G) entry has been repeatedly updated and needs to be deleted before a new entry is added
0x00100000	Indicates that an entry is successfully added

display multicast routing-table

Syntax **display multicast routing-table** [*group-address* [**mask** { *mask* | *mask-length* }] | *source-address* [**mask** { *mask* | *mask-length* }] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** } }] *

View Any view

Parameters *group-address*: Multicast group address.

source-address: Multicast source address.

mask: Mask of the multicast group/source address, 255.255.255.255 by default.

mask-length: Mask length of the multicast group/source address. For a multicast group address, this argument has an effective value range of 4 to 32; for a

multicast source address, this argument has an effective value range of 0 to 32. The system default is 32 in both cases.

incoming-interface: Displays multicast routing entries of which the incoming interface is the specified one.

interface-type interface-number: Specifies an interface by its type and number.

register: Specifies the register interface.

outgoing-interface: Displays multicast routing entries of which the outing interface is the specified one.

include: Displays routing entries of which the outgoing interface list includes the specified interface.

exclude: Displays routing entries of which the outgoing interface list excludes the specified interface.

match: Displays routing entries of which the outgoing interface list includes only the specified interface.

Description Use the **display multicast routing-table** command to view the multicast routing table information.

Related commands: **display multicast forwarding-table**.

Examples # View the routing information in the multicast routing table.

<Sysname> display multicast routing-table

Multicast routing table

Total 1 entry

00001. (172.168.0.2, 227.0.0.1)

Uptime: 00:00:28

Upstream Interface: Vlan-interface10

List of 2 downstream interfaces

1: Vlan-interface11

2: Vlan-interface12

Table 181 Field descriptions of the display multicast routing-table command

Field	Description
00001	Sequence number the (S, G) entry
(172.168.0.2, 227.0.0.1)	An (S, G) entry of the multicast forwarding table
Uptime	Length of time for which the (S, G) entry has been up, in hours:minutes:seconds

Table 181 Field descriptions of the display multicast routing-table command

Field	Description
Upstream interface	Upstream interface the (S, G) entry: multicast packets should arrive at this interface
List of 2 downstream interfaces	Downstream interface list: these interfaces need to forward multicast packets

display multicast routing-table static

Syntax **display multicast routing-table static** [**config**] [*source-address* { *mask-length* | *mask* }]

View Any view

Parameters **config**: Displays the configuration information of static routes.

source-address: Multicast source address.

mask: Mask of the multicast source address.

mask-length: Mask length of the multicast source address.

Description Use the **display multicast routing-table static** command to view the information of multicast static routes.

Examples # View the configuration information of multicast static routes.

```
<Sysname> display multicast routing-table static config
Multicast Routing Table
Routes : 1

 Mroute 10.10.0.0/16,  interface = Vlan-interface10
 Matched routing protocol = <none>, Route-policy = <none>
 Preference = 1, Order = 1
```

Table 182 Field descriptions of the display multicast routing-table static command

Field	Description
Routes	Number of multicast static routes
Mroute	Multicast route source address and its mask length
Interface	Outgoing interface to the multicast source
Matched routing protocol	If a protocol is configured, the multicast source address of the route should be the destination address of an entry in unicast routing table
Route-policy	Routing policy. The multicast source address of the route should match the routing policy
Preference	Route preference
Order	Sequence number of the route

display multicast rpf-info

Syntax **display multicast rpf-info** *source-address* [*group-address*]

View Any view

Parameters *source-address*: Multicast source address.

group-address: Multicast group address.

Description Use the **display multicast rpf-info** command to view the RPF information of a multicast source.

Related commands: **display multicast routing-table** and **display multicast forwarding-table**.

Examples # View the RPF information of multicast source 10.1.1.2.

<Sysname> display multicast rpf-info 10.1.1.2

RPF information about source 10.1.1.2:
RPF interface: Vlan-interface10, RPF neighbor: 20.1.1.1
Referenced route/mask: 10.1.1.0/24
Referenced route type: igp
Route selection rule: preference-preferred
Load splitting rule: disable

Table 183 Field descriptions of the display multicast rpf-info command

Field	Description
RPF information about source 10.1.1.2	Information of the RPF path to multicast source 10.1.1.2
RPF interface	RPF interface
RPF neighbor	RPF neighbor
Referenced route/mask	Referenced route and its mask length
Referenced route type	Type of the referenced route, which can be any of the following: ■ igp: unicast route (IGP) ■ egp: unicast route (BGP) ■ unicast route (directly connected) ■ unicast: other unicast route (such as unicast static route) ■ multicast static: multicast static route
Route selection rule	Rule for RPF route selection, which can be based on the preference of the routing protocol or based on the longest match on the destination address
Load splitting rule	Status of the load splitting rule (enabled/disabled)

ip rpf-route-static

Syntax **ip rpf-route-static** *source-address* { *mask* | *mask-length* } [*protocol* [*process-id*]] [**route-policy** *policy-name*] { *rpf-nbr-address* | *interface-type interface-number* } [**preference** *preference*] [**order** *order-number*]

undo ip rpf-route-static *source-address* { *mask* | *mask-length* } [*protocol* [*process-id*]] [**route-policy** *policy-name*]

View System view

Parameters *source-address*: Multicast source address.

mask: Mask of the multicast source address.

mask-length: Mask length of the multicast source address.

protocol: Routing protocol, which can have any of the following values:

- **bgp**: Specifies the BGP protocol
- **isis**: Specifies the IS-IS protocol
- **ospf**: Specifies the OSPF protocol
- **rip**: Specifies the RIP protocol

process-id: Process number of the unicast routing protocol. This argument must be provided if IS-IS, OSPF or RIP is the specified unicast routing protocol.

policy-name: Name of the multicast route match rule, a string of 1 to 19 characters.

rpf-nbr-address: Specifies an RPF neighbor by an IP address.

interface-type interface-number: Specifies an RPF neighbor by an interface type and interface number. Currently, for a Switch 8800, you can use this approach only if the interface type is POS.

order-number: Match order for routes on the same segment, in the range of 1 to 100.

preference: Route preference, 1 by default.

Description Use the **ip rpf-route-static** command to configure a multicast static route.

Use the **undo ip rpf-route-static** command to delete a multicast static route from the multicast static routing table.

By default, no multicast static route is configured.

Note that:

- The arguments *source-address* { *mask* | *mask-length* }, *protocol* and *policy-name* are critical elements in multicast static route configuration. The variation of any of these three arguments results in a different configuration.
- In the configuration, you can use the **display multicast routing-table static** command to check whether the multicast static route information contains this configuration. If you find a match, modify the corresponding fields without changing the configuration sequence; otherwise, add a multicast static route.
- When configuring a multicast static route, you can specify an RPF neighbor only by providing its IP address (*rpf-nbr-address*) rather than an interface type and interface number (*interface-type interface-number*) if the interface is a VLAN interface.
- Because outgoing interface iteration may fail or the specified interface may be in the down state, the multicast static route configured with this command may fail to take effect. Therefore, we recommend that you use the **display multicast routing-table static** command after you configure a multicast static route to check whether the route has been successfully configured or whether the route has taken effect.

Related commands: **display multicast routing-table static**.

Examples # Configure a multicast static route.

```
<Sysname> system-view
[Sysname] ip rpf-route-static 1.0.0.0 255.0.0.0 rip 1 route-policy m
ap1 11.0.0.1
```

multicast boundary

Syntax **multicast boundary** *group-address* { *mask* | *mask-length* }

undo multicast boundary { *group-address* { *mask* | *mask-length* } | **all** }

View VLAN interface view/POS interface view

Parameters *group-address*: Multicast group address.

mask: Mask of the multicast group address

mask-length: Mask length of the multicast group address.

all: Specifies to remove all forwarding boundaries configured on the interface.

Description Use the **multicast boundary** command to configure a multicast forwarding boundary.

Use the **undo multicast boundary** command to remove a multicast forwarding boundary.

By default, no multicast forwarding boundary is configured.

Note that:

- A multicast forwarding boundary sets the boundary condition for the multicast groups in the specified range. If the destination address of a multicast packet matches the set boundary condition, the packet will not be forwarded.
- If an interface needs to act as forwarding boundary for multiple multicast groups, just carry out this command on the interface once for each group.
- Assume that Set A and Set B are both multicast forwarding boundary sets to be configured, and B is a subset of A. If A has been configured on an interface, it is not allowed to configure B on the interface; if B has been configured on the interface before A is configured, the previously configured B will be removed.

Related commands: **display multicast boundary**.

Examples # Configure VLAN-interface 4 to be the forwarding boundary of multicast group 239.2.0.0/16.

```
<Sysname> system-view
[Sysname] interface vlan-interface 4
[Sysname-Vlan-interface4] multicast boundary 239.2.0.0 16
```

multicast forwarding-table downstream-limit

Syntax **multicast forwarding-table downstream-limit** *limit*

undo multicast forwarding-table downstream-limit

View System view

Parameters *limit*: Maximum number of downstream nodes (namely, the maximum number of outgoing interfaces) for a single route in the multicast forwarding table.

Description Use the **multicast forwarding-table downstream-limit** command to configure the maximum number of downstream nodes for a single route in the multicast forwarding table.

Use the **undo multicast forwarding-table limit** command to restore maximum number of downstream nodes for a single route to the system default.

By default, the maximum number of downstream nodes for a single route in the multicast forwarding table is 128.

The system-allowed maximum number varies with different device models. Refer to your specific device model.

Related commands: **display multicast forwarding-table**.

Examples # Set the maximum number of downstream nodes for a single route in the multicast forwarding table to 120.

```
<Sysname> system-view
[Sysname] multicast forwarding-table downstream-limit 120
```

multicast forwarding-table route-limit

Syntax **multicast forwarding-table route-limit** *limit*

undo multicast forwarding-table route-limit

View System view

Parameters *limit*: Maximum number of route entries in the multicast forwarding table.

Description Use the **multicast forwarding-table route-limit** command to configure the maximum number of route entries in the multicast forwarding table.

Use the **undo multicast forwarding-table route-limit** command to restore the maximum number of route entries in the multicast forwarding table to the system default.

By default, the maximum number of route entries in the multicast forwarding table is the maximum number allowed by the system.

By default, the maximum number of route entries in the multicast forwarding table is 512.

Related commands: **display multicast forwarding-table**.

Examples # Set the maximum number of routing entries in the multicast forwarding table to 200.

```
<Sysname> system-view
[Sysname] multicast forwarding-table route-limit 200
```

multicast load-splitting

Syntax **multicast load-splitting** { **source** | **source-group** }

undo multicast load-splitting

View System view

Parameters **source**: Specifies to implement per-source load splitting.

source-group: Specifies to implement per-source and per-group load splitting simultaneously.

Description Use the **multicast load-splitting** command to enable load splitting of multicast traffic.

Use the **undo multicast load-splitting** command to disable load splitting of multicast traffic.

By default, load splitting of multicast traffic is disabled.

Examples # Enable per-source load splitting of multicast traffic.

```
<Sysname> system-view
[Sysname] multicast load-splitting source
```

multicast longest-match

Syntax **multicast longest-match**

undo multicast longest-match

View System view

Parameters None

Description Use the **multicast longest-match** command to configure route selection based on the longest match, namely based on the mask length.

Use the **undo multicast longest-match** command to remove the configuration of route selection based on the longest match.

By default, routes are selected according to the order of route entries.

Examples # Configure route selection based on the longest match.

```
<Sysname> system-view
[Sysname] multicast longest-match
```

multicast routing-enable

Syntax **multicast routing-enable**

undo multicast routing-enable

View System view

Parameters None

Description Use the **multicast routing-enable** command to enable IP multicast routing.

Use the **undo multicast routing-enable** command to disable IP multicast routing.

IP multicast routing is disabled by default.

Note that:

- You must enable IP multicast routing before you can carry out other Layer 3 multicast commands.
- The device does not forward any multicast packets before IP multicast routing is enabled.

Examples # Enable IP multicast routing.

```
<Sysname> system-view
[Sysname] multicast routing-enable
```

reset multicast forwarding-table

Syntax **reset multicast forwarding-table** { { *group-address* [**mask** { *mask* | *mask-length* }] | *source-address* [**mask** { *mask* | *mask-length* }] | **incoming-interface** { *interface-type interface-number* | **register** } } * | **all** }

View User view

Parameters *group-address*: Multicast group address.

mask: Mask of the multicast group/source address, 255.255.255.255 by default.

mask-length: Mask length of the multicast group/source address. For a multicast group address, this argument has an effective value range of 4 to 32; for a multicast source address, this argument has an effective value range of 0 to 32. The system default is 32 in both cases in both cases.

source-address: Multicast source address.

incoming-interface: Clears multicast forwarding entries of which the incoming interface is the specified one.

interface-type interface-number: Specifies an interface by its type and number.

register: Specifies the register interface.

all: Specifies to clear all the forwarding entries from the multicast forwarding table.

Description Use the **reset multicast forwarding-table** command to clear the multicast forwarding table information.

When a forwarding entry is deleted from the multicast forwarding table, the corresponding route entry is also deleted from the multicast routing table.

Related commands: **reset multicast routing-table**, **display multicast routing-table**, and **display multicast forwarding-table**.

Examples # Clear the multicast forwarding entries related to multicast group 225.5.4.3 from the multicast forwarding table.

```
<Sysname> reset multicast forwarding-table 225.5.4.3
```

reset multicast routing-table

Syntax **reset multicast routing-table** { { *group-address* [**mask** { *mask* | *mask-length* }] | *source-address* [**mask** { *mask* | *mask-length* }] | **incoming-interface** { *interface-type interface-number* | **register** } } * | **all** }

View User view

Parameters *group-address*: Multicast group address.

mask: Mask of the multicast group/source address, 255.255.255.255 by default.

mask-length: Mask length of the multicast group/source address. For a multicast group address, this argument has an effective value range of 4 to 32; for a multicast source address, this argument has an effective value range of 0 to 32. The system default is 32 in both cases.

source-address: Multicast source address.

incoming-interface: Specifies the incoming interface of multicast routing entries.

interface-type interface-number: Specifies an interface by its type and number.

register: Specifies the register interface.

all: Specifies to clear all the routing entries from the multicast routing table.

Description Use the **reset multicast routing-table** command to clear multicast routing entries from the multicast routing table.

When a route entry is deleted from the multicast routing table, the corresponding forwarding entry is also deleted from the multicast forwarding table.

Related commands: **reset multicast forwarding-table, display multicast routing-table** and **display multicast forwarding-table**.

Examples # Clear the route entries related to multicast group 225.5.4.3 from the multicast routing table.

```
<Sysname> reset multicast routing-table 225.5.4.3
```

43 IPv6 Multicast Routing and Forwarding Configuration Commands

The term "router" in this document refers to a router in a generic sense or a Switch 8800 running an IP multicast routing protocol.

debugging mfib ipv6

Syntax **debugging mfib ipv6** { **all** | { **driver** | **no-cache** | **packet** | **register** | **route** | **sync** | **upcall** | **wrong-iif** } [*advanced-acl6-number*] } [**slot** *slot-id*]

undo debugging mfib ipv6 { **all** | { **driver** | **no-cache** | **packet** | **register** | **route** | **sync** | **upcall** | **wrong-iif** } [*advanced-acl6-number*] } [**slot** *slot-id*]

View User view

Parameters **all**: Turns on/off all types of IPv6 MFIB debugging.

driver: Turns on/off IPv6 MFIB interface driver debugging.

no-cache: Turns on/off IPv6 MFIB unmatched packet debugging.

packet: Turns on/off IPv6 MFIB packet debugging.

register: Turns on/off IPv6 MFIB register message debugging.

route: Turns on/off IPv6 MFIB route debugging.

sync: Turns on/off IPv6 MFIB synchronization message debugging.

upcall: Turns on/off debugging for packets that IPv6 MFIB reports to IPv6 MRM.

wrong-iif: Turns on/off IPv6 MFIB debugging for incoming interface errors. Currently, Switch 8800s do not support this function.

advanced-acl6-number: Advanced IPv6 ACL number.

slot *slot-id*: Specifies the number of the slot where the interface module resides.

Description Use the **debugging mfib ipv6** command to turn on IPv6 MFIB debugging.

Use the **undo debugging mfib ipv6** command to turn off IPv6 MFIB debugging.

By default, IPv6 MFIB debugging is off.

Table 184 Field descriptions of the debugging mfib ipv6 command

Field	Description
MFIB IPv6 packet debugging switch is on	IPv6 MFIB packet debugging is on.
MFIB IPv6 route debugging switch is on	IPv6 MFIB route debugging is on.
MFIB IPv6 sync debugging switch is on	IPv6 MFIB synchronization message debugging is on.
MFIB IPv6 no-cache debugging switch is on	IPv6 MFIB debugging for unmatched packets is on.
MFIB IPv6 wrong-iif debugging switch is on	IPv6 MFIB incoming interface error debugging is on.
MFIB IPv6 register debugging switch is on	IPv6 MFIB register message debugging is on.
MFIB IPv6 upcall debugging switch is on	Debugging for packets that IPv6 MFIB reports to IPv6 MRM is on.
MFIB IPv6 driver debugging switch is on	IPv6 MFIB debugging for interface drivers is on.

Table 185 Field descriptions of the debugging mfib ipv6 packet command

Field	Description
Receive packet	Received IPv6 packets
Drop packet	Dropped IPv6 packets
(sadd, gadd)	(S, G) entry
The TTL	TTL value of the IPv6 packet
Forward multicast packet	Forwarded IPv6 packets

Table 186 Field descriptions of the debugging mfib ipv6 route command

Field	Description
receive Add entry message from MRM	An Add entry message is received from IPv6 MRM.
receive Del entry message from MRM	A Del entry message is received from IPv6 MRM.
receive Set IIF message from MRM	A Set IIF message is received from IPv6 MRM.
receive Del OIF message from MRM	A Del OIF message is received from IPv6 MRM.
receive Add OIF message from MRM	An Add OIF message is received from IPv6 MRM.
The Following OIFs are added	The following OIFs are added.
(sadd, gadd)	(S, G) entry

Table 187 Field descriptions of the debugging mfib ipv6 sync command

Field	Description
added to updated list	An entry is added into the update list.
deleted from updated list	An entry is deleted from the updated list.
Encoded the ADD message	The ADD message is encapsulated.
Encoded the DEL message	The DEL message is encapsulated.
Encoded the MOD message	The MOD message is encapsulated.
(sadd, gadd)	(S, G) entry

Table 188 Field descriptions of the debugging mfib ipv6 no-cache command

Field	Description
Receive no cache report	An unmatched IPv6 packet is received.
No MFIB entry matches	No matching entries
(sadd, gadd)	(S, G) entry
Cache the packet	IPv6 packets are cached.

Table 189 Field descriptions of the debugging mfib ipv6 register command

Field	Description
Send register	An IPv6 register message is sent.
(sadd, gadd)	(S, G) entry
Dropping received register packet	An error IPv6 register messages is dropped.

Table 190 Field descriptions of the debugging mfib ipv6 upcall command

Field	Description
Send No cache up call	The corresponding message is sent to IPv6 MRM.
(sadd, gadd)	(S, G) entry

Table 191 Field descriptions of the debugging mfib ipv6 driver command

Field	Description
call driver	The driver interface is called.
Do not add to driver	Not adding entries to driver
downloaded to driver Failed	Failed to driver to driver .
(sadd, gadd)	(S, G) entry

Examples # Enable IPv6 PIM-DM on the corresponding interface and turn on IPv6 packet debugging.

```
<Sysname> debugging mfib ipv6 packet
*Jan 24 17:24:18:196 2003 Sysname MFIB/7/MFIB PACKET:Slot=3;
IPv6 Receive packet (40::2, FF1E::101:101), iif = Vlan-interface40,
TTL = 128(A08476)
```

// IPv6 multicast packets are received.

Enable IPv6 PIM-DM on the corresponding interface and turn on IPv6 MFIB route debugging.

```
<Sysname> debugging mfib ipv6 route
*Jan 24 17:24:24:772 2003 Sysname MFIB/7/MFIB ROUTE:
IPv6 Entry (40::2, FF1E::101:101) receive Add entry message from MRM
, OIF num is 1.(A111905)
```

// An Add Entry message is received from IPv6 MRM.

Enable IPv6 PIM-DM on the corresponding interface and enable debugging for packets that IPv6 MFIB reports to IPv6 MRM.

```
<Sysname> debugging mfib ipv6 upcall
*Jan 24 17:24:22:842 2003 Sysname MFIB/7/MFIB UPCALL:
IPv6 Send No cache up call (40::2, FF1E::101:101) to MRM.(A14624)
```

// IPv6 MFIB reports an unmatched packet to IPv6 MRM.

debugging mrm ipv6

Syntax **debugging mrm ipv6** { **all** | **event** | **packet** [*advanced-acl6-number*] | **route** [*advanced-acl6-number*] }

undo debugging mrm ipv6 { **all** | **event** | **packet** | **route** }

View User view

Parameters **all**: Turns on/off all types of debugging for IPv6 multicast routing management (MRM).

event: Turns on/off IPv6 MRM event debugging.

packet: Turns on/off IPv6 MRM packet debugging.

route: Turns on/off IPv6 MRM route debugging.

advanced-acl-number: Advanced IPv6 ACL number.

Description Use the **debugging mrm ipv6** command to turn on IPv6 MRM debugging.

Use the **undo debugging mrm ipv6** command to turn off IPv6 MRM debugging.

By default, IPv6 MRM debugging is off.

Table 192 Field descriptions of the debugging mrm ipv6 command

Field	Description
MRM IPv6 packet debugging switch is on	IPv6 MRM packet debugging is on.
MRM IPv6 route debugging switch is on	IPv6 MRM route debugging is on.
MRM IPv6 event debugging switch is on	IPv6 MRM event debugging is on.

Table 193 Field descriptions of the debugging mrm ipv6 packet command

Field	Description
Received	Received IPv6 packets

Table 193 Field descriptions of the debugging mrm ipv6 packet command

Field	Description
MFIB information(NOCACHE)	Types of received IPv6 packets
MFIB information(WRONGIF)	
MFIB information(ACTIVE)	
MFIB information(INACTIVE)	
MFIB information(SPT)	
MFIB information(CLEAR)	
MFIB information(REG-Timeout)	
Pim	
(*sadd, gadd*)	(S, G) entry

Table 194 Field descriptions of the debugging mrm ipv6 route command

Field	Description
lost the route	A route is deleted.
a new route	A new route is added.
(*sadd, gadd*)	(S, G) entry

Table 195 Field descriptions of the debugging mrm ipv6 event command

Field	Description
register interest/unregistered interest	Register/deregister
(*sadd, gadd*)	(S, G) entry
failed	Operation failed.

Examples # Enable IPv6 PIM-SM on the corresponding interface and turn on IPv6 MRM packet debugging.

```
<Sysname> debugging mrm ipv6 packet
*0.2467910 85 MRM/7/PACKET:
IPv6 Received MFIB information(NOCACHE) for (100::1, FF0E::101:101)
with incoming interface index 0x30f0188(C22380)
```

// An unmatched packet is received from IPv6 MFIB.

display multicast ipv6 boundary

Syntax **display multicast ipv6 boundary** [*ipv6-group-address* [*prefix-length*] | **interface** *interface-type interface-number*]

View Any view

Parameters *ipv6-group-address*: Displays the multicast boundary information persistent to a particular IPv6 multicast group.

prefix-length: Prefix length of an IPv6 multicast group address, in the range of 8 to 128. The system default is 128.

interface-type interface-number: Displays the multicast boundary information on a particular interface.

Description Use the **display multicast ipv6 boundary** command to view the IPv6 multicast boundary information.

Related commands: **multicast ipv6 boundary**.

Examples # View the IPv6 multicast boundary information configured on all interfaces.

```
<Sysname> display multicast ipv6 boundary
```

Multicast ipv6 boundary information

Boundary Interface

FF04::/16 Vlan-interface1

```
FF05::/16               Vlan-interface2
```

Table 196 Field descriptions of the display multicast ipv6 boundary command

Field	Description
Boundary	IPv6 multicast group corresponding to the IPv6 multicast boundary
Interface	IPv6 boundary interface corresponding to the IPv6 multicast boundary

display multicast ipv6 forwarding-table

Syntax **display multicast ipv6 forwarding-table** [*ipv6-source-address* [*prefix-length*] | *ipv6-group-address* [*prefix-length*] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { { **exclude** | **include** | **match** } { *interface-type interface-number* | **register** } } | **statistics** | **slot** *slot-id*] * [**port-info**]

View Any view

Parameters *ipv6-source-address*: Specifies an IPv6 multicast source.

ipv6-group-address: Specifies an IPv6 multicast group.

prefix-length: Prefix length of an IPv6 multicast group address or an IPv6 multicast source address. For an IPv6 multicast group address, this argument has an effective value range of 8 to 128; for an IPv6 multicast source address, this argument has an effective value range of 0 to 128. The system default is 128 in both cases.

incoming-interface: Displays the routing entries whose incoming interface is the specified ones.

interface-type interface-number: Interface type and interface number. Currently, only VLAN interfaces are supported for the Switch 8800s.

register: Specifies the register interface.

outgoing-interface: Displays the routing entries whose outgoing interface is the specified one.

exclude: Displays the routing entries whose outgoing interface list excludes the specified interface.

include: Displays the routing entries whose outgoing interface list includes the specified interface.

match: Displays the routing entries whose outgoing interface list includes and includes only the specified interface.

statistics: Specifies to display the statistics information of IPv6 multicast forwarding table.

slot *slot-id*: Specifies the slot number of an interface module. If you do not provide this option, the multicast forwarding table information of all cards will be displayed.

port-info: Displays Layer 2 port information.

Description Use the **display multicast ipv6 forwarding-table** command to display information of the IPv6 multicast forwarding table.

Related commands: **multicast ipv6 forwarding-table downstream-limit**, **multicast ipv6 forwarding-table route-limit**, and **display multicast ipv6 routing-table**.

Examples # Display information of an IPv6 multicast forwarding table.

```
<Sysname> display multicast ipv6 forwarding-table
Multicast Ipv6 Forwarding Table
Total 1 entries

00001. (2000:5::1:1000, FF1E::101:101)
     MID: 0, Flags: 0x0:0
     Uptime: 04:04:37, Timeout in: 00:03:26
     Incoming interface: Vlan-interface2
     List of 1 outgoing interfaces:
       1: Vlan-interface6
     Matched 146754 packets(10272780 bytes), Wrong If 0 packets
     Forwarded 139571 packets(9769970 bytes)
```

Table 197 Field descriptions of the display multicast ipv6 forwarding-table command

Field	Description
00001	Sequence number the (S, G) entry
(2000:5::1:1000, FF1E::101:101)	An (S, G) entry in the IPv6 multicast forwarding table
MID	(S, G) entry ID. Each (S, G) entry has a unique MID

Table 197 Field descriptions of the display multicast ipv6 forwarding-table command

Field	Description
Flags	Current state of the (S, G) entry. Different bits are used to indicate different states of the (S, G) entry. For the values and meanings of this field, see Table 198.
Uptime	Length of time since the (S, G) entry was installed
Timeout in	Remaining time of the (S, G) entry
Incoming interface	Incoming interface of the (S, G) entry
List of 1 outgoing interfaces	Outgoing interface of the (S, G) entry
Matched 146754 packets(10272780 bytes), Wrong If 0 packets	Number of matched IPv6 packets (number of bytes), number of packets with incoming interface errors
	These values are for reference only.
Forwarded 139571 packets(9769970 bytes)	Number of forwarded IPv6 multicast packets (number of bytes)
	These values are for reference only.

Table 198 Values and meanings of the Flags field

Value	Meaning
0x00000001	Indicates that a register-stop message needs to be sent.
0x00000002	Indicates whether the IPv6 multicast source corresponding to the (S, G) entry is active.
0x00000004	Indicates a null forwarding entry.
0x00000008	Indicates whether the RP is a border router or a border routing switch in an IPv6 PIM domain.
0x00000010	Indicates a register outgoing interface is present
0x00000400	Indicates a packet to be deleted
0x00008000	Indicates that the (S,G) entry is in smoothening process after active/standby switchover
0x00010000	Indicates that the (S, G) entry has been updated during the smoothening process.
0x00080000	Indicates that the (S, G) entry has been repeatedly updated and needs to be deleted before adding a new entry is added.
0x00100000	Indicates that a (S, G) entry is added successfully

display multicast ipv6 routing-table

Syntax **display multicast ipv6 routing-table** [*ipv6-source-address* [*prefix-length*] | *ipv6-group-address* [*prefix-length*] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { { **exclude** | **include** | **match** } { *interface-type interface-number* | **register** } }] *

View Any view

Parameters *ipv6-source-address*: IPv6 multicast source address.

ipv6-group-address: IPv6 multicast group address.

prefix-length: Prefix length of a multicast group address or an IPv6 multicast source address. For an IPv6 multicast group address, this argument has an effective value range of 8 to 128; for an IPv6 multicast source address, this argument has an effective value range of 0 to 128. The system default is 128 in both cases.

incoming-interface: Displays routing entries whose incoming interface is the specified one.

interface-type interface-number: Specifies an interface. Currently, only VLAN interfaces are supported for the Switch 8800s.

register: Specifies the register interface.

outgoing-interface: Displays routing entries whose outgoing interface is the specified ones.

exclude: Displays routing entries whose outgoing interface list excludes the specified interface.

include: Displays routing entries whose outgoing interface list includes the specified interface.

match: Displays routing entries whose outgoing interface list includes only the specified interface.

Description Use the **display multicast ipv6 routing-table** command to display the information of the IPv6 multicast routing table.

Related commands: **display multicast ipv6 forwarding-table**.

Examples # Display the information of the IPv6 multicast routing table.

```
<Sysname> display multicast ipv6 routing-table
IPv6 multicast routing table
 Total 1 entry

 00001. (2001::2, FF35::101:101)
       Uptime: 00:00:14
       Upstream Interface: Vlan-interface2
       List of 1 downstream interface
           1:  Vlan-interface6
```

Table 199 Field descriptions of the display multicast ipv6 routing-table command

Field	Description
00001	Sequence number the (S, G) entry
(2001::2, FF35::101:101)	An (S, G) entry in the IPv6 multicast forwarding table

Table 199 Field descriptions of the display multicast ipv6 routing-table command

Field	Description
Uptime	Length of time since the (S, G) entry was installed.
Upstream interface	Upstream interface of the (S, G) entry. Multicast packets for this (S, G) entry should arrive through this interface
List of 2 downstream interfaces	Downstream interface list. These interfaces need to forward multicast packets for this (S, G) entry.

display multicast ipv6 rpf-info

Syntax **display multicast ipv6 rpf-info** *ipv6-source-address* [*ipv6-group-address*]

View Any view

Parameters *ipv6-source-address*: Specify an IPv6 multicast source.

ipv6-group-address: Specifies an IPv6 multicast group.

Description Use the **display multicast ipv6 rpf-info** command to display RPF information for an IPv6 multicast source.

Related commands: **display multicast ipv6 routing-table** and **display multicast ipv6 forwarding-table**.

Examples # Display all RPF information for the multicast source 2001::101.

```
<Sysname> display multicast ipv6 rpf-info 2001::101
RPF information about source 2001::101:
     RPF interface: Vlan-interface5
     Referenced route/prefix length: 2001::101/64
     Referenced route type: igp
     Route selection rule: preference-preferred
     Load splitting rule: disable
```

Table 200 Field descriptions of the display multicast ipv6 rpf-info command

Field	Description
RPF information about source 2001::101	RPF information of the IPv6 multicast source 2001::101
RPF interface	The RPF interface
Referenced route/prefix length	Referenced route and prefix length
Referenced route type	Type of the referenced route
Route-route selecting rule	RPF route selection rule: by the priority of the routing protocol or by the longest match of the destination address in the routing table.
Load splitting rule	Load sharing rule

multicast ipv6 boundary

Syntax **multicast ipv6 boundary** *ipv6-group-address prefix-length*

undo multicast ipv6 boundary { *ipv6-group-address prefix-length* | **all** }

View VLAN interface view

Parameters *ipv6-group-address*: IPv6 multicast group address.

prefix-length: Prefix length of an IPv6 multicast group address.

all: Deletes all IPv6 multicast boundaries configured on the interface.

Description Use the **multicast ipv6 boundary** command to configure a multicast forwarding boundary.

Use the **undo multicast ipv6 boundary** command to delete the specified multicast forwarding boundary or all IPv6 multicast forwarding boundaries.

By default, no multicast forwarding boundary is configured.

Note that:

- A multicast forwarding boundary sets the boundary condition for the IPv6 multicast groups in the specified range. If the destination address of an IPv6 multicast packet matches the set boundary condition, the packet will not be forwarded.
- If an interface needs to act as forwarding boundary for multiple IPv6 multicast groups, just carry out this command on the interface once for each group.
- Assume that Set A and Set B are both multicast forwarding boundary sets to be configured, and that B is a subset of A. If A has been configured on an interface, it is not allowed to configure B on the interface; if B has been configured on the interface before A is configured, the previously configured B needs to be removed.

Related commands: **display multicast ipv6 boundary**.

Examples # Configure VLAN-interface 100 to be the forwarding boundary for IPv6 multicast group FF35::101:101/16.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] multicast ipv6 boundary FF35::101:101 16
```

multicast ipv6 forwarding-table downstream-limit

Syntax **multicast ipv6 forwarding-table downstream-limit** *limit*

undo multicast ipv6 forwarding-table downstream-limit

View System view

Parameters *limit*: Maximum number of downstream nodes for a single route in the IPv6 multicast forwarding table.

Description Use the **multicast ipv6 forwarding-table downstream-limit** command to configure the maximum number of downstream nodes for a single route in the IPv6 multicast forwarding table.

Use the **undo multicast ipv6 forwarding-table downstream-limit** command to restore the system default.

By default, the maximum number of downstream nodes for a single route in the IPv6 multicast forwarding table is 128.

Related commands: **display multicast ipv6 forwarding-table**.

Examples # Set the maximum number of downstream nodes for a single route in the IPv6 multicast forwarding table to 120.

```
<Sysname> system-view
[Sysname] multicast ipv6 forwarding-table downstream-limit 120
```

multicast ipv6 forwarding-table route-limit

Syntax **multicast ipv6 forwarding-table route-limit** *limit*

undo multicast ipv6 forwarding-table route-limit

View System view

Parameters *limit*: Maximum number of routing entries in the IPv6 multicast forwarding table.

Description

Use the **multicast ipv6 forwarding-table route-limit** command to configure the maximum number of routing entries in the IPv6 multicast forwarding table.

Use the **undo multicast ipv6 forwarding-table route-limit** command to restore the system default.

By default, the maximum number of routing entries in the IPv6 multicast forwarding table is 256.

Related commands: **display multicast ipv6 forwarding-table**.

Examples # Set the maximum number of routing entries in the IPv6 multicast forwarding table to 200.

```
<Sysname> system-view
[Sysname] multicast ipv6 forwarding-table route-limit 200
```

multicast ipv6 load-splitting

Syntax **multicast ipv6 load-splitting** {**source** | **source-group** }

undo multicast ipv6 load-splitting

View System view

Parameters **source**: Specifies to implement IPv6 multicast load splitting on a per-source basis.

source-group: Specifies to implement IPv6 multicast load splitting on a per-source and per-group basis.

Description Use the **multicast load-splitting** command to enable load splitting of IPv6 multicast traffic.

Use the **undo multicast load-splitting** command to disable load splitting of IPv6 multicast traffic.

By default, load splitting of IPv6 multicast traffic is disabled.

Examples # Enable load splitting of IPv6 multicast traffic on a per-source basis.

```
<Sysname> system-view
[Sysname] multicast ipv6 load-splitting source
```

multicast ipv6 routing-enable

Syntax **multicast ipv6 routing-enable**

undo multicast ipv6 routing-enable

View System view

Parameters None

Description Use the **multicast ipv6 routing-enable** command to enable IPv6 multicast routing.

Use the **undo multicast ipv6 routing-enable** command to disable IPv6 multicast routing.

IPv6 multicast routing is disabled by default.

Note that:

- You must enable IPv6 multicast routing before you can carry out other Layer 3 IPv6 multicast commands.
- The device does not forward any IPv6 multicast packets before IPv6 multicast routing is enabled.

Examples # Enable IPv6 multicast routing.

```
<Sysname> system-view
[Sysname] multicast ipv6 routing-enable
```

reset multicast ipv6 forwarding-table

Syntax **reset multicast ipv6 forwarding-table** { { *ipv6-source-address* [*prefix-length*] | *ipv6-group-address* [*prefix-length*] | **incoming-interface** { *interface-type interface-number* | **register** } } * | **all** }

View User view

Parameters *ipv6-source-address*: Specifies an IPv6 multicast source.

ipv6-group-address: Specifies an IPv6 multicast group.

prefix-length: Prefix length of an IPv6 multicast group or an IPv6 multicast source address. For an IPv6 multicast group address, this argument has an effective value range of 8 to 128; for an IPv6 multicast source address, this argument has an effective value range of 0 to 128. The system default is 128 in both cases.

incoming-interface: Clears IPv6 multicast forwarding entries of which the incoming interface is the specified one.

interface-type interface-number: Specifies an interface. Currently, only VLAN interfaces are supported for the Switch 8800s.

all: Clears all forwarding entries from the IPv6 multicast forwarding table.

Description Use the **reset multicast ipv6 forwarding-table** command to clear forwarding entries from the IPv6 multicast forwarding table.

When a forwarding entry is deleted from the IPv6 multicast forwarding table, the corresponding routing entry is also deleted from the IPv6 multicast routing table.

Related commands: **reset multicast IPv6 routing-table**, **display multicast ipv6 routing-table**, and **display multicast ipv6 forwarding-table**.

Examples # Clear the IPv6 multicast forwarding entries related to the IPv6 multicast group FF35::101:101 from the IPv6 multicast forwarding table.

```
<Sysname> reset multicast ipv6 forwarding-table ff35::101:101
```

reset multicast IPv6 routing-table

Syntax **reset multicast ipv6 routing-table** { { *ipv6-source-address* [*prefix-length*] | *ipv6-group-address* [*prefix-length*] | **incoming-interface** { *interface-type interface-number* | **register** } } * | **all** }

View User view

Parameters *ipv6-source-address*: Specifies an IPv6 multicast source.

ipv6-group-address: Specifies an IPv6 multicast group address.

prefix-length: Prefix length of an IPv6 multicast group address or an IPv6 multicast source address. For an IPv6 multicast group address, this argument has an effective value range of 8 to 128 for an IPv6 multicast source address, this argument has an effective value range of 0 to 128. The system default is 128 in both cases.

incoming-interface: Clears IPv6 multicast routing entries of which the incoming interface is the specified one.

interface-type interface-number: Specifies an interface. Currently, only VLAN interfaces are supported for the Switch 8800s.

register: Specifies a registration interface.

all: Clears all routing entries from the IPv6 multicast routing table.

Description Use the **reset multicast ipv6 routing-table** command to clear IPv6 routing entries from the IPv6 multicast routing table.

When a routing entry is deleted from the IPv6 multicast routing table, the corresponding forwarding entry is also deleted from the IPv6 multicast forwarding table.

Related commands: **reset multicast ipv6 forwarding-table**, **display multicast ipv6 forwarding-table** and **display multicast ipv6 routing-table**.

Examples # Clear the routing entries related to the IPv6 multicast group FF35::101:101 from the IPv6 multicast routing table.

```
<Sysname> reset multicast ipv6 routing-table ff35::101:101
```

44 IGMP CONFIGURATION COMMANDS

The term "router" in this document refers to a router in a generic sense or a Switch 8800 running IGMP.

debugging igmp

Syntax **debugging igmp** { **all** | **event** | **leave** [*basic-acl-number*] | **report** [*advanced-acl-number*] | **query** [*advanced-acl-number*] | **timer** }

undo debugging igmp { **all** | **event** | **leave | report | query** | **timer** }

View User view

Parameter **all**: Specifies all types of IGMP debugging.

event: Specifies IGMP event debugging.

leave: Specifies IGMP leave message debugging.

basic-acl-number: Basic ACL number.

report: Specifies IGMP report message debugging.

advanced-acl-number: Advanced ACL number.

query: Specifies IGMP query message debugging.

timer: Specifies IGMP timer debugging.

Description Use the **debugging igmp** command to enable IGMP debugging.

Use the **undo debugging igmp** command to disable IGMP debugging.

By default, IGMP debugging is disabled.

Field descriptions of the **debugging igmp** command

Field	Description
IGMP event debugging switch is on	IGMP event debugging is enabled.
IGMP leave debugging switch is on	IGMP leave message debugging is enabled.
IGMP query debugging switch is on	IGMP query message debugging is enabled.

Field	Description
IGMP report debugging switch is on	IGMP member report message debugging is enabled.
IGMP timer debugging switch is on	IGMP timer debugging is enabled.

Field descriptions of the **debugging igmp event** command

Field	Description
Creating/creation/created aux join/aux prune adding interface/deleting downstream deleting/unregister/deleted Enqueue/Dequeing Elected/ Un-elected	Event types include: ■ Creating/creation/created ■ Join/prune ■ Adding outgoing interface/deleting outgoing interface ■ Enqueuing/dequeuing ■ Elected/un-elected
Interface *interfacename*(*ifadd*)	Interface that responds to events (interface address)
(*sadd, gadd*)	(S, G) entry
(*, *gadd*)	(*, G) entry

Field descriptions of the **debugging igmp leave** command

Field	Description
LEAVE	IGMP leave message
Interfacename(*ifadd*)	Interface that receives messages (interface address)
group *gadd*	Address of the group that a host will leave
Ignoring	Ignoring the IGMP leave message

Field descriptions of the **debugging igmp query** command

Field	Description
version *<1-3>*	Version of the IGMP query
Interfacename(*ifadd*)	Interface that sends/receives messages (interface address)
Ignoring	Ignoring the IGMP query
Received/Send	Received/sent IGMP query
General/group specific query/group-source specific query	IGMP general query/group-specific query/group-and-source specific query
Group *gadd*	Group address to be queried

Field descriptions of the **debugging igmp report** command

Field	Description
Ignoring	Ignoring the IGMP membership report message
IS_IN/IS_EX/TO_IN/TO_EX/ALLOW/BLOCK	Record type of IGMPv3 membership report

Field	Description
Group *gadd*	Group address of IGMP membership report
(*sadd, gadd*)	(S, G) entry
v1/v2/v3	Version of IGMP membership report
Interfacename(*ifadd*)	Interface that sent/received messages (interface address)

Field descriptions of the **debugging igmp timer** command

Field	Description
Source *sadd* timeout	The multicast source timer times out.
Group *gadd* timeout	The multicast group timer times out.
Other querier present timeout	The other querier present interval timer times out.
Interfacename(*ifadd*)	Interface that sends/receives messages (interface address)
Deleting v1 host timer	IGMPv1 host timer times out.
Deleting v2 host timer	IGMPv2 host timer times out.
Setting v1 host timer	Setting IGMPv1 host timer
Setting v2 host timer	Setting IGMPv2 host timer

Example # Enable IGMP timer debugging.

```
<Sysname> debugging igmp timer
*0.20405286 85 IGMP/7/TIMER:Setting v2 host timer for group 235.1.1.
1 on interface Vlan-interface20(1.1.1.1) (B033137)
```

// IGMPv2 membership report is received and IGMPv2 host timer is set.

```
*0.20429101 85 IGMP/7/TIMER:Group 235.1.1.1 timeout. Deleting group record a
ssociated with interface Vlan-interface20(1.1.1.1). (B012920)
```

// The multicast group timer times out.

display igmp group

Syntax **display igmp group** [*group-address* | **interface** *interface-type interface-number*] [**static** | **verbose**]

View Any view

Parameter *group-address*: Multicast group address.

interface *interface-type interface-number*: Displays the IGMP multicast group information about a particular interface.

static: Displays the information of statically joined IGMP multicast groups.

verbose: Displays the detailed information of IGMP multicast groups.

Description Use the **display igmp group** command to view IGMP multicast group information.

Note that:

- If you do not specify an interface and a multicast group address, this command will display the IGMP multicast group information on all interfaces.
- If you do not specify the **static** keyword, this command will display the detailed information about the dynamically joined IGMP multicast groups.

Example # Display the information about dynamically joined IGMP multicast groups on all interfaces.

```
<Sysname> display igmp group
Total 3 IGMP Group(s).
Interface group report information
 Vlan-interface245(192.168.245.2):
 Total 3 IGMP Groups reported
  Group Address       Last Reporter   Uptime      Expires
   239.192.0.1     192.168.245.1   00:02:25    00:01:53
   239.192.245.1   192.168.245.1   00:02:17    00:01:49
   239.255.255.250 192.168.245.111 00:02:24    00:01:55
```

Field descriptions of the **display igmp group** command

Field	Description
Group address	Multicast group address
Last reporter	Address of the last host that reported its multicast membership
Uptime	Length of time for which the multicast group has been up (hours:minutes:seconds)
Expires	Length of time in which the multicast group will expire (hours:minutes:seconds)

display igmp group port-info

Syntax **display igmp group port-info** [**vlan** *vlan-id*] [**slot** *slot-number*] [**verbose**]

View Any view

Parameter *vlan-id*: VLAN ID. If you do not specify a VLAN, this command will display the information of Ethernet ports in all VLANs.

slot-number: Slot number.

verbose: Displays the detailed information about the multicast group.

Description Use the **display igmp group port-info** command to view IGMP Ethernet port information.

Example # View detailed information of IGMP Ethernet ports.

```
<Sysname> display igmp group port-info verbose
    Total 4 IP Group(s).
    Total 4 IP Source(s).
    Total 4 MAC Group(s).

  Port flags: D-Dynamic port, S-Static port, A-Aggregation port, C-Copy port
  Subvlan flags: R-Real VLAN, C-Copy VLAN
  Vlan(id):12.
    Total 1 IP Group(s).
    Total 1 IP Source(s).
    Total 1 MAC Group(s).
    Router port(s):total 1 port.
            Eth2/1/15                           (D)
    IP group(s):the following ip group(s) match to one mac group.
      IP group address:225.1.1.1
        (10.1.1.3, 225.1.1.1):
          Attribute:    MFIB
          Host port(s):total 0 port.
    MAC group(s):
      MAC group address:0100-5e01-0101
          Host port(s):total 0 port.

  Vlan(id):245.
    Total 3 IP Group(s).
    Total 3 IP Source(s).
    Total 3 MAC Group(s).
    Router port(s):total 0 port.
    IP group(s):the following ip group(s) match to one mac group.
      IP group address:239.192.0.1
        (0.0.0.0, 239.192.0.1):
          Attribute:    Host Board
          Host port(s):total 1 port.
            Eth2/1/20                           (D)
    MAC group(s):
      MAC group address:0100-5e40-0001
          Host port(s):total 1 port.
            Eth2/1/20
    IP group(s):the following ip group(s) match to one mac group.
      IP group address:239.255.255.250
        (0.0.0.0, 239.255.255.250):
          Attribute:    Host Board
          Host port(s):total 1 port.
            Eth2/1/20                           (D)
    MAC group(s):
      MAC group address:0100-5e7f-fffa
          Host port(s):total 1 port.
            Eth2/1/20
    IP group(s):the following ip group(s) match to one mac group.
      IP group address:239.192.245.1
        (0.0.0.0, 239.192.245.1):
          Attribute:    Host Board
          Host port(s):total 1 port.
            Eth2/1/20                           (D)
    MAC group(s):
      MAC group address:0100-5e40-f501
          Host port(s):total 1 port.
            Eth2/1/20
```

Field descriptions of the **display igmp group port-info** command

Field	Description
Total 4 IP Group(s).	Total number of IP multicast groups

Field	Description
Total 4 IP Source(s).	Total number of IP multicast sources
Total 4 MAC Group(s).	Total number of MAC multicast groups
Port flags: D-Dynamic port, S-Static port, A-Aggregation port	Port flags: D for dynamic port, S for static port, A for aggregation port
Router port(s)	Number of router ports
IP group address	Address of IP multicast group
MAC group address	Address of MAC multicast group
Attribute	Attribute of IP multicast group
Host port(s)	Number of host member ports

display igmp interface

Syntax **display igmp interface** [*interface-type interface-number*] [**verbose**]

View Any view

Parameter *interface-type interface-number*: Specifies an interface to display the IGMP information about. If no interface is specified, this command will display the related information of all IGMP-enabled interfaces.

verbose: Displays the detailed IGMP configuration and running information.

Description Use the **display igmp interface** command to view IGMP configuration and running information of the specified interface or all IGMP-enabled interfaces.

Example # View the IGMP configuration and running status on all IGMP-enabled interfaces.

```
<Sysname> display igmp interface
Interface information
 Vlan-interface240(10.1.2.2):
   IGMP is enabled
   Current IGMP version is 2
   Value of query interval for IGMP(in seconds): 60
   Value of other querier present interval for IGMP(in seconds): 125
   Value of maximum query response time for IGMP(in seconds): 10
   Querier for IGMP: 10.1.2.2 (this router)

 Vlan-interface245(192.168.245.2):
   IGMP is enabled
   Current IGMP version is 2
   Value of query interval for IGMP(in seconds): 60
   Value of other querier present interval for IGMP(in seconds): 125
   Value of maximum query response time for IGMP(in seconds): 10
   Querier for IGMP: 192.168.245.2 (this router)
  Total 3 IGMP Groups reported
```

Field descriptions of the **display igmp interface** command

Field	Description
Vlan-interface240(10.1.2.2)	Interface name (IP address)
IGMP is enabled	IGMP is enabled.
Current IGMP version	Version of IGMP currently running on the interface
Value of query interval for IGMP(in seconds)	IGMP general query interval, in seconds
Value of other querier present interval for IGMP(in seconds)	Other querier present interval, in seconds
Value of maximum query response time for IGMP(in seconds)	Maximum response time for IGMP general queries, in seconds
Querier for IGMP	IP address of the querier
Total 3 IGMP Groups reported	Total number of groups recorded on the interface.

display igmp routing-table

Syntax **display igmp routing-table** [*group-address* [**mask** { *mask* | *mask-length* }] | *source-address* [**mask** { *mask* | *mask-length* }]] *

View Any view

Parameter *group-address*: Multicast group address.

source-address: Multicast source address.

mask: Subnet mask of the multicast group/source address, 255.255.255.255 by default.

mask-length: Subnet mask length of the multicast group/source address. For a multicast source address, this argument has an effective value range of 0 to 32; for a multicast group address, this argument has an effective value range of 4 to 32. The system default is 32 in both cases.

Description Use the **display igmp routing-table** command to view the routing information of the IGMP routing table.

In an IGMP routing table, (S,G) entries appear as independent entries, each having a unique upstream, meaning that the multicast source is reachable through this interface. Also, each entry has a downstream list, indicating which interfaces need to implement multicast forwarding.

Example # View IGMP routing table information

```
<Sysname> display igmp routing-table
Routing table
 Total 2 entries

 00001. (*, 225.1.1.1)
       List of 1 downstream interface
        Vlan-interface245 (20.1.1.1),
                   Protocol: STATIC
```

```
00002. (*, 239.255.255.250)
      List of 1 downstream interface
       Vlan-interface246 (20.20.20.20),
                  Protocol: IGMP
```

Field descriptions of the **display igmp routing-table** command

Field	Description
00001	Sequence number the (*, G) entry
(*, 225.1.1.1)	An (*, G) entry of the IGMP routing table
List of 1 downstream interface	Downstream interface list: these interfaces need to forward multicast packets

fast-leave (IGMP view)

Syntax **fast-leave** [**group-policy** *acl-number*]

undo fast-leave

View IGMP view

Parameters *acl-number*: Basic ACL number.

Description Use the **fast-leave** command to enable the fast-leave function for multicast group members globally.

Use the **undo fast-leave** command to disable the fast-leave function globally.

By default, the fast-leave function is disabled, namely, the IGMP querier sends an IGMP group-specific query upon receiving an IGMP leave message from a host, instead of sending a Leave notification directly to the upstream.

This command is the same as the **igmp fast-leave** command for interface view, but the value configured by the **igmp fast-leave** command has a higher priority, that is, the system gives priority to configurations made in interface view.

- *The configurations made by the **fast-leave** command in IGMP view are effective only for POS interfaces rather than VLAN interfaces.*
- *To enable the fast leave feature in a VLAN, you can use the **igmp-snooping fast-leave** or the **fast-leave** command. For more information, see "IGMP Snooping Configuration Commands" on page 703.*

Related commands: **igmp fast-leave**, **last-member-query-interval**.

Examples # Enable the fast leave function globally.

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] fast-leave
```

igmp

Syntax **igmp**

undo igmp

View System view

Parameters None

Description Use the **igmp** command to enter IGMP view.

Use the **undo igmp** command to remove configurations performed in IGMP view.

IP multicast must be enabled on the device before this command can take effect.

Related commands: **igmp enable**, and **multicast routing-enable**.

Examples # Enter IGMP view.

```
<Sysname> system-view
[Sysname] multicast routing-enable
[Sysname] igmp
[Sysname-igmp]
```

igmp enable

Syntax **igmp enable**

undo igmp enable

View VLAN interface view/POS interface view

Parameters None

Description Use the **igmp enable** command to enable IGMP on the current interface.

Use the **undo igmp enable** command to disable IGMP on the current interface.

By default, IGMP is disabled on an interface.

Note that:

- IP multicast must be enabled on the device before this command is meaningful.
- Before IGMP is enabled on an interface, any other IGMP feature configured on the interface will not take effect.
- After IGMP is enabled on a VLAN interface, IGMP Snooping cannot be enabled in the VLAN corresponding to the VLAN interface, and vice versa.

Related commands: **igmp**, **multicast routing-table**.

Examples # Enable IGMP on Vlan-interface11.

```
<Sysname> system-view
[Sysname] interface vlan-interface 11
[Sysname-Vlan-interface11] igmp enable
```

igmp fast-leave

Syntax **igmp fast-leave** [**group-policy** *acl-number*]

undo igmp fast-leave

View POS interface view

Parameters *acl-number*: Basic ACL number. If you do not include this option in your command, this command will take effect for all multicast groups.

Description Use the **igmp fast-leave** command to enable the fast leave function on the current interface for multicast group members.

Use the **undo igmp fast-leave** command to disable the fast leave function on the current interface.

By default, the fast leave function is disabled, namely, the IGMP querier sends an IGMP group-specific query upon receiving an IGMP leave message from a host, instead of sending a Leave notification directly to the upstream.

Related commands: **fast-leave**, **igmp lastmember-queryinterval**.

By using the **group-policy** keyword, you can configure an ACL rule to implement control specific to certain groups.

*To enable fast leave on an Ethernet port, you can use the **igmp-snooping fast-leave** or **fast-leave** command. For more information, refer to "IGMP Snooping Configuration Commands" on page 703.*

Examples # Enable fast leave for multicast group members on POS4/1/1.

```
<Sysname> system-view
[Sysname] interface pos 4/1/1
[Sysname-Pos4/1/1] igmp fast-leave
```

igmp group-policy

Syntax **igmp group-policy** *acl-number* [*version-number*]

undo igmp group-policy

View POS interface view

Parameters *acl-number*: Basic or advanced ACL number.

version-number: IGMP version. By default, the system supports IGMPv1, IGMPv2 and IGMPv3 concurrently.

Description Use the **igmp group-policy** command to configure a multicast group filter on the current interface.

Use the **undo igmp group-policy** command to remove the configured multicast group filter.

Be default, no multicast group filter is configured, namely a host can join any multicast group.

- *When you use an advanced ACL as a filter, the source address in the ACL rule is the address of the multicast source specified in the IGMPv3 reports, rather than the source address in the IP packets.*
- *To configure a multicast group filter on an Ethernet port, you can use the **igmp-snooping group-policy** or **group-policy** command. For more information, refer to "IGMP Snooping Configuration Commands" on page 703.*

Related commands: display igmp group

Examples # Configure an ACL rule so that hosts on the subnet attached to POS4/1/1 can join multicast group 225.1.1.1 only.

```
<Sysname> system-view
[Sysname] acl number 2005
[Sysname-acl-basic-2005] rule permit source 225.1.1.1 0
[Sysname-acl-basic-2005] quit
[Sysname] interface pos 4/1/1
[Sysname-Pos4/1/1] igmp group-policy 2005
```

igmp last-member-query-interval

Syntax **igmp last-member-query-interval** *interval*

undo igmp last-member-query-interval

View VLAN interface view/POS interface view

Parameters *interval*: IGMP last-member query interval in seconds.

Description Use the **igmp last-member-query-interval** command to configure the last-member query interval on the current interface.

Use the **undo igmp last-member-query-interval** command to restore the last member query interval to the system default on the current interface.

By default, the last-member query interval is 1 second.

Related commands: **last-member-query-interval**, **igmp robust-count**, **display igmp interface**.

Examples # Set the last-member query interval to 3 seconds on Vlan-interface11.

```
<Sysname> system-view
[Sysname] interface vlan-interface 11
[Sysname-Vlan-interface11] igmp last-member-query-interval 3
```

igmp max-response-time

Syntax **igmp max-response-time** *interval*

undo igmp max-response-time

View VLAN interface view/POS interface view

Parameters *interval*: Maximum response time in seconds for IGMP general queries.

Description Use the **igmp max-response-time** command to configure the maximum response time for IGMP general queries on the current interface.

Use the **undo igmp max-response-time** command to restore the maximum response time for IGMP general queries to the system default.

By default, the maximum response time for IGMP general queries is 10 seconds.

Related commands: **max-response-time**, **igmp timer other-querier-present**, **display igmp interface**.

Examples # Set the maximum response time for IGMP general queries to 8 seconds on Vlan-interface11.

```
<Sysname> system-view
[Sysname] interface vlan-interface 11
[Sysname-Vlan-interface11] igmp max-response-time 8
```

igmp require-router-alert

Syntax **igmp require-router-alert**

undo igmp require-router-alert

View VLAN interface view/POS interface view

Parameters None

Description Use the **igmp require-router-alert** command to configure the interface to discard IGMP messages that do not carry the Router-Alert option.

Use the **undo igmp require-router-alert** command to restore the default configuration.

By default, the device does not check the Router-Alert option, namely it passes all the IGMP messages it receives to the upper layer protocol for processing.

After you use the **igmp require-router-alert** command, when the interface receives an IGMP message, the device checks the Router-Alert option carried in the IGMP message. If the device finds that the message does not carry the Router-Alert option, the device discards the IGMP message.

Related commands: **require-router-alert**, **igmp send-router-alert**.

Examples # Configure Vlan-interface11 to discard IGMP messages that do not carry the Router-Alert option.

```
<Sysname> system-view
[Sysname] interface vlan-interface 11
[Sysname-Vlan-interface11] igmp require-router-alert
```

igmp robust-count

Syntax **igmp robust-count** *robust-value*

undo igmp robust-count

View VLAN interface view/POS interface view

Parameters *robust-value*: IGMP last-member query count.

Description Use the **igmp robust-count** command to configure the IGMP last-member query count.

Use the **undo igmp robust-count** command to restore the system default.

By default, the IGMP last-member query count is 2.

This command is effective only when IGMPv2 or IGMPv3 is running on the IGMP querier. When IGMPv1 is running on a host, it will not send a leave message when it leaves a group. In this case, this command does not work.

Related commands: **robust-count**, **igmp last-member-query-interval**, **display igmp interface**.

Examples # Set the IGMP last-member query count to 3 on Vlan-interface11.

```
<Sysname> system-view
[Sysname] interface vlan-interface 11
[Sysname-Vlan-interface11] igmp robust-count 3
```

igmp send-router-alert

Syntax **igmp send-router-alert**

undo igmp send-router-alert

View VLAN interface view/POS interface view

Parameters None

Description Use the **igmp send-router-alert** command on the current interface to enable insertion of the Router-Alert option in IGMP messages to be sent.

Use the **undo igmp send-router-alert** command on the current interface to disable insertion of the Router-Alert option in IGMP messages to be sent.

By default, IGMP messages are sent with the Router-Alert option.

Related commands: **igmp require-router-alert**, **igmp require-router-alert**.

Examples # Disable insertion of the Router-Alert option into IGMP messages that leave Vlan-interface11.

```
<Sysname> system-view
[Sysname] interface vlan-interface 11
[Sysname-Vlan-interface11] undo igmp send-router-alert
```

igmp static-group

Syntax **igmp static-group** *group-address* [**source** *source-address*]

undo igmp static-group { **all** | *group-address* [**source** *source-address*] }

View POS interface view

Parameters **all**: Specifies to remove all static multicast groups that the current interface has joined.

group-address: Multicast group address.

source-address: Multicast source address.

Description Use the **igmp static-group** command to configure the current interface to be a statically connected member of the specified multicast group.

Use the **undo igmp static-group** command to remove the current interface as a statically connected member of the specified multicast group.

By default, an interface is not a static member of any multicast group.

If the specified multicast address is in the SSM multicast address range, and if a multicast source address is specified in the command, multicasts carrying the (S,G) entry, namely the source address information, can be sent out through this interface.

*To configure an Ethernet port to be a static member of a multicast group, you can use the **igmp-snooping static-group** command. For more information, refer to "IGMP Snooping Configuration Commands" on page 703.*

Examples # Configure POS4/1/1 to be a statically connected member of multicast group 224.1.1.1.

```
<Sysname> system-view
[Sysname] interface pos4/1/1
[Sysname-Pos4/1/1] igmp static-group 224.1.1.1
```

Configure POS4/1/1 so that it can forward multicasts that multicast source 192.168.1.1 sends to multicast group 232.1.1.1.

```
<Sysname> system-view
[Sysname] interface pos4/1/1
[Sysname-Pos4/1/1] igmp static-group 232.1.1.1 source 192.168.1.1
```

igmp timer other-querier-present (VLAN interface view/POS interface view)

Syntax **igmp timer other-querier-present** *interval*

undo igmp timer other-querier-present

View VLAN interface view/POS interface view

Parameters *interval*: Other querier present interval in seconds.

Description Use the **igmp timer other-querier-present** command to configure the other querier present interval on the current interface.

Use the **undo igmp timer other-querier-present** command to restore the default configuration.

By default, the other querier present interval is 125 seconds.

Related commands: **timer other-querier-present**, **igmp timer query**, **igmp robust-count**, **igmp max-response-time**, **display igmp interface**.

Examples # Set the other querier present interval to 200 seconds on Vlan-interface11.

```
<Sysname> system-view
[Sysname] interface vlan-interface 11
[Sysname-Vlan-interface11] igmp timer other-querier-present 200
```

igmp timer query

Syntax **igmp timer query** *interval*

undo igmp timer query

View VLAN interface view/POS interface view

Parameters *interval*: IGMP query interval in seconds, namely the interval between IGMP general queries sent by the querier.

Description Use the **igmp timer query** command to configure the IGMP query interval on the current interface.

Use the **undo igmp timer query** command to restore the system default.

By default, the IGMP query interval is 60 seconds.

The IGMP querier periodically sends IGMP general queries to decide whether any multicast group member exists on the local subnet. You can modify this interval as required.

Related commands: **timer query**, **igmp timer other-querier-present**, **display igmp interface**.

Examples # Set the IGMP general query interval to 125 seconds on Vlan-interface11.

```
<Sysname> system-view
[Sysname] interface vlan-interface 11
[Sysname-Vlan-interface11] igmp timer query 125
```

igmp version

Syntax **igmp version** *version-number*

undo igmp version

View VLAN interface view/POS interface view

Parameters *version-number*: IGMP version.

Description Use the **igmp version** command to configure the IGMP version on the current interface.

Use the **undo igmp version** command to restore the IGMP version to the system default.

The default IGMP version is version 2.

All systems (including hosts and routers) on the same subnet must run the same version of IGMP, and cannot automatically switch between different IGMP versions.

Related commands: **version**.

Examples # Set the IGMP version to IGMPv1 on Vlan-interface11.

```
<Sysname> system-view
[Sysname] interface vlan-interface 11
[Sysname-Vlan-interface11] igmp version 1
```

last-member-query-interval (IGMP view)

Syntax **last-member-query-interval** *interval*

undo last-member-query-interval

View IGMP view

Parameters *interval*: Last-member query interval in seconds.

Description Use the **last-member-query-interval** command to configure the global IGMP last-member query interval.

Use the **undo last-member-query-interval** command to restore the global IGMP last member query interval to the system default.

By default, the IGMP last-member query interval is 1 second.

This command is the same as the **igmp last-member-query-interval** command for interface view, but the value configured by the **igmp last-member-query-interval** command has a higher priority, that is, the system gives priority to configurations made in interface view.

Related commands: **igmp last-member-query-interval**, **robust-count**, **display igmp interface**.

Examples # Set the global IGMP last-member interval to 3 seconds.

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] lastmember-queryinterval 3
```

max-response-time (IGMP view)

Syntax **max-response-time** *interval*

undo igmp max-response-time

View IGMP view

Parameters *interval*: Maximum response time for IGMP general queries in seconds.

Description Use the **max-response-time** command to configure the maximum response time for IGMP general queries.

Use the **undo max-response-time** command to restore globally the maximum response time for IGMP general queries to the system default.

By default, the maximum response time for IGMP general queries is 10 seconds.

This command is the same as the **igmp max-response-time** command for interface view, but the value configured by the **igmp max-response-time** command has a higher priority, that is, the system gives priority to configurations made in interface view.

Related commands: **igmp max-response-time**, **timer other-querier-present**, **display igmp interface**.

Examples # Set the maximum response time for IGMP general queries to 8 seconds globally.

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] max-response-time 8
```

require-router-alert

Syntax **require-router-alert**

undo require-router-alert

View IGMP view

Parameters None

Description Use the **require-router-alert** command to configure the router to discard IGMP messages that do not carry the Router-Alert option.

Use the **undo require-router-alert** command to restore the default configuration.

By default, the device does not check the Router-Alert option, namely it handles all the IGMP messages it received to the upper layer protocol for processing.

After you use the **require-router-alert** command, when an IGMP message arrives, the device checks the Router-Alert option carried in the IGMP message. If the device finds that the message does not carry the Router-Alert option, the device discards the IGMP message.

This command is the same as the **igmp require-router-alert** command for interface view, but the value configured by the **igmp require-router-alert**

command has a higher priority, that is, the system gives priority to configurations made in interface view.

Related commands: **igmp require-router-alert**.

Examples # Configure the router to discard IGMP messages that do not carry the Router-Alert option.

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] require-router-alert
```

reset igmp group

Syntax **reset igmp group** { **all** | **interface** *interface-type interface-number* { **all** | *group-address* [**mask** { *mask* | *mask-length* }] [*source-address* [**mask** { *mask* | *mask-length* }]] } }

View User view

Parameters **all**: Specifies to clear all IGMP forwarding entries.

interface *interface-type interface-number*: Clears the IGMP forwarding entries on the specified interface.

group-address: Multicast group address.

source-address: Multicast source address.

mask: Subnet mask of the multicast group/source address, 255.255.255.255 by default.

mask-length: Subnet mask length of the multicast group/source address. For a multicast group address, this argument has an effective value range of 4 to 32; for a multicast source address, this argument has an effective value range of 0 to 32. The system default is 32 in both cases.

Description Use the **reset igmp group** command to clear IGMP forwarding entries.

Note that:

- When clearing the IGMP forwarding entries of a VLAN interface, this command also clears the IGMP Snooping forwarding entries for that VLAN.
- This command cannot clear IGMP forwarding entries of static joins.

Related commands: **display igmp group**.

Examples # Clear all the IGMP and IGMP Snooping entries on all interfaces.

```
<Sysname> reset igmp group all
```

Clear all IGMP forwarding entries on Vlan-interface100 and all IGMP Snooping forwarding entries in VLAN 100.

```
<Sysname> reset igmp group interface vlan-interface 100 all
```

Clear the IGMP forwarding entries of multicast group 225.0.0.1 on Vlan-interface100 and all the IGMP Snooping forwarding entries of this multicast group in VLAN 100.

```
<Sysname> reset igmp group interface vlan-interface 100 225.0.0.1
```

Clear the IGMP forwarding entries of multicast groups on subnet 225.1.1.0/24 on Vlan-interface100 and the IGMP Snooping forwarding entries of multicast groups on this subnet in VLAN 100.

```
<Sysname> reset igmp group interface vlan-interface 100 225.1.1.0 mask 24
```

robust-count (IGMP view)

Syntax **robust-count** *robust-value*

undo robust-count

View IGMP view

Parameters *robust-value*: IGMP last-member query count.

Description Use the **robust-count** command to configure the IGMP last-member query count globally.

Use the **undo robust-count** command to restore the default setting.

By default, the IGMP last-member query count is 2.

This command is the same as the **igmp robust-count** command for interface view, but the value configured by the **igmp robust-count** command has a higher priority, that is, the system gives priority to configurations made in interface view.

Related commands: **igmp robust-count**, **last-member-query-interval**, **timer other-querier-present**, **display igmp interface**.

Examples # Set the global value of the IGMP last-member query count to 3.

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] robust-count 3
```

send-router-alert (IGMP view)

Syntax **send-router-alert**

undo send-router-alert

View IGMP view

Parameters None

Description Use the **send-router-alert** command to enable globally the insertion of the Router-Alert option into IGMP messages to be sent.

Use the **undo send-router-alert** command to disable globally the insertion of the Router-Alert option into IGMP messages to be sent.

By default, an IGMP message carries the Router-Alert option.

This command is the same as the **igmp send-router-alert** command for interface view, but the value configured by the **igmp send-router-alert** command has a higher priority, that is, the system gives priority to configurations made in interface view.

Related commands: **igmp send-router-alert**, **require-router-alert**.

Examples # Globally disable the insertion of the Router-Alert option in IGMP messages to be sent.

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] send-router-alert
```

timer other-querier-present (IGMP view)

Syntax **timer other-querier-present** *interval*

undo timer other-querier-present

View IGMP view

Parameters *interval*: Other querier present interval.

Description Use the **timer other-querier-present** command to configure the global other querier present interval.

Use the **undo timer other-querier-present** command to restore the global other querier present interval to the default setting.

By default, the other querier present interval is 125 seconds.

This command is the same as the **igmp timer other-querier-present** command for interface view, but the value configured by the **igmp timer other-querier-present** command has a higher priority, that is, the system gives priority to configurations made in interface view.

Related commands: **igmp timer other-querier-present**, **timer query**, **robust-count**, **max-response-time**, **display igmp interface**.

Examples # Set the global value of the other querier present interval to 200 seconds.

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] timer other-querier-present 200
```

timer query (IGMP view)

Syntax **timer query** *interval*

undo timer query

View IGMP view

Parameters *interval*: IGMP query interval in seconds, namely interval between IGMP general queries sent by the querier.

Description Use the **timer query** command to configure the IGMP query interval globally.

Use the **undo timer query** command to restore the default setting.

By default, IGMP query interval is 60 seconds.

This command is the same as the **igmp timer query** command for interface view, but the value configured by the **igmp timer query** command has a higher priority, that is, the system gives priority to configurations made in interface view.

Related commands: **igmp timer query**, **timer other-querier-present**, **display igmp interface**.

Examples # Set the global value of the IGMP query interval to 125 seconds.

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] timer query 125
```

version (IGMP view)

Syntax **version** *version-number*

undo version

View IGMP view

Parameters *version-number*: IGMP version.

Description Use the **version** command to configure the global IGMP version.

Use the **undo version** command to restore the global IGMP version to the system default.

The default IGMP version is version 2.

This command is the same as the **igmp version** command for interface view, but the value configured by the **igmp version** command has a higher priority, that is, the system gives priority to configurations made in interface view.

Related commands: **igmp version**.

Examples # Set the global IGMP version to IGMPv1.

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] version 1
```

45 IGMP SNOOPING CONFIGURATION COMMANDS

debugging igmp-snooping

Syntax **debugging igmp-snooping** { **all** | **event** | **abnormal** | **driver** | **group** | **timer** | **ipc** { **receive** | **send** } | **packet** [**vlan** *vlan-id* [**port** *port-type port-number*]] }

undo debugging igmp-snooping { **all** | **event** | **abnormal** | **driver** | **group** | **timer** | **ipc** { **receive** | **send** } | **packet** }

View User view

Parameters **all**: Specifies all types of debugging for IGMP Snooping.

event: Specifies event debugging for IGMP-Snooping.

abnormal: Specifies abnormal information debugging for IGMP-Snooping.

driver: Specifies driver debugging for IGMP-Snooping.

group: Specifies group debugging for IGMP-Snooping.

timer: Specifies timer debugging for IGMP-Snooping.

ipc: Specifies debugging for IPC packets.

receive: Specifies debugging for received IPC packets.

send: Specifies debugging for sent IPC packets.

packet: Specifies debugging for IGMP messages.

vlan *vlan-id*: Specifies a VLAN ID.

port *port-type port-number*: Specifies a port by its type and number.

Description Use the **debugging igmp-snooping** command to enable debugging for IGMP Snooping.

Use the **undo debugging igmp-snooping** command to disable debugging for IGMP Snooping.

By default, debugging for IGMP Snooping is disabled.

Examples # Enable all types of debugging for IGMP Snooping.

```
<Sysname> debugging igmp-snooping all
```

display igmp-snooping group

Syntax **display igmp-snooping group** [**vlan** *vlan-id*] [**slot** *slot-id*] [**verbose**]

View Any view

Parameters **vlan** *vlan-id*: Displays the multicast group information in the specified VLAN. If you do not specify a VLAN, this command will display the multicast group information in all VLANs.

slot *slot-id*: Displays the multicast group information in the specified module.

verbose: Specifies to display the detailed information of multicast groups.

Description Use the **display igmp-snooping group** command to view the multicast group information learned by IGMP Snooping.

Examples # View the detailed information of multicast groups in VLAN 2 learned by IGMP Snooping.

```
<Sysname> display igmp-snooping group vlan 2 verbose
    Total 1 IP Group(s).
    Total 1 IP Source(s).
    Total 1 MAC Group(s).

  Port flags: D-Dynamic port, S-Static port, A-Aggregation port, C-Copy port
  Subvlan flags: R-Real VLAN, C-Copy VLAN
  Vlan(id):2.
    Total 1 IP Group(s).
    Total 1 IP Source(s).
    Total 1 MAC Group(s).
    Router port(s):total 1 port.
            Ethernet1/1/1                                   (D) ( 00:01:30 )
    IP group(s):the following ip group(s) match to one mac group.
      IP group address:224.1.1.1
        (1.1.1.1, 224.1.1.1):
          Attribute:    Host Port
          Host port(s):total 1 port.
            Ethernet1/1/10                                  (D) ( 00:03:23 )
    MAC group(s):
      MAC group address:0100-5e01-0101
          Host port(s):total 1 port.
            Ethernet1/1/10
```

Table 201 Description of the fields of the display igmp-snooping group command

Field	Description
Total 1 IP Group(s)	Total number of IP multicast groups
Total 1 IP Source(s)	Total number of multicast sources
Total 1 MAC Group(s)	Total number of MAC multicast groups
Port flags: D-Dynamic port, S-Static port, A-Aggregation port, C-Copy port	Port flags: D for dynamic port, S for static port, A for aggregation port, C for port copied from a (*, G) entry to an (S, G) entry

Table 201 Description of the fields of the display igmp-snooping group command

Field	Description
Subvlan flags: R-Real VLAN, C-Copy VLAN	Sub-VLAN flags: R for real egress sub-VLAN under the current entry, C for sub-VLAN copied from a (*, G) entry to an (S, G) entry
Router port(s)	Number of router ports
IP group address	Address of IP multicast group
MAC group address	Address of MAC multicast group
Attribute	Attribute of IP multicast group
Host port(s)	Number of host member ports

display igmp-snooping statistics

Syntax **display igmp-snooping statistics**

View Any view

Parameters None

Description Use the **display igmp-snooping statistics** command to view the statistics information of IGMP messages learned by IGMP Snooping.

Examples # View the statistics information of IGMP messages learned by IGMP Snooping.

```
<Sysname> display igmp-snooping statistics
  Received IGMP general  query packet(s) number:0.
  Received IGMP V1 report packet(s) number:0.
  Received IGMP V2 report packet(s) number:19.
  Received IGMP leave  packet(s) number:0.
  Received IGMP V2 specific query packet(s) number:0.
  Sent     IGMP V2 specific query packet(s) number:0.
  Received IGMP V3 report packet(s) number:1.
  Received IGMP V3 specific query packet(s) number:0.
  Received IGMP V3 specific sg query packet(s) number:0.
  Sent     IGMP V3 specific query packet(s) number:0.
  Sent     IGMP V3 specific sg query packet(s) number:0.
  Received error IGMP packet(s) number:19.
```

Table 202 Description of the fields of the display igmp-snooping statistics command

Field	Description
general query packet(s)	General query message(s)
specific query packet(s)	Group-specific query message(s)
report packet(s)	Report message(s)
leave packet(s)	Leave message(s)
specific sg query packet(s)	Group-and-source-specific query message(s)
error IGMP packets	IGMP messages with errors

drop-unknown (IGMP Snooping view)

Syntax **drop-unknown**

undo drop-unknown

View IGMP Snooping view

Parameters None

Description Use the **drop-unknown** command to enable globally the function of dropping unknown multicast data.

Use the **undo drop-unknown** command to disable globally the function of dropping unknown multicast data.

By default, this function is disabled, that is, unknown multicast data is flooded.

This command works only on an IGMP Snooping-enabled VLAN, but not on a VLAN with IGMP enabled on its VLAN interface.

Examples # Globally enable the device to drop unknown multicast data.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] drop-unknown
```

fast-leave (IGMP Snooping view)

Syntax **fast-leave** [**vlan** *vlan-list*]

undo fast-leave [**vlan** *vlan-list*]

View IGMP Snooping view

Parameters **vlan** *vlan-list*: Configures the fast leave feature for the specified VLAN(s). You can provide up to 10 VLAN lists, by each of which you can specify an individual VLAN in the form of *vlan-id* or a VLAN range in the form of *start-vlan-id* **to** *end-vlan-id*, where the start VLAN ID must be greater than the end VLAN ID.

Description Use the **fast-leave** command to enable the fast leave feature globally.

Use the **undo fast-leave** command to disable the fast leave feature globally.

By default, the fast leave feature is globally disabled.

Note that:

- This command works on an IGMP Snooping-enabled VLAN or on a VLAN with IGMP enabled on its VLAN interface.

- If you do not specify any VLAN, the command will take effect for all VLANs; if you specify a VLAN or multiple VLANs, the command will take effect for the specified VLAN(s) only.

Related commands: **igmp-snooping fast-leave**.

Examples # Enable the fast leave feature globally in VLAN 2.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] fast-leave vlan 2
```

group-policy (IGMP Snooping view)

Syntax **group-policy** *acl-number* [**vlan** *vlan-list*]

undo group-policy [**vlan** *vlan-list*]

View IGMP Snooping view

Parameters *acl-number*: Basic ACL number.

vlan *vlan-list*: Configures a multicast group filter for the specified VLAN(s). You can provide up to 10 VLAN lists, by each of which you can specify an individual VLAN in the form of *vlan-id* or a VLAN range in the form of *start-vlan-id* **to** *end-vlan-id*, where the start VLAN ID must be greater than the end VLAN ID.

Description Use the **group-policy** command to configure a global multicast group filter.

Use the **undo group-policy** command to remove the configured global multicast group filter.

By default, no global multicast group filter is configured, namely a host can join any multicast group.

Note that:

- This command works on an IGMP Snooping-enabled VLAN or on a VLAN with IGMP enabled on its VLAN interface.
- If you do not specify any VLAN, the command will take effect for all VLANs; if you specify a VLAN or multiple VLANs, the command will take effect for the specified VLAN(s) only.
- If the specified ACL does not exist or the ACL rule is null, all multicast groups will be filtered out.
- You can configure different ACL rules for a port in different VLANs; for a given VLAN, a newly configured ACL rule will override the existing one.

Related commands: **igmp-snooping group-policy**.

Examples # Configure ACL 2000 as the multicast group filter in VLAN 2.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] group-policy 2000 vlan 2
```

host-aging-time (IGMP Snooping view)

Syntax **host-aging-time** *interval*

undo host-aging-time

View IGMP Snooping view

Parameters *interval*: Member port aging time, in units of seconds.

Description Use the **host-aging-time** command to configure the aging time of group member ports globally.

Use the **undo host-aging-time** command to restore the default setting.

By default, the aging time of group member ports is 260 seconds.

This command works only on an IGMP Snooping-enabled VLAN, but not on a VLAN with IGMP enabled on its VLAN interface.

Related commands: **igmp-snooping host-aging-time**.

Examples # Set the aging time of group member ports globally to 300 seconds.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] host-aging-time 300
```

igmp-snooping (System view)

Syntax **igmp-snooping**

undo igmp-snooping

View System view

Parameters None

Description Use the **igmp-snooping** command to enable IGMP Snooping globally and enter IGMP Snooping view.

Use the **undo igmp-snooping** command to disable IGMP Snooping globally.

By default, IGMP Snooping is disabled.

Related commands: **igmp-snooping enable**.

CAUTION: *If you execute the* ***undo igmp-snooping*** *command on the IGMP Snooping-enabled switch, all the IGMP Snooping configurations will be lost.*

Examples # Enable IGMP Snooping globally and enter IGMP Snooping view.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping]
```

igmp-snooping enable

Syntax **igmp-snooping enable**

undo igmp-snooping enable

View VLAN view

Parameters None

Description Use the **igmp-snooping enable** command to enable IGMP Snooping in the current VLAN.

Use the **undo igmp-snooping enable** command to disable IGMP Snooping in the current VLAN.

By default, IGMP Snooping is disabled in a VLAN.

Note that:

- IGMP Snooping must be enabled globally before it can be enabled in a VLAN.
- After enabling IGMP Snooping in a VLAN, you cannot enable IGMP and/or PIM on the corresponding VLAN interface, and vice versa.

Related commands: **igmp-snooping**.

Examples # Enable IGMP Snooping in VLAN 2.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
```

igmp-snooping fast-leave

Syntax **igmp-snooping fast-leave** [**vlan** *vlan-list*]

undo igmp-snooping fast-leave [**vlan** *vlan-list*]

View Ethernet interface view/Port group view

Parameters **vlan** *vlan-list*: Configures the fast leave feature for the specified VLAN(s). You can provide up to 10 VLAN lists, by each of which you can specify an individual VLAN in the form of *vlan-id* or a VLAN range in the form of *start-vlan-id* **to** *end-vlan-id*, where the start VLAN ID must be greater than the end VLAN ID.

Description Use the **igmp-snooping fast-leave** command to enable the fast leave feature on the current port or group of ports.

Use the **undo igmp-snooping fast-leave** command to disable the fast leave feature on the current port or group of ports.

By default, the fast leave feature is disabled.

Note that:

- This command works on an IGMP Snooping-enabled VLAN or on a VLAN with IGMP enabled on its VLAN interface.
- If you do not specify any VLAN in Ethernet interface view, the command will take effect on the port no matter which VLAN the port belongs to; if you specify a VLAN or multiple VLANs, the command will take effect on the port only if the port belongs to the specified VLAN(s).
- If you do not specify any VLAN in port group view, the command will take effect on all the ports in this group no matter which VLANs these port belong to; if you specify a VLAN or multiple VLANs, the command will take effect on those ports in this group that belong to the specified VLAN(s).

Related commands: **fast-leave**.

Examples # Enable the fast leave feature on Ethernet1/1/1, which belongs to VLAN 2.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1/1
[Sysname-Ethernet1/1/1] igmp-snooping fast-leave vlan 2
```

igmp-snooping general-query source-ip

Syntax **igmp-snooping general-query source-ip** { **current-interface** | *ip-address* }

undo igmp-snooping general-query source-ip

View VLAN view

Parameters **current-interface**: Sets the source address of IGMP general queries to the address of the current VLAN interface. If the current VLAN interface does not have an IP address, the default IP address 0.0.0.0 will be used as the source IP address of IGMP general queries.

ip-address: Specifies the source address of IGMP general queries, which can be any legal IP address.

Description Use the **igmp-snooping general-query source-ip** command to configure the source address of IGMP general queries.

Use the **undo igmp-snooping general-query source-ip** command to restore the default configuration.

By default, the source IP address of IGMP general queries is 0.0.0.0.

This command takes effect only if IGMP Snooping is enabled in the VLAN.

Examples # Set the IP address of the interface of VLAN 2 to 10.1.1.1, with the subnet mask of 255.255.255.0, and specify this IP address as the source IP address of IGMP general queries.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ip address 10.1.1.1 255.255.255.0
[Sysname-Vlan-interface2] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping general-query source-ip current-interface
```

igmp-snooping group-limit

Syntax **igmp-snooping group-limit** *limit* [**vlan** *vlan-list*]

undo igmp-snooping group-limit [**vlan** *vlan-list*]

View Ethernet interface view/Port group view

Parameters *limit*: Maximum number of multicast groups that can pass the port(s).

vlan *vlan-list*: Configures the maximum number of multicast groups that can pass the ports in the specified VLAN(s). You can provide up to 10 VLAN lists, by each of which you can specify an individual VLAN in the form of *vlan-id* or a VLAN range in the form of *start-vlan-id* **to** *end-vlan-id*, where the start VLAN ID must be greater than the end VLAN ID.

Description Use the **igmp-snooping group-limit** command to configure the maximum number of multicast groups that can pass the port(s).

Use the **undo igmp-snooping group-limit** command to restore the default setting.

The default value is 512.

Note that:

- This command works on an IGMP Snooping-enabled VLAN or on a VLAN with IGMP enabled on its VLAN interface.

- If you do not specify any VLAN in Ethernet interface view, the command will take effect on the port no matter which VLAN the port belongs to; if you specify a VLAN or multiple VLANs, the command will take effect on the port only if the port belongs to the specified VLAN(s).
- If you do not specify any VLAN in port group view, the command will take effect on all the ports in this group no matter which VLANs these port belong to; if you specify a VLAN or multiple VLANs, the command will take effect on those ports in this group that belong to the specified VLAN(s).

Examples # Specify to allow a maximum of 10 multicast groups to pass Ethernet1/1/1, which belongs to VLAN 2.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1/1
[Sysname-Ethernet1/1/1] igmp-snooping group-limit 10 vlan 2
```

igmp-snooping group-policy

Syntax **igmp-snooping group-policy** *acl-number* [**vlan** *vlan-list*]

undo igmp-snooping group-policy [**vlan** *vlan-list*]

View Ethernet interface view/Port group view

Parameters *acl-number*: Basic ACL number.

vlan *vlan-list*: Configures a multicast group filter in the specified VLAN(s). You can provide up to 10 VLAN lists, by each of which you can specify an individual VLAN in the form of *vlan-id* or a VLAN range in the form of *start-vlan-id* **to** *end-vlan-id*, where the start VLAN ID must be greater than the end VLAN ID.

Description Use the **igmp-snooping group-policy** command to configure a multicast group filter on the current port(s).

Use the **undo igmp-snooping group-policy** command to remove a multicast group filter on the current port(s).

Be default, no multicast group filter is configured on an interface, namely a host can join any multicast group

Note that:

- This command works on an IGMP Snooping-enabled VLAN or on a VLAN with IGMP enabled on its VLAN interface.
- If you do not specify any VLAN in Ethernet interface view, the command will take effect on the port no matter which VLAN the port belongs to; if you specify a VLAN or multiple VLANs, the command will take effect on the port only if the port belongs to the specified VLAN(s).
- If you do not specify any VLAN in port group view, the command will take effect on all the ports in this group no matter which VLANs these port belong

to; if you specify a VLAN or multiple VLANs, the command will take effect on those ports in this group that belong to the specified VLAN(s).

- If the specified ACL does not exist or the ACL rule is null, all multicast groups will be filtered out.
- You can configure different ACL rules for a port in different VLANs; for a given VLAN, a newly configured ACL rule will override the existing one.

Related commands: **group-policy**.

Examples # Configure ACL 2000 as the multicast group filter on Ethernet1/1/1, which belongs to VLAN 2.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1/1
[Sysname-Ethernet1/1/1] igmp-snooping group-policy 2000 vlan 2
```

igmp-snooping host-aging-time

Syntax **igmp-snooping host-aging-time** *interval*

undo igmp-snooping host-aging-time

View VLAN view

Parameters *interval*: Member port aging time, in units of seconds.

Description Use the **igmp-snooping host-aging-time** command to configure the aging time of group member ports in the current VLAN.

Use the **undo igmp-snooping host-aging-time** command to restore the default setting.

By default, the aging time of group member ports is 260 seconds.

This command takes effect only if IGMP Snooping is enabled in the VLAN.

Related commands: **host-aging-time**.

Examples # Set the aging time of group member ports to 300 seconds in VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping host-aging-time 300
```

igmp-snooping host-join

Syntax **igmp-snooping host-join** *group-address* [**source-ip** *source-address*] **vlan** *vlan-id*

undo igmp-snooping host-join *group-address* [**source-ip** *source-address*] **vlan** *vlan-id*

View Ethernet interface view/Port group view

Parameters **vlan** *vlan-id*: Specifies the VLAN that comprises the Ethernet port(s).

group-address: Address of the multicast group that the simulated host is to join, in the range of 224.0.1.0 to 239.255.255.255.

source-address: Address of the multicast source that the simulated host is to join. The value of this argument should be a valid unicast address or 0.0.0.0. If the value is 0.0.0.0, this means that no multicast source is specified.

Description Use the **igmp-snooping host-join** command to enable the simulated (*, G) or (S, G) joining function.

Use the **undo igmp-snooping host-join** command to disable the simulated (*, G) or (S, G) joining function.

By default, this function is disabled.

Note that:

- This command works on an IGMP Snooping-enabled VLAN or on a VLAN with IGMP enabled on its VLAN interface.
- The **source-ip** *source-address* option in the command is meaningful only for IGMP Snooping version 3. If IGMP Snooping version 2 is running, although you can include **source-ip** *source-address* in your command, the simulated host responses with only an IGMPv2 report when receiving a query message.
- If configured in Ethernet interface view, this feature takes effect on the port only if the port belongs to the specified VLAN.
- If configured in port group view, this feature takes effect only on those ports in this port group that belong to the specified VLAN.

Examples # Configure Ethernet1/1/1 in VLAN 2 to join (1.1.1.1, 224.1.1.1) as a simulated host.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping version 3
[Sysname-vlan2] quit
[Sysname] interface ethernet 1/1/1
[Sysname-Ethernet1/1/1] igmp-snooping host-join 224.1.1.1 source-ip
1.1.1.1 vlan 2
```

igmp-snooping last-member-query-interval

Syntax **igmp-snooping last-member-query-interval** *interval*

undo igmp-snooping last-member-query-interval

View VLAN view

Parameters *interval*: Interval between IGMP last-member queries, in units of seconds.

Description Use the **igmp-snooping last-member-query-interval** command to configure the interval between IGMP last-member queries in the VLAN.

Use the **undo igmp-snooping last-member-query-interval** command to restore the default setting.

By default, the IGMP last-member query interval is 1 second.

This command takes effect only if IGMP Snooping is enabled in the VLAN.

Related commands: **last-member-query-interval**.

Examples # Set the interval between IGMP last-member queries to 3 seconds in VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping last-member-query-interval 3
```

igmp-snooping max-response-time

Syntax **igmp-snooping max-response-time** *interval*

undo igmp-snooping max-response-time

View VLAN view

Parameters *interval*: Maximum response time to IGMP general queries, in units of seconds.

Description Use the **igmp-snooping max-response-time** command to configure the maximum response time to IGMP general queries in the VLAN.

Use the **undo igmp-snooping max-response-time** command to restore the default setting.

By default, the maximum response time to IGMP general queries is 10 seconds.

This command takes effect only if IGMP Snooping is enabled in the VLAN.

Related commands: **max-response-time** and **igmp-snooping query-interval**.

Examples # Set the maximum response time to IGMP general queries to 5 seconds in VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping max-response-time 5
```

igmp-snooping overflow-replace

Syntax **igmp-snooping overflow-replace** [**vlan** *vlan-list*]

undo igmp-snooping overflow-replace [**vlan** *vlan-list*]

View Ethernet interface view/Port group view

Parameters **vlan** *vlan-list*: Configures the multicast group replacement function in the specified VLAN(s). You can provide up to 10 VLAN lists, by each of which you can specify an individual VLAN in the form of *vlan-id* or a VLAN range in the form of *start-vlan-id* **to** *end-vlan-id*, where the start VLAN ID must be greater than the end VLAN ID.

Description Use the **igmp-snooping overflow-replace** command to enable the multicast group replacement function on the current port(s).

Use the **undo igmp-snooping overflow-replace** command to disable the multicast group replacement function on the current port(s).

By default, the multicast group replacement function is disabled.

Note that:

- This command works on an IGMP Snooping-enabled VLAN or on a VLAN with IGMP enabled on its VLAN interface.
- If you do not specify any VLAN in Ethernet interface view, the command will take effect on the port no matter which VLAN the port belongs to; if you specify a VLAN or multiple VLANs, the command will take effect on the port only if the port belongs to the specified VLAN(s).
- If you do not specify any VLAN in port group view, the command will take effect on all the ports in this group no matter which VLANs these port belong to; if you specify a VLAN or multiple VLANs, the command will take effect on those ports in this group that belong to the specified VLAN(s).

Related commands: **overflow-replace**.

Examples # Enable the multicast group replacement function on Ethernet1/1/1, which belongs to VLAN 2.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1/1
[Sysname-Ethernet1/1/1] igmp-snooping overflow-replace vlan 2
```

igmp-snooping querier

Syntax **igmp-snooping querier**

undo igmp-snooping querier

View VLAN view

Parameters None

Description Use the **igmp-snooping querier** command to enable the IGMP Snooping querier function.

Use the **undo igmp-snooping querier** command to disable the IGMP Snooping querier function.

By default, the IGMP Snooping querier function is disabled.

This command takes effect only if IGMP Snooping is enabled in the VLAN.

Examples # Enable the IGMP Snooping querier function in VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping querier
```

igmp-snooping query-interval

Syntax **igmp-snooping query-interval** *interval*

undo igmp-snooping query-interval

View VLAN view

Parameters *interval*: Interval between IGMP general queries, in units of seconds.

Description Use the **igmp-snooping query-interval** command to configure the interval between IGMP general queries.

Use the **undo igmp-snooping query-interval** command to restore the default setting.

By default, the IGMP general query interval is 60 seconds.

This command takes effect only if IGMP Snooping is enabled in the VLAN.

CAUTION: *In the configuration, make sure that the IGMP general query interval is larger than the maximum response time for IGMP general queries.*

Related commands: **igmp-snooping querier**, **igmp-snooping max-response-time** and **max-response-time**.

Examples # Set the interval between IGMP general queries to 20 seconds in VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping query-interval 20
```

igmp-snooping router-aging-time

Syntax **igmp-snooping router-aging-time** *interval*

undo igmp-snooping router-aging-time

View VLAN view

Parameters *interval*: Router port aging time, in units of seconds.

Description Use the **igmp-snooping router-aging-time** command to configure the aging time of router ports in the current VLAN.

Use the **undo igmp-snooping router-aging-time** command to restore the default setting.

By default, the aging time of router ports is 105 seconds.

This command takes effect only if IGMP Snooping is enabled in the VLAN.

Related commands: **router-aging-time**.

Examples # Set the aging time of router ports to 100 seconds in VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping router-aging-time 100
```

igmp-snooping special-query source-ip

Syntax **igmp-snooping special-query source-ip** { **current-interface** | *ip-address* }

undo igmp-snooping special-query source-ip

View VLAN view

Parameters **current-interface**: Sets the source address of IGMP group-specific queries to the address of the current VLAN interface. If the current VLAN interface does not have an IP address, the default IP address 0.0.0.0 will be used as the source IP address of IGMP group-specific queries.

ip-address: Sets the source address of IGMP group-specific queries to the specified address.

Description Use the **igmp-snooping special-query source-ip** command to configure the source IP address of IGMP group-specific queries.

Use the **undo igmp-snooping special-query source-ip** command to restore the default configuration.

By default, the source IP address of IGMP group-specific queries is 0.0.0.0.

This command takes effect only if IGMP Snooping is enabled in the VLAN.

Examples # Set the IP address of the interface of VLAN 2 to 10.1.1.1, with the subnet mask of 255.255.255.0, and specify this IP address as the source IP address of IGMP group-specific queries.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ip address 10.1.1.1 255.255.255.0
[Sysname-Vlan-interface2] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping special-query source-ip current-interface
```

igmp-snooping static-group

Syntax **igmp-snooping static-group** *group-address* [**source-ip** *source-address*] **vlan** *vlan-id*

undo igmp-snooping static-group *group-address* [**source-ip** *source-address*] **vlan** *vlan-id*

View Ethernet interface view/Port group view

Parameters *group-address*: Address of the multicast group to be statically joined, in the range of 224.0.0.0 to 239.255.255.255.

source-address: Address of multicast source to be statically joined. The value of this argument should be a valid unicast address or 0.0.0.0. If the value is 0.0.0.0, this means no multicast source is specified.

vlan *vlan-id*: Specifies the VLAN that comprises the Ethernet port(s).

Description Use the **igmp-snooping static-group** command to enable the static (*, G) or (S, G) joining function, namely to configure the current port or port group as static multicast group member(s) or static source-group member(s).

Use the **undo igmp-snooping static-group** command to disable the static (*, G) or (S, G) joining function.

By default, this function is disabled.

Note that:

- This command works on an IGMP Snooping-enabled VLAN or on a VLAN with IGMP enabled on its VLAN interface.
- The **source-ip** *source-address* option in the command is meaningful only for IGMP Snooping version 3. If IGMP Snooping version 2 is running, although you can include the **source-ip** *source-address* option in your command, the configuration will not take effect.
- If configured in Ethernet interface view, this feature takes effect on the port only if the port belongs to the specified VLAN.
- If configured in port group view, this feature takes effect only on those ports in this port group that belong to the specified VLAN.

Examples # Configure Ethernet1/1/1 in VLAN 2 to be a static member port for (1.1.1.1, 224.1.1.1).

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping version 3
[Sysname-vlan2] quit
[Sysname] interface ethernet 1/1/1
[Sysname-Ethernet1/1/1] igmp-snooping static-group 224.1.1.1 source-
ip 1.1.1.1 vlan 2
```

igmp-snooping static-router-port

Syntax **igmp-snooping static-router-port vlan** *vlan-id*

undo igmp-snooping static-router-port vlan *vlan-id*

View Ethernet interface view/Port group view

Parameters **vlan** *vlan-id*: Specifies a VLAN in which one or more static router ports are to be configured.

Description Use the **igmp-snooping static-router-port** command to enable the static router port function.

Use the **undo igmp-snooping static-router-port** command to disable the static router port function.

By default, the static router port function is not enabled.

Note that:

- This command works on an IGMP Snooping-enabled VLAN or on a VLAN with IGMP enabled on its VLAN interface.
- If configured in Ethernet interface view, this feature takes effect on the port only if the port belongs to the specified VLAN.

- If configured in port group view, this feature takes effect only on those ports in this port group that belong to the specified VLAN.

Examples # Enable the static router port function on Ethernet1/1/1, which belongs to VLAN 2.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1/1
[Sysname-Ethernet1/1/1] igmp-snooping static-router-port vlan 2
```

igmp-snooping version

Syntax **igmp-snooping version** *version-number*

undo igmp-snooping version

View VLAN view

Parameters *version-number*: IGMP snooping version.

Description Use the **igmp-snooping version** command to configure the IGMP Snooping version.

Use the **undo igmp-snooping version** command to restore the default setting.

By default, the IGMP version is 2.

This command can take effect only if IGMP Snooping is enabled in the VLAN.

Related commands: **igmp-snooping enable**.

Examples # Enable IGMP Snooping in VLAN 2, and set the IGMP Snooping version to version 3.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping version 3
```

last-member-query-interval (IGMP Snooping view)

Syntax **last-member-query-interval** *interval*

undo last-member-query-interval

View IGMP Snooping view

Parameters *interval*: Interval between IGMP last-member queries, in units of seconds.

Description Use the **last-member-query-interval** command to configure the interval between IGMP last-member queries globally.

Use the **undo last-member-query-interval** command to restore the default setting.

By default, the interval between IGMP last-member queries is 1 second.

This command works only on an IGMP Snooping-enabled VLAN, but not on a VLAN with IGMP enabled on its VLAN interface.

Related commands: **igmp-snooping last-member-query-interval**.

Examples # Set the interval between IGMP last-member queries globally to 3 seconds.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] last-member-query-interval 3
```

max-response-time (IGMP Snooping view)

Syntax **max-response-time** *interval*

undo max-response-time

View IGMP Snooping view

Parameters *interval*: Maximum response time to IGMP general queries, in units of seconds.

Description Use the **max-response-time** command to configure the maximum response time to IGMP general queries globally.

Use the **undo max-response-time** command to restore the default value.

By default, the maximum response time to IGMP general queries is 10 seconds.

This command works only on an IGMP Snooping-enabled VLAN, but not on a VLAN with IGMP enabled on its VLAN interface.

Related commands: **igmp-snooping max-response-time** and **igmp-snooping query-interval**.

Examples # Set the maximum response time to IGMP general queries globally to 5 seconds.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] max-response-time 5
```

overflow-replace (IGMP Snooping view)

Syntax **overflow-replace** [**vlan** *vlan-list*]

undo overflow-replace [**vlan** *vlan-list*]

View IGMP Snooping view

Parameters **vlan** *vlan-list*: Configures the multicast group replacement function for the specified VLAN(s). You can provide up to 10 VLAN lists, by each of which you can specify an individual VLAN in the form of *vlan-id* or a VLAN range in the form of *start-vlan-id* **to** *end-vlan-id*, where the start VLAN ID must be greater than the end VLAN ID.

Description Use the **overflow-replace** command to enable the multicast group replacement function.

Use the **undo overflow-replace** command to disable the multicast group replacement function.

By default, the multicast group replacement function is disabled.

Note that:

- This command works on an IGMP Snooping-enabled VLAN or on a VLAN with IGMP enabled on its VLAN interface.
- If you do not specify any VLAN, the command will take effect for all VLANs; if you specify a VLAN or multiple VLANs, the command will take effect for the specified VLAN(s) only.

Related commands: **igmp-snooping overflow-replace**.

Examples # Enable the multicast group replacement function in VLAN 2.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] overflow-replace vlan 2
```

report-aggregation

Syntax **report-aggregation**

undo report-aggregation

View IGMP Snooping view

Parameters None

Description Use the **report-aggregation** command to enable IGMP report suppression.

Use the **undo report-aggregation** command to disable IGMP report suppression.

By default, IGMP report suppression is enabled.

This command works on an IGMP Snooping-enabled VLAN or on a VLAN with IGMP enabled on its VLAN interface.

Examples # Disable IGMP report suppression.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] undo report-aggregation
```

reset igmp-snooping group

Syntax **reset igmp-snooping group** { *group-address* | **all** } [**vlan** *vlan-id*]

View User view

Parameters *group-address*: Address of the multicast group of which the IGMP Snooping entries are to be cleared. The value range is 224.0.1.0 to 239.255.255.255.

all: Specifies to clear all IGMP Snooping entries.

vlan *vlan-id*: Specifies a VLAN in which all IGMP Snooping entries are to be cleared.

Description Use the **reset igmp-snooping group** command to clear IGMP Snooping entries.

Note that:

- This command works only on an IGMP Snooping-enabled VLAN, but not on a VLAN with IGMP enabled on its VLAN interface.
- This command cannot clear IGMP Snooping forwarding entries of static joins.

Examples # Clear all IGMP Snooping entries saved in the switch.

```
<Sysname> reset igmp-snooping group all
```

reset igmp-snooping statistics

Syntax **reset igmp-snooping statistics**

View User view

Parameters None

Description Use the **reset igmp-snooping statistics** command to clear the statistics information of IGMP messages learned by IGMP Snooping.

Examples # Clear the statistics information of all kinds of IGMP messages learned by IGMP Snooping.

```
<Sysname> reset igmp-snooping statistics
```

router-aging-time (IGMP Snooping view)

Syntax **router-aging-time** *interval*

undo router-aging-time

View IGMP Snooping view

Parameters *interval*: Router port aging time, in units of seconds.

Description Use the **router-aging-time** command to configure the aging time of router ports globally.

Use the **undo router-aging-time** command to restore the default setting.

By default, the aging time of router ports is 105 seconds.

This command works only on an IGMP Snooping-enabled VLAN, but not on a VLAN with IGMP enabled on its VLAN interface.

Related commands: **igmp-snooping router-aging-time**.

Examples # Set the aging time of router ports globally to 100 seconds.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] router-aging-time 100
```

46 PIM CONFIGURATION COMMANDS

auto-rp enable

Syntax **auto-rp enable**

undo auto-rp enable

View PIM view

Parameters None

Description Use the **auto-rp enable** command to enable auto-RP.

Use the **undo auto-rp enable** command to disable auto-RP.

By default, auto-RP is disabled.

Related commands: **static-rp**.

Examples # Enable auto-RP.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] auto-rp enable
```

bsr-policy (PIM view)

Syntax **bsr-policy** *acl-number*

undo bsr-policy

View PIM view

Parameters *acl-number*: Basic ACL number. When an ACL is defined, the **source** keyword in the **rule** command specifies a legal BSR source address range.

Description Use the **bsr-policy** command to configure a legal BSR address range to guard against BSR spoofing.

Use the **undo bsr-policy** command to remove the restriction of the BSR address range.

By default, there are no restrictions on the BSR address range, namely all the received BSR messages are regarded to be valid.

Examples # Configure a BSR filtering policy so that only the devices on the segment 10.1.1.0/24 can become the BSR.

```
<Sysname> system-view
[Sysname] acl number 2001
[Sysname-acl-basic-2001] rule permit source 10.1.1.0 0.0.0.255
[Sysname-acl-basic-2001] quit
[Sysname] pim
[Sysname-pim] bsr-policy 2001
```

c-bsr (PIM view)

Syntax **c-bsr** *interface-type interface-number* [*hash-length* [*priority*]]

undo c-bsr

View PIM view

Parameters *interface-type interface-number*: Specifies an interface by its type and number. This configuration can take effect only if PIM-SM is enabled on the interface.

hash-length: Hash mask length for RP selection calculation, 30 by default. If you do not include this keyword in your command, the corresponding global setting will be used.

priority: Priority of the C-BSR, 0 by default. If you do not include this keyword in your command, the corresponding global setting will be used. A larger value of this argument means a higher priority.

Description Use the **c-bsr** command to configure the specified interface as a C-BSR.

Use the **undo c-bsr** command to remove the related C-BSR configuration.

No C-BSR is configured by default.

Related commands: **pim sm**, **c-bsr priority**, and **c-rp**.

Examples # Configure VLAN-interface 4 to be a C-BSR.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] c-bsr vlan-interface 4
```

c-bsr admin-scope

Syntax **c-bsr admin-scope**

undo c-bsr admin-scope

View PIM view

Parameters None

Description Use the **c-bsr admin-scope** command to enable BSR administrative scoping to implement RP-Set distribution based on BSR admin-scope regions.

Use the **undo c-bsr admin-scope** command to disable BSR administrative scoping.

By default, BSR administrative scoping is disabled, namely only one BSR can present in each PIM-SM domain.

Related commands: **c-bsr**, **c-bsr group**, and **c-bsr global**.

Examples # Enable BSR administrative scoping.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] c-bsr admin-scope
```

c-bsr global

Syntax **c-bsr global** [**hash-length** *hash-length* | **priority** *priority*] *

undo c-bsr global

View PIM view

Parameters *hash-length*: Hash mask length for RP selection calculation in the global scope zone. If you do not include this keyword in your command, the corresponding global setting will be used.

priority: Priority of the C-BSR in the global scope zone. If you do not include this keyword in your command, the corresponding global setting will be used. A larger value of this argument means a higher priority.

Description Use the **c-bsr global** command to configure a C-BSR for the global scope zone.

Use the **undo c-bsr global** command to remove the C-BSR configuration for the global scope zone.

By default, no C-BSRs are configured for the global scope zone.

Related commands: **c-bsr group**, **c-bsr hash-length**, and **c-bsr priority**.

Examples # Configure the device to be a C-BSR for the global scope zone, with the priority of 1.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] c-bsr global priority 1
```

c-bsr group

Syntax **c-bsr group** *group-address* { *mask* | *mask-length* } [**hash-length** *hash-length* | **priority** *priority*] *

undo c-bsr group *group-address*

View PIM view

Parameters *group-address*: Multicast group address.

mask: Mask of the multicast group address.

mask-length: Mask length of the multicast group address.

hash-length: Hash mask length for RP selection calculation in the BSR admin-scope region corresponding to the specified multicast group. If you do not include this keyword in your command, the corresponding global setting will be used.

priority: Priority of the C-BSR in the BSR admin-scope region corresponding to a multicast group. If you do not include this keyword in your command, the corresponding global setting will be used. A larger value of this argument means a higher priority.

Description Use the **c-bsr group** command to configure a C-BSR for the BSR admin-scope region associated with the specified group.

Use the **undo c-bsr group** command to remove the C-BSR configuration for the BSR admin-scope region associated with the specified group.

By default, no C-BSRs are configured for BSR admin-scope regions.

Related commands: **c-bsr global**, **c-bsr admin-scope**, **c-bsr hash-length**, and **c-bsr priority**.

Examples # Configure the device to be a C-BSR in the BSR admin-scope region associated with the multicast group address 239.0.0.0/8, with the priority of 10.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] c-bsr group 239.0.0.0 255.0.0.0 priority 10
```

c-bsr hash-length (PIM view)

Syntax **c-bsr hash-length** *hash-length*

undo c-bsr hash-length

View PIM view

Parameters *hash-length*: Hash mask length for RP selection calculation.

Description Use the **c-bsr hash-length** command to configure the global Hash mask length for RP selection calculation.

Use the **undo c-bsr hash-length** command to restore the system default.

By default, the Hash mask length for RP selection calculation is 30.

Related commands: **c-bsr**, **c-bsr global**, and **c-bsr group**.

Examples # Set the global Hash mask length for RP selection calculation to 16.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] c-bsr hash-length 16
```

c-bsr holdtime (PIM view)

Syntax **c-bsr holdtime** *interval*

undo c-bsr holdtime

View PIM view

Parameters *interval*: Bootstrap timeout in seconds.

Description Use the **c-bsr holdtime** command to configure the bootstrap timeout time, namely the length of time a C-BSR waits before it must receive a bootstrap message from the BSR.

Use the **undo c-bsr holdtime** command to restore the default setting.

By default, the bootstrap timeout value is determined by this formula: Bootstrap timeout = Bootstrap interval × 2 + 10.

The default bootstrap interval is 60 seconds, so the default bootstrap timeout = 60 × 2 + 10 = 130 (seconds).

Related commands: **c-bsr** and **c-bsr interval**.

Examples # Set the bootstrap timeout time to 150 seconds.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] c-bsr holdtime 150
```

c-bsr interval (PIM view)

Syntax **c-bsr interval** *interval*

undo c-bsr interval

View PIM view

Parameters *interval*: Bootstrap interval in seconds.

Description Use the **c-bsr interval** command to configure the bootstrap interval, namely the interval at which the BSR sends bootstrap messages.

Use the **undo c-bsr interval** command to restore the default setting.

By default, the bootstrap interval value is determined by this formula: Bootstrap interval = (Bootstrap timeout - 10) ÷ 2.

The default bootstrap timeout is 130 seconds, so the default bootstrap interval = (130 - 10) ÷ 2 = 60 (seconds).

Related commands: **c-bsr** and **c-bsr holdtime**.

Examples # Set the bootstrap interval to 30 seconds.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] c-bsr interval 30
```

c-bsr priority (PIM view)

Syntax **c-bsr priority** *priority*

undo c-bsr priority

View PIM view

Parameters *priority*: Priority of the C-BSR. A larger value of this argument means a higher priority.

Description Use the **c-bsr priority** command to configure the global C-BSR priority.

Use the **undo c-bsr priority** command to restore the default setting.

By default, the C-BSR priority is 0.

Related commands: **c-bsr**, **c-bsr global**, and **c-bsr group**.

Examples # Set the global C-BSR priority to 5.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] c-bsr priority 5
```

c-rp (PIM view)

Syntax **c-rp** *interface-type interface-number* [**group-policy** *acl-number* | **priority** *priority* | **holdtime** *hold-interval* | **advertisement-interval** *adv-interval*] *

undo c-rp *interface-type interface-number*

View PIM view

Parameters *interface-type interface-number*: Specifies an interface, the IP address of which will be advertised as a C-RP address.

acl-number: Basic ACL number. This ACL defines a range of multicast groups the C-RP is going to serve, rather than defining a filtering rule. Any group range matching the **permit** statement in the ACL will be advertised as an RP served group, while configurations matching other statements like **deny** will not take effect.

priority: Priority of the C-RP, defaulting to 0. A larger value of this argument means a lower priority.

hold-interval: C-RP timeout time, in seconds. The default value is 150 seconds. If you do not provide this argument in your command, the corresponding global setting will be used.

adv-interval: C-RP-Adv interval in seconds. The default value is 60 seconds. If you do not provide this argument in your command, the corresponding global setting will be used.

Description Use the **c-rp** command to configure the specified interface a C-RP.

Use the **undo c-rp** command to remove the related C-RP configuration.

No C-RPs are configured by default.

Note that:

- If you do not specify a group range for the C-RP, the C-RP will serve all multicast groups.

- If you wish a device to be a C-RP for multiple group ranges, you need to include these multiple group ranges in multiple rules in the ACL corresponding to the **group-policy** keyword.
- If you carry out this command repeatedly on the same interface, the last configuration will take effect.

Related commands: **c-bsr**.

Examples # Configure VLAN-interface 100 to be a C-RP for multicast groups 225.1.0.0/16 and 226.2.0.0/16, with a priority of 10.

```
<Sysname> system-view
[Sysname] acl number 2069
[Sysname-acl-basic-2069] rule permit source 225.1.0.0 0.0.255.255
[Sysname-acl-basic-2069] rule permit source 226.2.0.0 0.0.255.255
[Sysname-acl-basic-2069] quit
[Sysname] pim
[Sysname-pim] c-rp vlan-interface 100 group-policy 2069 priority 10
```

c-rp advertisement-interval (PIM view)

Syntax **c-rp advertisement-interval** *interval*

undo c-rp advertisement-interval

View PIM view

Parameters *interval*: C-RP-Adv interval in seconds.

Description Use the **c-rp advertisement-interval** command to configure the interval at which C-RP-Adv messages are sent.

Use the **undo c-rp advertisement-interval** command to restore the default setting.

By default, the C-RP-Adv interval is 60 seconds.

Related commands: **c-rp**.

Examples # Set the global C-RP-Adv interval to 30 seconds.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] c-rp advertisement-interval 30
```

c-rp holdtime (PIM view)

Syntax **c-rp holdtime** *interval*

undo c-rp holdtime

View PIM view

Parameters *interval*: C-RP timeout in seconds.

Description Use the **c-rp holdtime** command to configure the global C-RP timeout time, namely the length of time the BSR waits before it must receive a C-RP-Adv message from C-RPs.

Use the **undo c-rp holdtime** command to restore the default setting.

By default, the C-RP timeout time is 150 seconds.

Because a non-BSR router refreshes its C-RP timeout time through BSR bootstrap messages, to prevent loss of BSR bootstrap messages, make sure that the C-RP timeout time is not smaller than the interval at which the BSR sends bootstrap messages. The recommended C-RP timeout setting is 2.5 times the bootstrap interval or longer.

Related commands: **c-rp** and **c-bsr interval**.

Examples # Set the global C-RP timeout time to 200 seconds.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] c-rp holdtime 200
```

crp-policy (PIM view)

Syntax **crp-policy** *acl-number*

undo crp-policy

View PIM view

Parameters *acl-number*: Advanced ACL number. When the ACL is defined, the **source** keyword in the **rule** command specifies the address of a C-RP and the **destination** keyword specifies the address range of the multicast groups that the C-RP will serve.

Description Use the **crp-policy** command to configure a legal C-RP address range and the range of served multicast groups, so as to guard against C-RP spoofing.

Use the **undo crp-policy** command to remove the restrictions in C-RP address ranges and the ranges of served multicast groups.

By default, there are no restrictions on C-RP address ranges and the address ranges of served groups, namely all received C-RP messages are accepted.

Examples # Configure a C-RP address range and a range of served multicast groups so that only routers in the address range of 1.1.1.1/32 can be C-RPs and these C-RPs can serve only multicast groups in the address range of 225.1.0.0/16.

```
<Sysname> system-view
[Sysname] acl number 3100
[Sysname-acl-adv-3100] rule permit ip source 1.1.1.1 0 destination 2
25.1.0.0 0.0.255.255
[Sysname-acl-adv-3100] quit
[Sysname] pim
[Sysname-pim] crp-policy 3100
```

debugging pim

Syntax **debugging pim** { **all** | **event** [*advanced-acl-number*] | **routing-table** [*advanced-acl-number*] | **neighbor** [*basic-acl-number*] [**receive** | **send**] | **assert** [*advanced-acl-number*] [**receive** | **send**] | **rp** [**receive** | **send**] | **join-prune** [*advanced-acl-number*] [**receive** | **send**] | **register** [*advanced-acl-number*] | **msdp** [*advanced-acl-number*] | **state-refresh** [*advanced-acl-number*] [**receive** | **send**] }

undo debugging pim { **all** | **event** | **routing-table** | **neighbor** [**receive** | **send**] | **assert state-refresh** [**receive** | **send**] | **rp** [**receive** | **send**] | **join-prune** [**receive** | **send**] | **register** | **msdp** }

View User view

Parameters **all**: Specifies all types of PIM debugging.

event: Specifies PIM event debugging.

advanced-acl-number: Advanced ACL number.

routing-table: Specifies PIM debugging for routing table state changes.

neighbor: Specifies PIM neighbor debugging.

basic-acl-number: Basic ACL number.

receive: Specifies PIM debugging for received messages.

send: Specifies PIM debugging for sent messages.

assert: Specifies PIM debugging for assert messages.

rp: Specifies PIM RP debugging.

join-prune: Specifies PIM debugging for join-prune messages.

register: Specifies PIM debugging for register messages.

msdp: Specifies PIM-MSDP interaction debugging.

state-refresh: Specifies PIM state-refresh debugging.

Description Use the **debugging pim** command to enable PIM debugging.

Use the **undo debugging pim** command to disable PIM debugging.

By default, PIM debugging is disabled.

Table 203 Field descriptions of the debugging pim assert command

Field	Description
receiving	Assert message received
sending	Assert message sent
on *interfacename*	Interface on which the message was received or sent
pref	Preference value
metric	Metric value
rpt set	RPT bit: 1
rpt unset	RPT bit: 0
reserved field non-zero	Reserved field is non-zero
unknown neighbor	Unknown neighbor
truncated assert packet	Message length is invalid
bad group address	Incorrect group address
bad group mask	Incorrect group address mask
unknown group family	Group address family error
group boundary	Group boundary
bad source address	Incorrect source address
locally scoped	Node-local or link-local scope
Fsm:assert	Assert state machine
current state	Current state of the assert state machine
received event	Type of event received by the assert state machine
loser	The assert state machine is in the Loser state
winner	The assert state machine is in the Winner state
noinfo	The assert state machine is in the Noinfo state
state1->state2	The assert state machine changed from *state1* to *state2*

Table 204 Field descriptions of the debugging pim event command

Field	Description
unsupported PIM version	PIM version not supported
PIM packet too short	The PIM message length is too short
checksum error	Checksum error

Table 204 Field descriptions of the debugging pim event command

Field	Description
non-pim interface	A PIM message is received on a non-PIM-enabled interface.
unsupported type	PIM messages of the specified type are not supported
Socket set option error	Failed to set socket option
Packet send error	Failed to send PIM message
Source address is one of the interfaces address	The source address is the address of the local interface
Source address *address* is invalid	The source address is invalid
Invalid source mask	Incorrect source address mask
Active event received	A source-active event was received.
Inactive event received	A source-inactive event was received.
Clear event received	A clear-entry event was received.
Wrong IIF	Incorrect incoming interface
NoInfo	The downstream state machine is in the Noinfo state.
PPending	The downstream state machine is in the Prune Pending state.
Pruned	The PIM-DM downstream state machine is in the Pruned state.
Joined	The PIM-SM downstream state machine is in the Joined state.
Forwarding	The PIM-DM upstream state machine is in the Forward state.
Pruned	The PIM-DM upstream state machine is in the Pruned state.
AckPending	The PIM-DM upstream state machine is in the Ack Pending state.
Joined	The PIM-SM (S, G) or (*, G) upstream state machine is in the Joined state.
NotJoined	The PIM-SM (S, G) or (*, G) upstream state machine is in the Not Joined state.
PruneTmp	The PIM-SM (S, G, RPT) downstream state machine is in the Prune Tmp state.
PPendingTmp	The PIM-SM (S, G, RPT) downstream state machine is in the Prune Pending Tmp state.
PPT Expired	The prune pending timer timed out.
RPF_Interface changed	The RPF interface changed.
Genid changed	The neighbor generation ID changed.
PT Expired	The prune timer timed out.
Failed to pass MSF	Failed to pass multicast source filtering
NotOriginator	The originator state machine is in the Not Originator state.
Originator	The originator state machine is in the Originator state.
SAT Expired	The source-alive timer timed out.

Table 204 Field descriptions of the debugging pim event command

Field	Description
Join suppressed	The device received a join message to the upstream neighbor on the incoming interface and suppressed its own join message
Override it	The device received a prune message to the upstream neighbor on the incoming interface and sent a join message
ET Expired	The PIM-SM downstream interface aging timer timed out.
register downstream	Registering the outgoing interface
Mcast-Boundary-Changed	Multicast boundary change event

Table 205 Field descriptions of the debugging pim join-assert command

Field	Description
JP	Join/prune message
GFT	Graft message
GAK	Graft-ack message
receiving	Message received
sending	Message sent
unknown address	Unknown address, address decoding failed
bad group address, mask or family	Incorrect group address, mask or family
Bad source address, mask or family	Incorrect source address, mask or family
Upstream	Upstream neighbor information in the message
Groups	Number of groups in the message
Group: *addr*/*mask* --- m joins n prunes	Group information in the message: group address/mask length --- m joins and n prunes
Join: *addr*/*mask* flag	Join: source address/ mask flag
Message truncated. Ignoring message	The message was dropped due to invalid message length
Unable to decode address	Address decoding failed
Upstream neighbor is not this router. Ignoring	The message was dropped because the upstream neighbor is not this device.
group boundary detected for *address1* on *address2*	*address1* is within the multicast boundary configured on the interface corresponding to *address2*
Group *address1* ignored in message on *address2*	*address1* is within the multicast boundary configured on the interface corresponding to *address2*, and this group is ignored
Message from unknown neighbor	A message was received from an unknown neighbor.
Join/Prune received for non-local neighbor	A join/prune message for a non-local upstream neighbor was received
Override timer expires	The prune override timer timed out.

Table 206 Field descriptions of the debugging pim neighbor command

Field	Description
HEL	PIM hello message

Table 206 Field descriptions of the debugging pim neighbor command

Field	Description
hello packet	PIM hello message
receiving	Message received
sending	Message sent
on *interfacename*	Interface on which the message was received or sent
Option: *m*, length: *n*	PIM hello message option: option value, option length: length value
Holdtime:	Holdtime field of the PIM hello message
Tbit	Tbit option
Lan delay	LAN delay option
Override interval	Override interval option
DR priority	DR priority option
Genid	Generation ID option
Version	Version field of the state refresh option
Refresh interval	State refresh interval field
Reserved	Reserved field of the state refresh option
Secondary address(es)	Address in the address list option
Unknown option value	Unknown option
without SR capability	No state refresh capability
Elected as DR on interface *interfacename*	Elected as the DR for the network attached to *interfacename*
Unelected as DR on interface *interfacename*	No longer the DR for the network attached to *interfacename*
PIM Neighbor *address* on interface *interfacename* timed out	Neighbor *address* on *interfacename* timed out

Table 207 Field descriptions of the debugging pim register command

Field	Description
REG	Register message
RSP	Register-stop message
Register Stop	Register stopped
receiving	Message received
sending	Message sent
Border bit	Boundary bit
Null bit	Null bit
src	Source address of the IP packet
dst	Destination address of the IP packet
Non-DR interface	Non-DR interface
probe	Probe message
ignored	Message dropped

Table 208 Field descriptions of the debugging pim routing-table command

Field	Description
Creating	Creating entries
Deleting	Deleting entries
mrt	Multicast routing table
Add oil	Adding outgoing interfaces
Del oil	Deleting outgoing interfaces
Null iif	Null incoming interface
Adding iif	Adding incoming interfaces
Deleting iif	Deleting incoming interfaces
RP is not found	RP is not found

Table 209 Field descriptions of the debugging pim rp command

Field	Description
receiving	Message received
sending	Message sent
auto-RP announce	auto-RP announce message
auto-RP discovery	auto-RP discovery message
C-RP	Candidate RP
CRP	Candidate RP
BSR	BSR bootstrap message
prefix count	Prefix count field in the C-RP advertisement message
priority	Priority field in the C-RP advertisement message
holdtime	Holdtime field in the C-RP advertisement message
Admin Scope Zone	BSR admin-scope region
Bad BSR address	Incorrect BSR address
frag	Fragment tag field in the BSR bootstrap message
pri	Priority field in the BSR bootstrap message
hash mask len	Hash mask length field in the BSR bootstrap message
Group *address/length*: frags *m,* C-RP's *n*	The frags filed corresponding to *address/length* in the BSR bootstrap message is set to m. The number of C-RPs is n.
address pri: *m*, holdtime: *n*	The priority of C-RP address in the BSR bootstrap message is m and holtime is n
Auto-RP discovery packet: RP agent *address*, RP count m, Holdtime n	An auto-RP discovery message was received: RP agent is *address*; RP count is m; and holdtime is n
delete RP-Set	Deleting an RP set
too short length	Message length is too short.
wrong RP agent address	Incorrect RP agent address
wrong RP address	Incorrect RP address
bad group address	Incorrect group address
bad group mask length	Incorrect group mask
bad BSR address	Incorrect BSR address
bad BSR address family	Incorrect BSR address family

Table 209 Field descriptions of the debugging pim rp command

Field	Description
bad BSR hash mask length	Incorrect BSR hash mask length
bad scope zone mask	Incorrect admin-scope mask
Unknown group address family	Incorrect group address family
not directly connected source	Address of a source not directly connected
unknown neighbor	Unknown neighbor
ACL	Access control list
Bad frag-rp-count field	Incorrect frag-rp-count field in the BSR bootstrap message
Bad frag-rp field length	Incorrect total length of frag-rp fields in the BSR bootstrap message
BSR mechanism	BSR mechanism independent of administrative scoping
Upstream to BSR	Upstream to the BSR
no BSR is available	No available BSR.
add register vif	Adding a register virtual interface
Remove register vif	Removing a register virtual interface
Expiring CRP	Aged C-RP
Lose the ASBSR election	Device lost the BSR election for the BSR admin-scope region
Lose the BSR election	Lose the BSR election
locally scoped	Node-local or link-local scope
RP changed	The RP changed.
pending state	The BSR changed to the pending state.
Update the BSR's state to elected	The BSR changed to the elected state.
RPF Failure	RPF check failed.
admin scope multicast address	Address in the admin-scope range

Table 210 Field descriptions of the debugging pim state refresh command

Field	Description
SRM	State refresh message
sending	Message sent
receiving	Message received
Message truncated	Message length is invalid
bad group address	Incorrect group address
Invalid group mask length	Incorrect group mask length
Group address	Group address
Source address	Source address
Originator address	Address of the state refresh message originator
preference	Preference field of the message
metric	Metric field of the message
mask length	Mask length field of the message
ttl	TTL value of the message

Table 210 Field descriptions of the debugging pim state refresh command

Field	Description
prune indicator	Prune indicator flag bit
prune now	Prune now indicator flag bit
assert override	Assert override flag bit

Examples # Enable debugging for receiving PIM assert messages.

```
<Sysname> debugging pim assert receive
*0.594609 router PIM/7/ASSERT:(public net): PIM ver 2 AST receiving
30.1.1.2 ->224.0.0.13 on Vlan-interface30  (P012343)
*0.594609 router PIM/7/ASSERT:(public net): For 229.0.0.1/32 from 10
0.1.1.11, rpt unset, pref 10, metric 3 (P012351)
```

// A PIMv2 assert message is received on VLAN-interface 30, with the source address of 30.1.1.2, the destination address of 224.0.0.13, the multicast group address of 229.0.0.1, and the multicast source address of 100.1.1.11, without RPT bit set. The priority is 10 and the metric value is 3.

display pim bsr-info

Syntax **display pim bsr-info**

View Any view

Parameters None

Description Use the **display pim bsr-info** command to view the BSR information in the PIM-SM domain and the locally configured C-RP information in effect.

Related commands: **c-bsr** and **c-rp**.

Examples # View the BSR information in the current PIM-SM domain and the locally configured C-RP information in effect.

```
<Sysname> display pim bsr-info
Vpn-instance: public net
Elected BSR Address: 12.12.12.9
     Priority: 0
     Hash mask length: 30
     State: Accept Preferred
     Scope: Not scoped
     Uptime: 00:01:16
     Next BSR message scheduled at: 00:01:54
Candidate BSR Address: 12.1.1.1
     Priority: 0
     Hash mask length: 30
     State: Candidate
     Scope: Not scoped

Candidate RP: 12.12.12.9(LoopBack1)
```

```
Priority: 0
HoldTime: 150
Advertisement Interval: 60
Next advertisement scheduled at: 00:00:48
```

Table 211 Field descriptions of the display pim bsr-info command

Field	Description
Vpn-instance	VPN instance name
Elected BSR Address	Address of the elected BSR
Candidate BSR Address	Address of a candidate BSR
Priority	BSR priority
Hash mask length	Hash mask length for RP selection calculation
State	BSR state
Scope	Scope of the BSR
Uptime	Length of time for which this BSR has been up
Next BSR message scheduled at	Length of time in which the BSR will expire
Candidate RP	Address of the C-RP
Priority	Priority of the C-RP
HoldTime	Timeout time of the C-RP
Advertisement Interval	Interval at which the C-RP sends advertisement messages
Next advertisement scheduled at	Length of time in which the C-RP will send the next advertisement message

display pim claimed-route

Syntax **display pim claimed-route** [*source-address*]

View Any view

Parameters *source-address*: Multicast source address persistent to which the unicast route information is to be displayed. If you do not provide this argument, this command will display the information about all unicast routes used by PIM.

Description Use the **display pim claimed-route** command to view the information of unicast routes used by PIM.

If an (S, G) is marked SPT, this (S, G) entry uses a unicast route.

Examples # View the information of all unicast routes used by PIM.

```
<Sysname> display pim claimed-route
Vpn-instance: public net
RPF information about: 172.168.0.0
     RPF interface: Vlan-interface22, RPF neighbor: 172.168.0.2
     Referenced route/mask: 172.168.0.0/24
     Referenced route type: unicast (direct)
     RPF-route selecting rule: preference-preferred
     The (S,G) or (*,G) list dependent on this route entry
     (172.168.0.12, 227.0.0.1)
```

Table 212 Field descriptions of the display pim claimed-route command

Field	Description
Vpn-instance	VPN instance name
RPF interface:	RPF interface type and number
RPF neighbor:	IP address of the RPF neighbor
Referenced route/mask:	Address/mask of the referenced route
Referenced route type:	Type of the referenced route
RPF-route selecting rule:	Rule of RPF route selection
The (S,G) or (*,G) list dependent on this route entry	(S, G) or (*, G) entries using this route

display pim control-message counters

Syntax **display pim control-message counters** [**message-type** { **probe** | **register** | **register-stop** } | [**interface** *interface-type interface-number* | **message-type** { **assert** | **bsr** | **crp** | **graf**t | **graft-ack** | **hello** | **join-prune** | **state-refresh** }] *]

View Any view

Parameters **interface** *interface-type interface-number*: Displays the number of PIM control messages on the specified interface.

assert: Assert message.

bsr: Bootstrap message.

crp: C-RP-Adv message.

graft: Graft message.

graft-ack: Graft-ack message

hello: Hello message

join-prune: Join/prune message

probe: Null register message.

register: Register message.

register-stop: Register-stop message.

state-refresh: State refresh message.

Description Use the **display pim control-message counters** command to view the statistics information of PIM control messages.

Register messages, register-stop messages, and probe messages are for global statistics, so you cannot view the statistics of these messages on the specified interface.

Examples # View the statistics information of all types of PIM control messages on all interfaces.

```
<Sysname> display pim control-message counters
Vpn-instance: public net
PIM global control-message counters:
              Received           Sent      Invalid
Register            20           37           2
Register-Stop       25           20           1
Probe               10           5            0

PIM control-message counters for interface: Pos4/1/1
              Received         Sent         Invalid
Assert          10           5            0
Graft               20           37           2
Graft-Ack           25           20           1
Hello               1232             453          0
Join/Prune      15           30           21
State-Refresh       8            7            1
BSR             3243             589          1
CRP             53           32           0
```

Table 213 Field descriptions of display pim control-message counters

Field	Description
Vpn-instance	VPN instance name
Received	Number of messages received
Sent	Number of messages sent
Invalid	Number of invalid messages
Register	Register messages
Register-Stop	Register-stop messages
Probe	Null register messages
Assert	Assert messages
Graft	Graft messages
Graft-Ack	Graft-ack messages
Hello	Hello messages
Join/Prune	Join/prune messages
State Refresh	State refresh messages
BSR	Bootstrap messages
CRP	C-RP-Adv messages

display pim grafts

Syntax **display pim grafts**

View Any view

Parameters None

Description Use the **display pim grafts** command to view the information about unacknowledged graft messages.

Examples # View the information about unacknowledged graft messages.

```
<Sysname> display pim grafts
Vpn-instance: public net
Source                Group               Age              RetransmitIn
192.168.10.1          224.1.1.1           00:00:24         00:00:02
```

Table 214 Field descriptions of the display pim grafts command

Field	Description
Vpn-instance	VPN instance name
Source	Multicast source address in the graft message
Group	Multicast group address in the graft message
Age	Time in which the graft message will get aged out, in hours:minutes:seconds
RetransmitIn	Time in which the graft message will be retransmitted, in hours:minutes:seconds

display pim interface

Syntax **display pim interface** [*interface-type interface-number*] [**verbose**]

View Any view

Parameters *interface-type interface-number*: Displays the PIM information on a particular interface.

verbose: Displays the detailed PIM information.

Description Use the **display pim interface** command to view the PIM information on the specified interface or all interfaces.

Examples # View the PIM information on all interfaces.

```
<Sysname> display pim interface
Vpn-instance: public net
 Interface           NbrCnt HelloInt   DR-Pri     DR-Address
 Vlan10              0      30         1          10.1.1.1       (local)
 Vlan12              1      30         1          12.1.1.2
```

Table 215 Field descriptions of the display pim interface command

Field	Description
Vpn-instance	VPN instance name
Interface	Interface name
NbrCnt	Number of PIM neighbors
HelloInt	Hello interval
DR-Pri	Priority for DR election
DR-Address	DR IP address

display pim join-prune

Syntax **display pim join-prune mode** { **sm** [**flags** *flag-value*] | **ssm** } [**interface** *interface-type interface-number* | **neighbor** *neighbor-address*] * [**verbose**]

View Any view

Parameters **mode**: Displays the information of joint/prune messages to send in the specified PIM mode. PIM modes include **sm** and **ssm**, which represent PIM-SM and PIM-SSM respectively.

flags *flag-value*: Displays PIM routing entries containing the specified flag. Values and meanings of *flag-value* are as follows:

- **rpt**: Specifies routing entries on the RPT.
- **spt**: Specifies routing entries on the SPT.
- **wc**: Specifies wildcard routing entries.

interface-type interface-number: Displays the information of joint/prune messages to send on the specified interface.

neighbor-address: Displays the information of joint/prune messages to send to the specified PIM neighbor.

verbose: Displays the detailed information of joint/prune messages to send.

Description Use the **display pim join-prune** command to view the information about the join/prune messages to send.

Examples # View the information of joint/prune messages to send in the PIM-SM mode.

```
<Sysname> display pim join-prune mode sm
Vpn-instance: public net

 Expiry Time: 14 sec
 Upstream nbr: 12.1.1.1 (Vlan-interface12)
 0 (*, G) join(s), 1 (S, G) join(s), 0 (S, G, rpt) prune(s)

 Expiry Time: 46 sec
 Upstream nbr: 12.1.1.1 (Vlan-interface12)
 1 (*, G) join(s), 0 (S, G) join(s), 0 (S, G, rpt) prune(s)
 --------------------------------------------------------------------
 Total (*, G) join(s): 1, (S, G) join(s): 1, (S, G, rpt) prune(s): 0
```

Table 216 Field descriptions of the display pim join-prune command

Field	Description
Vpn-instance	VPN instance name
Expiry Time:	Expiry time of sending join/prune messages
Upstream nbr:	IP address of the upstream PIM neighbor and the interface connecting to it
(*, G) join(s)	Number of (*, G) joins to send

Table 216 Field descriptions of the display pim join-prune command

Field	Description
(S, G) join(s)	Number of (S, G) joins to send
(S, G, rpt) prune(s)	Number of (S, G, rpt) prunes

display pim neighbor

Syntax **display pim neighbor** [**interface** *interface-type interface-number* | *neighbor-address* | **verbose**] *

View Any view

Parameters *interface-type interface-number*: Displays the PIM neighbor information on a particular interface.

neighbor-address: Displays the information of a particular PIM neighbor.

verbose: Displays the detailed PIM neighbor information.

Description Use the **display pim neighbor** command to view the PIM neighbor information.

Examples # View the information of all PIM neighbors.

```
<Sysname> display pim neighbor
Vpn-instance: public net
 Total Number of Neighbors = 1

 Neighbor        Interface           Uptime   Expires  Dr-Priority
 12.1.1.1        Vlan12              00:07:28 00:01:33 1
```

Table 217 Field descriptions of the display pim neighbor command

Field	Description
Vpn-instance	VPN instance name
Total Number of Neighbors	Total number of PIM neighbors
Neighbor	Ip address of the PIM neighbor
Interface	Interface connecting the PIM neighbor
Uptime	Length of time for which the PIM neighbor has been up, in hours:minutes:seconds
Expires	Length of time in which the PIM neighbor will expire, in hours:minutes:seconds
Dr-Priority	Designated router priority

display pim routing-table

Syntax **display pim routing-table** [*group-address* [**mask** { *mask-length* | *mask* }] | *source-address* [**mask** { *mask-length* | *mask* }] | **incoming-interface** [*interface-type interface-number* | **register**] | **outgoing-interface** { **include** |

exclude | **match** } { *interface-type interface-number* | **register** } | **mode** *mode-type* | **flags** *flag-value* | **fsm**] *

View Any view

Parameters *group-address*: Multicast group address.

mask: Mask of the multicast group/source address, 255.255.255.255 by default.

mask-length: Mask length of the multicast group/source address, 32 by default.

source-address: Multicast source address.

incoming-interface: Displays routing entries that contain the specified interface as the incoming interface

interface-type interface-number: Specifies an interface by its type and number.

register: Specifies the register interface. This keyword is valid only if *mode-type* is not specified or is **sm**.

outgoing-interface: Displays routing entries of which the outgoing interface is the specified interface.

include: Displays routing entries of which the outgoing interface list includes the specified interface.

exclude: Displays routing entries of which the outgoing interface list does not includes the specified interface.

match: Displays routing entries of which the outgoing interface list includes only the specified interface.

mode *mode-type*: Specifies a PIM mode, where *mode-type* can have the following values:

- **dm**: Specifies PIM-DM
- **sm**: Specifies PIM-SM
- **ssm**: Specifies PIM-SSM

flags *flag-value*: Displays routing entries containing the specified flag(s). The values of *flag-value* and their meanings are as follows:

- **2msdp**: Specifies routing entries to be contained in the next SA message to notify an MSDP peer.
- **act**: Specifies multicast routing entries to which actual data has arrived
- **del**: Specifies multicast routing entries scheduled to be deleted
- **ext**: Specifies routing entries containing outgoing interfaces contributed by other multicast routing protocols
- **loc**: Specifies multicast routing entries on devices directly connecting to the same segment with the multicast source

- **msdp**: Specifies to routing entries learned from MSDP SA messages
- **niif**: Specifies multicast routing entries containing unknown incoming interfaces
- **nonbr**: Specifies routing entries with PIM neighbor searching failure
- **rpt**: Specifies routing entries on RPT branches where (S, G) prunes have been sent to the RP.
- **spt**: Specifies routing entries on the SPT.
- **swt**: Specifies routing entries in the process of RPT-to-SPT switchover.
- **wc**: Specifies wildcard routing entries.

fsm: Displays the detailed information of the finite state machine (FSM).

Description Use the **display pim routing-table** command to view PIM routing table information.

Related commands: **display multicast routing-table** (*Multicast Routing and Forwarding Commands* in the *IP Multicast Volume*).

Examples # View the content of the PIM routing table.

```
<Sysname> display pim routing-table
Vpn-instance: public net
 Total 4 (*, G) entries; 1 (S, G) entry

(*, 225.1.1.1)
     RP: 12.1.1.2 (local)
     Protocol: pim-sm, Flag: WC
     UpTime: 00:16:19
     Upstream interface: Register
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: LoopBack0
             Protocol: static, UpTime: 00:16:19, Expires: -

 (10.1.1.3, 225.1.1.1)
     RP: 12.1.1.2 (local)
     Protocol: pim-sm, Flag: SPT 2MSDP ACT
     UpTime: 00:07:16
     Upstream interface: Vlan-interface12
         Upstream neighbor: 12.1.1.1
         RPF prime neighbor: 12.1.1.1
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: LoopBack0
             Protocol: pim-sm, UpTime:  - , Expires:  -

 (*, 239.192.0.1)
     RP: 12.1.1.2 (local)
     Protocol: pim-sm, Flag: WC
     UpTime: 00:06:53
     Upstream interface: Register
```

```
        Upstream neighbor: NULL
        RPF prime neighbor: NULL
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: Vlan-interface245
            Protocol: igmp, UpTime: 00:06:52, Expires: -

(*, 239.192.245.1)
    RP: 12.1.1.1
    Protocol: pim-sm, Flag: WC
    UpTime: 00:06:45
    Upstream interface: Vlan-interface12
        Upstream neighbor: 12.1.1.1
        RPF prime neighbor: 12.1.1.1
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: Vlan-interface245
            Protocol: igmp, UpTime: 00:06:45, Expires: -

 (*, 239.255.255.250)
    RP: 12.1.1.2 (local)
    Protocol: pim-sm, Flag: WC
    UpTime: 00:06:53
    Upstream interface: Register
        Upstream neighbor: NULL
        RPF prime neighbor: NULL
    Downstream interface(s) information:
    Total number of downstreams: 1
        1: Vlan-interface245
            Protocol: igmp, UpTime: 00:06:53, Expires: -
```

Table 218 Field descriptions of the display pim routing-table command

Field	Description
Vpn-instance	VPN instance name
Total 0 (*, G) entry; 1 (S, G) entry	Number of (S, G) and (*, G) entries in the PIM routing table
(10.1.1.3, 225.1.1.1)	An (S, G) entry in the PIM routing table
(*, 239.192.0.1)	A (*, G) entry in the PIM routing table
Protocol	PIM mode, PIM-SM or PIM-DM
Flag	Flag of an (S, G) or (*, G) entry in the PIM routing table ■ SPT: indicates the (S, G) routing entry is on the SPT. ■ RPT: indicates the (S, G) or (*, G) routing entry is on the RPT. ■ WC: Indicates a (*, G) entry ■ LOC: Indicates this device directly connects to the multicast source
Uptime	Length of time for which the (S, G) or (*, G) entry has existed, in hours:minutes:seconds
Upstream interface	Upstream (incoming) interface of the (S, G) or (*, G) entry
Upstream neighbor	Upstream neighbor of the (S, G) or (*, G) entry

Table 218 Field descriptions of the display pim routing-table command

Field	Description
RPF prime neighbor	RPF neighbor of the (S, G) or (*, G) entry ■ For a (*, G) entry, if this device is the RP, the RPF neighbor of this (*, G) entry is NULL ■ For a (S, G) entry, if this device directly connects to the multicast source, the RPF neighbor of this (S, G) entry is NULL
Downstream interface(s) information	Information of the downstream interface(s), including: ■ Number of downstream interfaces ■ Downstream interface name ■ PIM mode on the downstream interface(s) ■ Uptime of the downstream interface(s) ■ Expiry time of the downstream interface(s)

display pim rp-info

Syntax **display pim rp-info** [*group-address*]

View Any view

Parameters *group-address*: Address of the multicast group of which the RP information is to be displayed. If you do not provide a group address, this command will display the RP information corresponding to all multicast groups.

Description Use the **display pim rp-info** command to view the RP information.

Note that:

- The RP information includes the information of RPs dynamically found by the BSR mechanism and static RPs.
- Because a non-BSR router refreshes its local RP-Set only based on the received BSR bootstrap messages, the system does not delete an RP even if its expiry time is 0. Instead, the system waits for the next bootstrap message from the BSR: if the bootstrap message does not contain information of the RP, the system will delete it.

Examples # View the RP information corresponding to the multicast group 224.0.1.1.

```
<Sysname> display pim rp-info 224.0.1.1
Vpn-instance: public net
BSR RP Address is: 2.2.2.2
     Priority: 0
     HoldTime: 150
     Uptime: 03:01:10
     Expires: 00:02:30
 RP mapping for this group is: 2.2.2.2
```

View the RP information corresponding to all multicast groups.

```
<Sysname> display pim rp-info
Vpn-instance: public net
PIM-SM BSR RP information:
 Group/MaskLen: 224.0.0.0/4
     RP: 2.2.2.2
     Priority: 0
     HoldTime: 150
     Uptime: 03:01:36
     Expires: 00:02:29
```

Table 219 Field descriptions of the display pim rp-info command

Field	Description
Vpn-instance	VPN instance name
BSR RP Address is	IP address of the BSR RP
Group/MaskLen	The multicast group served by the RP
RP	IP address of the RP
Priority	RP priority
HoldTime	RP timeout time
Uptime	Length of time for which the RP has been up, in hours:minutes:seconds
Expires	Length of time in which the RP will expire, in hours:minutes:seconds
RP mapping for this group is:	The IP address of the RP serving the current multicast group

hello-option dr-priority (PIM view)

Syntax **hello-option dr-priority** *priority*

undo hello-option dr-priority

View PIM view

Parameters *priority*: Router priority for DR election. A larger value of this argument means a higher priority.

Description Use the **hello-option dr-priority** command to configure the global value of the router priority for DR election.

Use the **undo hello-option dr-priority** command to restore the default setting.

By default, the router priority for DR election is 1.

Related commands: **pim hello-option dr-priority**.

Examples # Set the router priority for DR election to 3.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] hello-option dr-priority 3
```

hello-option holdtime (PIM view)

Syntax **hello-option holdtime** *interval*

undo hello-option holdtime

View PIM view

Parameters *interval*: PIM neighbor timeout time in seconds.

Description Use the **hello-option holdtime** command to configure the PIM neighbor timeout time.

Use the **undo hello-option holdtime** command to restore the default setting.

By default, the PIM neighbor timeout time is 105 seconds.

This command is effective for both PIM-DM and PIM-SM.

Related commands: **pim hello-option holdtime**.

Examples # Set the global value of the PIM neighbor timeout time to 120 seconds.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] hello-option holdtime 120
```

hello-option lan-delay (PIM view)

Syntax **hello-option lan-delay** *interval*

undo hello-option lan-delay

View PIM view

Parameters *interval*: Prune delay in milliseconds.

Description Use the **hello-option lan-delay** command to configure the global value of prune delay time, namely the length of time the device must wait upon receiving a prune message from downstream before taking the prune action. Within this period of time, if the device receives a prune override message from that downstream device, the prune action will be cancelled.

Use the **undo hello-option lan-delay** command to restore the default setting.

By default, the prune delay to 500 milliseconds.

This command is effective for both PIM-DM and PIM-SM.

Related commands: **hello-option override-interval**, **pim hello-option override-interval**, and **pim hello-option lan-delay**.

Examples # Set the prune delay to 200 milliseconds globally.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] hello-option lan-delay 200
```

hello-option neighbor-tracking (PIM view)

Syntax **hello-option neighbor-tracking**

undo hello-option neighbor-tracking

View PIM view

Parameters None

Description Use the **hello-option neighbor-tracking** command to globally disable join suppression, namely enable neighbor tracking.

Use the **undo hello-option neighbor-tracking** command to enable join suppression.

By default, join suppression is enabled, namely neighbor tracking is disabled.

This command is effective for both PIM-DM and PIM-SM.

Related commands: **pim hello-option neighbor-tracking**.

Examples # Disable join suppression globally.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] hello-option neighbor-tracking
```

hello-option override-interval (PIM view)

Syntax **hello-option override-interval** *interval*

undo hello-option override-interval

View PIM view

Parameters *interval*: Prune override interval in milliseconds.

Description Use the **hello-option override-interval** command to configure the global value of the prune override interval.

Use the **undo hello-option override-interval** command to restore the default setting.

By default, the prune override interval is 2,500 milliseconds.

This command is effective for both PIM-DM and PIM-SM.

Related commands: **hello-option lan-delay**, **pim hello-option lan-delay**, and **pim hello-option override-interval**.

Examples # Set the prune override interval to 2,000 milliseconds globally.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] hello-option override-interval 2000
```

holdtime assert (PIM view)

Syntax **holdtime assert** *interval*

undo holdtime assert

View PIM view

Parameters *interval*: Assert timeout time in seconds.

Description Use the **holdtime assert** command to configure the global value of the assert timeout time.

Use the **undo holdtime assert** command to restore the default setting.

By default, the assert timeout time is 180 seconds.

This command is effective for both PIM-DM and PIM-SM.

Related commands: **holdtime join-prune**, **pim holdtime join-prune**, and **pim holdtime assert**.

Examples # Set the global value of the assert timeout time to 100 seconds.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] holdtime assert 100
```

holdtime join-prune (PIM view)

Syntax **holdtime join-prune** *interval*

undo holdtime join-prune

View PIM view

Parameters *interval*: Join/prune timeout time in seconds.

Description Use the **holdtime join-prune** command to configure the global value of the join/prune timeout time.

Use the **undo holdtime join-prune** command to restore the default setting.

By default, the join/prune timeout time is 210 seconds.

Related commands: **holdtime assert**, **pim holdtime assert**, and **pim holdtime join-prune**.

Examples # Set the global value of the join/prune timeout time to 280 seconds.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] holdtime join-prune 280
```

jp-pkt-size (PIM view)

Syntax **jp-pkt-size** *packet-size*

undo jp-pkt-size

View PIM view

Parameters *packet-size*: Maximum size of join/prune messages in bytes.

Description Use the **jp-pkt-size** command to configure the maximum size of join/prune messages.

Use the **undo jp-pkt-size** command to restore the default setting.

By default, the maximum size of join/prune messages is 8,100 bytes.

Related commands: **jp-queue-size**.

Examples # Set the maximum size of join/prune messages to 1,500 bytes.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] jp-pkt-size 1500
```

jp-queue-size (PIM view)

Syntax **jp-queue-size** *queue-size*

undo jp-queue-size

View PIM view

Parameters *queue-size*: Maximum number of (S, G) entries in a join/prune message.

Description Use the **jp-queue-size** command to configure the maximum number of (S, G) entries in a join/prune message.

Use the **undo jp-queue-size** command to restore the default setting.

By default, a join/prune messages contains a maximum of 1,020 (S, G) entries.

Related commands: **jp-pkt-size**.

Examples # Configure a join/prune messages to contain a maximum of 2,000 (S, G) entries.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] jp-queue-size 2000
```

pim

Syntax **pim**

undo pim

View System view

Parameters None

Description Use the **pim** command to enter PIM view.

Use the **undo pim** command to remove all configurations performed in PIM view.

IP multicast must be enabled on the device before this command can take effect.

Related commands: **multicast routing-enable** in *Multicast Routing and Forwarding Commands* of the *IP Multicast Volume*.

Examples # Enable IP multicast routing and enter PIM view.

```
<Sysname> system-view
[Sysname] multicast routing-enable
[Sysname] pim
[Sysname-pim]
```

pim bsr-boundary

Syntax **pim bsr-boundary**

undo pim bsr-boundary

View VLAN interface view/POS interface view

Parameters None

Description Use the **pim bsr-boundary** command to configure a BSR admin-scope region boundary on the current interface.

Use the **undo pim bsr-boundary** command to remove the configured BSR admin-scope region boundary.

By default, no BSR admin-scope region boundary is configured.

Related commands: **c-bsr**, and **multicast boundary** in *Multicast Routing and Forwarding Commands* of the *IP Multicast Volume*.

Examples # Configure VLAN-interface 100 to be the boundary of the BSR admin-scope region.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim bsr-boundary
```

pim dm

Syntax **pim dm**

undo pim dm

View VLAN interface view/POS interface view

Parameters None

Description Use the **pim dm** command to enable PIM-DM.

Use the **undo pim dm** command to disable PIM-DM.

By default, PIM-DM is disabled.

CAUTION: *After PIM-DM is enabled on a VLAN interface, IGMP snooping cannot be enabled in the VLAN corresponding to the VLAN interface, and vice versa.*

Related commands: **pim sm**.

Examples # Enable PIM-DM on VLAN-interface 4.

```
<Sysname> system-view
[Sysname] interface vlan-interface 4
[Sysname-Vlan-interface4] pim dm
```

pim hello-option dr-priority (VLAN interface view/POS interface view)

Syntax **pim hello-option dr-priority** *priority*

undo pim hello-option dr-priority

View VLAN interface view/POS interface view

Parameters *priority*: Router priority for DR election. A larger value of this argument means a higher priority.

Description Use the **pim hello-option dr-priority** command to configure the router priority for DR election on the current interface.

Use the **undo pim hello-option dr-priority** command to restore the default setting.

By default, the router priority for DR election is 1.

This command is the same as the **hello-option dr-priority** command for PIM view, with the exception of the view in which it is carried out. Configurations performed in PIM view are effective to all interfaces, while configurations performed in interface view are effective to the current interface only. The system gives priority to configurations made in interface view. Configurations made in PIM view are used only if the corresponding configurations have not been carried out in interface view.

Related commands: **hello-option dr-priority**.

Examples # Set the router priority for DR election to 3 on VLAN-interface 4.

```
<Sysname> system-view
[Sysname] interface vlan-interface 4
[Sysname-Vlan-interface4] pim hello-option dr-priority 3
```

pim hello-option holdtime (VLAN interface view/POS interface view)

Syntax **pim hello-option holdtime** *interval*

undo pim hello-option holdtime

View VLAN interface view/POS interface view

Parameters *interval*: PIM neighbor timeout time in seconds.

Description Use the **pim hello-option holdtime** command to configure the PIM neighbor timeout time on the current interface.

Use the **undo pim hello-option holdtime** command to restore the default setting.

By default, the PIM neighbor timeout time is 105 seconds.

This command is the same as the **hello-option holdtime** command for PIM view, with the exception of the view in which it is carried out. Configurations performed in PIM view are effective to all interfaces, while configurations performed in interface view are effective to the current interface only. The system gives priority to configurations made in interface view. Configurations made in PIM view are used only if the corresponding configurations have not been carried out in interface view.

Related commands: **hello-option holdtime**.

Examples # Set the PIM neighbor timeout time to 120 seconds on VLAN-interface 4.

```
<Sysname> system-view
[Sysname] interface vlan-interface 4
[Sysname-Vlan-interface4] pim hello-option holdtime 120
```

pim hello-option lan-delay (VLAN interface view/POS interface view)

Syntax **pim hello-option lan-delay** *interval*

undo pim hello-option lan-delay

View VLAN interface view/POS interface view

Parameters *interval*: Prune delay in milliseconds.

Description Use the **pim hello-option lan-delay** command to configure the prune delay time on the current interface.

Use the **undo pim hello-option lan-delay** command to restore the default setting.

By default, the prune delay to 500 milliseconds.

This command is the same as the **hello-option lan-delay** command for PIM view, with the exception of the view in which it is carried out. Configurations performed in PIM view are effective to all interfaces, while configurations performed in interface view are effective to the current interface only. The system gives priority to configurations made in interface view. Configurations made in PIM view are used only if the corresponding configurations have not been carried out in interface view.

Related commands: **pim hello-option override-interval**, **hello-option override-interval**, and **hello-option lan-delay**.

Examples # Set the prune delay time to 200 milliseconds on VLAN-interface 4.

```
<Sysname> system-view
[Sysname] interface vlan-interface 4
[Sysname-Vlan-interface4] pim hello-option lan-delay 200
```

pim hello-option neighbor-tracking (VLAN interface view/POS interface view)

Syntax **pim hello-option neighbor-tracking**

undo pim hello-option neighbor-tracking

View VLAN interface view/POS interface view

Parameters None

Description Use the **pim hello-option neighbor-tracking** command to disable join suppression, namely enable neighbor tracking, on the current interface.

Use the **undo pim hello-option neighbor-tracking** command to enable join suppression.

By default, join suppression is enabled, namely neighbor tracking is disabled.

This command is the same as the **hello-option neighbor-tracking** command for PIM view, with the exception of the view in which it is carried out. Configurations performed in PIM view are effective to all interfaces, while configurations performed in interface view are effective to the current interface only. The system gives priority to configurations made in interface view. Configurations made in PIM view are used only if the corresponding configurations have not been carried out in interface view.

Related commands: **hello-option neighbor-tracking**.

Examples # Disable join suppression on VLAN-interface 4.

```
<Sysname> system-view
[Sysname] interface vlan-interface 4
[Sysname-Vlan-interface4] pim hello-option neighbor-tracking
```

pim hello-option override-interval

Syntax **pim hello-option override-interval** *interval*

undo pim hello-option override-interval

View VLAN interface view/POS interface view

Parameters *interval*: Prune override interval in milliseconds.

Description Use the **pim hello-option override-interval** command to configure the prune override interval on the current interface.

Use the **undo pim hello-option override-interval** command to restore the default setting.

By default, the prune override interval is 2,500 milliseconds.

This command is the same as the **hello-option override-interval** command for PIM view, with the exception of the view in which it is carried out. Configurations performed in PIM view are effective to all interfaces, while configurations performed in interface view are effective to the current interface only. The system gives priority to configurations made in interface view. Configurations made in PIM view are used only if the corresponding configurations have not been carried out in interface view.

Related commands: **pim hello-option lan-delay**, **hello-option lan-delay**, and **hello-option override-interval**.

Examples # Set the prune override interval to 2,000 milliseconds on VLAN-interface 4.

```
<Sysname> system-view
[Sysname] interface vlan-interface 4
[Sysname-Vlan-interface4] pim hello-option override-interval 2000
```

pim holdtime assert

Syntax **pim holdtime assert** *interval*

undo pim holdtime assert

View VLAN interface view/POS interface view

Parameters *interval*: Assert timeout time in seconds.

Description Use the **pim holdtime assert** command to configure the assert timeout time on the current interface.

Use the **undo pim holdtime assert** command to restore the default setting.

By default, the assert timeout time is 180 seconds.

This command is the same as the **holdtime assert** command for PIM view, with the exception of the view in which it is carried out. Configurations performed in PIM view are effective to all interfaces, while configurations performed in interface view are effective to the current interface only. The system gives priority to configurations made in interface view. Configurations made in PIM view are used only if the corresponding configurations have not been carried out in interface view.

Related commands: **holdtime join-prune**, **pim holdtime join-prune**, and **holdtime assert**.

Examples # Set the assert timeout time to 100 seconds on VLAN-interface 4.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface4] pim holdtime assert 100
```

pim holdtime join-prune

Syntax **pim holdtime join-prune** *interval*

undo pim holdtime join-prune

View VLAN interface view/POS interface view

Parameters *interval*: Join/prune timeout time in seconds, with an effective range of 1 to 65,535.

Description Use the **pim holdtime join-prune** command to configure the join/prune timeout time on the interface.

Use the **undo pim holdtime join-prune** command to restore the default setting.

By default, the join/prune timeout time is 210 seconds.

This command is the same as the **holdtime join-prune** command for PIM view, with the exception of the view in which it is carried out. Configurations performed in PIM view are effective to all interfaces, while configurations performed in interface view are effective to the current interface only. The system gives priority to configurations made in interface view. Configurations made in PIM view are used only if the corresponding configurations have not been carried out in interface view.

Related commands: **holdtime assert**, **pim holdtime assert**, and **holdtime join-prune**.

Examples # Set the join/prune timeout time to 280 seconds on VLAN-interface 4.

```
<Sysname> system-view
[Sysname] interface vlan-interface 4
[Sysname-Vlan-interface4] pim holdtime join-prune 280
```

pim require-genid

Syntax **pim require-genid**

undo pim require-genid

View VLAN interface view/POS interface view

Parameters None

Description Use the **pim require-genid** command enable rejection of hello messages without Generation_ID.

Use the **undo pim require-genid** command to restore the default configuration.

By default, hello messages without Generation_ID are accepted.

Examples # Enable VLAN-interface 4 to reject hello messages without Generation_ID.

```
<Sysname> system-view
[Sysname] interface vlan-interface 4
[Sysname-Vlan-interface4] pim require-genid
```

pim sm

Syntax **pim sm**

undo pim sm

View VLAN interface view/POS interface view

Parameters None

Description Use the **pim sm** command to enable PIM-SM.

Use the **undo pim sm** command to disable PIM-SM.

By default, PIM-SM is disabled.

CAUTION: *After PIM-SM is enabled on a VLAN interface, IGMP snooping cannot be enabled in the VLAN corresponding to the VLAN interface, and vice versa.*

Related commands: **pim dm**, **ssm-policy**.

Examples # Enable PIM-SM on VLAN-interface 4.

```
<Sysname> system-view
[Sysname] interface vlan-interface 4
[Sysname-Vlan-interface4] pim sm
```

pim state-refresh-capable

Syntax **pim state-refresh-capable**

undo pim state-refresh-capable

View VLAN interface view/POS interface view

Parameters None

Description Use the **pim state-refresh-capable** command to enable the state fresh feature on the interface.

Use the **undo pim state-refresh-capable** command to disable the state fresh feature.

By default, the state refresh feature is enabled.

Related commands: **state-refresh-interval**, **state-refresh-rate-limit**, and **state-refresh-ttl**.

Examples # Disable state refresh on VLAN-interface 4.

```
<Sysname> system-view
[Sysname] interface vlan-interface 4
[Sysname-Vlan-interface4] undo pim state-refresh-capable
```

pim timer graft-retry

Syntax **pim timer graft-retry** *interval*

undo pim timer graft-retry

View VLAN interface view/POS interface view

Parameters *interval*: Graft retry period in seconds.

Description Use the **pim timer graft-retry** command to configure the graft retry period.

Use the **undo pim timer graft-retry** command to restore the default setting.

By default, the graft retry period is 3 seconds.

Related commands: timer graft-retry

Examples # Set the graft retry period to 80 seconds on VLAN-interface 4.

```
<Sysname> system-view
[Sysname] interface vlan-interface 4
[Sysname-Vlan-interface4] pim timer graft-retry 80
```

pim timer hello (VLAN interface view/POS interface view)

Syntax **pim timer hello** *interval*

undo pim timer hello

View VLAN interface view/POS interface view

Parameters *interval*: Hello interval in seconds.

Description Use the **pim timer hello** command to configure on the current interface the interval at which hello messages are sent.

Use the **undo pim timer hello** command to restore the default setting.

By default, hello messages are sent at the interval of 30 seconds.

This command is the same as the **timer hello** command for PIM view, with the exception of the view in which it is carried out. Configurations performed in PIM view are effective to all interfaces, while configurations performed in interface view are effective to the current interface only. The system gives priority to configurations made in interface view. Configurations made in PIM view are used only if the corresponding configurations have not been carried out in interface view.

Related commands: **timer hello**.

Examples # Set the hello interval to 40 seconds on VLAN-interface 4.

```
<Sysname> system-view
[Sysname] interface vlan-interface 4
[Sysname-Vlan-interface4] pim timer hello 40
```

pim timer join-prune (VLAN interface view/POS interface view)

Syntax **pim timer join-prune** *interval*

undo pim timer join-prune

View VLAN interface view/POS interface view

Parameters *interval*: Join/prune interval in seconds.

Description Use the **pim timer join-prune** command to configure on the current interface the interval at which join/prune messages are sent.

Use the **undo pim timer join-prune** command to restore the default setting.

By default, the join/prune interval is 60 seconds.

This command is the same as the **timer join-prune** command for PIM view, with the exception of the view in which it is carried out. Configurations performed in PIM view are effective to all interfaces, while configurations performed in interface view are effective to the current interface only. The system gives priority to configurations made in interface view. Configurations made in PIM view are used only if the corresponding configurations have not been carried out in interface view.

Related commands: **timer join-prune**.

Examples # Set the join/prune interval to 80 seconds on VLAN-interface 4.

```
<Sysname> system-view
[Sysname] interface vlan-interface 4
[Sysname-Vlan-interface4] pim timer join-prune 80
```

pim triggered-hello-delay (VLAN interface view/POS interface view)

Syntax **pim triggered-hello-delay** *interval*

undo pim trigged-hello-delay

View VLAN interface view/POS interface view

Parameters *interval*: Maximum delay in seconds between hello messages.

Description Use the **pim triggered-hello-delay** command to configure the maximum delay between hello messages.

Use the **undo pim triggered-hello-delay** command to restore the default setting.

By default, the maximum delay between hello messages is 5 seconds.

Examples # Set the maximum delay between hello messages to 3 seconds on VLAN-interface 4.

```
<Sysname> system-view
[Sysname] interface vlan-interface 4
[Sysname-Vlan-interface4] pim trigged-hello-delay 3
```

probe-interval (PIM view)

Syntax **probe-interval** *interval*

undo probe-interval

View PIM view

Parameters *interval*: Probe time in seconds.

Description Use the **probe-interval** command to configure the probe time, namely the interval at which the DR sends null register messages before the register suppression timer expires.

Use the **undo probe-interval** command to restore the default setting.

By default, the probe time is 5 seconds.

Related commands: **register-suppression-timeout**.

Examples # Set the probe time to 6 seconds.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] probe-interval 6
```

register-whole-checksum (PIM view)

Syntax **register-whole-checksum**

undo register-whole-checksum

View PIM view

Parameters None

Description Use the **register-whole-checksum** command to configure the router to calculate the checksum based on the entire register messages.

Use the **undo register-whole-checksum** command to restore the default configuration.

By default, the checksum is calculated based on the header in the register message.

Related commands: **register-policy** and **register-suppression-timeout**.

Examples # Configure the router to calculate the checksum based on the entire register messages.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] register-whole-checksum
```

register-policy (PIM view)

Syntax **register-policy** *acl-number*

undo register-policy

View PIM view

Parameters *acl-number*: Advanced ACL number. Only register messages that match the **permit** statement of the ACL can be accepted by the RP.

Description Use the **register-policy** command to configure an ACL rule to filter register messages.

Use the **undo register-policy** command to remove the configured register filtering rule.

By default, no register filtering rule is configured.

Related commands: **register-suppression-timeout**.

Examples # Configure the RP to accept only those register messages for multicast traffic from multicast sources in the range of 10.10.0.0/16 to multicast groups in the range of 225.1.0.0/16.

```
<Sysname> system-view
[Sysname] acl number 3000
[Sysname-acl-adv-3000] rule permit ip source 10.10.0.0 0.0.255.255 d
estination 225.1.0.0 0.0.255.255
[Sysname-acl-adv-3000] quit
[Sysname] pim
[Sysname-pim] register-policy 3000
```

register-suppression-timeout (PIM view)

Syntax **register-suppression-timeout** *interval*

undo register-suppression-timeout

View PIM view

Parameters *interval*: Register suppression timeout in seconds.

Description Use the **register-suppression-timeout** command to configure the register suppression timeout time.

Use the **undo register-suppression-timeout** command to restore the default setting.

By default, the register suppression timeout time is 60 seconds.

Related commands: **probe-interval** and **register-policy**.

Examples # Set the register suppression timeout time to 70 seconds.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] register-suppression-timeout 70
```

reset pim control-message counters

Syntax **reset pim control-message counters** [**interface** *interface-type interface-number*]

View User view

Parameters **interface** *interface-type interface-number*: Specifies an interface on which the PIM control message counter is to be reset. If no interface is specified, this command will clear the statistics information of PIM control messages on all interfaces.

Description Use the **reset pim control-message counters** command to reset PIM control message counters.

Examples # Reset PIM control message counters on all interfaces.

```
<Sysname> reset pim control-message counters
```

source-lifetime (PIM view)

Syntax **source-lifetime** *interval*

undo source-lifetime

View PIM view

Parameters *interval*: Multicast source lifetime in seconds.

Description Use the **source-lifetime** command to configure the multicast source lifetime.

Use the **undo source-lifetime** command to restore the default setting.

By default, the lifetime of a multicast source is 210 seconds.

Related commands: **state-refresh-interval**.

Examples # Set the multicast source lifetime to 200 seconds.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] source-lifetime 200
```

source-policy (PIM view)

Syntax **source-policy** *acl-number*

undo source-policy

View PIM view

Parameters *acl-number*: Basic or advanced ACL number.

Description Use the **source-policy** command to configure a multicast data filter.

Use the **undo source-policy** command to remove the configured multicast data filter.

By default, no multicast data filter is configured.

Note that:

- If you specify a basic ACL, the device filters all the received multicast packets based on the source address, and discards packets that fail the source address match.
- If you specify an advanced ACL, the device filters all the received multicast packets based on the source and group addresses, and discards packets that fail the match.
- If this command is executed repeatedly, the last configuration will take effect.

Examples # Configure the router to accept multicast packets originated from 10.10.1.2 and discard multicast packets originated from 10.10.1.1.

```
<Sysname> system-view
[Sysname] acl number 2001
[Sysname-acl-basic-2001] rule permit source 10.10.1.2 0
[Sysname-acl-basic-2001] rule deny source 10.10.1.1 0
[Sysname-acl-basic-2001] quit
[Sysname] pim
[Sysname-pim] source-policy 2001
```

spt-switch-threshold (PIM view)

Syntax **spt-switch-threshold infinity** [**group-policy** *acl-number* [**order** *order-value*]]

undo spt-switch-threshold [**group-policy** *acl-number*]

View PIM view

Parameters **group-policy** *acl-number*: Disables RPT-to-SPT switchover for multicast groups that match the specified multicast policy. In this option, *acl-number* refers to a basic ACL number, in the range of 2000 to 2999. If you do not include this option in your command, this command will take effect for all multicast groups.

order *order-value*: Specifies the order of the ACL in the group-policy list, where *order-value* has an effective range of 1 to (the largest order value in the existing group-policy list + 1), but the value range should not include the original order value of the ACL in the group-policy list. If you have assigned an *order-value* to a certain ACL, do not specify the same *order-value* for another ACL; otherwise the system will give error information. If you do not specify an *order-value*, the order value of the ACL will remain the same in the group-policy list.

Description Use the **spt-switch-threshold infinity** command to disable RPT-to-SPT switchover.

Use the **undo spt-switch-threshold** command to restore the default configuration.

By default, the Switch 8800 switches to the SPT immediately after it receives the first multicast packet from the RPT.

Note that:

- To adjust the order of an existing ACL in the group-policy list, you can use the *acl-number* argument to specify this ACL and set its *order-value*. This will insert the ACL to the position of *order-value* in the group-policy list. The order of the other existing ACLs in the group-policy list will remain unchanged.
- To use an ACL that does not exist in the group-policy list, you can use the *acl-number* argument to specify an ACL and set its *order-value*. This will insert the ACL to the position of *order-value* in the group-policy list. If you do not include the **order** *order-value* option in your command, the ACL will be appended to the end of the group-policy list.
- If you use this command multiple times on the same multicast group, the first traffic rate configuration matched in sequence will take effect.
- To avoid forwarding failure, do not disable RPT-to-SPT switchover on a switch that may become an RP (namely, a static RP or a C-RP).

Examples # Disable RPT-to-SPT switchover on a switch.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] spt-switch-threshold infinity
```

ssm-policy

Syntax **ssm-policy** *acl-number*

undo ssm-policy

View PIM view

Parameters *acl-number*: Basic ACL number.

Description Use the **ssm-policy** command to configure the SSM group range.

Use the **undo ssm-policy** command to restore the system default.

By default, the SSM group range is 232.0.0.0/8.

This command allows you to define an address range of permitted or denied multicast sources or groups. If the match succeeds, the multicast mode will be PIM-SSM; otherwise the multicast mode will be PIM-SM.

Examples # Configure 232.1.0.0/16 as the permitted group address range in the PIM-SSM domain.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 232.1.0.0 0.0.255.255
[Sysname-acl-basic-2000] quit
[Sysname] pim
[Sysname-pim] ssm-policy 2000
```

state-refresh-interval (PIM view)

Syntax **state-refresh-interval** *interval*

undo state-refresh-interval

View PIM view

Parameters *interval*: State refresh interval in seconds.

Description Use the **state-refresh-interval** command to configure the interval between state refresh messages.

Use the **undo state-refresh-interval** command to restore the default setting.

By default, the state refresh interval is 60 seconds.

Related commands: **pim state-refresh-capable**, **state-refresh-rate-limit**, and **state-refresh-ttl**.

Examples # Set the state refresh interval to 70 seconds.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] state-refresh-interval 70
```

state-refresh-rate-limit (PIM view)

Syntax **state-refresh-rate-limit** *interval*

undo state-refresh-rate-limit

View PIM view

Parameters *interval*: Time to wait before receiving a new refresh message.

Description Use the **state-refresh-rate-limit** command to configure the time the router must wait before receiving a new state refresh message.

Use the **undo state-refresh-rate-limit** command to restore the default setting.

By default, the device waits 30 seconds before receiving a new state refresh message.

Related commands: **pim state-refresh-capable**, **state-refresh-interval**, and **state-refresh-ttl**.

Examples Configure the device to wait 45 seconds before receiving a new state refresh message.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] state-refresh-rate-limit 45
```

state-refresh-ttl (PIM view)

Syntax **state-refresh-ttl** *ttl-value*

undo state-refresh-ttl

View PIM view

Parameters *ttl-value*: Time-to-live (TTL) value of state refresh messages.

Description Use the **state-refresh-ttl** command to configure the TTL value of state refresh messages.

Use the **undo state-refresh-ttl** command to restore the default setting.

By default, the TTL value of state refresh messages is 255.

Related commands: **pim state-refresh-capable**, **state-refresh-interval**, and **state-refresh-rate-limit**.

Examples # Configure the device to send PIM state refresh messages with a TTL of 45.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] state-refresh-ttl 45
```

static-rp (PIM view)

Syntax **static-rp** *rp-address* [*acl-number*] [**preferred**]

undo static-rp *rp-address*

View PIM view

Parameters *rp-address*: IP address of the static RP to be configured. This address must be a legal unicast IP address.

acl-number: Basic ACL number. If you provide this argument, the configured static RP will serve only those groups that pass the ACL filtering; otherwise, the configured static RP will serve the all-system group 224.0.0.0/4.

preferred: Specifies to give priority to the static RP if the static RP conflicts with the dynamic RP. If you do not include the **preferred** keyword in your command, the dynamic RP will be given priority, and the static RP takes effect on if no dynamic RP exists in the network or when the dynamic RP fails.

Description Use the **static-rp** command to configure a static RP.

Use the **undo static-rp** command to configure a static RP.

By default, no static RP is configured.

Note that:

- PIM-SM or PIM-DM cannot be enabled on an interface that serves as a static RP.
- When the ACL rule applied on a static RP changes, a new RP must be elected for all the multicast groups.
- You can configure multiple static RPs by using this command repeatedly. However, if you carry out this command multiple times and specify the same static RP address or reference the same ACL rule, the last configuration will override the previous one. If multiple static RPs have been configured for the same multicast group, the one with the highest IP address will be chosen to serve the multicast group.
- You can configure up to 50 static RPs on the same device.

Related commands: **display pim rp-info** and **auto-rp enable**.

Examples # Configure the interface with the IP address 11.110.0.6 to be a static RP that serves the multicast groups defined in ACL 2001, and give priority to this static RP in the case of static/dynamic RP conflict.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] static-rp 11.110.0.6 2001 preferred
```

timer hello (PIM view)

Syntax **timer hello** *interval*

undo timer hello

View PIM view

Parameters *interval*: Hello interval in seconds.

Description Use the **timer hello** command to configure the hello interval globally.

Use the **undo timer hello** command to restore the default setting.

By default, hello messages are sent at the interval of 30 seconds.

Examples # Set the global hello interval to 40 seconds.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] timer hello 40
```

timer join-prune (PIM view)

Syntax **timer join-prune** *interval*

undo timer join-prune

View PIM view

Parameters *interval*: Join/prune interval in seconds.

Description Use the **timer join-prune** command to configure the join/prune interval globally.

Use the **undo timer join-prune** command to restore the default setting.

By default, the join/prune interval is 60 seconds.

Related commands: **pim timer join-prune**.

Examples # Set the global join/prune interval to 80 seconds.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] timer join-prune 80
```

47 MSDP CONFIGURATION COMMANDS

cache-sa-enable

Syntax **cache-sa-enable**

undo cache-sa-enable

View MSDP view

Parameters None

Description Use the **cache-sa-enable** command to enable the SA message cache mechanism.

Use the **undo cache-sa-enable** command to disable the SA message cache mechanism.

By default, the SA message cache mechanism is enabled.

Examples # Disable the SA message cache mechanism.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] undo cache-sa-enable
```

debugging msdp

Syntax **debugging msdp** { **all** | **connect** | **event** | **packet** | **source-active** }

undo debugging msdp { **all** | **connect** | **event** | **packet** | **source-active** }

View User view

Parameters **all**: Specifies all types of debugging for MSDP.

connect: Specifies debugging for MSDP peer connection resets.

event: Specifies debugging for MSDP events.

packets: Specifies debugging for MSDP messages.

source-active: Specifies MSDP source-active debugging.

Description Use the **debugging msdp** command to enable debugging for MSDP.

Use the **undo debugging msdp** command to disable debugging for MSDP.

By default, debugging for MSDP is disabled.

Table 220 Field descriptions of the debugging msdp command

Field	Description
MSDP event debugging switch is on	MSDP event debugging is enabled.
MSDP packet debugging switch is on	MSDP message debugging is enabled.
MSDP connect debugging switch is on	Debugging for MSDP peer connection resets is enabled.
MSDP source-active debugging switch is on	MSDP source-active debugging is enabled.

Table 221 Field descriptions of the debugging msdp event command

Field	Description
Originating/adding/sending SA message	Creating/adding/sending SA message
SA/SA with data/	SA message/SA message with data/
Notification/	Notification/
SA request/	SA request/
SA response	SA response
(*sadd, gadd*)	(S,G) entry
Creating/Deleting	Creating/Deleting timer
TCP listening/	TCP listening/
Connection accepted/	Connection accepted/
TCP connection established/	TCP connection established/
TCP connect/	TCP connection/
ConnectRetry/	Connection retry/
Connection reset/	Connection reset/
State error/	State error/
Peer reset/	MSDP peer connection reset/
SessionRetry	Session retry
Can not pass acl filter/passed acl filter	SA message failed ACL filtering/SA messages passed ACL filtering
Static RPF peer/	Static RPF neighbor/
E-MBGP peer/	E-MBGP neighbor/
I-MBGP peer/	I-MBGP neighbor/
NOT BGP peer/	NOT BGP neighbor/
NOT MBGP peer	NOT MBGP neighbor

Table 222 Field descriptions of the debugging msdp packet command

Field	Description

Table 222 Field descriptions of the debugging msdp packet command

Reading from peer blocked/	Message reading blocked/
Retrying read/	Retrying reading/
Reading from peer failed/	Reading failed/
Received illegal message from peer/	Illegal character read/
Received n-bytes message/	Total size of messages read is n bytes
	Types of messages read:
SA-TLV/	SA/
SA-Request TLV/	SA request/
SA-Response TLV/	SA response/
KeepAlive TLV/	KeepAlive/
Notification TLV/	Notification
Sending/	Sending SA/
Received/	Received SA/
SA message discarded/	Discarded SA/
Forwarding	Forwarding SA

Table 223 Field descriptions of the debugging msdp source-active command

Field	Description
RPF check failed/	RPF check failed/
RPF check passed	RPF check succeeded
	Conditions for a successful RPF check:
Only one peer/	Only one MSDP peer/
Peer is original RP/	MSDP peer address is an RP address/
Peer belongs mesh-group/	MSDP peer belongs to a mesh group/
Static RPF peer/	Static RPF peer/
MSDP Peer is E-MBGP peer/	MSDP peer is an E-MBGP neighbor/
Peer's AS is the next-AS to RP/	MSDP peer is in the next AS to the RP/
MSDP Peer is I-MBGP peer/	MSDP peer is an I-MBGP neighbor/
Peer is the next-hop to RP	MSDP peer is the next hop to the RP

Examples # Enable MSDP event debugging.

```
<Sysname> debugging msdp event
*Aug 25 09:33:13:130 2006 ar2 MSDP/7/EVENT:
11.11.11.11: TCP listening (H12726)
```

// Server 11.11.11.11 starts TCP listening

```
*Aug 25 09:35:45:790 2006 ar2 MSDP/7/EVENT:
11.11.11.11: Connection accepted (H12850)
*Aug 25 09:35:45:790 2006 ar2 MSDP/7/EVENT:
11.11.11.11: TCP connection established (H12854)
```

// TCP connection established

```
*Aug 25 09:35:45:790 2006 ar2 MSDP/7/EVENT:
11.11.11.11: Sending message to peer: keepalive (H101045)
```

// Sending KeepAlive message to MSDP peer

```
*Aug 25 09:35:45:790 2006 ar2 MSDP/7/EVENT:
11.11.11.11: Originating SA message for peer (H10859)
```

// Sending SA message (if any) to peer

Enable MSDP message debugging.

```
<Sysname> debugging msdp packet
*Aug 25 09:39:07:162 2006 ar2 MSDP/7/PACKET:
11.11.11.11: Sending a 3-bytes message to peer (H17119)
```

// Sending a 3-byte message to MSDP peer

```
*Aug 25 09:39:07:162 2006 ar2 MSDP/7/PACKET:
11.11.11.11: Sending to peer success, 3-bytes sent (H17143)
```

// Message successfully sent to MSDP peer

```
*Aug 25 09:39:07:162 2006 ar2 MSDP/7/PACKET:
11.11.11.11: Received 3-bytes message 1 from peer (H13471)
```

// MSDP peer received 1 message, total size being 3 bytes

```
*Aug 25 09:39:07:162 2006 ar2 MSDP/7/PACKET:
11.11.11.11: KeepAlive TLV (H131441)
```

// This message is a KeepAlive message

Enable MSDP source-active debugging.

```
<Sysname> debugging msdp source-active
*Aug 25 09:52:08:924 2006 ar2 MSDP/7/SOURCE-ACTIVE:
11.11.11.11: Only one peer, passed RPF check (H132426)
```

// Because there is only one MSDP peer, the SA message passed the RPF check

display msdp brief

Syntax **display msdp brief** [**state** { **connect** | **down** | **listen** | **shutdown** | **up** }]

View Any view

Parameters **state**: Displays the information of MSDP peers in the specified state.

connect: Displays the information of MSDP peers in the connecting state.

down: Displays the information of MSDP peers in the down state.

listen: Displays the information of MSDP peers in the listening state.

shutdown: Displays the information of MSDP peers in the deactivated state.

up: Displays the information of MSDP peers in the in-session state.

Description Use the **display msdp brief** command to view the brief information of MSDP peers.

Examples # View the brief information of MSDP peers in all states.

```
<Sysname> display msdp brief
MSDP Peer Brief Information
  Configured   Up           Listen       Connect      Shutdown     Down
  1            1            0            0            0            0

  Peer's Address     State   Up/Down time   AS     SA Count  Reset Count
20.20.20.20        Up      00:00:13       100    0         0
```

Table 224 Field descriptions of the display msdp brief command

Field	Description
Peer's Address	MSDP peer address
State	MSDP peer status: ■ Up: Session set up; MSDP peer in session ■ Listen: Session set up; local device as server, in listening state ■ Connect: Session not set up; local device as client, in connecting state ■ Shutdown: Deactivated ■ Down: Connection failed
Up/Down time	Time passed since MSDP peer connection establishment/failure
AS	Number of the AS where the MSDP peer is located. "?" indicates that the system was unable to obtain the AS number
SA Count	Number of (S, G) entries
Reset Count	MSDP peer connection reset times

display msdp peer-status

Syntax **display msdp peer-status** [*peer-address*]

View Any view

Parameters *peer-address*: Specifies an MSDP peer by its address. If you do not provide this argument, this command will display the detailed status information of all MSDP peers.

Description Use the **display msdp peer-status** command to view the detailed MSDP peer status information.

Related commands: **peer connect-interface**, **peer description**, **peer mesh-group**, **peer minimum-ttl**, **peer request-sa-enable**, **peer sa-cache-maximum**, **peer sa-policy**, and **peer sa-request-policy**.

Examples # View the detailed status information of all MSDP peers.

```
<Sysname> display msdp peer-status
  MSDP Peer 20.20.20.20, AS 100
  Description:
  Information about connection status:
    State: Up
    Up/down time: 14:41:08
    Resets: 0
    Connection interface: LoopBack0 (20.20.20.30)
    Number of sent/received messages: 867/947
    Number of discarded output messages: 0
    Elapsed time since last connection or counters clear: 14:42:40
  Information about (Source, Group)-based SA filtering policy:
    Import policy: none
    Export policy: none
  Information about SA-Requests:
    Policy to accept SA-Request messages: none
    Sending SA-Requests status: disable
  Minimum TTL to forward SA with encapsulated data: 0
  SAs learned from this peer: 0, SA-cache maximum for the peer: none
  Input queue size: 0, Output queue size: 0
  Counters for MSDP message:
    Count of RPF check failure: 0
    Incoming/outgoing SA messages: 0/0
    Incoming/outgoing SA requests: 0/0
    Incoming/outgoing SA responses: 0/0
Incoming/outgoing data packets: 0/0
```

Table 225 Field descriptions of the display msdp peer-status command

Field	Description
MSDP Peer	MSDP peer address
AS	Number of the AS where the MSDP peer is located. "?" indicates that the system was unable to obtain the AS number
State	MSDP peer status: ■ Up: Session set up; MSDP peer in session ■ Listen: Session set up; local device as server, in listening state ■ Connect: Session not set up; local device as client, in connecting state ■ Shutdown: Deactivated ■ Down: Connection failed
Resets	Number of times the MSDP peer connection is reset
Up/Down time	Time passed since MSDP peer connection establishment/failure
Connection interface	Interface and its IP address used for setting up a TCP connection with the remote MSDP peer
Number of sent/received messages	Number of SA messages sent and received through this connection
Number of discarded output messages	Number of discarded outgoing messages
Elapsed time since last connection or counters clear	Time passed since the information of the MSDP peer was last cleared

Table 225 Field descriptions of the display msdp peer-status command

Field	Description
Information about (Source, Group)-based SA filtering policy	SA message filtering list information ■ Import policy: Filter list for receiving SA messages from the specified MSDP peer ■ Export policy: Filter list for forwarding SA messages from the specified MSDP peer
Information about SA-Requests	SA requests information ■ Policy to accept SA-Request messages: Filtering rule for receiving or forwarding SA messages from the specified MSDP peer ■ Sending SA-Requests status: Whether enabled to send an SA request message to the designated MSDP peer upon receiving a new Join message
Minimum TTL to forward SA with encapsulated data	Minimum TTL of multicast packet encapsulated in SA messages
SAs learned from this peer	Number of cached SA messages
SA-cache maximum for the peer	Maximum number of SA messages from the specified MSDP peer that can cached
Input queue size	Data size cached in the input queue
Output queue size	Data size cached in the output queue
Counters for MSDP message	MSDP peer statistics: ■ Count of RPF check failure: Number of SA messages discarded due to RPF check failure ■ Incoming/outgoing SA messages: Number of SA messages received and sent ■ Incoming/outgoing SA requests: Number of SA request received and sent ■ Incoming/outgoing SA responses: Number of SA responses received and sent ■ Incoming/outgoing data packets: Number of received and sent SA messages encapsulated with multicast data

display msdp sa-cache

Syntax **display msdp sa-cache** [*group-address* | *source-address* | *as-number*] *

View Any view

Parameters *group-address*: Multicast group address in the (S, G) entry.

source-address: Multicast source address in the (S, G) entry.

as-number: AS number.

Description Use the **display msdp sa-cache** command to view the information of (S, G) entries in the MSDP cache.

Note that:

- This command gives the corresponding output only after the **cache-sa-enable** command is executed.
- If you do not provide a source address, this command will display the information of all sources in the specified multicast group.
- If you do not provide a group address and a source address, this command will display the information of all cached entries.
- If you do not provide an AS number, this command will display the information related to all ASs.

Related commands: **cache-sa-enable**.

Examples # View the information of (S, G) entries in the MSDP cache.

```
<Sysname> display msdp sa-cache
MSDP Total Source-Active Cache - 5 entries
(Source, Group)                 Origin RP      Pro  AS    Uptime   Expires
(10.10.1.2, 225.1.1.1)            10.10.10.10     BGP  100   00:00:10 00:05:50
(10.10.1.3, 225.1.1.1)            10.10.10.10     BGP  100   00:00:11 00:05:49
(10.10.1.2, 225.1.1.2)            10.10.10.10     BGP  100   00:00:11 00:05:49
(10.10.2.1, 225.1.1.2)            10.10.10.10     BGP  100   00:00:11 00:05:49
(10.10.1.2, 225.1.2.2)            10.10.10.10     BGP  100   00:00:11 00:05:49

 MSDP matched 5 entries
```

Table 226 Field descriptions of the display msdp sa-cache command

Field	Description
(Source, Group)	(S, G) entry: (source address, group address)
Origin RP	Address of the RP that generated the (S, G) entry
Pro	Type of protocol from which the AS number is originated. "?" indicates that the system was unable to obtain the protocol type
AS	AS number of the origin RP. "?" indicates that the system was unable to obtain the AS number
Uptime	Length of time for which the cached (S, G) entry has been existing, in hours: minutes: seconds
Expires	Length of time in which the cached (S, G) entry will expire, in hours: minutes: seconds

display msdp sa-count

Syntax **display msdp sa-count** [*as-number*]

View Any view

Parameters *as-number*: AS number.

Description Use the **display msdp sa-count** command to view the number of SA messages in the MSDP cache.

This command gives the corresponding output only after the **cache-sa-enable** command is executed.

Related commands: **cache-sa-enable**.

Examples # View the number of SA messages in the MSDP cache.

```
<Sysname> display msdp sa-count
Number of cached Source-Active entries, counted by Peer
  Peer's Address     Number of SA
  10.10.10.10        5

  Number of source and group, counted by AS
  AS     Number of source    Number of group
  ?      3                      3

Total 5 Source-Active entries
```

Table 227 Field descriptions of the display msdp sa-count command

Field	Description
Number of cached Source-Active entries, counted by Peer	Number of SA messages counted by peer
Peer's Address	MSDP peer addresses
Number of SA	Number of SA messages from this peer
AS	Number of the AS where the MSDP peer is located. "?" indicates that the system was unable to obtain the AS number
Number of source	Number of multicast sources from this AS
Number of group	Number of multicast groups from this AS

encap-data-enable

Syntax **encap-data-enable**

undo encap-data-enable

View MSDP view

Parameters None

Description Use the **encap-data-enable** command to enable register message encapsulation in SA messages.

Use the **undo encap-data-enable** command to disable register message encapsulation in SA messages.

By default, an SA messages contains only a (S, G) entry. No register message is encapsulated in an SA message.

Examples # Enable register message encapsulation in SA messages.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] encap-data-enable
```

import-source

Syntax **import-source** [**acl** *acl-number*]

undo import-source

View MSDP view

Parameters *acl-number*: Basic or advanced ACL number. A basic ACL is used to filter the multicast sources; while an advanced ACL is used to the multicast sources or multicast groups. If you do not provide this argument in your command, no multicast source information will be advertised.

During ACL matching, the protocol ID in the ACL rule is not checked.

Description Use the **import-source** command to configure a rule of creating (S, G) entries.

Use the **undo import-source** command to remove any rule of creating (S, G) entries.

By default, when an SA message is created, there are no restrictions on the (S, G) entries to be advertised in it, namely all the (S, G) entries within the domain are advertised in the SA message.

In addition to controlling SA message creation by using this command, you can also configure a filtering rule for forwarding and receiving SA messages by using the **peer sa-policy** command.

Related commands: **peer sa-policy**.

Examples # Configure the MSDP peer to advertise only the (S, G) entries of multicast sources on the 10.10.0.0/16 subnet and with multicast group address of 225.1.0.0/16 when creating an SA message.

```
<Sysname> system-view
[Sysname] acl number 3101
[Sysname-acl-adv-3101] rule permit ip source 10.10.0.0 0.0.255.255 d
estination 225.1.0.0 0.0.255.255
[Sysname-acl-adv-3101] quit
[Sysname] msdp
[Sysname-msdp] import-source acl 3101
```

msdp

Syntax **msdp**

undo msdp

View System view

Parameters None

Description Use the **msdp** command to enable MSDP and enter MSDP view.

Use the **undo msdp** command to disable MSDP and remove the configurations performed in MSDP view to free the resources occupied by MSDP.

By default, MSDP is disabled.

IP multicast must be enabled on the device before this command can take effect..

Related commands: **peer connect-interface**, **peer description**, **peer mesh-group**, **peer minimum-ttl**, **peer request-sa-enable**, **peer sa-cache-maximum**, **peer sa-policy**, and **peer sa-request-policy**.

Examples # Enable MSDP and enter MSDP view

```
<Sysname> system-view
[Sysname] multicast routing-enable
[Sysname] msdp
[Sysname-msdp]
```

originating-rp

Syntax **originating-rp** *interface-type interface-number*

undo originating-rp

View MSDP view

Parameters *interface-type interface-number*: Specifies an interface by its type and number.

Description Use the **originating-rp** command to configure the address of the specified interface as the RP address of SA messages.

Use the **undo originating-rp** command to remove the configuration of using the interface address as the RP address of SA messages.

Be default, the PIM RP address is used as the RP address of SA messages.

Examples # Specify the IP address of VLAN-interface 4 as the RP address of SA messages.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] originating-rp ethernet 4
```

peer connect-interface

Syntax **peer** *peer-address* **connect-interface** *interface-type interface-number*

undo peer *peer-address*

View MSDP view

Parameters *peer-address*: MSDP peer address.

interface-type interface-number: Specifies an interface by its type and number. The local routing switch will use the IP address of the specified interface as the source IP address when setting up a TCP connection with the remote MSDP peer.

Description Use the **peer connect-interface** command to create an MSDP peer connection.

Use the **undo peer connect-interface** command to remove an MSDP peer.

No MSDP peer connection created by default.

Be sure to carry out this command before you use any other **peer** command; otherwise the system will prompt that the peer does not exist.

Related commands: **static-rpf-peer**.

Examples # Configure the router with the IP address of 125.10.7.6 as the MSDP peer of the local routing switch, with interface VLAN-interface 4 as the local connection port.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] peer 125.10.7.6 connect-interface vlan-interface 4
```

peer description

Syntax **peer** *peer-address* **description** *text*

undo peer *peer-address* **description**

View MSDP view

Parameters *peer-address*: MSDP peer address.

text: Descriptive string of 1 to 80 characters, case sensitive.

Description Use the **peer description** command to configure a descriptive string that describes the specified MSDP peer.

Use the **undo peer description** command to delete the configured descriptive string of the specified MSDP peer.

By default, an MSDP peer has no description information.

Related commands: **display msdp peer-status**.

Examples # Configure a descriptive string "SWITCH CstmrA" for the switch with the IP address of 125.10.7.6.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] peer 125.10.7.6 description SWITCH CstmrA
```

peer mesh-group

Syntax **peer** *peer-address* **mesh-group** *name*

undo peer *peer-address* **mesh-group**

View MSDP view

Parameters *peer-address*: MSDP peer address.

name: Mesh group name, a case-sensitive string of 1 to 32 characters.

Description Use the **peer mesh-group** command to configure an MSDP peer as a mesh group member.

Use the **undo peer mesh-group** command to remove an MSDP peer as a mesh group member.

By default, an MSDP peer does not belong to any mesh group.

Examples # Configure the MSDP peer with the IP address of 125.10.7.6 as a member of the mesh group "Grp1".

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] peer 125.10.7.6 mesh-group Grp1
```

peer minimum-ttl

Syntax **peer** *peer-address* **minimum-ttl** *ttl-value*

undo peer *peer-address* **minimum-ttl**

View MSDP view

Parameters *peer-address*: MSDP peer address.

ttl-value: Time-to-Live (TTL) value.

Description Use the **peer minimum-ttl** command to configure the minimum TTL value of multicast packets encapsulated in SA messages.

Use the **undo peer minimum-ttl** command to restore the default setting.

By default, the minimum TTL value of a multicast packet encapsulated in an SA message is 0.

Related commands: **display msdp peer-status**.

Examples # Set the minimum TTL value of multicast packets to be encapsulated in SA messages to 10 so that only multicast packets whose TTL value is larger than or equal to 10 can be forwarded to the MSDP peer 110.10.10.1.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] peer 110.10.10.1 minimum-ttl 10
```

peer request-sa-enable

Syntax **peer** *peer-address* **request-sa-enable**

undo peer *peer-address* **request-sa-enable**

View MSDP view

Parameters *peer-address*: MSDP peer address.

Description Use the **peer request-sa-enable** command to enable the device to send SA request messages.

Use the **undo peer request-sa-enable** command to disable the device from sending SA request messages.

By default, no SA request message is sent.

Note that before you can enable the device to send SA requests, you must disable the SA message cache mechanism.

Related commands: **cache-sa-enable**.

Examples # Disable the SA message cache mechanism, and enable the switch to send an SA request message to the MSDP peer 125.10.7.6.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] undo cache-sa-enable
[Sysname-msdp] peer 125.10.7.6 request-sa-enable
```

peer sa-cache-maximum

Syntax **peer** *peer-address* **sa-cache-maximum** *sa-limit*

undo peer *peer-address* **sa-cache-maximum**

View MSDP view

Parameters *peer-address*: MSDP peer address.

sa-limit: Maximum number of SA messages that the device can cache.

Description Use the **peer sa-cache-maximum** command to configure the maximum number of SA messages that the routing switch can cache.

Use the **undo peer sa-cache-maximum** command to restore the default setting.

By default, the device can cache a maximum of 8,192 SA messages.

Related commands: **display msdp sa-count**, **display msdp peer-status**, and **display msdp brief**.

Examples # Allow the device to cache a maximum of 100 SA messages from the MSDP peer 125.10.7.6.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] peer 125.10.7.6 sa-cache-maximum 100
```

peer sa-policy

Syntax **peer** *peer-address* **sa-policy** { **import** | **export** } [**acl** *acl-number*]

undo peer *peer-address* **sa-policy** { **import** | **export** }

View MSDP view

Parameters **import**: Specifies to filter SA messages from the specified MSDP peer.

export: Specifies to filter SA messages forwarded to the specified MSDP peer.

peer-address: MSDP peer address.

acl-number: Advanced ACL number. If you do not provide an ACL number, all SA messages carrying (S, G) entries will be filtered off.

Description Use the **peer sa-policy** command to configure a filtering rule for receiving or forwarding SA messages.

Use the **undo peer sa-policy** command to restore the default setting.

By default, SA messages received or to be forwarded are not filtered, namely, all SA messages are accepted or forwarded.

In addition to controlling SA message receiving and forwarding by using this command, you can also configure a filtering rule for creating SA messages using the **import-source** command.

Related commands: **display msdp peer-status** and **import-source**.

Examples # Configure a filtering rule so that SA messages will forwarded to MSDP peer 125.10.7.6 only if they match ACL 3100.

```
<Sysname> system-view
[Sysname] acl number 3100
[Sysname-acl-adv-3100] rule permit ip source 170.15.0.0 0.0.255.255
destination 225.1.0.0 0.0.255.255
[Sysname-acl-adv-3100] quit
[Sysname] msdp
[Sysname-msdp] peer 125.10.7.6 connect-interface vlan-interface 4
[Sysname-msdp] peer 125.10.7.6 sa-policy export acl 3100
```

peer sa-request-policy

Syntax **peer** *peer-address* **sa-request-policy** [**acl** *acl-number*]

undo peer *peer-address* **sa-request-policy**

View MSDP view

Parameters *peer-address*: MSDP peer address.

acl-number: Basic ACL number. If you provide this argument, the SA requests of only the multicast groups that match the ACL will be accepted and other SA requests will be ignored; if you do not provide this argument, all SA requests will be ignored.

Description Use the **peer sa-request-policy** command to configure a filtering rule for SA request messages.

Use the **undo peer sa-request-policy** command to remove the configured SA request filtering rule.

Be default, SA request messages are not filtered.

Related commands: **display msdp peer-status**.

Examples # Configure an SA request filtering rule so that SA messages from the MSDP peer 175.58.6.5 will be accepted only if the multicast group address in the SA messages is in the range of 225.1.1.0/24.

```
<Sysname> system-view
[Sysname] acl number 2001
```

```
[Sysname-acl-basic-2001] rule permit source 225.1.1.0 0.0.0.255
[Sysname-acl-basic-2001] quit
[Sysname] msdp
[Sysname-msdp] peer 175.58.6.5 sa-request-policy acl 2001
```

reset msdp peer

Syntax **reset msdp peer** [*peer-address*]

View User view

Parameters *peer-address*: Specifies an MSDP peer by its address. If you do not provide this argument, the TCP connections with all MSDP peers will be reset.

Description Use the **reset msdp peer** command to reset the TCP connection with the specified MSDP peer or the TCP connections with all MSDP peers and clear all the statistics information of the MSDP peer(s).

Related commands: **display msdp peer-status**.

Examples # Reset TCP connection with the MSDP peer 125.10.7.6 and clear all the statistics information of this MSDP peer.

```
<Sysname> reset msdp peer 125.10.7.6
```

reset msdp sa-cache

Syntax **reset msdp sa-cache** [*group-address*]

View User view

Parameters *group-address*: Address of the multicast group related to which the (S, G) entries are to be cleared from the MSDP cache. If you do not provide this argument, the command will clear all the cached (S, G) entries.

Description Use the **reset msdp sa-cache** command to clear (S, G) entries from the MSDP cache.

Related commands: **cache-sa-enable** and **display msdp sa-cache**.

Examples # Clear the (S, G) entries related to the multicast group 225.5.4.3 from the MSDP cache.

```
<Sysname> reset msdp sa-cache 225.5.4.3
```

reset msdp statistics

Syntax **reset msdp statistics** [*peer-address*]

View User view

Parameters *peer-address*: Specifies an MSDP peer by its address. If you do not provide this argument, the command will clear the statistics information of all MSDP peers.

Description Use the **reset msdp statistics** command to clear the statistics information of the specified MSDP peer or all MSDP peers without resetting the MSDP peer(s).

Examples # Clear the statistics information of the MSDP peer 125.10.7.6.

```
<Sysname> reset msdp statistics 125.10.7.6
```

shutdown (MSDP view)

Syntax **shutdown** *peer-address*

undo shutdown *peer-address*

View MSDP view

Parameters *peer-address*: MSDP peer address.

Description Use the **shutdown** command to deactivate manually the connection with the specified MSDP peer.

Use the **undo shutdown** command to reactivate the connection with the specified MSDP peer.

By default, the connections with all MSDP peers are active.

Related commands: **display msdp peer-status**.

Examples # Deactivate the connection with the MSDP peer 125.10.7.6.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] shutdown 125.10.7.6
```

static-rpf-peer

Syntax **static-rpf-peer** *peer-address* [**rp-policy** *ip-prefix-name*]

undo static-rpf-peer *peer-address*

View MSDP view

Parameters *peer-address*: MSDP peer address.

rp-policy *ip-prefix-name*: Specifies a filtering policy based on the RP address in SA messages, where *ip-prefix-name* is the filtering policy name, a case-sensitive string of 1 to 19 characters.

Description Use the **static-rpf-peer** command to configure a static RPF peer.

Use the **undo static-rpf-peer** command to remove a static RPF peer.

No static RPF peer is configured by default.

When you configure multiple static RPF peers, observe the following rules:

- If you use the **rp-policy** keyword for all the static RPF peers, all the static RPF peers will be activated concurrently. SA messages will be filtered as per the configured prefix list and only those SA messages whose RP addresses pass the filtering will be accepted. If multiple static RPF peers use the same filtering policy at the same time, when a peer receives an SA message, it will forward the SA message to the other peers.
- If you use the **rp-policy** keyword for none of the static RPF peers, according to the configuration sequence, only the first static RPF peer whose connection is in the UP state will be activated, and all SA messages from this peer will be accepted while the SA messages from other static RPF peers will be discarded. When this active static RPF peer fails (for example, when the configuration is removed or when the connection is torn down), based on the configuration sequence, the next RPF peer with its connection in the UP state will be selected as the activated RPF peer according to the configuration sequence.

Related commands: **display msdp peer-status** and **ip prefix-list**.

Examples # Configure static RPF peers.

```
<Sysname> system-view
[Sysname] ip ip-prefix list1 permit 130.10.0.0 16 great-equal 16 less-equal 32
[Sysname] msdp
[Sysname-msdp] peer 130.10.7.6 connect-interface vlan-interface 4
[Sysname-msdp] static-rpf-peer 130.10.7.6 rp-policy list1
```

timer retry

Syntax **timer retry** *interval*

undo timer retry

View MSDP view

Parameters *interval*: Interval between MSDP peer connection retries, in seconds.

Description Use the **timer retry** command to configure the interval between MSDP peer connection retries.

Use the **undo timer retry** command to restore the default setting.

By default, the interval between MSDP peer connection retries is 30 seconds.

Related commands: **display msdp peer-status**.

Examples # Set the MSDP peer connection retry interval to 60 seconds.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] timer retry 60
```

48 MLD CONFIGURATION COMMANDS

The term "router" in this document refers to a router in a generic sense or a Switch 8800 running MLD.

debugging mld

Syntax **debugging mld** { **all** | **done** [*basic-acl6-number*] | **event** | **query** [*advanced-acl6-number*] [**receive** | **send**] | **report** [*advanced-acl6-number*] | **timer** }

undo debugging mld { **all** | **done** | **event** | **query** [**receive** | **send**] | **report** | **timer** }

View User view

Parameter **all**: Turns on/off all types of debugging for MLD.

done: Turns on/off MLD done message debugging.

basic-acl6-number: Specifies the number of the basic IPv6 access control list.

event: Turns on/off MLD event debugging.

query: Turns on/off MLD query message debugging.

advanced-acl6-number: Specifies the number of the advanced IPv6 access control list.

receive: Turns on/off debugging for received MLD query messages.

send: Turns on/off debugging for sent MLD query messages.

report: Turns on/off debugging for MLD report messages.

timer: Turns on/off debugging for MLD timers.

Description Use the **debugging mld** command to enable MLD debugging.

Use the **undo debugging mld** command to disable MLD debugging.

By default, MLD debugging is disabled.

Table 228 Field descriptions of the debugging mld command

Field	Description
MLD event debugging switch is on	The MLD event debugging is enabled.
MLD done debugging switch is on	The debugging for the MLD done message is enabled.
MLD query receive debugging switch is on	The debugging for the received MLD query message is enabled.
MLD query send debugging switch is on	The debugging for the sent MLD query message is enabled.
MLD report debugging switch is on	The debugging for the MLD report message is enabled.
MLD timer debugging switch is on	The debugging for the MLD timer is enabled.

Table 229 Field descriptions of the debugging mld event command

Field	Description
Creating/creation/created aux join/aux prune adding interface/deleting downstream deleteing/unregister/deleted	Event types, including Creating/creation/created Join/prune Adding outgoing interface/removing outgoing interface
Enqueue/Dequeuing	Enqueuing/dequeuing
Elected/ Un-elected	Elected/Lost the election
Interface interfacename(ifadd)	Interface that responded the event (interface address)
(sadd, gadd)	(S, G) entry
(*, gadd)	(*, G) entry

Table 230 Field descriptions of the debugging mld done command

Field	Description
DONE	Message type: MLD done message
Interfacename(ifadd)	Interface on which the message was received (interface address)
group gadd	IPv6 group address in the done message
Ignoring	Ignoring this MLD done message

Table 231 Field descriptions of the debugging mld query send command

Field	Description
version	The version of the MLD query message
Interfacename(ifadd)	Interface on which the message was received/sent (interface address)
Ignoring	Ignoring this MLD query message
Send	Sent MLD query message
With/without s-bit	With/without the S-bit set
General/group specific query	MLD general query/multicast-address-specific query
Group gadd	The queried IPv6 group address

Table 232 Field descriptions of the debugging mld query receive command

Field	Description
version	The version of the MLD query message
Interfacename(ifadd)	Interface on which the message was received/sent (interface address)
Ignoring	Ignoring this MLD query message
Received	Received MLD query message
General/group specific query	MLD general query/multicast-address-specific query
Group gadd	The queried IPv6 group address

Table 233 Field descriptions of the debugging mld report command

Field	Description
Ignoring	Ignoring this MLD membership report message
IS_IN/IS_EX/TO_IN/TO_EX/ALLOW/BLOCK	Record type of the MLDv2 membership report message
Group gadd	IPv6 group address in the MLD membership report message
(sadd, gadd)	(S, G) entry
v1	Version of the MLD membership report message
Interfacename(ifadd)	Interface on which the message was received/sent (interface address)

Table 234 Field descriptions of the debugging mld timer command

Field	Description
Lmqi timeout for group	LMQI timer timed out
Other querier present interval	Other querier present timer timed out
Interfacename(ifadd)	Interface on which the message was received/sent (interface address)
Deleting v1 host timer	MLDv1 host aging timer timed out
Setting v1 host timer	Setting MLDv1 host aging timer

Example # Enabling MLD event debugging

```
<Sysname> debugging mld event
*0.852518 85 MLD/7/EVENT:Elected querier on interface Vlan-interface
11(FE80::200:5EFF:FE01:6C00) (G10297)
```

// The interface is elected as the MLD querier

```
*0.813059 85 MLD/7/EVENT:Un-elected querier on interface Vlan-interf
ace11(FE80::200:5EFF:FE01:6C00) (G10456)
```

// The interface becomes a non-querier

```
*0.886956 85 MLD/7/EVENT:MLDV2 (*, FF0E::101:101) aux join received
on interface Vlan-interface11(FE80::200:5EFF:FE01:6C00) (G01600)
```

// The interface receives a join message

```
*0.886956 85 MLD/7/EVENT:(*, FF0E::101:101) entry created in global
MRT (G01609)
*0.886956 85 MLD/7/EVENT:Adding interface Vlan-interface11(FE80::200
:5EFF:FE01:6C00) to downstream IN tree for (*, FF0E::101:101) (G0162
9)
*0.886956 85 MLD/7/EVENT:Creating group(FF0E::101:101) for interface
 Vlan-interface11(FE80::200:5EFF:FE01:6C00) (G013082)
```

// Group FF0E::101:101 is added in an entry, with VLAN-interface 11 as the outgoing interface

```
*0.886956 85 MLD/7/EVENT:Enqueue group(FF0E::101:101) on interface V
lan-interface11(FE80::200:5EFF:FE01:6C00) in group_calq. (G014076)
```

// An aging timer is set for the group

```
*0.1223796 85 MLD/7/EVENT:Dequeing group(FF0E::101:101) on interface
 Vlan-interface11(FE80::200:5EFF:FE01:6C00) from group_calq. (G01402
8)
*0.1223796 85 MLD/7/EVENT:Enqueue group(FF0E::101:101) on interface
Vlan-interface11(FE80::200:5EFF:FE01:6C00) in group_calq. (G014076)
```

// The aging timer is reset when an MLD done message is received on the interface

```
*0.1224808 85 MLD/7/EVENT:Lmqi timeout for group(FF0E::101:101), sen
ding last listener query on interface Vlan-interface11(FE80::200:5EF
F:FE01:6C00). (G013428)
*0.1224808 85 MLD/7/EVENT:Enqueue group(FF0E::101:101) on interface
Vlan-interface11(FE80::200:5EFF:FE01:6C00) in group_calq. (G014076)
```

// An MLD multicast-address-specific query is sent out when LMQI timer times out

```
*0.1225820 85 MLD/7/EVENT:Group(FF0E::101:101) expired and sources e
mpty. Deleting this group on interface Vlan-interface11(FE80::200:5E
FF:FE01:6C00). (G013318)
*0.1225820 85 MLD/7/EVENT:Deleting group(FF0E::101:101) on interface
 Vlan-interface11(FE80::200:5EFF:FE01:6C00) (G014170)
*0.1225820 85 MLD/7/EVENT:Group(FF0E::101:101) deleted (G01805)
```

// As no MLD membership report is received, the group is removed from the table entry

display mld group

Syntax **display mld group** [*ipv6-group-address* | **interface** *interface-type interface-number*] [**static** | **verbose**]

View Any view

Parameter *ipv6-group-address*: Specified an IPv6 multicast group.

interface-type interface-number: Specifies an interface by its type and number. At present, only VLAN interfaces are supported for the Switch 8800s.

static: Displays the information about statically joined IPv6 multicast groups

verbose: Displays detailed information.

Description Use the **display mld group** command to view information about IPv6 multicast groups.

Note that:

- If you do not specify an interface and a multicast group address, the information of IPv6 multicast groups on all interfaces will be displayed.
- If you specify only a multicast group address, the information of the IPv6 multicast group corresponding to this address will be displayed.
- If you specify only an interface, the information of IPv6 multicast groups on this interface will be displayed.
- If you do not specify the **static** keyword, the information of only dynamically joined IPv6 multicast groups will be displayed.

Example # View the detailed information about dynamically joined IPv6 multicast groups on all interfaces.

```
<Sysname> display mld group verbose
Interface group report information
Vlan-interface2 (FE80::101)
  Total 2 MLD Groups reported
   Group: FF34::101:101
     Uptime: 00:01:46
     Expires: off
     Last reporter: FE80::10
     Last-listener-query-counter: 0
     Last-listener-query-timer-expiry: off
     Group mode: include
     Version1-host-present-timer-expiry: off
     Source list:
       Source: 3333::2
          Uptime: 00:01:46
          Expires: 00:10:09
          Last-listener-query-counter: 0
          Last-listener-query-timer-expiry: off
       Source: 4444::1
          Uptime: 00:01:46
          Expires: 00:10:09
          Last-listener-query-counter: 0
          Last-listener-query-timer-expiry: off
   Group: FF35::101:101
     Uptime: 00:01:34
     Expires: off
     Last reporter: FE80::10
     Last-listener-query-counter: 0
     Last-listener-query-timer-expiry: off
     Group mode: exclude
     Version1-host-present-timer-expiry: off
     Source list:
       Source: 1111::1
          Uptime: 00:01:34
```

```
      Expires: 00:10:09
      Last-listener-query-counter: 0
      Last-listener-query-timer-expiry: off
   Source: 2222::2
      Uptime: 00:01:34
      Expires: 00:10:09
      Last-listener-query-counter: 0
      Last-listener-query-timer-expiry: off
```

Table 235 Field descriptions of the display mld group command

Field	Description
Group	IPv6 multicast group address
Uptime	Amount of time since the IPV6 multicast group was added in the table entry
Expires	Remaining time of the IPv6 multicast group
Last reporter	IPv6 address of the last host that has reported group membership
Last-listener-query-counter	Number of multicast-address-specific queries sent
Last-listener-query-timer-expiry	Remaining time of the last-listener query response delay timer
Group mode	Multicast group filter mode
Version1-host-present-timer-expiry	MLDv1 host timeout time
Source list	List of multicast sources
Source	Multicast source address

display mld group port-info

Syntax **display mld group port-info** [**vlan** *vlan-id*] [**slot** *slot-id*] [**verbose**]

View Any view

Parameter *vlan-id*: Displays the information about Layer 2 ports in the specified VLAN. If you do not specify a VLAN ID, the information of Layer 2 ports in all VLANs will be displayed.

slot *slot-id*: Displays the information about Layer 2 ports on the specified module.

verbose: Displays the detailed information about Layer 2 ports.

Description Use the **display mld group port-info** command to view the MLD layer 2 port information.

Example # View the detailed information about MLD Layer 2 ports.

```
<Sysname> display mld group port-info verbose
    Total 1 IP Group(s).
    Total 1 IP Source(s).
    Total 1 MAC Group(s).

  Port flags: D-Dynamic port, S-Static port, A-Aggregation port, C-Copy port
  Subvlan flags: R-Real VLAN, C-Copy VLAN
```

```
Vlan(id):2.
  Total 1 IP Group(s).
  Total 1 IP Source(s).
  Total 1 MAC Group(s).
  Router port(s):total 1 port.
          Eth1/1/1                                    (D) ( 00:01:30 )
  IP group(s):the following ip group(s) match to one mac group.
    IP group address: FF34::101:101
      (FE80::1, FF34::101:101):
        Attribute:    Host Port
        Host port(s):total 1 port.
          Eth1/1/2                                    (D) ( 00:03:23 )
  MAC group(s):
    MAC group address:3333-0101-0101
        Host port(s):total 1 port.
          Eth1/1/2
```

Table 236 Field descriptions of the display mld group port-info command

Field	Description
Total 1 IP Group(s).	Total number of IPv6 multicast groups
Total 1 IP Source(s).	Total number of IPv6 multicast sources
Total 1 MAC Group(s).	Total number of MAC multicast groups
Port flags: D-Dynamic port, S-Static port, A-Aggregation port, C-Copy port	Port flag: D stands for dynamic port, S for static port, A for aggregated port, and C for port copied from a (*,G) entry to an (S, G) entry.
Subvlan flags: R-Real VLAN, C-Copy VLAN	Sub-VLAN flag: R stands for real egress sub-VLAN under the current entry, and C for sub-VLAN copied from a (*,G) entry to an (S, G) entry.
Router port(s)	Number of router ports
IP group address	Address of an IPv6 multicast group
MAC group address	Address of a MAC multicast group
Attribute	Attribute of an IPv6 multicast group
Host port(s)	Number of host member ports

display mld interface

Syntax **display mld interface** [*interface-type interface-number*] [**verbose**]

View Any view

Parameter *interface-type interface-number*: Specifies a interface by its type and number. If you do not specify an interface, the information of all interfaces running MLD will be displayed. At present, only VLAN interfaces are supported by the Switch 8800s.

verbose: Displays detailed MLD configuration and running information.

Description Use the **display mld interface** command to view MLD configuration and running information on the specified interface or all MLD-enabled interfaces.

Example # View the detailed MLD configuration and running information on VLAN-interface 2.

```
<Sysname> display mld interface vlan-interface2 verbose
Vlan-interface2 (FE80::200:AFF:FE01:101):
   MLD is enabled
   Current MLD version is 1
   Value of query interval for MLD(in seconds): 125
   Value of other querier present interval for MLD(in seconds): 255
   Value of maximum query response time for MLD(in seconds): 10
   Value of last listener query interval(in seconds): 1
   Value of startup query interval(in seconds): 31
   Value of startup query count: 2
   General query timer expiry (hours:minutes:seconds): 00:00:23
   Querier for MLD: FE80::200:AFF:FE01:101 (this router)
   MLD activity: 1 joins, 0 leaves
   Multicast ipv6 routing on this interface: enabled
   Robustness: 2
   Require-router-alert: disabled
   Startup-query-timer-expiry: off
   Other-querier-present-timer-expiry: off
```

Table 237 Field descriptions of the display mld group port-info command

Field	Description
Vlan-interface2 (FE80::200:AFF:FE01:101):	Interface name (IPv6 link-local address)
Current MLD version is 2	Version number of the MLD run on the interface
MLD group policy	MLD group policy
Value of query interval for MLD (in seconds)	Interval between general query messages (in seconds)
Value of other querier present interval for MLD (in seconds)	Timeout time for non-queriers (in seconds)
Value of maximum query response time for MLD (in seconds)	Maximum response delay of general query messages (in seconds)
Value of last listener query interval (in seconds)	Interval for sending multicast-address-specific messages (in seconds)
Value of startup query interval(in seconds)	Interval between MLD queries on startup
Value of startup query count	Number of MLD general queries sent on startup
General query timer expiry	Remaining time of the MLD general query timeout timer
Querier for MLD	IPv6 link-local address of the MLD querier
MLD activity	Statistics of MLD activity statistics (number of join and done messages)
Robustness	Robustness variable of an MLD querier (namely, last listener query count)
Require-router-alert	Indicates whether MLD messages without the Router-Alert option is discarded
Startup-query-timer-expiry	Remaining time of the startup query timer
Other-querier-present-timer-expiry	Remaining time of the MLD other querier present timer

display mld routing-table

Syntax **display mld routing-table** [*ipv6-source-address* [*prefix-length*] | *ipv6-group-address* [*prefix-length*]] *

View Any view

Parameter *ipv6-source-address*: Specifies an IPv6 multicast source.

prefix-length: Prefix length of the specified IPv6 multicast source or IPv6 multicast group address. For an IPv6 multicast source address, this argument has an effective value range of 0 to 128; for an IPv6 multicast group address, it has an effective value range of 8 to 128. The system default is 128 in both cases.

Ipv6-group-address: Specifies an IPv6 multicast group.

Description Use the **display mld routing-table** command to view the information of the MLD routing table.

Example # View the information of the MLD routing table.

```
<Sysname> display mld routing-table
Routing table
 Total 1 entry

 00001. (*, FF1E::101:101)
       List of 1 downstream interface
        Vlan-interface2 (FE80::200:5EFF:FE71:3800),
                    Protocol: MLD
```

Table 238 Field descriptions of the display mld routing-table command

Field	Description
00001	Sequence number of the (*, G) entry
(*, FF1E::101:101)	An (*, G) entry in the MLD routing table
List of 1 downstream interface	List of downstream interfaces, namely the interfaces to which the multicast data for this group be forwarded

last-listener-query-interval (MLD view)

Syntax **last-listener-query-interval** *interval*

undo last-listener-query-interval

View MLD view

Parameter *interval*: MLD last listener query interval, in seconds.

Description Use the **last-listener-query-interval** command to configure the MLD last listener query interval globally.

Use the **undo last-listener-query-interval** command to restore the system default.

By default, the last listener query interval is 1 second.

Related command: **mld last-listener-query-interval**, **robust-count** and **display mld interface**.

Example # Set the MLD last listener query interval to 3 seconds globally.

```
<Sysname> system-view
[Sysname] mld
[Sysname-mld] lastlistener-queryinterval 3
```

max-response-time (MLD view

max-response-time (MLD view)

Syntax **max-response-time** *interval*

undo max-response-time

View MLD view

Parameter *interval*: Maximum response delay for MLD general query messages, in seconds.

Description Use the **max-response-time** command to configure the maximum response delay for general queries globally.

Use the **undo max-response-time** command to restore the system default.

By default, the maximum response delay for general queries is 10 seconds.

Related command: **mld max-response-time**, **timer other-querier-present**, and **display mld interface**.

Example # Set the maximum response delay for MLD general queries to 8 seconds globally.

```
<Sysname> system-view
[Sysname] mld
[Sysname-mld] max-response-time 8
```

mld

Syntax **mld**

undo mld

View System view

Parameter None

Description Use the **mld** command to enter MLD view.

Use the **undo mld** command to remove the configurations made in MLD view.

This command can take effect only after IPv6 multicast routing is enabled on the device.

Related command: **multicast ipv6 routing-enable**.

Example # Enter MLD view.

```
<Sysname> system-view
[Sysname] multicast ipv6 routing-enable
[Sysname] mld
[Sysname-mld]
```

mld enable

Syntax **mld enable**

undo mld enable

View VLAN interface view

Parameter None

Description Use the **mld enable** command to enable MLD on the current interface.

Use the **undo mld enable** command to disable MLD on the current interface.

By default, MLD is disabled on the interface.

Note that:

- This command can take effect only after IPv6 multicast routing is enabled on the device.
- Other MLD configurations performed on the interface can take effect only after MLD is enabled on the interface.
- After MLD is enabled on a VLAN interface, it is not allowed to enable MLD Snooping in the corresponding VLAN, and vice versa.

Related command: **mld**.

Example # Enable MLD on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] mld enable
```

mld last-listener-query-interval

Syntax **mld last-listener-query-interval** *interval*

undo mld last-listener-query-interval

View VLAN interface view

Parameter *interval*: MLD last listener query interval, in seconds.

Description Use the **mld last-listener-query-interval** command to configure the MLD last listener query interval.

Use the **undo mld last-listener-query-interval** command to restore the system default.

By default, the MLD last listener query interval is 1 second.

Related command: **last-listener-query-interval**, **mld robust-count**, **display mld interface.**

Example # Set the MLD last listener query interval to 3 on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] mld last-listener-query-interval 3
```

mld max-response-time

Syntax **mld max-response-time** *interval*

undo mld max-response-time

View VLAN interface view

Parameter *interval*: Maximum response delay for MLD general query messages, in seconds.

Description Use the **mld max-response-time** command to configure the maximum response delay for MLD general query messages on the current interface.

Use the **undo mld max-response-time** command to restore the system default.

By default, the maximum response delay for MLD general query messages is 10 seconds.

The maximum query response delay determines how long it takes the device to find whether any group member exists on the local subnet.

Related commands: **max-response-time**, **mld timer other-querier-present**, **display mld interface**

Example # Set the maximum response delay for MLD general query messages to 8 seconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] mld max-response-time 8
```

mld require-router-alert

Syntax **mld require-router-alert**

undo mld require-router-alert

View VLAN interface view

Parameter None

Description Use the **mld require-router-alert** command to configure the interface to discard MLD messages without the Router-Alert option.

Use the **undo mld require-router-alert** command to restore the default configuration.

By default, the device does not check the Router-Alert option, that is, it sends all the received MLD messages to the upper-layer protocol for processing no matter whether they have the Router-Alert option.

Related commands: **require-router-alert**, **mld send-router-alert**.

Example # Configure VLAN-interface 100 to discard MLD messages without the Router-Alert option.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] mld require-router-alert
```

mld robust-count

Syntax **mld robust-count** *robust-value*

undo mld robust-count

View VLAN interface view

Parameter *robust-value*: MLD robustness variable, namely the MLD last-listener query count.

Description Use the **mld robust-count** command to configure the MLD last-listener query count.

Use the **undo mld robust-count** command to restore the system default.

By default, the MLD last listener query count is 2.

Related command: **robust-count**, **mld last-listener-query-interval**, **mld timer other-querier-present**, **display mld interface**.

Example # Set the MLD last listener query count to 3 on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] mld robust-count 3
```

mld send-router-alert

Syntax **mld send-router-alert**

undo mld send-router-alert

View VLAN interface view

Parameter None

Description Use the **mld send-router-alert** command to enable insertion of the Router-Alert option into MLD messages to be sent from the current interface.

Use the **undo mld send-router-alert** command to disable insertion of the Router-Alert option into MLD messages to be sent from the current interface.

By default, MLD messages carry the Router-Alert option.

Related command: **send-router-alert** and **mld require-router-alert**.

Example # Configure VLAN-interface 100 to sent MLD messages without the Router-Alert option .

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] undo mld send-router-alert
```

mld timer other-querier-present

Syntax **mld timer other-querier-present** *interval*

undo mld timer other-querier-present

View VLAN interface view

Parameter *interval*: Other querier present interval in seconds.

Description Use the **mld timer other-querier-present** command to configure the other querier present interval on the current interface.

Use the **undo mld timer other-querier-present** command to restore the default configuration.

By default, the other querier present interval is determined by the following formula:

[Other querier present interval] = [MLD query interval] times [robustness variable] plus [maximum response delay] divided by two.

By default, the values of the three parameters in the above-mentioned formula are 125, 2, and 10, respectively, so the default other querier present interval is 125 x 2 + 10 / 2 = 255 (seconds).

Related command: **timer other-querier-present, mld timer query, mld robust-count, mld max-response-time**, **and display mld interface**.

Example # Set the other querier present interval to 200 seconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface100
[Sysname-Vlan-interface100] mld timer other-querier-present 200
```

mld timer query

Syntax **mld timer query** *interval*

undo mld timer query

View VLAN interface view

Parameter *interval*: MLD query interval, namely the amount of time in seconds between MLD general queries.

Description Use the **mld timer query** command to configure the MLD query interval on the current interface.

Use the **undo mld timer query** command to restore the system default.

By default, the query interval is 125 seconds.

The device sends MLD general queries at a configurable interval so as to determine whether any IPv6 multicast group member exist on the local subnet. The administrator can modify this query interval as required based on the actual networking situation.

Related command: **timer query**, **mld timer other-querier-present**, **display mld interface**.

Example # Set the query interval to 200 seconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] mld timer query 200
```

mld version

Syntax **mld version** *version-number*

undo mld version

View VLAN interface view

Parameter *version-number*: MLD version. At present, the Switch 8800s support only MLDv1.

Description Use the **mld version** command to configure the MLD version on the current interface.

Use the **undo mld version** command to restore the default MLD version.

By default, the MLD version is MLDv1.

Related command: **version**.

Example # Set the MLD version to version 1 on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] mld version 1
```

require-router-alert

Syntax **require-router-alert**

undo require-router-alert

View MLD view

Parameter None

Description Use the **require-router-alert** command to globally configure the device to discard MLD messages without the Router-Alert option.

Use the **undo require-router-alert** command to restore the default configuration.

By default, the device does not check the Router-Alert option, that is, it forwards all received MLD messages to the upper layer protocol for processing.

Related command: **mld require-router-alert**, **send-router-alert**.

Example # Globally configure the device to discard MLD messages without the Router-Alert option.

```
<Sysname> system-view
[Sysname] mld
[Sysname-mld] require-router-alert
```

reset mld group

Syntax **reset mld group** { **all** | **interface** *interface-type interface-number* { **all** | *ipv6-group-address* [*prefix-length*] [*ipv6-source-address* [*prefix-length*]] } }

View User view

Parameter **all**: Clears all MLD forwarding entries.

interface *interface-type interface-number*: Specifies an interface by its type and number. At present, only VLAN interfaces are supported for the Switch 8800s.

ipv6-group-address: Specifies an IPv6 multicast group.

ipv6-source-address: Specifies an IPv6 multicast source.

prefix-length: Prefix length of the specified IPv6 multicast source or IPv6 multicast group. For a multicast source address, this argument has an effective value range of 0 to 128; for an IPv6 multicast group address, it has an effective value range of 8 to 128. The system default is 128 in both cases.

Description Use the **reset mld group** command to clear MLD forwarding entries.

Note that:

- When you clear MLD forwarding entries for a VLAN interface, the MLD Snooping forwarding entries for the VLAN will also be cleared.
- Using the **reset mld group** command may cause currently active receivers to stop receiving multicast information. .

Related command: **display mld group**.

Example # Clear all MLD and MLD Snooping forwarding entries on all interfaces.

```
<Sysname> reset mld group all
```

Clear all MLD forwarding entries on VLAN-interface 100 and MLD Snooping forwarding entries for VLAN 100.

```
<Sysname> reset mld group interface vlan-interface 100 all
```

Clear MLD forwarding entries for the IPv6 multicast group FF35::101:101 on VLAN-interface 100 and all the MLD Snooping forwarding entries for this multicast group in VLAN 100.

```
<Sysname> reset mld group interface vlan-interface ff35::101:101
```

robust-count (MLD view)

Syntax **robust-count** *robust-value*

undo robust-count

View MLD view

Parameter *robust-value*: MLD robustness variable, namely the last listener query count.

Description Use the **robust-count** command to configure the MLD robustness variable globally.

Use the **undo robust-count** command to restore the system default.

By default, the MLD robustness variable is 2.

Related command: **mld robust-count**, **lastlistener-queryinterval**, **timer other-querier-present**, **display mld interface**.

Example # Set the MLD robustness variable to 3 globally.

```
<Sysname> system-view
[Sysname] mld
[Sysname-mld] robust-count 3
```

send-router-alert (MLD view

send-router-alert (MLD view)

Syntax **send-router-alert**

undo send-router-alert

View MLD view

Parameter None

Description Use the **send-router-alert** command to globally enable the insertion of the Router-Alert option into MLD messages to be sent.

Use the **undo send-router-alert** command to globally disable the insertion of the Router-Alert option into MLD messages to be sent.

By default, MLD messages carry the Router-Alert option.

Related command: **mld send-router-alert**, **require-router-alert**.

Example # Globally disable insertion of the Router-Alert option into MLD messages to be sent.

```
<Sysname> system-view
[Sysname] mld
[Sysname-mld] undo send-router-alert
```

timer other-querier-present (MLD view)

Syntax **timer other-querier-present** *interval*

undo timer other-querier-present

View MLD view

Parameter *interval*: Other querier present interval in seconds.

Description Use the **timer other-querier-present** command to configure the other querier present interval globally.

Use the **undo timer other-querier-present** command to restore the system default.

By default, the other querier present interval is determined by the following formula:

[Other querier present interval] = [MLD query interval] times [robustness variable] plus [maximum response delay] divided by two.

By default, the values of the three parameters in the above-mentioned formula are 125, 2, and 10, respectively, so the default timeout time for non-queriers is 125 x 2 + 10 / 2 = 255 (seconds).

Related command: **mld timer other-querier-present**, **timer query**, **robust-count**, **max-response-time**, **display mld interface**.

Example # Globally set the timeout time for non-queriers to 200 seconds.

```
<Sysname> system-view
[Sysname] mld
[Sysname-mld] timer other-querier-present 200
```

timer query (MLD view)

Syntax **timer query** *interval*

undo timer query

View MLD view

Parameter *interval*: Query interval, namely, amount of time in seconds between MLD general query messages.

Description Use the **timer query** command to configure the query interval globally.

Use the **undo timer query** command to restore the system default.

By default, the query interval is 125 seconds.

Related command: **mld timer query**, **timer other-querier-present**, **display mld interface**.

Example # Set the query interval to 200 seconds globally.

```
<Sysname> system-view
[Sysname] mld
[Sysname-mld] timer query 200
```

version (MLD view)

Syntax **version** *version-number*

undo version

View MLD view

Parameter *version-number*: MLD version number. At present, the Switch 8800s support only MLDv1.

Description Use the **version** command to configure the MLD version globally.

Use the **undo version** command to restore the default MLD version.

By default, the MLD version is version 1.

Related command: **mld version**.

Example # Set the MLD version to MLDv1 globally .

```
<Sysname> system-view
[Sysname] mld
[Sysname-mld] version 1
```

49 MLD SNOOPING CONFIGURATION COMMANDS

debugging mld-snooping

Syntax **debugging mld-snooping** { **all** | **event** | **abnormal** | **driver** | **group** | **timer** | **ipc** { **receive** | **send** } | **packet** [**vlan** *vlan-id* [**port** *port-type port-number*]] }

undo debugging mld-snooping { **all** | **event** | **abnormal** | **driver** | **group** | **timer** | **ipc** { **receive** | **send** } | **packet** }

View User view

Parameters **all**: Turns on/off all types of debugging for MLD Snooping.

event: Turns on/off MLD Snooping event debugging.

abnormal: Turns on/off debugging for abnormal MLD-Snooping information.

driver: Turns on/off MLD Snooping driver debugging.

group: Turns on/off MLD Snooping group debugging.

timer: Turns on/off MLD Snooping timer debugging.

ipc: Turns on/off IPC packet debugging.

receive: Turns on/off debugging for received IPC packets.

send: Turns on/off debugging for sent IPC packets.

packet: Turns on/off MLD message debugging.

vlan *vlan-id*: Specifies a VLAN.

port *port-type port-number*: Specifies a port.

Description Use the **debugging mld-snooping** command to turn on debugging for MLD Snooping. Use the **undo debugging mld-snooping** command to turn off debugging for MLD Snooping.

By default, MLD Snooping debugging is off.

Examples # Turn on all types of debugging for MLD Snooping.

```
<Sysname> debugging mld-snooping all
```

display mld-snooping group

Syntax **display mld-snooping group** [**vlan** *vlan-id*] [**slot** *slot-id*] [**verbose**]

View Any view

Parameters **vlan** *vlan-id*: Displays the IPv6 multicast group information in the specified VLAN.

slot *slot-id*: Displays the IPv6 multicast group information in the specified module.

verbose: Displays the detailed IPv6 multicast group information.

Description Use the **display mld-snooping group** command to view the IPv6 multicast group information learned by MLD Snooping.

Examples # View the detailed information of IPv6 multicast groups in VLAN 2 learned by MLD Snooping.

```
<Sysname> display mld-snooping group vlan 2 verbose
    Total 1 IP Group(s).
   Total 0 IP Source(s).
    Total 1 MAC Group(s).

  Port flags: D-Dynamic port, S-Static port, A-Aggregation port
  Vlan(id):2.
    Total 1 IP Group(s).
    Total 1 MAC Group(s).
    Router port(s):total 0 port.
    IP group(s):the following ip group(s) match to one mac group.
        IP group address: FF1E::101:101
        Attribute:Host Port
        Host port(s):total 1 port.
          Ethernet1/1/1                                    (D) ( 00:04:18 )
    MAC group(s):
        MAC group address:3333-0101-0101
        Host port(s):total 1 port.
          Ethernet1/1/1
```

Table 239 Field descriptions of the display mld-snooping group command

Field	Description
Total 1 IP Group(s)	Total number of IPv6 multicast groups
Total 1 IP Source(s)	Total number of IPv6 multicast sources
Total 1 MAC Group(s)	Total number of MAC multicast groups
Port flags: D-Dynamic port, S-Static port, A-Aggregation port	Port flags: D for dynamic port, S for static port, A for aggregation port
Router port(s)	Number of router ports
IP group address	Address of IPv6 multicast group
MAC group address	Address of MAC multicast group
Attribute	Attribute of IPv6 multicast group
Host port(s)	Number of host member ports

display mld-snooping statistics

Syntax **display mld-snooping statistics**

View Any view

Parameters None

Description Use the **display mld-snooping statistics** command to view the statistics information of MLD messages learned by MLD Snooping.

Examples # View the statistics information of all kinds of MLD messages learned by MLD Snooping.

```
<Sysname> display mld-snooping statistics
  Received MLD general query packet(s) number:0.
  Received MLD specific query packet(s) number:0.
  Received MLD V1 report packet(s) number:0.
  Received MLD done packet(s) number:0.
  Sent MLD specific query packet(s) number:0.
  Received error MLD packet(s) number:0.
```

Table 240 Field descriptions of the display mld-snooping statistics command

Field	Description
general query packet(s)	General query messages
specific query packet(s)	Multicast-address-specific query messages
report packet(s)	Report messages
done packet(s)	Done messages
error MLD packet(s)	Error MLD messages

drop-unknown (MLD Snooping view)

Syntax **drop-unknown**

undo drop-unknown

View MLD Snooping view

Parameters None

Description Use the **drop-unknown** command to enable globally the function of dropping unknown IPv6 multicast data.

Use the **undo drop-unknown** command to disable globally the function of dropping unknown IPv6 multicast data.

By default, this function is disabled, that is, unknown IPv6 multicast traffic is flooded within the VLAN.

Note that this command works only on an MLD Snooping-enabled VLAN, but not on a VLAN with MLD enabled on its VLAN interface.

Examples # Globally enable the function of dropping unknown IPv6 multicast data.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] drop-unknown
```

fast-leave (MLD Snooping view)

Syntax **fast-leave** [**vlan** *vlan-list*]

undo fast-leave [**vlan** *vlan-list*]

View MLD Snooping view

Parameters **vlan** *vlan-list*: Defines one or multiple VLANs. You can provide up to 10 VLAN lists, by each of which you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* **to** *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID.

Description Use the **fast-leave** command to enable the fast leave feature globally.

Use the **undo fast-leave** command to disable the fast leave feature globally.

By default, the fast leave feature is disabled globally.

Note that:

- This command works on an MLD Snooping-enabled VLAN or on a VLAN with MLD enabled on its VLAN interface.
- If you do not specify any VLAN, the command will take effect for all VLANs; if you specify a VLAN or multiple VLANs, the command will take effect for the specified VLAN(s) only.

Related commands: **mld-snooping fast-leave**.

Examples # Enable the fast leave feature globally in VLAN 2.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] fast-leave vlan 2
```

group-policy (MLD Snooping view)

Syntax **group-policy** *acl6-number* [**vlan** *vlan-list*]

undo group-policy [**vlan** *vlan-list*]

View MLD Snooping view

Parameters *Acl6-number*: Basic IPv6 ACL number.

vlan *vlan-list*: Defines one or multiple VLANs. You can provide up to 10 VLAN lists, by each of which you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* **to** *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID.

Description Use the **group-policy** command to configure a global IPv6 multicast group filter.

Use the **undo group-policy** command to remove the configured global IPv6 multicast group filter.

By default, no IPv6 multicast group filter is configured globally, namely, a host can join any IPv6 multicast group.

Note that:

- This command works on an MLD Snooping-enabled VLAN or on a VLAN with MLD enabled on its VLAN interface.
- If you do not specify any VLAN, the command will take effect for all VLANs; if you specify a VLAN or multiple VLANs, the command will take effect for the specified VLAN(s) only.
- If the specified IPv6 ACL does not exist or the ACL rule is null, all IPv6 multicast groups will be filtered out.
- You can configure different IPv6 ACL rules for each port in different VLANs; for a given VLAN, a newly configured IPv6 ACL rule will override the existing one.

Related commands: **mld-snooping group-policy**.

Examples # Configure ACL 2000 as the IPv6 multicast group filter in VLAN 2.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] group-policy 2000 vlan 2
```

host-aging-time (MLD Snooping view)

Syntax **host-aging-time** *interval*

undo host-aging-time

View MLD Snooping view

Parameters *interval*: Member port aging time, in seconds.

Description Use the **host-aging-time** command to configure the global aging time of group member ports.

Use the **undo host-aging-time** command to restore the default setting.

By default, the aging time of member ports is 260 seconds.

This command works only on an MLD Snooping-enabled VLAN, but not on a VLAN with MLD enabled on its VLAN interface.

Related commands: **mld-snooping host-aging-time**.

Examples # Set the aging time of group member ports globally to 300 seconds.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] host-aging-time 300
```

last-listener-query-interval (MLD Snooping view)

Syntax **last-listener-query-interval** *interval*

undo last-listener-query-interval

View MLD Snooping view

Parameters *interval*: MLD last listener query interval, namely the interval between MLD multicast-address-specific queries, in seconds.

Description Use the **last-listener-query-interval** command to configure the MLD last listener query interval globally.

Use the **undo last-listener-query-interval** command to restore the system default.

By default, the MLD last listener query interval is 1 second.

This command works only on an MLD Snooping-enabled VLAN, but not on a VLAN with MLD enabled on its VLAN interface.

Related commands: **mld-snooping last-listener-query-interval**.

Examples # Set the MLD last listener query interval to 3 seconds globally.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] last-listener-query-interval 3
```

max-response-time (MLD Snooping view)

Syntax **max-response-time** *interval*

undo max-response-time

View MLD Snooping view

Parameters *interval*: Maximum response delay, namely the maximum length of time in seconds member hosts are allowed to wait before sending MLD reports in response to an MLD general query.

Description Use the **max-response-time** command to configure the maximum response delay globally.

Use the **undo max-response-time** command to restore the system default.

By default, the maximum response delay is 10 seconds.

This command works only on an MLD Snooping-enabled VLAN, but not on a VLAN with MLD enabled on its VLAN interface.

Related commands: **mld-snooping max-response-time** and **mld-snooping query-interval**.

Examples # Set the maximum response delay to 5 seconds globally.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] max-response-time 5
```

mld-snooping

Syntax **mld-snooping**

undo mld-snooping

View System view

Parameters None

Description Use the **mld-snooping** command to enable MLD Snooping globally and enter MLD Snooping view.

Use the **undo mld-snooping** command to disable MLD Snooping globally.

By default, MLD Snooping is disabled.

Related commands: **mld-snooping enable**.

Examples # Enable MLD Snooping and enter MLD Snooping view.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping]
```

mld-snooping enable

Syntax **mld-snooping enable**

undo mld-snooping enable

View VLAN view

Parameters None

Description Use the **mld-snooping enable** command to enable MLD Snooping in the current VLAN.

Use the **undo mld-snooping enable** command to disable MLD Snooping in the current VLAN.

By default, MLD Snooping is disabled in a VLAN.

- *Before enabling MLD Snooping in a VLAN, you must globally enable MLD Snooping in system view.*
- *After MLD Snooping is enabled in a VLAN, it is not allowed to enable MLD or IPv6 PIM on the corresponding VLAN interface, and vice versa.*

Related commands: **mld-snooping**.

Examples # Enable MLD Snooping in VLAN 2.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
```

mld-snooping fast-leave

Syntax **mld-snooping fast-leave** [**vlan** *vlan-list*]

undo mld-snooping fast-leave [**vlan** *vlan-list*]

View Ethernet interface view/Port group view

Parameters **vlan** *vlan-list*: Defines one or multiple VLANs. You can provide up to 10 VLAN lists, by each of which you can specify an individual VLAN in the form of *vlan-id*, or a

VLAN range in the form of *start-vlan-id* **to** *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID.

Description Use the **mld-snooping fast-leave** command to enable the fast leave feature on the current port or group of ports.

Use the **undo mld-snooping fast-leave** command to disable the fast leave feature on the current port or group of ports.

By default, the fast leave feature is disabled.

Note that:

- This command works on an MLD Snooping-enabled VLAN or on a VLAN with MLD enabled on its VLAN interface.
- If you do not specify any VLAN in Ethernet interface view, the command will take effect for the port no matter which VLAN the port belongs to; if you specify a VLAN or multiple VLANs, the command will take effect for the port only if the port belongs to the specified VLAN(s).
- If you do not specify any VLAN in port group view, the command will take effect for all the ports in this group no matter which VLANs these port belong to; if you specify a VLAN or multiple VLANs, the command will take effect for those ports in this group that belong to the specified VLAN(s).

Related commands: **fast-leave**.

Examples # Enable the fast leave feature on Ethernet1/1/1, which belongs to VLAN 2.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1/1
[Sysname-Ethernet1/1/1] mld-snooping fast-leave vlan 2
```

mld-snooping general-query source-ip

Syntax **mld-snooping general-query source-ip** { **current-interface** | *ipv6-address* }

undo mld-snooping general-query source-ip

View VLAN view

Parameters **current-interface**: Specify the IPv6 link-local address of the current VLAN interface as the source IPv6 address of MLD general queries..

ipv6-address: Specifies the source IPv6 address of MLD general queries, which can be any legal IPv6 link-local address.

Description Use the **mld-snooping general-query source-ip** command to configure the source IPv6 address of MLD general queries.

Use the **undo mld-snooping general-query source-ip** command to restore the default configuration.

By default, the source IPv6 address of MLD general queries is FE80::02FF:FFFF:FE00:0001.

This command takes effect only if MLD Snooping is enabled in the VLAN.

Examples # In VLAN 2, specify FE80:0:0:1::1 as the source IPv6 address of MLD general queries.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping general-query source-ip fe80:0:0:1::1
```

mld-snooping group-limit

Syntax **mld-snooping group-limit** *limit* [**vlan** *vlan-list*]

undo mld-snooping group-limit [**vlan** *vlan-list*]

View Ethernet interface view/Port group view

Parameters *limit*: Maximum number of IPv6 multicast groups that can pass the port(s).

vlan *vlan-list*: Defines one or multiple VLANs. You can provide up to 10 VLAN lists, by each of which you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* **to** *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID.

Description Use the **mld-snooping group-limit** command to configure the maximum number of IPv6 multicast groups that can pass the port(s).

Use the **undo mld-snooping group-limit** command to restore the default setting.

By default, the maximum number of IPv6 multicast groups allowed to pass the port (s) is 1024.

Note that:

- This command works on an MLD Snooping-enabled VLAN or on a VLAN with MLD enabled on its VLAN interface.
- If you do not specify any VLAN in Ethernet interface view, the command will take effect for the port no matter which VLAN the port belongs to; if you specify a VLAN or multiple VLANs, the command will take effect for the port only if the port belongs to the specified VLAN(s).

- If you do not specify any VLAN in port group view, the command will take effect for all the ports in this group no matter which VLANs these port belong to; if you specify a VLAN or multiple VLANs, the command will take effect for those ports in this group that belong to the specified VLAN(s).

Examples # Specify to allow a maximum of 10 IPv6 multicast groups to pass Ethernet1/1/1, which belongs to VLAN 2.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1/1
[Sysname-Ethernet1/1/1] mld-snooping group-limit 10 vlan 2
```

mld-snooping group-policy

Syntax **mld-snooping group-policy** *acl6-number* [**vlan** *vlan-list*]

undo mld-snooping group-policy [**vlan** *vlan-list*]

View Ethernet interface view/Port group view

Parameters *acl6-number*: Basic IPv6 ACL number.

vlan *vlan-list*: Defines one or multiple VLANs. You can provide up to 10 VLAN lists, by each of which you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* **to** *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID.

Description Use the **mld-snooping group-policy** command to configure an IPv6 multicast group filter on the current port(s).

Use the **undo mld-snooping group-policy** command to remove the configured IPv6 multicast group filter on the current port(s).

By default, no IPv6 multicast group filter is configured on a port, namely a host can join any IPv6 multicast group.

Note that:

- This command works on an MLD Snooping-enabled VLAN or on a VLAN with MLD enabled on its VLAN interface.
- If you do not specify any VLAN in Ethernet interface view, the command will take effect for the port no matter which VLAN the port belongs to; if you specify a VLAN or multiple VLANs, the command will take effect for the port only if the port belongs to the specified VLAN(s).
- If you do not specify any VLAN in port group view, the command will take effect for all the ports in this group no matter which VLANs these port belong to; if you specify a VLAN or multiple VLANs, the command will take effect for those ports in this group that belong to the specified VLAN(s).
- If the specified ACL does not exist or the ACL rule is null, all IPv6 multicast groups will be filtered out.

- You can configure different IPv6 ACL rules for each port in different VLANs; for a given VLAN, a newly configured IPv6 ACL rule will override the existing one.

Related commands: **group-policy**.

Examples # Configure ACL 2000 as the IPv6 multicast group filter on Ethernet1/1/1, which belongs to VLAN 2.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1/1
[Sysname-Ethernet1/1/1] mld-snooping group-policy 2000 vlan 2
```

mld-snooping host-aging-time

Syntax **mld-snooping host-aging-time** *interval*

undo mld-snooping host-aging-time

View VLAN view

Parameters *interval*: Member port aging time, in seconds.

Description Use the **mld-snooping host-aging-time** command to configure the aging time of IPv6 multicast group member ports in the current VLAN.

Use the **undo mld-snooping host-aging-time** command to restore the system default.

By default, the member port aging time is 260 seconds.

This command takes effect only if MLD Snooping is enabled in the VLAN.

Related commands: **host-aging-time**.

Examples # Set the aging time of group member ports to 300 seconds in VLAN 2.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping host-aging-time 300
```

mld-snooping host-join

Syntax **mld-snooping host-join** *ipv6-group-address* **vlan** *vlan-id*

undo mld-snooping host-join *ipv6-group-address* **vlan** *vlan-id*

View Ethernet interface view/Port group view

Parameters **vlan** *vlan-id*: Specifies a VLAN that comprises the Ethernet port(s)

ipv6-group-address: Address of the IPv6 multicast group the current port(s) will join as simulated member host(s).

Description Use the **mld-snooping host-join** command to configure the current port or port group to join the specified IPv6 multicast group as simulated member host(s).

Use the **undo mld-snooping host-join** command to remove the current port or port group as simulated member host(s) for the specified IPv6 multicast group.

By default, this function is disabled.

Note that:

- This command works on an MLD Snooping-enabled VLAN or on a VLAN with MLD enabled on its VLAN interface.
- If configured in Ethernet interface view, this feature takes effect on the port only if the port belongs to the specified VLAN.
- If configured in port group view, this feature takes effect only on those ports in this port group that belong to the specified VLAN.

Examples # # Configure Ethernet1/1/1 in VLAN 2 to join the IPv6 multicast group FF1E::101:101 as a simulated host. .

```
<Sysname> system-view
[Sysname] interface ethernet 1/1/1
[Sysname-Ethernet1/1/1] mld-snooping host-join ff1e::101:101 vlan 2
```

mld-snooping last-listener-query-interval

Syntax **mld-snooping last-listener-query-interval** *interval*

undo mld-snooping last-listener-query-interval

View VLAN view

Parameters *interval*: MLD last listener query interval, namely the interval between MLD multicast-address-specific queries, in seconds.

Description Use the **mld-snooping last-listener-query-interval** command to configure the MLD last listener query interval in the VLAN.

Use the **undo mld-snooping last-listener-query-interval** command to restore the system default.

By default, the MLD last member query interval is 1 second.

This command takes effect only if MLD Snooping is enabled in the VLAN.

Related commands: **last-listener-query-interval**.

Examples # Set the MLD last member query interval to 3 seconds in VLAN 2.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping last-listener-query-interval 3
```

mld-snooping max-response-time

Syntax **mld-snooping max-response-time** *interval*

undo mld-snooping max-response-time

View VLAN view

Parameters *interval*: Maximum response delay, namely the maximum length of time in seconds member hosts are allowed to wait before sending MLD reports in response to an MLD general query.

Description Use the **mld-snooping max-response-time** command to configure the maximum response delay in the VLAN.

Use the **undo mld-snooping max-response-time** command to restore the system default.

By default, the maximum response delay is 10 seconds.

This command takes effect only if MLD Snooping is enabled in the VLAN.

Related commands: **max-response-time** and **mld-snooping query-interval**.

Examples # Set the maximum response delay to 5 seconds in VLAN 2.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping max-response-time 5
```

mld-snooping overflow-replace

Syntax **mld-snooping overflow-replace** [**vlan** *vlan-list*]

undo mld-snooping overflow-replace [**vlan** *vlan-list*]

View Ethernet interface view/Port group view

Parameters **vlan** *vlan-list*: Defines one or multiple VLANs. You can provide up to 10 VLAN lists, by each of which you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* **to** *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID.

Description Use the **mld-snooping overflow-replace** command to enable the IPv6 multicast group replacement function on the current port(s).

Use the **undo mld-snooping overflow-replace** command to disable the IPv6 multicast group replacement function on the current port(s).

By default, the IPv6 multicast group replacement function is disabled.

Note that:

- This command works on an MLD Snooping-enabled VLAN or on a VLAN with MLD enabled on its VLAN interface.
- If you do not specify any VLAN in Ethernet interface view, the command will take effect for the port no matter which VLAN the port belongs to; if you specify a VLAN or multiple VLANs, the command will take effect for the port only if the port belongs to the specified VLAN(s).
- If you do not specify any VLAN in port group view, the command will take effect for all the ports in this group no matter which VLANs these port belong to; if you specify a VLAN or multiple VLANs, the command will take effect for those ports in this group that belong to the specified VLAN(s).

Related commands: **overflow-replace**.

Examples # Enable the IPv6 multicast group replacement function on Ethernet1/1/1, which belongs to VLAN 2.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1/1
[Sysname-Ethernet1/1/1] mld-snooping overflow-replace vlan 2
```

mld-snooping querier

Syntax **mld-snooping querier**

undo mld-snooping querier

View VLAN view

Parameters None

Description Use the **mld-snooping querier** command to enable the MLD Snooping querier function in the VLAN.

Use the **undo mld-snooping querier** command to disable the MLD Snooping querier function in the VLAN.

By default, the MLD Snooping querier function is disabled.

This command takes effect only if MLD Snooping is enabled in the VLAN.

Examples # Enable the MLD Snooping querier function in VLAN 2.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping querier
```

mld-snooping query-interval

Syntax **mld-snooping query-interval** *interval*

undo mld-snooping query-interval

View VLAN view

Parameters *interval*: Interval between MLD general queries, in seconds.

Description Use the **mld-snooping query-interval** command to configure the interval between MLD general queries.

Use the **undo mld-snooping query-interval** command to restore the default setting.

By default, the interval between MLD general queries is 125 seconds.

This command takes effect only if MLD Snooping is enabled in the VLAN.

Related commands: **mld-snooping querier**, **mld-snooping max-response-time** and **max-response-time**.

Examples # Set the interval between MLD general queries to 20 seconds in VLAN2.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping querier
[Sysname-vlan2] mld-snooping query-interval 20
```

mld-snooping router-aging-time

Syntax **mld-snooping router-aging-time** *interval*

undo mld-snooping router-aging-time

View VLAN view

Parameters *interval*: Router port aging time, in seconds.

Description Use the **mld-snooping router-aging-time** command to configure the aging time of router ports in the current VLAN.

Use the **undo mld-snooping router-aging-time** command to restore the default setting.

By default, the router port aging time is 260 seconds.

This command takes effect only if MLD Snooping is enabled in the VLAN.

Related commands: **router-aging-time**.

Examples # Set the aging time of router ports to 100 seconds in VLAN 2.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping router-aging-time 100
```

mld-snooping special-query source-ip

Syntax **mld-snooping special-query source-ip** { **current-interface** | *ipv6-address* }

undo mld-snooping special-query source-ip

View VLAN view

Parameters **current-interface**: Specifies the source IPv6 link-local address of the VLAN interface of the current VLAN as the source IPv6 address of MLD multicast-address-specific queries.

ipv6-address: Specifies an IPv6 link-local address as the source IPv6 address of MLD multicast-address-specific queries.

Description Use the **mld-snooping special-query source-ip** command to configure the source IPv6 address of MLD multicast-address-specific queries.

Use the **undo mld-snooping special-query source-ip** command to restore the system default.

By default, the source IPv6 address of MLD multicast-address-specific queries is FE80::02FF:FFFF:FE00:0001.

This command takes effect only if MLD Snooping is enabled in the VLAN.

Examples # In VLAN 2, specify FE80:0:0:1::1 as the source IPv6 address of MLD multicast-address-specific queries.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping special-query source-ip fe80:0:0:1::1
```

mld-snooping static-group

Syntax **mld-snooping static-group** *ipv6-group-address* **vlan** *vlan-id*

undo mld-snooping static-group *ipv6-group-address* **vlan** *vlan-id*

View Ethernet interface view/Port group view

Parameters *ipv6-group-address*: Address of a IPv6 multicast group the current port(s) will join as static member port(s).

vlan *vlan-id*: Specifies a VLAN that comprises the current Ethernet port(s).

Description Use the **mld-snooping static-group** command to configure the current port or port group to join the specified IPv6 multicast group as static member port(s).

Use the **undo mld-snooping static-group** command to remove the current port or port group as static member port(s) for the specified IPv6 multicast group.

By default, the static member port function is disabled.

Note that:

- This command works on an MLD Snooping-enabled VLAN or on a VLAN with MLD enabled on its VLAN interface.
- If configured in Ethernet interface view, this feature takes effect on the port only if the port belongs to the specified VLAN.
- If configured in port group view, this feature takes effect only on those ports in this port group that belong to the specified VLAN.

Examples # Configure Ethernet1/1/1 in VLAN 2 to join the IPv6 multicast group FF1E::101:101 as a static member port.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1/1
[Sysname-Ethernet1/1/1] mld-snooping static-group ff1e::101:101 vlan 2
```

mld-snooping static-router-port

Syntax **mld-snooping static-router-port vlan** *vlan-id*

undo mld-snooping static-router-port vlan *vlan-id*

View Ethernet interface view/Port group view

Parameters **vlan** *vlan-id*: Specifies a VLAN that comprises the current Ethernet port(s).

Description Use the **mld-snooping static-router-port** command to configure the current port(s) as static router port(s).

Use the **undo mld-snooping static-router-port** command to remove the current port(s) as static router port(s).

By default, the static router port function is disabled.

Note that:

- This command works on an MLD Snooping-enabled VLAN or on a VLAN with MLD enabled on its VLAN interface.
- If configured in Ethernet interface view, this feature takes effect on the port only if the port belongs to the specified VLAN.
- If configured in port group view, this feature takes effect only on those ports in this port group that belong to the specified VLAN.

Examples # Configure Ethernet1/1/1, which belongs to VLAN 2, as a static router port.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1/1
[Sysname-Ethernet1/1/1] mld-snooping static-router-port vlan 2
```

overflow-replace (MLD Snooping view)

Syntax **overflow-replace** [**vlan** *vlan-list*]

undo overflow-replace [**vlan** *vlan-list*]

View MLD Snooping view

Parameters **vlan** *vlan-list*: Defines one or multiple VLANs. You can provide up to 10 VLAN lists, by each of which you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* **to** *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID.

Description Use the **overflow-replace** command to enable the IPv6 multicast group replacement function globally.

Use the **undo overflow-replace** command to disable the IPv6 multicast group replacement function globally.

By default, the IPv6 multicast group replacement function is disabled globally.

Note that:

- This command works on an MLD Snooping-enabled VLAN or on a VLAN with MLD enabled on its VLAN interface.
- If you do not specify any VLAN, the command will take effect for all VLANs; if you specify a VLAN or multiple VLANs, the command will take effect for the specified VLAN(s) only.

Related commands: **mld-snooping overflow-replace**.

Examples # Enable the IPv6 multicast group replacement function globally in VLAN2.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] overflow-replace vlan 2
```

report-aggregation

Syntax **report-aggregation**

undo report-aggregation

View MLD Snooping view

Parameters None

Description Use the **mld-snooping report-aggregation** command to enable MLD report suppression.

Use the **undo mld-snooping report-aggregation** command to disable MLD report suppression.

By default, MLD report suppression is enabled.

This command works on an MLD Snooping-enabled VLAN or on a VLAN with MLD enabled on its VLAN interface.

Examples # Disable MLD report suppression.

```
<Sysname> system-view
[Sysname] undo report-aggregation
```

reset mld-snooping group

Syntax **reset mld-snooping group** { *ipv6-group-address* | **all** } [**vlan** *vlan-id*]

View User view

Parameters *ipv6-group-address*: Address of the IPv6 multicast group of which the MLD Snooping entries are to be cleared.

all: Specifies to clear all MLD Snooping entries.

vlan *vlan-id*: Specifies a VLAN in which the specified MLD Snooping entry or all MLD Snooping entries are to be cleared.

Description Use the **reset mld-snooping group** command to clear MLD Snooping entries.

Note that:

- This command works only on an MLD Snooping-enabled VLAN, but not on a VLAN with MLD enabled on its VLAN interface.
- This command cannot clear MLD Snooping entries of static joins.

Examples # Clear all MLD Snooping entries saved in the device.

```
<Sysname> reset mld-snooping group all
```

reset mld-snooping statistics

Syntax **reset mld-snooping statistics**

View User view

Parameters None

Description Use the **reset mld-snooping statistics** command to clear the statistics information of MLD messages learned by MLD Snooping.

Examples # Clear the statistics information of all kinds of MLD messages learned by MLD Snooping.

```
<Sysname> reset mld-snooping statistics
```

router-aging-time (MLD Snooping view)

Syntax **router-aging-time** *interval*

undo router-aging-time

View MLD Snooping view

Parameters *interval*: Router port aging time, in seconds.

Description Use the **router-aging-time** command to configure the aging time of router ports globally.

Use the **undo router-aging-time** command to restore the system default.

By default, the router port aging time is 260 seconds.

This command works only on an MLD Snooping-enabled VLAN, but not on a VLAN with MLD enabled on its VLAN interface.

Related commands: **mld-snooping router-aging-time**.

Examples # Set the aging time of router ports globally to 100 seconds.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] router-aging-time 100
```

50 IPv6 PIM CONFIGURATION COMMANDS

The term "router" in this document refers to a router in a generic sense or a Switch 8800 running IPv6 PIM.

bsr-policy (Pv6 PIM view)

Syntax **bsr-policy** *acl6-number*

undo bsr-policy

View IPv6 PIM view

Parameters *acl6-number*: Basic IPv6 ACL number. When an IPv6 ACL is defined, the **source** keyword in the **rule** command specifies a legal BSR source IPv6 address range.

Description Use the **bsr-policy** command to configure a legal range of BSR global unicast addresses so that the device discards any bootstrap messages from out of the configured address range to guard against BSR spoofing.

Use the **undo bsr-policy** command to remove the restore the system default.

By default, there are no restrictions on the BSR address range, namely all the received BSR messages are regarded to be valid.

Examples # Configure a legal BSR address range so that only routers with an address in the range of 2001::2/64 can become the BSR.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule 0 permit source 2001::2 64
[Sysname-acl6-basic-2000] quit
[Sysname] multicast ipv6 routing-enable
[Sysname-pim6] bsr-policy 2000
```

c-bsr (IPv6 PIM view)

Syntax **c-bsr** *ipv6-address* [*hash-length* [*priority*]]

undo c-bsr

View IPv6 PIM view

Parameters *ipv6-address*: IPv6 global unicast address of the interface that is to act as a C-BSR.

hash-length: Hash mask length for RP selection calculation. If you do not include this keyword in your command, the corresponding global setting will be used.

priority: Priority of the C-BSR, 0 by default. If you do not include this keyword in your command, the corresponding global setting will be used. A larger value of this argument means a higher priority.

Description Use the **c-bsr** command to configure the specified interface as a C-BSR.

Use the **undo c-bsr** command to restore the system default.

No C-BSR is configured by default.

Related commands: **pim ipv6 sm**, **c-bsr hash-length**, **c-bsr priority** and **c-rp**.

Examples # Configure the interface with an IPv6 global unicast address of 1101::1 as a C-BSR.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] c-bsr 1101::1
```

c-bsr hash-length (IPv6 PIM view)

Syntax **c-bsr hash-length** *hash-length*

undo c-bsr hash-length

View IPv6 PIM view

Parameters *hash-length*: Hash mask length for RP selection calculation.

Description Use the **c-bsr hash-length** command to configure the global Hash mask length for RP selection calculation.

Use the **undo c-bsr hash-length** command to restore the system default.

By default, the Hash mask length for RP selection calculation is 126.

Related commands: **c-bsr**.

Examples # Set the global Hash mask length for RP selection calculation to 16.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] c-bsr hash-length 16
```

c-bsr holdtime (Pv6 PIM view)

Syntax **c-bsr holdtime** *interval*

undo c-bsr holdtime

View IPv6 PIM view

Parameters *interval*: Bootstrap timeout in seconds.

Description Use the **c-bsr holdtime** command to configure the bootstrap timeout time, namely the length of time the device as a C-BSR waits before it must receive a bootstrap message from the BSR.

Use the **undo c-bsr holdtime** command to restore the system default.

By default, the bootstrap timeout value is determined by this formula: Bootstrap timeout = Bootstrap interval × 2 + 10.

The default bootstrap interval is 60 seconds, so the default bootstrap timeout = 60 × 2 + 10 = 130 (seconds).

Related commands: **c-bsr** and **c-bsr interval**.

Examples # Set the bootstrap timeout time to 150 seconds.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] c-bsr holdtime 150
```

c-bsr interval (Pv6 PIM view)

Syntax **c-bsr interval** *interval*

undo c-bsr interval

View IPv6 PIM view

Parameters *interval*: Bootstrap interval in seconds.

Description Use the **c-bsr interval** command to configure the bootstrap interval, namely the interval the BSR waits between sending bootstrap messages.

Use the **undo c-bsr interval** command to restore the system default.

By default, the bootstrap interval value is determined by this formula: Bootstrap interval = (Bootstrap timeout - 10) ÷ 2.

The default bootstrap timeout is 130 seconds, so the default bootstrap interval = (130 - 10) ÷ 2 = 60 (seconds).

Related commands: **c-bsr** and **c-bsr holdtime**.

Examples # Set the bootstrap interval to 30 seconds.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] c-bsr interval 30
```

c-bsr priority (Pv6 PIM view)

Syntax **c-bsr priority** *priority*

undo c-bsr priority

View IPv6 PIM view

Parameters *priority*: Priority of the C-BSR. A larger value means a higher priority.

Description Use the **c-bsr priority** command to configure the global C-BSR priority.

Use the **undo c-bsr priority** command to restore the system default.

By default, the C-BSR priority is 0.

Related commands: **c-bsr**.

Examples # Set the global C-BSR priority to 5.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] c-bsr priority 5
```

c-rp (IPv6 PIM view)

Syntax **c-rp** *ipv6-address* [**group-policy** *acl6-number* | **priority** *priority* | **holdtime** *hold-interval* | **advertisement-interval** *adv-interval*] *

undo c-rp *ipv6-address*

View IPv6 PIM view

Parameters *ipv6-address*: IPv6 global unicast address of the interface that is to act as a C-RP.

acl6-number: Basic IPv6 ACL number. This IPv6 ACL defines a range of IPv6 multicast groups the C-RP is going to serve, rather than defining a filtering rule. Any IPv6 multicast group range that matches the **permit** statement in the ACL will

be advertised as an RP served group, while configurations matching other statements like **deny** will not take effect.

priority: Priority of the C-RP, 0 by default. A larger value means a lower priority.

hold-interval: C-RP timeout time, in seconds. If you do not include this argument in your command, the corresponding global setting will be used.

adv-interval: C-RP-Adv interval in seconds. If you do not include this argument in your command, the corresponding global setting will be used.

Description Use the **c-rp** command to configure the specified interface a C-RP.

Use the **undo c-rp** command to remove the related C-RP configuration.

No C-RPs are configured by default.

Note that:

- If you do not specify an IPv6 multicast group range for the C-RP, the C-RP will serve all IPv6 multicast groups.
- If you wish a device to be a C-RP for multiple group ranges, you need to include these group ranges in multiple rules in the IPv6 ACL corresponding to the **group-policy** keyword.
- If you carry out this command repeatedly on the same interface, the last configuration will take effect.

Related commands: **c-bsr**.

Examples # Configure the interface with an IPv6 global unicast address of 2001::1 to be a C-RP for IPv6 multicast group FF35:0:1391::/96, with a priority of 10.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule permit source ff35:0:1391:: 96
[Sysname-acl6-basic-2000] quit
[Sysname] pim ipv6
[Sysname-pim6] c-rp 2001::1 group-policy 2000 priority 10
```

c-rp advertisement-interval (Pv6 PIM view)

Syntax **c-rp advertisement-interval** *interval*

undo c-rp advertisement-interval

View IPv6 PIM view

Parameters *interval*: C-RP-Adv interval in seconds.

Description Use the **c-rp advertisement-interval** command to configure globally the interval the device waits between sending C-RP-Adv messages.

Use the **undo c-rp advertisement-interval** command to restore the system default.

By default, the C-RP-Adv interval is 60 seconds.

Related commands: **c-rp**.

Examples # Set the global C-RP-Adv interval to 30 seconds.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] c-rp advertisement-interval 30
```

c-rp holdtime (IPv6 PIM view)

Syntax **c-rp holdtime** *interval*

undo c-rp holdtime

View IPv6 PIM view

Parameters *interval*: C-RP timeout in seconds.

Description Use the **c-rp holdtime** command to configure globally the C-RP timeout time, namely the length of time the BSR waits before it must receive a C-RP-Adv message from a C-RP.

Use the **undo c-rp holdtime** command to restore the system default.

By default, the C-RP timeout time is 150 seconds.

Because a non-BSR router refreshes its C-RP timeout time through BSR bootstrap messages, to prevent loss of BSR bootstrap messages, the C-RP timeout time should be longer than the bootstrap interval. The recommended C-RP timeout setting is 2.5 times the bootstrap interval or longer.

Related commands: **c-rp** and **c-bsr interval**.

Examples # Set the global C-RP timeout time to 200 seconds.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] c-rp holdtime 200
```

crp-policy (IPv6 PIM view)

Syntax **crp-policy** *acl6-number*

undo crp-policy

View IPv6 PIM view

Parameters *acl6-number*: Advanced IPv6 ACL number. When configuring the IPv6 ACL, use the **source** keyword in the **rule** command to specify the IPv6 address of a C-RP and the **destination** keyword to specify the address range of the IPv6 multicast groups that the C-RP will serve.

Description Use the **crp-policy** command to configure a legal C-RP address range and the range of served IPv6 multicast groups, so as to guard against C-RP spoofing.

Use the **undo crp-policy** command to restore the system default.

By default, there are no restrictions on C-RP address ranges and the address ranges of served groups, namely all received C-RP messages are assumed to be legal.

Examples # Configure a C-RP address range so that only routers in the address range of 2001::2/64 can be C-RPs.

```
<Sysname> system-view
[Sysname] acl ipv6 number 3000
[Sysname-acl6-adv-3000] rule 0 permit ipv6 source 2001::2 64
[Sysname-acl6-adv-3000] quit
[Sysname] pim ipv6
[Sysname-pim6] crp-policy 3000
```

debugging pim ipv6

Syntax **debugging pim ipv6** { **all** | **event** [*advanced-acl6-number*] | **routing-table** [*advanced-acl6-number*] | **neighbor** [*basic-acl6-number*] [**receive** | **send**] | **assert** [*advanced-acl6-number*] [**receive** | **send**] | **rp** [**receive** | **send**] | **join-prune** [*advanced-acl6-number*] [**receive** | **send**] | **register** [*advanced-acl6-number*] | **state-refresh** [*advanced-acl6-number*] [**receive** | **send**] }

undo debugging pim ipv6 { **all** | **event** | **routing-table** | **neighbor** [**receive** | **send**] | **assert state-refresh** [**receive** | **send**] | **rp** [**receive** | **send**] | **join-prune** [**receive** | **send**] | **register** }

View User view

Parameters **all**: Turns on/off all types of IPv6 PIM debugging.

event: Turns on/off event debugging.

advanced-acl6-number: Advanced IPv6 ACL number.

routing-table: Turns on/off debugging for IPv6 PIM multicast routing table state changes.

neighbor: Turns on/off neighbor information debugging.

basic-acl6-number: Basic IPv6 ACL number.

receive: Turns on/off debugging for received messages.

receive: Turns on/off debugging for sent messages.

assert: Turns on/off debugging for assert messages.

rp: Turns on/off RP debugging.

join-prune: Turns on/off debugging for join and prune messages.

register: Turns on/off PIM debugging for register messages.

state-refresh: Turns on/off state-refresh debugging.

Description Use the **debugging pim ipv6** command to turn on IPv6 PIM debugging.

Use the **undo debugging pim ipv6** command to turn off IPv6 PIM debugging.

By default, IPv6 PIM debugging is disabled.

Table 241 Field descriptions of the debugging pim ipv6 assert command

Field	Description
receiving	Assert message received
sending	Assert message sent
on interfacename	Interface on which the message was received or sent
pref	Value of the preference field
metric	Value of the metric field
rpt set	RPT bit: 1
rpt unset	RPT bit: 0
reserved field non-zero	The Reserved field is non-zero.
unknown neighbor	Unknown neighbor
truncated assert packet	Invalid packet size
bad group address	Incorrect IPv6 group address
bad group mask	Incorrect IPv6 group address prefix
unknown group family	Group address family error
group boundary	Group boundary
bad source address	Incorrect source address
locally scoped	Node-local or link-local scope
Fsm:assert	Assert state machine
current state	Current state of the assert state machine
received event	Type of the event received by the assert state machine
loser	The assert state machine is in the Loser state
winner	The assert state machine is in the Winner state
noinfo	The assert state machine is in the Noinfo state

Table 241 Field descriptions of the debugging pim ipv6 assert command

Field	Description
state1->state2	The assert state machine changed from state1 to state2.

Table 242 Field descriptions of the debugging pim ipv6 event command

Field	Description
unsupported PIM version	The IPv6 PIM version is not supported
PIM packet too short	Too small packet size of IPv6 PIM message
checksum error	Checksum error
non-pim interface	An IPv6 PIM message was received on a non-PIM-enabled interface.
unsupported type	The specified IPv6 PIM message type is not supported.
Socket set option error	Failed to set socket option
Packet send error	Failed to send IPv6 PIM message
Source address is one of the interfaces address	The source address is the address of a local interface.
Source address *address* is invalid	The source address is invalid.
Invalid source mask	Incorrect source address prefix
Active event received	A source-active event was received.
Inactive event received	A source-inactive event was received.
Clear event received	A clear-entry event was received.
Wrong IF	Incorrect incoming interface
NoInfo	The downstream state machine is in the Noinfo state.
PPending	The downstream state machine is in the Prune Pending state.
Pruned	The IPv6 PIM-DM downstream state machine is in the Pruned state.
Joined	The IPv6 PIM-SM downstream state machine is in the Joined state.
Forwarding	The IPv6 PIM-DM upstream state machine is in the Forward state.
Pruned	The IPv6 PIM-DM upstream state machine is in the Pruned state.
AckPending	The IPv6 PIM-DM upstream state machine is in the Ack Pending state.
Joined	The IPv6 PIM-SM (S, G) or (*, G) upstream state machine is in the Joined state.
NotJoined	The IPv6 PIM-SM (S, G) or (*, G) upstream state machine is in the Not Joined state.
PruneTmp	The IPv6 PIM-SM (S, G, RPT) downstream state machine is in the Prune Tmp state.
PPendingTmp	The IPv6 PIM-SM (S, G, RPT) downstream state machine is in the Prune Pending Tmp state.
PPT Expired	The Prune Pending timer timed out.
RPF_Interface changed	The RPF interface changed.
Genid changed	The neighbor generation ID changed.

Table 242 Field descriptions of the debugging pim ipv6 event command

Field	Description
PT Expired	The prune timer timed out.
Failed to pass MSF	Failed to pass multicast source filtering
NotOriginator	The originator state machine is in the Not Originator state.
Originator	The originator state machine is in the Originator state.
SAT Expired	The source-alive timer timed out.
Join suppressed	The device received a join message to the upstream neighbor on the incoming interface and suppressed its own join message.
Override it	The device received a prune message to the upstream neighbor on the incoming interface and sent a join message.
ET Expired	The IPv6 PIM-SM downstream interface aging timers timed out.
register downstream	Registering the outgoing interface
Mcast-Boundary-Changed	Multicast boundary change event

Table 243 Field descriptions of the debugging pim ipv6 join-prune command

Field	Description
JP	Join/prune message
GFT	Graft message
GAK	Graft-ack message
receiving	Messages received
sending	Message sent
unknown address	Unknown address, address decoding failed
bad group address, mask or family	Incorrect IPv6 group address, prefix, or family
Bad source address, mask or family	Incorrect source address, prefix or family
Upstream	Upstream neighbor information in the message
Groups	Number of groups in the message
Group: addr/mask --- m joins n prunes	Group information in the message: IPv6 group address/prefix length - m joins and n prunes
Join: addr/mask flag	Join: source address/ prefix flag
Message truncated. Ignoring message	The message was dropped due to invalid packet size.
Unable to decode address	Address decoding failed
Upstream neighbor is not this router. Ignoring	The message was dropped because the upstream neighbor is not this device.
group boundary detected for address1 on address2	address1 is within the multicast boundary configured on the interface corresponding to address2.
Group address1 ignored in message on address2	address1 is within the multicast boundary configured on the interface corresponding to address2, and this group is ignored
Message from unknown neighbor	A message was received from an unknown neighbor.

Table 243 Field descriptions of the debugging pim ipv6 join-prune command

Field	Description
Join/Prune received for non-local neighbor	A join/prune message for a non-local upstream neighbor was received.
Override timer expires	The prune override timer timed out.

Table 244 Field descriptions of the debugging pim ipv6 neighbor command

Field	Description
HEL	IPv6 PIM hello message
hello packet	IPv6 PIM hello message
receiving	Message received
sending	Message sent
on interfacename	Interface on which the message was received or sent
Option: m, length: n	IPv6 PIM hello message option: option value, option length: length value
Holdtime:	Holdtime field of the IPv6 PIM hello message
Tbit	Tbit option
Lan delay	LAN delay option
Override interval	Override interval option
DR priority	DR priority option
Genid	Generation ID option
Version	Version field of the state refresh option
Refresh interval	State refresh interval
Reserved	Reserved field of the state refresh option
Secondary address(es)	Address(es) in the address list option
Unknown option value	Unknown option
without SR capability	No state refresh capability
Elected as DR on interface interfacename	Elected as the DR for the network attached to *interfacename*
Unelected as DR on interface interfacename	No longer the DR for the network attached to *interfacename*
PIM Neighbor address on interface interfacename timed out	Neighbor address on *interfacename* timed out.

Table 245 Field descriptions of the debugging pim ipv6 register command

Field	Description
REG	Register message
RSP	Register-stop message
Register Stop	Register stopped
receiving	Message received
sending	Message sent
Border bit	Boundary bit
Null bit	Null bit
src	Source address of the IPv6 packet
dst	Destination address of the IPv6 packet

Table 245 Field descriptions of the debugging pim ipv6 register command

Field	Description
Non-DR interface	Non-DR interface
probe	Probe message
ignored	Message dropped

Table 246 Field descriptions of the debugging pim ipv6 routing-table command

Field	Description
Creating	Creating entries
Deleting	Deleting entries
mrt	IPv6 multicast routing table
Add oil	Adding outgoing interface
Del oil	Deleting outgoing interface
Null iif	Null incoming interface
Adding iif	Adding incoming interface
Deleting iif	Deleting incoming interface
RP is not found	RP is not found

Table 247 Field descriptions of the debugging pim ipv6 rp command

Field	Description
receiving	Message received
sending	Message sent
auto-RP announce	auto-RP announce message
auto-RP discovery	auto-RP discovery message
C-RP	Candidate RP
CRP	Candidate RP
BSR	BSR bootstrap message
prefix count	Prefix count field in the C-RP advertisement message
priority	Priority field in the C-RP advertisement message
holdtime	Holdtime field in the C-RP advertisement message
Admin Scope Zone	BSR admin-scope region
Bad BSR address	Incorrect BSR address
frag	Fragment tag field in the BSR bootstrap message
pri	Priority field in the BSR bootstrap message
hash mask len	Hash mask length field in the BSR bootstrap message
Group address/length: frags m, C-RP's n	The frags filed corresponding to *address/length* in the BSR bootstrap message is m, and the number of C-RPs is n.
address pri: m, holdtime: n	The priority of C-RP address in the BSR bootstrap message is m and holdtime is n.
Auto-RP discovery packet: RP agent address, RP count m, Holdtime n	An auto-RP discovery message was received: RP agent is address, RP count is m, and holdtime is n

Table 247 Field descriptions of the debugging pim ipv6 rp command

Field	Description
delete RP-Set	Deleting an RP set
too short length	Too small packet size
wrong RP agent address	Incorrect RP agent address
wrong RP address	Incorrect RP address
bad group address	Incorrect IPv6 group address
bad group mask length	Incorrect group address prefix
bad BSR address	Incorrect BSR address
bad BSR address family	Incorrect BSR address family
bad BSR hash mask length	Incorrect BSR hash mask length
bad scope zone mask	Incorrect admin-scope region prefix
Unknown group address family	Incorrect IPv6 group address family
not directly connected source	Address of a source not directly connected
unknown neighbor	unknown neighbor
ACL	Access control list
Bad frag-rp-count field	Incorrect frag-rp-count field in the BSR bootstrap message
Bad frag-rp field length	Incorrect total length of frag-rp fields in the BSR bootstrap message
BSR mechanism	BSR mechanism independent of administrative scoping
Upstream to BSR	Upstream to the BSR device
no BSR is available	No available BSR
add register vif	Adding a register virtual interface
Remove register vif	Removing a register virtual interface
Expiring CRP	Aged C-RP
Lose the ASBSR election	The device lost BSR election for the BSR admin-scope region
Lose the BSR election	The device lost BSR election
locally scoped	Node-local or link-local scope
RP changed	The RP changed.
pending state	The BSR changed to the pending state.
Update the BSR's state to elected	The BSR changed to the elected state.
RPF Failure	RPF check failed.
admin scope multicast address	Address in the admin-scope range

Table 248 Field descriptions of the debugging pim ipv6 state-refresh command

Field	Description
SRM	State refresh message
sending	Message sent
receiving	Message received
Message truncated	Invalid packet size
bad group address	Incorrect IPv6 group address
Invalid group mask length	Incorrect group address prefix length

Table 248 Field descriptions of the debugging pim ipv6 state-refresh command

Field	Description
Group address	IPv6 group address
Source address	Source address
Originator address	Address of the state refresh message originator
preference	Preference field of the message
metric	Metric field of the message
mask length	Prefix length field of the message
ttl	TTL value of the message
prune indicator	Prune Indicator flag bit
prune now	Prune Now indicator flag bit
assert override	Assert Override flag bit

Examples # Turn on debugging for sent IPv6 PIM assert messages.

```
<Sysname> debugging pim ipv6 assert send
*0.7328718 router PIM/7/ASSERT:IPv6:(public net): PIM ver 2 AST send
ing FE80::2E0:FCFF:FE02:1A01 -> FF02::D on Vlan-interface20  (P01234
3)
*0.7328718 router PIM/7/ASSERT:IPv6:(public net): For FF0E::101:101/
128 from 100:100::168, rpt unset, pref 0, metric 0 (P012351)
```

// An IPv6 PIMv2 assert message is received through VLAN-interface 20, with the source address of FE80::2E0:FCFF:FE02:1A01, destination address of FF02::D, multicast group address of FF0E::101:101/128, and multicast source address of 100:100::168, without the RPT bit set. The priority is 0 and the metric value is 0.

display pim ipv6 bsr-info

Syntax **display pim ipv6 bsr-info**

View Any view

Parameters None

Description Use the **display pim ipv6 bsr-info** command to view the BSR information in the IPv6 PIM-SM domain and the locally configured C-RP information in effect.

Related commands: **c-bsr** and **c-rp**.

Examples # View the BSR information in the IPv6 PIM-SM domain and the locally configured C-RP information in effect.

```
<Sysname> display pim ipv6 bsr-info
Vpn-instance: public net
 Elected BSR Address: 2004::2
     Priority: 0
     Hash mask length: 126
```

```
     State: Elected
     Uptime: 00:01:10
     Next BSR message scheduled at: 00:00:48
 Candidate BSR Address: 2004::2
     Priority: 0
     Hash mask length: 126
     State: Elected

Candidate RP: 2001::1(LoopBack1)
     Priority: 0
     HoldTime: 130
     Advertisement Interval: 60
     Next advertisement scheduled at: 00:00:48
```

Table 249 Field descriptions of the display pim ipv6 bsr-info command

Field	Description
Vpn-instance: public net	VPN instance name
Elected BSR Address	IPv6 global unicast address of the elected BSR
Priority	BSR priority
Hash mask length	Hash mask length for RP selection calculation
State	BSR state
Uptime	Length of time since the BSR was up
Next BSR message scheduled at	Length of time the BSR waits before sending the next bootstrap message
Candidate RP	C-RP address
Priority	C-RP priority
HoldTime	Timeout time of the C-RP
Advertisement Interval	Interval the C-RP waits between sending C-RP-Adv messages
Next advertisement scheduled at	Length of time the C-RP waits before sending the next C-RP-Adv message

display pim ipv6 claimed-route

Syntax **display pim ipv6 claimed-route** [*ipv6-source-address*]

View Any view

Parameters *ipv6-source-address*: Displays the information of the IPv6 unicast route to a particular IPv6 multicast source. If you do not provide this argument, this command will display the information about all IPv6 unicast routes used by IPv6 PIM.

Description Use the **display pim ipv6 claimed-route** command to view the information of IPv6 unicast routes used by IPv6 PIM.

If an (S, G) is marked SPT, this (S, G) entry uses an IPv6 unicast route.

Examples # View the information of the IPv6 unicast route to the multicast source 2001::2.

```
<Sysname> display pim ipv6 claimed-route 2001::2
Vpn-instance: public net
 RPF information about: 2001::2
     RPF interface: Vlan-interface22, RPF neighbor: FE80::A01:100:1
     Referenced prefix/prefix length: 2001::/64
     Referenced route type: igp
     RPF-route selecting rule: preference-preferred
     The (S, G) or (*, G) list dependent on this route entry
     (2001::2, FF35::101:101)
```

Table 250 Field descriptions of the display pim ipv6 claimed-route command

Field	Description
Vpn-instance: public net	VPN instance name
RPF information about	RPF information about the specified address
RPF interface:	RPF interface type and number
RPF neighbor:	Address of the RPF neighbor
Referenced prefix/prefix length:	Destination address/prefix of the IPv6 PIM route
Referenced route type:	Name of the routing protocol
RPF-route selecting rule:	Rule of RPF route selection
The (S,G) or (*,G) list dependent on this route entry	(S,G) or (*, G) entries using this route

display pim ipv6 control-message counters

Syntax **display pim ipv6 control-message counters** [**message-type** { **probe** | **register** | **register-stop** } | [**interface** *interface-type interface-number* | **message-type** { **assert** | **bsr** | **crp** | **graft** | **graft-ack** | **hello** | **join-prune** | **state-refresh** }] *]

View Any view

Parameters *interface-type interface-number*: Displays the number of IPv6 PIM control messages on the specified interface. Currently, only VLAN interfaces are supported for the Switch 8800s.

assert: Assert messages

bsr: Bootstrap messages

crp: C-RP-Adv messages

graft: Graft messages

graft-ack: Graft-ack messages

hello: Hello messages

join-prune: Join/prune messages

probe: Null register messages

register: Register messages

register-stop: Register-stop messages

state-refresh: State refresh messages

Description Use the **display pim ipv6 control-message counters** command to view the statistics information of IPv6 PIM control messages.

Since register, register-stop, and probe messages are counted globally, you cannot view the statistics on these messages on a specific interface.

Examples # View the statistics information of all types of IPv6 PIM control messages on all interfaces.

```
<Sysname> display pim ipv6 control-message counters
Vpn-instance: public net
PIM global control-message counters:
Received        Sent            Invalid
Register            20          37          2
Register-Stop       25          20          1
Probe               10          5           0

PIM control-message counters for interface: Vlan-interface12
Received        Sent            Invalid
Assert          10          5           0
Graft               20          37          2
Graft-Ack           25          20          1
Hello               1232            453         0
Join/Prune      15          30          21
State-Refresh       8           7           1
BSR             3243            589         1
C-RP                53          32          0
```

Table 251 Field descriptions of the display pim ipv6 control-message counters command

Field	Description
Vpn-instance	VPN instance name
Received	Number of messages received
Sent	Number of messages sent
Invalid	Number of invalid messages
Register	Register messages
Register-Stop	Register-stop messages
Probe	Null register messages
Assert	Assert messages
Graft	Graft messages
Graft-Ack	Graft-ack messages
Hello	Hello messages
Join/Prune	Join/prune messages
State Refresh	State refresh messages
BSR	Bootstrap messages
C-RP	C-RP-Adv messages

display pim ipv6 grafts

Syntax **display pim ipv6 grafts**

View Any view

Parameters None

Description Use the **display pim ipv6 grafts** command to view the information about unacknowledged graft messages.

Examples # View the information about unacknowledged graft messages.

```
<Sysname> display pim ipv6 grafts
Source             Group             Age           RetransmitIn
1004::2         ff35::101:101        00:00:24      00:00:02
```

Table 252 Field descriptions of the display pim ipv6 grafts command

Field	Description
Source	IPv6 multicast source address in the graft message
Group	IPv6 multicast group address in the graft message
Age	Remaining aging time of the graft message
RetransmitIn	Length of time before a retry graft message is sent

display pim ipv6 interface

Syntax **display pim ipv6 interface** [*interface-type interface-number*] [**verbose**]

View Any view

Parameters *interface-type interface-number*: Displays the IPv6 PIM information on a particular interface. Currently, only VLAN interfaces are supported for the Switch 8800s.

verbose: Displays the detailed IPv6 PIM information.

Description Use the **display pim ipv6 interface** command to view the IPv6 PIM information on the specified interface or all interfaces.

Examples # View the detailed IPv6 PIM information on VLAN-interface 12.

```
<Sysname> display pim ipv6 interface vlan-interface12 verbose
 Vpn-instance: public net
 Interface: Vlan-interface12, FE80::200:5EFF:FE04:8700
     PIM version: 2
     PIM mode: Dense
     PIM DR: FE80::200:AFF:FE01:101 (local)
     PIM DR Priority (configured): 1
```

```
PIM neighbor count: 0
PIM hello interval: 30 s
PIM LAN delay (negotiated): 500 ms
PIM LAN delay (configured): 500 ms
PIM hello override interval (negotiated): 2500 ms
PIM hello override interval (configured): 2500 ms
PIM neighbor tracking (configured): disabled
PIM neighbor tracking (negotiated): disabled
PIM generation ID: 0X13A7BA06
PIM require generation ID: disabled
PIM hello hold interval: 105 s
PIM assert hold interval: 180 s
PIM triggered hello delay: 5 s
PIM J/P interval: 60 s
PIM J/P hold interval: 210 s
PIM state-refresh processing: enabled
PIM state-refresh interval: 60 s
PIM graft retry interval: 3 s
PIM state-refresh capability on network: capable
Number of routers on network not using DR priority: 0
Number of routers on network not using LAN delay: 0
Number of routers on network not using neighbor tracking: 1
```

Table 253 Field descriptions of the display pim ipv6 interface command

Field	Description
Vpn-instance	VPN instance name
Interface	Interface name and its IPv6 address
PIM version	IPv6 PIM version
PIM mode	IPv6 PIM mode, dense or sparse
PIM DR	IPv6 address of the DR
PIM DR Priority	Priority for DR election
PIM neighbor count	Total number of IPv6 PIM neighbors
PIM hello interval	Interval between IPv6 PIM hello messages
PIM LAN delay (negotiated)	Negotiated prune delay
PIM LAN delay (configured)	Configured prune delay
PIM override interval (negotiated)	Negotiated prune override interval
PIM override interval (configured)	Configured prune override interval
PIM neighbor tracking (negotiated)	Negotiated neighbor tracking status (enabled/disabled)
PIM neighbor tracking (configured)	Configured neighbor tracking status (enabled/disabled)
PIM generation ID	Generation_ID value
PIM require generation ID	Rejection of Hello messages without Generation_ID (enabled/disabled)
PIM hello hold interval	IPv6 PIM neighbor timeout time
PIM hello assert interval	Assert timeout time
PIM triggered hello delay	Maximum delay of sending hello messages
PIM J/P interval	Join/prune interval
PIM J/P hold interval	Join/prune timeout time
PIM BSR domain border	BSR administrative scoping status (enabled/disabled)

Table 253 Field descriptions of the display pim ipv6 interface command

Field	Description
Number of routers on network not using DR priority	Number of routers not using the DR priority field on the subnet where the interface resides
Number of routers on network not using LAN delay	Number of routers not using the LAN delay field on the subnet where the interface resides
Number of routers on network not using neighbor tracking	Number of routers not using neighbor tracking on the subnet where the interface resides

display pim ipv6 join-prune

Syntax **display pim ipv6 join-prune mode** { **sm** [**flags** *flag-value*] | **ssm** } [**interface** *interface-type interface-number* | **neighbor** *ipv6-neighbor-address*] * [**verbose**]

View Any view

Parameters **mode**: Displays the information of join/prune messages to send in the specified IPv6 PIM mode. IPv6 PIM modes include **sm** and **ssm**, which represent IPv6 PIM-SM and IPv6 PIM-SSM respectively. Currently, Switch 8800s do not support **ssm** - this keyword does work in the command on a Switch 8800.

flags *flag-value*: Specifies to display IPv6 PIM routing entries containing the specified flag(s).Values and meanings of *flag-value* are as follows:

- **rpt**: Specifies routing entries on the RPT.
- **spt**: Specifies routing entries on the SPT.
- **wc**: Specifies wildcard routing entries.

interface-type interface-number: Displays the information of join/prune messages to send on the specified interface. Currently, only VLAN interfaces are supported for the Switch 8800s.

ipv6-neighbor-address: Displays the information of join/prune messages to send to the specified IPv6 PIM neighbor.

verbose: Displays the detailed information of join/prune messages to send.

Description Use the **display pim join-prune** command to view the information about the join/prune messages to send.

Examples # View the information of join/prune messages to send in the IPv6 PIM-SM mode.

```
<Sysname> display pim ipv6 join-prune mode sm
Vpn-instance: public net

 Expiry Time: 22 sec
 Upstream nbr: FE80::20F:E2FF:FE1D:A6A3 (Vlan-interface12)
 0 (*, G) join(s), 1 (S, G) join(s), 0 (S, G, rpt) prune(s)
 Expiry Time: 50 sec
 Upstream nbr: FE80::2E0:FCFF:FE03:1004 (Vlan-interface22)
 1 (*, G) join(s), 0 (S, G) join(s), 1 (S, G, rpt) prune(s)
```

```
------------------------------------------------------------------
Total (*, G) join(s): 1, (S, G) join(s): 1, (S, G, rpt) prune(s): 1
```

Table 254 Field descriptions of the display pim join-prune command

Field	Description
Vpn-instance	VPN instance name
Expiry Time	Waiting time before ending join/prune messages
Upstream nbr:	IPv6 address of the upstream IPv6 PIM neighbor and the interface connecting to it
(*, G) join(s)	Number of (*, G) joins to send
(S, G) join(s)	Number of (S, G) joins to send
(S, G, rpt) prune(s)	Number of (S, G, rpt) prunes

display pim ipv6 neighbor

Syntax **display pim ipv6 neighbor** [**interface** *interface-type interface-number* | *ipv6-neighbor-address* | **verbose**] *

View Any view

Parameters *interface-type interface-number*: Displays the IPv6 PIM neighbor information on a particular interface. Currently, only VLAN interfaces are supported for the Switch 8800s.

ipv6-neighbor-address: Displays the information of a particular IPv6 PIM neighbor.

verbose: Displays the detailed IPv6 PIM neighbor information.

Description Use the **display pim ipv6 neighbor** command to view the IPv6 PIM neighbor information.

Examples # View the information of all IPv6 PIM neighbors.

```
<Sysname> display pim neighbor
 Vpn-instance: public net
Total Number of Neighbors = 2
 Neighbor           Interface    Uptime        Expires       Dr-Priority
 FE80::A01:101:1    Vlan12       02:50:49      00:01:31      1
 FE80::A01:102:1    Vlan22       02:49:39      00:01:42      1
```

Table 255 Field descriptions of the display pim ipv6 neighbor command

Field	Description
Vpn-instance	VPN instance name
Total Number of Neighbors	Total number of IPv6 PIM neighbors
Neighbor	IPv6 address of the PIM neighbor
Interface	Interface connecting the IPv6 PIM neighbor
Uptime	Length of time since the IPv6 PIM neighbor was up
Expires	Remaining time before the IPv6 PIM neighbor expires
Dr-Priority	Designated router priority

display pim ipv6 routing-table

Syntax **display pim ipv6 routing-table** [*ipv6-group-address* [*prefix-length*] | *ipv6-source-address* [*prefix-length*] | **incoming-interface** [*interface-type interface-number* | **register**] | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** } | **mode** *mode-type* | **flags** *flag-value* | **fsm**] *

View Any view

Parameters *ipv6-group-address*: Specifies an IPv6 multicast group.

ipv6-source-address: Specifies an IPv6 multicast source by its IPv6 global unicast address.

prefix-length: Prefix length of the IPv6 multicast group/source address. For an IPv6 multicast group address, the effective range is 8 to 128; for an IPv6 multicast source address, the effective range is 0 to 128. The default value is 128 in both cases.

incoming-interface: Displays routing entries that contain the specified interface as the incoming interface.

interface-type interface-number: Specifies an interface by its type and number. Currently, only VLAN interfaces are supported for the Switch 8800s.

register: Specifies the register interface. This keyword is valid only if *mode-type* is not specified or is **sm**.

outgoing-interface: Displays routing entries that contain the specified interface as the outgoing interface.

include: Displays routing entries of which the OIL includes the specified interface. This keyword must be followed by the interface type and number.

exclude: Displays routing entries of which the OIL excludes the specified interface. This keyword must be followed by the interface type and number.

match: Displays routing entries of which the OIL includes only the specified interface. If no interface type and number is specified, this command displays those routing entries with an empty OIL.

mode *mode-type*: Specifies an IPv6 PIM mode, where *mode-type* can have the following values:

- **dm**: Specifies IPv6 PIM-DM.
- **sm**: Specifies IPv6 PIM-SM.
- **ssm**: Specifies IPv6 PIM-SSM. Currently, the Switch 8800s do not support this value - if **ssm** is specified, the *mode-type* argument does dot take effect.

flags *flag-value*: Displays IPv6 PIM routing entries containing the specified flag(s). The values of *flag-value* and their meanings are as follows:

- **act**: Specifies IPv6 multicast routing entries to which actual data has arrived.
- **del**: Specifies IPv6 multicast routing entries scheduled to be deleted.
- **ext**: Specifies IPv6 routing entries containing outgoing interfaces contributed by other IPv6 multicast routing protocols.
- **loc**: Specifies IPv6 multicast routing entries on routers directly connecting to the same segment with the IPv6 multicast source.
- **niif**: Specifies IPv6 multicast routing entries containing unknown incoming interfaces.
- **nonbr**: Specifies routing entries with IPv6 PIM neighbor searching failure.
- **rpt**: Specifies routing entries on RPT branches where (S, G) prunes have been sent to the RP.
- **spt**: Specifies routing entries on the SPT.
- **swt**: Specifies routing entries in the process of RPT-to-SPT switchover.
- **wc**: Specifies wildcard routing entries.

fsm: Displays the detailed information of the finite state machine (FSM).

Description Use the **display pim ipv6 routing-table** command to view IPv6 PIM routing table information.

Related commands: **display ipv6 multicast routing-table** in *IPv6 Multicast Routing and Forwarding Commands* in the *IP Multicast Volume*.

Examples # View the content of the IPv6 PIM routing table.

```
<Sysname> display pim ipv6 routing-table
Vpn-instance: public net

 Total 0 (*, G) entry; 1 (S, G) entry

(2001::2, FF35::101:101)
     Protocol: pim-dm, Flag:
     UpTime: 00:04:24
     Upstream interface: Vlan-interface12
         Upstream neighbor: FE80::A01:100:1
         RPF prime neighbor: FE80::A01:100:1
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: Vlan-interface122
             Protocol: pim-dm, UpTime: 00:04:24, Expires: 00:02:47
```

Table 256 Field descriptions of the display pim ipv6 routing-table command

Field	Description
Vpn-instance	VPN instance name
Total 0 (*, G) entry; 1 (S, G) entry	Number of (S, G) and (*, G) entries in the IPv6 PIM routing table
(2001::2, FF35::101:101)	An (S, G) entry in the IPv6 PIM routing table
Protocol	IPv6 PIM mode, IPv6 PIM-SM or IPv6 PIM-DM

Table 256 Field descriptions of the display pim ipv6 routing-table command

Field	Description
Flag	Flag of an (S, G) or (*, G) entry in the IPv6 PIM routing table ■ SPT: indicates the (S, G) routing entry is on the SPT. ■ RPT: indicates the (S, G) or (*, G) routing entry is on the RPT. ■ WC: indicates a (*, G) entry. ■ LOC: indicates this router directly connects to the IPv6 multicast source.
Uptime	Length of time since the (S, G) or (*, G) entry was installed in the routing table
Upstream interface	Upstream (incoming) interface of the (S, G) or (*, G) entry
Upstream neighbor	Upstream neighbor of the (S, G) or (*, G) entry
RPF prime neighbor	RPF neighbor of the (S, G) or (*, G) entry ■ For a (*, G) entry, if this router is the RP, the RPF neighbor of this (*, G) entry is NULL. ■ For a (S, G) entry, if this router directly connects to the IPv6 multicast source, the RPF neighbor of this (S, G) entry is NULL.
Downstream interface(s) information	Information of the downstream interface(s), including: ■ Number of downstream interfaces ■ Downstream interface name ■ IPv6 PIM mode configured on this downstream interface ■ Length of time since this downstream interface was up ■ Remaining aging time of this downstream interface

display pim ipv6 rp-info

Syntax **display pim ipv6 rp-info** [*ipv6-group-address*]

View Any view

Parameters *ipv6-group-address*: Specifies an IPv6 multicast group. If you do not provide a group address, this command will display the RP information corresponding to all IPv6 multicast groups.

Description Use the **display pim ipv6 rp-info** command to view the RP information.

Note that:

- The RP information includes the information of RPs dynamically found by the BSR mechanism and static RPs.

- Because a non-BSR router refreshes its local RP-Set only based on the received BSR bootstrap messages, the system does not delete an RP even if its expiry time is 0. Instead, the system waits for the next bootstrap message from the BSR: if the bootstrap message does not contain information of the RP, the system will delete it.

Examples # View the RP information corresponding to the IPv6 multicast group FF0E::101:101.

```
<Sysname> display pim ipv6 rp-info ff0e::101:101
Vpn-instance: public net
 PIM-SM BSR RP information:
 prefix/prefix length: FF0E::101:101/64
     RP: 2004::2
     Priority: 0
     HoldTime: 130
     Uptime: 00:05:19
     Expires: 00:02:11
```

Table 257 Field descriptions of the display pim ipv6 rp-info command

Field	Description
Vpn-instance	VPN instance name
prefix/prefix length	The IPv6 multicast group served by the RP
RP	IPv6 global unicast address of the RP
Priority	RP priority
HoldTime	Timeout time of the RP
Uptime	Length of time since the RP was up
Expires	Remaining time of the RP

embedded-rp

Syntax **embedded-rp** [*acl6-number*]

undo embedded-rp

View IPv6 PIM view

Parameters *acl6-number*: Basic IPv6 ACL number.

Description Use the **embedded-rp** command to enable embedded RP.

Use the **undo embedded-rp** command to disable embedded RP.

By default, embedded RP is enabled.

Examples # Enable embedded RP for the IPv6 multicast group FF7E:140:22::101:101/64.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule permit source ff7e:140:22::101:101 64
[Sysname-acl6-basic-2000] quit
```

```
[Sysname] pim ipv6
[Sysname-pim6] embedded-rp 2000
```

hello-option dr-priority (IPv6 PIM view)

Syntax **hello-option dr-priority** *priority*

undo hello-option dr-priority

View IPv6 PIM view

Parameters *priority*: Priority for DR election. A larger value means a higher priority.

Description Use the **hello-option dr-priority** command to configure the global value of the priority for DR election.

Use the **undo hello-option dr-priority** command to restore the system default.

By default, the priority for DR election is 1.

Related commands: **pim ipv6 hello-option dr-priority**.

Examples # Set the priority for DR election to 3.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] hello-option dr-priority 3
```

hello-option holdtime (IPv6 PIM view)

Syntax **hello-option holdtime** *interval*

undo hello-option holdtime

View IPv6 PIM view

Parameters *interval*: IPv6 PIM neighbor timeout time in seconds.

Description Use the **hello-option holdtime** command to configure the IPv6 PIM neighbor timeout time.

Use the **undo hello-option holdtime** command to restore the system default.

By default, the IPv6 PIM neighbor timeout time is 105 seconds.

Related commands: **pim ipv6 hello-option holdtime**.

Examples # Set the IPv6 PIM neighbor timeout time to 120 seconds globally.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] hello-option holdtime 120
```

hello-option lan-delay (IPv6 PIM view)

Syntax **hello-option lan-delay** *interval*

undo hello-option lan-delay

View IPv6 PIM view

Parameters *interval*: LAN-delay time in milliseconds.

Description Use the **hello-option lan-delay** command to configure the global value of the LAN-delay time, namely the length of time the device waits between receiving a prune message from downstream and taking the prune action. If the device receives a prune override message from that downstream device within this length of time, the prune action will be overridden.

Use the **undo hello-option lan-delay** command to restore the system default.

By default, the LAN-delay time is 500 milliseconds.

Related commands: **pim ipv6 hello-option lan-delay**, **hello-option override-interval** and **pim ipv6 hello-option override-interval**.

CAUTION:

- *If the prune delay as the result of negotiation among all the devices on the same link is different from the default value, the larger value will be used.*
- *LAN-delay causes the upstream device to delay processing received messages or sending messages. If the LAN-delay setting is too small, it may cause the upstream device to stop forwarding IPv6 multicast packets before a downstream device sends a prune override message. Therefore, be cautious when configuring this option.*
- *LAN-delay is the length of time the current device waits for a prune override message from the downstream device before taking the prune action. The downstream devices that receive this hello message will modify their corresponding parameters.*

Examples # Set the prune delay to 200 milliseconds globally.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] hello-option lan-delay 200
```

hello-option neighbor-tracking (IPv6 PIM view)

Syntax **hello-option neighbor-tracking**

undo hello-option neighbor-tracking

View IPv6 PIM view

Parameters None

Description Use the **hello-option neighbor-tracking** command to globally disable join suppression, namely enable neighbor tracking.

Use the **undo hello-option neighbor-tracking** command to enable join suppression.

By default, join suppression is enabled, namely neighbor tracking is disabled.

Related commands: **pim ipv6 hello-option neighbor-tracking**.

Examples # Disable join suppression globally.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] hello-option neighbor-tracking
```

hello-option override-interval

Syntax **hello-option override-interval** *interval*

undo hello-option override-interval

View IPv6 PIM view

Parameters *interval*: Prune override interval in milliseconds.

Description Use the **hello-option override-interval** command to configure the global value of the prune override interval.

Use the **undo hello-option override-interval** command to restore the system default.

By default, the prune override interval is 2,500 milliseconds.

*The **hello-option override-interval** command sets the length of time a downstream device is allowed to wait before sending a prune override message. When a device receives a prune message from a downstream device, it does not prune off the downstream interface immediately; instead, it maintains the current forwarding state for a period of time defined by LAN-delay. If the downstream*

device needs to continue receiving IPv6 multicast data, it must send a prune override message within the prune override interval; otherwise, the upstream device will perform the prune action when the LAN-delay timer times out.

Related commands: **hello-option lan-delay**, **pim ipv6 hello-option lan-delay** and **pim ipv6 hello-option override-interval**.

Examples # Set the prune override interval to 2,000 milliseconds globally.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] hello-option override-interval 2000
```

holdtime assert (IPv6 PIM view)

Syntax **holdtime assert** *interval*

undo holdtime assert

View IPv6 PIM view

Parameters *interval*: Assert timeout time in seconds.

Description Use the **holdtime assert** command to configure the global value of the assert timeout time.

Use the **undo holdtime assert** command to restore the system default.

By default, the assert timeout time is 180 seconds.

Related commands: **holdtime join-prune**, **pim ipv6 holdtime join-prune** and **pim ipv6 holdtime assert**.

Examples # Set the global value of the assert timeout time to 100 seconds.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] holdtime assert 100
```

holdtime join-prune (IPv6 PIM view)

Syntax **holdtime join-prune** *interval*

undo holdtime join-prune

View IPv6 PIM view

Parameters *interval*: Join/prune timeout time in seconds.

Description Use the **holdtime join-prune** command to configure the global value of the join/prune timeout time.

Use the **undo holdtime join-prune** command to restore the system default.

By default, the join/prune timeout time is 210 seconds.

Related commands: **holdtime assert**, **pim ipv6 holdtime assert** and **pim ipv6 holdtime join-prune**.

Examples # Set the global value of the join/prune timeout time to 280 seconds.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] holdtime join-prune 280
```

jp-pkt-size (IPv6 PIM view)

Syntax **jp-pkt-size** *packet-size*

undo jp-pkt-size

View IPv6 PIM view

Parameters *packet-size*: Maximum size of join/prune messages in bytes.

Description Use the **jp-pkt-size** command to configure the maximum size of join/prune messages.

Use the **undo jp-pkt-size** command to restore the system default.

By default, the maximum size of join/prune messages is 8,100 bytes.

Related commands: **jp-queue-size**.

Examples # Set the maximum size of join/prune messages to 1,500 bytes.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] jp-pkt-size 1500
```

jp-queue-size (IPv6 PIM view)

Syntax **jp-queue-size** *queue-size*

undo jp-queue-size

View IPv6 PIM view

Parameters *queue-size*: Maximum number of (S, G) entries in a join/prune message.

Description Use the **jp-queue-size** command to configure the maximum number of (S, G) entries in a join/prune message.

Use the **undo jp-queue-size** command to restore the system default.

By default, a join/prune messages contains a maximum of 1,020 (S, G) entries.

Related commands: **jp-pkt-size**.

Examples # Configure a join/prune messages to contain a maximum of 2,000 (S, G) entries.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] jp-queue-size 2000
```

pim ipv6

Syntax **pim ipv6**

undo pim ipv6

View System view

Parameters None

Description Use the **pim ipv6** command to enter IPv6 PIM view.

Use the **undo pim ipv6** command to remove all configurations performed in IPv6 PIM view.

IPv6 multicast must be enabled on the device before this command can take effect.

Related commands: **multicast ipv6 routing-enable** in *IPv6 Multicast Routing and Forwarding Commands* in the *IP Multicast Volume*.

Examples # Enable IPv6 multicast routing and enter IPv6 PIM view.

```
<Sysname> system-view
[Sysname] multicast ipv6 routing-enable
[Sysname] pim ipv6
[Sysname-pim6]
```

pim ipv6 bsr-boundary

Syntax **pim ipv6 bsr-boundary**

undo pim ipv6 bsr-boundary

View VLAN interface view

Parameters None

Description Use the **pim ipv6 bsr-boundary** command to configure a BSR admin-scope region boundary on the current interface.

Use the **undo pim ipv6 bsr-boundary** command to remove the configured BSR admin-scope region boundary.

By default, no BSR admin-scope region boundary is configured.

Related commands: **c-bsr**.

Examples # Configure VLAN-interface 100 to be the boundary of the BSR admin-scope region.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 bsr-boundary
```

pim ipv6 dm

Syntax **pim ipv6 dm**

undo pim ipv6 dm

View VLAN interface view

Parameters None

Description Use the **pim ipv6 dm** command to enable IPv6 PIM-DM.

Use the **undo pim ipv6 dm** command to disable IPv6 PIM-DM.

CAUTION: *After IPv6 PIM-DM is enabled on a VLAN interface, MLD snooping cannot be enabled in the corresponding VLAN, and vice versa.*

By default, IPv6 PIM-DM is disabled.

Examples # Enable IPv6 PIM-DM on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 dm
```

pim ipv6 hello-option dr-priority

Syntax **pim ipv6 hello-option dr-priority** *priority*

undo pim ipv6 hello-option dr-priority

View VLAN interface view

Parameters *priority*: Priority for DR election. A larger value means a higher priority.

Description Use the **pim ipv6 hello-option dr-priority** command to configure the priority for DR election on the current interface.

Use the **undo pim ipv6 hello-option dr-priority** command to restore the system default.

By default, the priority for DR election is 1.

This command is the same as the **hello-option dr-priority** command for IPv6 PIM view, with the exception of the view in which it is carried out. Configurations performed in IPv6 PIM view are effective to all interfaces, while configurations performed in interface view are effective to the current interface only. The system gives priority to configurations made in interface view. Configurations made in IPv6 PIM view are used only if the corresponding configurations have not been carried out in interface view.

Related commands: **hello-option dr-priority**.

Examples # Set the priority for DR election to 3 on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 hello-option dr-priority 3
```

pim ipv6 hello-option holdtime

Syntax **pim ipv6 hello-option holdtime** *interval*

undo pim ipv6 hello-option holdtime

View VLAN interface view

Parameters *interval*: IPv6 PIM neighbor timeout time in seconds.

Description Use the **pim ipv6 hello-option holdtime** command to configure the PIM neighbor timeout time on the current interface.

Use the **undo pim ipv6 hello-option holdtime** command to restore the system default.

By default, the IPv6 PIM neighbor timeout time is 105 seconds.

This command is the same as the **hello-option holdtime** command for IPv6 PIM view, with the exception of the view in which it is carried out. Configurations

performed in IPv6 PIM view are effective to all interfaces, while configurations performed in interface view are effective to the current interface only. The system gives priority to configurations made in interface view. Configurations made in IPv6 PIM view are used only if the corresponding configurations have not been carried out in interface view.

Related commands: **hello-option holdtime**.

Examples # Set the IPv6 PIM neighbor timeout time to 120 seconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 hello-option holdtime 120
```

pim ipv6 hello-option lan-delay

Syntax **pim ipv6 hello-option lan-delay** *interval*

undo pim ipv6 hello-option lan-delay

View VLAN interface view

Parameters *interval*: Prune delay in milliseconds.

Description Use the **pim ipv6 hello-option lan-delay** command to configure the LAN-delay time, namely the length of time the device waits before taking a prune action, on the current interface.

Use the **undo pim ipv6 hello-option lan-delay** command to restore the system default.

By default, the LAN-delay time is 500 milliseconds.

This command is the same as the **hello-option lan-delay** command for IPv6 PIM view, with the exception of the view in which it is carried out. Configurations performed in IPv6 PIM view are effective to all interfaces, while configurations performed in interface view are effective to the current interface only. The system gives priority to configurations made in interface view. Configurations made in IPv6 PIM view are used only if the corresponding configurations have not been carried out in interface view.

Related commands: **pim ipv6 hello-option override-interval**, **hello-option override-interval**, and **hello-option lan-delay**.

Examples # Set the LAN-delay time to 200 milliseconds on VLAN-interface100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 hello-option lan-delay 200
```

pim ipv6 hello-option neighbor-tracking

Syntax **pim ipv6 hello-option neighbor-tracking**

undo pim ipv6 hello-option neighbor-tracking

View VLAN interface view

Parameters None

Description Use the **pim ipv6 hello-option neighbor-tracking** command to disable join suppression, namely enable neighbor tracking, on the current interface.

Use the **undo pim ipv6 hello-option neighbor-tracking** command to enable join suppression.

By default, join suppression is enabled, namely neighbor tracking is disabled.

This command is the same as the **hello-option neighbor-tracking** command for IPv6 PIM view, with the exception of the view in which it is carried out. Configurations performed in IPv6 PIM view are effective to all interfaces, while configurations performed in interface view are effective to the current interface only. The system gives priority to configurations made in interface view. Configurations made in IPv6 PIM view are used only if the corresponding configurations have not been carried out in interface view.

Related commands: **hello-option neighbor-tracking**.

Examples # Enable neighbor tracking on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 hello-option neighbor-tracking
```

pim ipv6 hello-option override-interval

Syntax **pim ipv6 hello-option override-interval** *interval*

undo pim ipv6 hello-option override-interval

View VLAN interface view

Parameters *interval*: Prune override interval in milliseconds.

Description Use the **pim ipv6 hello-option override-interval** command to configure the prune override interval on the current interface.

Use the **undo pim ipv6 hello-option override-interval** command to restore the system default.

By default, the prune override interval is 2,500 milliseconds.

This command is the same as the **hello-option override-interval** command for IPv6 PIM view, with the exception of the view in which it is carried out. Configurations performed in IPv6 PIM view are effective to all interfaces, while configurations performed in interface view are effective to the current interface only. The system gives priority to configurations made in interface view. Configurations made in IPv6 PIM view are used only if the corresponding configurations have not been carried out in interface view.

Related commands: **pim ipv6 hello-option lan-delay**, **hello-option lan-delay**, and **hello-option override-interval**.

Examples # Set the prune override interval to 2,000 milliseconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 hello-option override-interval 2000
```

pim ipv6 holdtime assert

Syntax **pim ipv6 holdtime assert** *interval*

undo pim ipv6 holdtime assert

View VLAN interface view

Parameters *interval*: Assert timeout time in seconds.

Description Use the **pim ipv6 holdtime assert** command to configure the assert timeout time on the current interface.

Use the **undo pim ipv6 holdtime assert** command to restore the system default.

By default, the assert timeout time is 180 seconds.

This command is the same as the **holdtime assert** command for IPv6 PIM view, with the exception of the view in which it is carried out. Configurations performed in IPv6 PIM view are effective to all interfaces, while configurations performed in interface view are effective to the current interface only. The system gives priority to configurations made in interface view. Configurations made in IPv6 PIM view are used only if the corresponding configurations have not been carried out in interface view.

Related commands: **holdtime assert**.

Examples # Set the assert timeout time to 100 seconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 holdtime assert 100
```

pim ipv6 holdtime join-prune

Syntax **pim ipv6 holdtime join-prune** *interval*

undo pim ipv6 holdtime join-prune

View VLAN interface view

Parameters *interval*: Join/prune timeout time in seconds.

Description Use the **pim ipv6 holdtime join-prune** command to configure the join/prune timeout time on the interface.

Use the **undo pim ipv6 holdtime join-prune** command to restore the system default.

By default, the join/prune timeout time is 210 seconds.

This command is the same as the **holdtime join-prune** command for IPv6 PIM view, with the exception of the view in which it is carried out. Configurations performed in IPv6 PIM view are effective to all interfaces, while configurations performed in interface view are effective to the current interface only. The system gives priority to configurations made in interface view. Configurations made in IPv6 PIM view are used only if the corresponding configurations have not been carried out in interface view.

Related commands: **holdtime join-prune**.

Examples # Set the join/prune timeout time to 280 seconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 holdtime join-prune 280
```

pim ipv6 require-genid

Syntax **pim ipv6 require-genid**

undo pim ipv6 require-genid

View VLAN interface view

Parameters None

Description Use the **pim ipv6 require-genid** command enable rejection of hello messages without Generation_ID.

Use the **undo pim ipv6 require-genid** command to restore the default configuration.

By default, hello messages without Generation_ID are accepted.

Examples # Enable VLAN-interface 100 to reject hello messages without Generation_ID.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 require-genid
```

pim ipv6 sm

Syntax **pim ipv6 sm**

undo pim ipv6 sm

View VLAN interface view

Parameters None

Description Use the **pim ipv6 sm** command to enable IPv6 PIM-SM.

Use the **undo pim ipv6 sm** command to disable IPv6 PIM-SM.

By default, IPv6 PIM-SM is disabled.

CAUTION: *After IPv6 PIM-SM is enabled on a VLAN interface, MLD Snooping cannot be enabled in the corresponding VLAN, and vice versa.*

Related commands: **pim ipv6 dm**.

Examples # Enable IPv6 PIM-SM on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 sm
```

pim ipv6 state-refresh-capable

Syntax **pim ipv6 state-refresh-capable**

undo pim ipv6 state-refresh-capable

View VLAN interface view

Parameters None

Description Use the **pim ipv6 state-refresh-capable** command to enable the state fresh feature on the interface.

Use the **undo pim ipv6 state-refresh-capable** command to disable the state fresh feature.

By default, the state refresh feature is enabled.

Related commands: **state-refresh-interval**, **state-refresh-rate-limit**, and **state-refresh-ttl**.

Examples # Disable state refresh on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] undo pim ipv6 state-refresh-capable
```

pim ipv6 timer graft-retry

Syntax **pim ipv6 timer graft-retry** *interval*

undo pim ipv6 timer graft-retry

View VLAN interface view

Parameters *interval*: IPv6 PIM-DM graft retry period in seconds.

Description Use the **pim ipv6 timer graft-retry** command to configure the graft retry period, namely the length of time the device waits between sending graft messages before a graft-ack is received.

Use the **undo pim ipv6 timer graft-retry** command to restore the system default.

By default, the graft retry period is 3 seconds.

Examples # Set the graft retry period to 80 seconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 timer graft-retry 80
```

pim ipv6 timer hello

Syntax **pim ipv6 timer hello** *interval*

undo pim ipv6 timer hello

View VLAN interface view

Parameters *interval*: Hello interval in seconds.

Description Use the **pim ipv6 timer hello** command to configure the hello interval, namely the length of time the device waits between sending hello messages, on the current interface.

Use the **undo pim ipv6 timer hello** command to restore the system default.

By default, the hello interval is 30 seconds.

This command is the same as the **timer hello** command for IPv6 PIM view, with the exception of the view in which it is carried out. Configurations performed in IPv6 PIM view are effective to all interfaces, while configurations performed in interface view are effective to the current interface only. The system gives priority to configurations made in interface view. Configurations made in IPv6 PIM view are used only if the corresponding configurations have not been carried out in interface view.

Related commands: **timer hello**.

Examples # Set the hello interval to 40 seconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 timer hello 40
```

pim ipv6 timer join-prune

Syntax **pim ipv6 timer join-prune** *interval*

undo pim ipv6 timer join-prune

View VLAN interface view

Parameters *interval*: Join/prune interval in seconds.

Description Use the **pim ipv6 timer join-prune** command to configure the prune/join interval, namely the length of time the device waits between sending prune/join messages, on the current interface.

Use the **undo pim ipv6 timer join-prune** command to restore the system default.

By default, the join/prune interval is 60 seconds.

This command is the same as the **timer join-prune** command for IPv6 PIM view, with the exception of the view in which it is carried out. Configurations performed in IPv6 PIM view are effective to all interfaces, while configurations performed in interface view are effective to the current interface only. The system gives priority to configurations made in interface view. Configurations made in IPv6 PIM view are used only if the corresponding configurations have not been carried out in interface view.

Related commands: **timer join-prune**.

Examples # Set the join/prune interval to 80 seconds on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 timer join-prune 80
```

pim ipv6 triggered-hello-delay

Syntax **pim ipv6 triggered-hello-delay** *interval*

undo pim ipv6 trigged-hello-delay

View VLAN interface view

Parameters *interval*: Maximum hello delay in seconds.

Description Use the **pim ipv6 triggered-hello-delay** command to configure the maximum hello delay, namely the maximum length of time the device waits before sending a hello message.

Use the **undo pim ipv6 triggered-hello-delay** command to restore the system default.

By default, the maximum hello delay is 5 seconds.

Examples # Set the maximum hello delay to 3 seconds on VLAN-interface100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim ipv6 trigged-hello-delay 3
```

probe-interval (IPv6 PIM view)

Syntax **probe-interval** *interval*

undo probe-interval

View IPv6 PIM view

Parameters *interval*: Probe time in seconds.

Description Use the **probe-interval** command to configure the probe time. In a probe suppression cycle, the DR sends a null register message, a certain length of time define by the problem time before the register suppression timer expires, to the RP to indicate that the IPv6 multicast source is active.

Use the **undo probe-interval** command to restore the system default.

By default, the probe time is 5 seconds.

Related commands: **register-suppression-timeout**.

Examples # Set the probe time to 6 seconds.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] probe-interval 6
```

register-whole-checksum (IPv6 PIM view)

Syntax **register-whole-checksum**

undo register-whole-checksum

View IPv6 PIM view

Parameters None

Description Use the **register-whole-checksum** command to configure the router to calculate the checksum based on the entire register message.

Use the **undo register-whole-checksum** command to restore the system default.

By default, the checksum is calculated based only on the header in the register message.

Related commands: **register-policy** and **register-suppression-timeout**.

Examples # Configure the router to calculate the checksum based on the entire register message.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] register-whole-checksum
```

register-policy (IPv6 PIM view)

Syntax **register-policy** *acl6-number*

undo register-policy

View IPv6 PIM view

Parameters *acl6-number*: Advanced IPv6 ACL number. Only those register messages that match the **permit** statement of the IPv6 ACL can be accepted by the RP.

Description Use the **register-policy** command to configure an IPv6 ACL rule to filter register messages.

Use the **undo register-policy** command to remove the configured register filtering rule.

By default, no register filtering rule is configured.

Within an IPv6 PIM-SM domain, the DR sends register messages with different source/group addresses to the RP. You can configure a filtering rule to accept or reject certain register messages so that the RP can serve specific IPv6 multicast groups.

If an (S, G) entry is denied by the ACL, or the action for this entry is not defined, the RP will send a register-stop message to the DR to stop the registration process for the multicast stream.

CAUTION: *Only register messages that match the* ***permit*** *statement of the ACL can be accepted by the RP. The RP will reject all register messages if you specify an ACL without a rule definition.*

Examples # Configure a register filtering policy on the RP so that only IPv6 multicast sources on the subnet 3:1::/64 can send register messages to the IPv6 multicast groups on the subnet FF35:13::/64.

```
<Sysname> system-view
[Sysname] acl ipv6 number 3000
[Sysname-acl6-adv-3000] rule permit ipv6 source 3:1:: 64 destination
 ff35:13:: 64
[Sysname-acl6-adv-3000] quit
[Sysname] pim ipv6
[Sysname-pim6] register-policy 3000
```

register-suppression-timeout (IPv6 PIM view)

Syntax **register-suppression-timeout** *interval*

undo register-suppression-timeout

View IPv6 PIM view

Parameters *interval*: Register suppression timeout in seconds.

Description Use the **register-suppression-timeout** command to configure the register suppression timeout time.

Use the **undo register-suppression-timeout** command to restore the system default.

By default, the register suppression timeout time is 60 seconds.

Note that:

- When a device, as a DR, receives an (S, G)-specific register-stop message from the RP, the device immediately stops sending register messages with encapsulated multicast data and enters the register suppression state.
- A smaller timeout setting causes bursts of multicast data to flow to the RP more frequently, and a larger timeout setting results in a larger delay for new receivers to join a multicast group.
- Defining a probe time setting in the **probe-interval** command reduces bursts of register messages, and a appropriately reduced setting of the suppression timeout time reduces the delay for new receivers to join a multicast group.

Related commands: **probe-interval**.

Examples # Set the register suppression timeout time to 70 seconds.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] register-suppression-timeout 70
```

reset pim ipv6 control-message counters

Syntax **reset pim ipv6 control-message counters** [**interface** *interface-type interface-number*]

View User view

Parameters **interface** *interface-type interface-number*: Specifies to reset the IPv6 PIM control message counter on a particular interface. Currently, only VLAN interfaces are supported for the Switch 8800s.

Description Use the **reset pim ipv6 control-message counters** command to reset IPv6 PIM control message counters.

Examples # Reset IPv6 PIM control message counters on all interfaces.

```
<Sysname> reset pim ipv6 control-message counters
```

source-lifetime (IPv6 PIM view)

Syntax **source-lifetime** *interval*

undo source-lifetime

View IPv6 PIM view

Parameters *interval*: IPv6 multicast source lifetime in seconds.

Description Use the **source-lifetime** command to configure the IPv6 multicast source lifetime.

Use the **undo source-lifetime** command to restore the system default.

By default, the lifetime of an IPv6 multicast source is 210 seconds.

Related commands: **state-refresh-interval**.

Examples # Set the IPv6 multicast source lifetime to 200 seconds.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] source-lifetime 200
```

source-policy (IPv6 PIM view

source-policy (IPv6 PIM view)

Syntax **source-policy** *acl6-number*

undo source-policy

View IPv6 PIM view

Parameters *acl6-number*: Basic or advanced IPv6 ACL number.

Description Use the **source-policy** command to configure an IPv6 multicast data filter.

Use the **undo source-policy** command to remove the configured IPv6 multicast data filter.

By default, no IPv6 multicast data filter is configured.

Note that:

- If you specify a basic ACL, the device filters the received IPv6 multicast packets based on the source address, and discards packets that fail the source address match.
- If you specify an advanced ACL, the device filters the received IPv6 multicast packets based on the source and group addresses, and discards packets that fail the match.
- If this command is executed repeatedly, the last configuration will take effect.

Examples # Configure the router to accept IPv6 multicast packets originated from 3121::1 and discard IPv6 multicast packets originated from 3121::2.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule permit source 3121::1 128
[Sysname-acl6-basic-2000] rule deny source 3121::2 128
[Sysname-acl6-basic-2000] quit
[Sysname] pim ipv6
[Sysname-pim6] source-policy 2000
[Sysname-pim6] quit
```

spt-switch-threshold (IPv6 PIM view)

Syntax **spt-switch-threshold infinity** [**group-policy** *acl6-number* [**order** *order-value*]]

undo spt-switch-threshold [**group-policy** *acl6-number*]

View IPv6 PIM view

Parameters **group-policy** *acl6-number*: Specifies an IPv6 group policy. RPT-to-SPT switchover will be disabled for IPv6 multicast groups that match the specified group policy. In this option, *acl6-number* refers to a basic IPv6 ACL number, in the range of 2000 to 2999. If you do not include this option in your command, the configuration will apply on all IPv6 multicast groups.

order *order-value*: Specifies the order of the IPv6 ACL in the group-policy list, where *order-value* has an effective range of 1 to (the largest order value in the existing group-policy list + 1), but the value range should not include the original order value of the IPv6 ACL in the group-policy list. If you have assigned an *order-value* to a certain IPv6 ACL, do not specify the same *order-value* for another IPv6 ACL; otherwise the system will give error information. If you do not specify an *order-value*, the order value of the IPv6 ACL will remain the same in the group-policy list.

Description Use the **spt-switch-threshold** command to disable RPT-to-SPT switchover.

Use the **undo spt-switch-threshold** command to restore the system default.

By default, the device switches to the SPT immediately after it receives the first IPv6 multicast packet from the RPT.

Note that:

- To adjust the order of an IPv6 ACL that already exists in the group-policy list, you can use the *acl6-number* argument to specify this IPv6 ACL and set its order-value. This will insert the IPv6 ACL to the position of order-value in the group-policy list. The order of the other existing IPv6 ACLs in the group-policy list will remain unchanged.
- To use an IPv6 ACL that does not exist in the group-policy list, you can use the *acl6-number* argument to specify an IPv6 ACL and set its order-value. This will insert the IPv6 ACL to the position of order-value in the group-policy list. If you do not include the **order** *order-value* option in your command, the ACL will be appended to the end of the group-policy list.
- If you use this command multiple times on the same IPv6 multicast group, the first traffic rate configuration matched in sequence will take effect.
- To avoid forwarding failure, do not include the **infinity** keyword in the **spt-switch-threshold** command on a switch that may become an RP (namely, a static RP or a C-RP).

Examples # Disable RPT-to-SPT switchover.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] spt-switch-threshold infinity
```

state-refresh-interval (IPv6 PIM view)

Syntax **state-refresh-interval** *interval*

undo state-refresh-interval

View IPv6 PIM view

Parameters *interval*: State refresh interval in seconds.

Description Use the **state-refresh-interval** command to configure the interval between state refresh messages.

Use the **undo state-refresh-interval** command to restore the system default.

By default, the state refresh interval is 60 seconds.

Related commands: **pim ipv6 state-refresh-capable**, **state-refresh-rate-limit**, and **state-refresh-ttl**.

Examples # Set the state refresh interval to 70 seconds.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] state-refresh-interval 70
```

state-refresh-rate-limit (IPv6 PIM view)

Syntax **state-refresh-rate-limit** *interval*

undo state-refresh-rate-limit

View IPv6 PIM view

Parameters *interval*: Time to wait before receiving a new refresh message, in seconds.

Description Use the **state-refresh-rate-limit** command to configure the time the router must wait before receiving a new state refresh message.

Use the **undo state-refresh-rate-limit** command to restore the system default.

By default, the device waits 30 seconds before receiving a new state refresh message.

Related commands: **pim ipv6 state-refresh-capable**, **state-refresh-interval**, and **state-refresh-ttl**.

Examples Configure the device to wait 45 seconds before receiving a new state refresh message.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] state-refresh-rate-limit 45
```

state-refresh-ttl (IPv6 PIM view)

Syntax **state-refresh-ttl** *ttl-value*

undo state-refresh-ttl

View IPv6 PIM view

Parameters *ttl-value*: TTL value of state refresh messages.

Description Use the **state-refresh-ttl** command to configure the TTL value of state refresh messages.

Use the **undo state-refresh-ttl** command to restore the system default.

By default, the TTL value of state refresh messages is 255.

Related commands: **pim ipv6 state-refresh-capable**, **state-refresh-interval**, and **state-refresh-rate-limit**.

Examples # Set the TTL value of state refresh messages to 45.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] state-refresh-ttl 45
```

static-rp (IPv6 PIM view)

Syntax **static-rp** *ipv6-rp-address* [*acl6-number*] [**preferred**]

undo static-rp *rp-address*

View IPv6 PIM view

Parameters *ipv6-rp-address*: IPv6 address of the static RP to be configured. This address must be a valid, globally scoped IPv6 unicast address.

acl6-number: Basic IPv6 ACL number. If you provide this argument, the configured static RP will serve only those IPv6 multicast groups that pass the filtering; otherwise, the configured static RP will serve the all IPv6 multicast groups.

preferred: Specifies to give priority to the static RP if the static RP conflicts with the dynamic RP. If you do not include the **preferred** keyword in your command,

the dynamic RP will be given priority, and the static RP takes effect on if no dynamic RP exists in the network or when the dynamic RP fails.

Description Use the **static-rp** command to configure a static RP.

Use the **undo static-rp** command to restore the system default.

By default, no static RP is configured.

Note that:

- IPv6 PIM-SM or IPv6 PIM-DM cannot be enabled on an interface that serves as a static RP. Use this command to designate the same RP address on all the devices in the IPv6 PIM domain.
- When the IPv6 ACL rule applied on a static RP changes, a new RP must be elected for all IPv6 multicast groups.
- You can configure multiple static RPs by carrying out this command repeatedly. However, if you carry out this command multiple times and specify the same static RP address or reference the same IPv6 ACL rule, the last configuration will override the previous one. If multiple static RPs have been configured for the same IPv6 multicast group, the one with the highest IPv6 address will be chosen to serve the group.
- You can configure up to 50 static RPs on the same device.

Related commands: **display pim ipv6 rp-info**.

Examples # Configure the interface with an IPv6 address of 2001::2 as a static RP.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] static-rp 2001::2
```

timer hello (IPv6 PIM view)

Syntax **timer hello** *interval*

undo timer hello

View IPv6 PIM view

Parameters *interval*: Hello interval in seconds.

Description Use the **timer hello** command to configure the hello interval globally.

Use the **undo timer hello** command to restore the system default.

By default, hello messages are sent at the interval of 30 seconds.

This command is the same as the **pim ipv6 timer hello** command for IPv6 PIM view, with the exception of the view in which it is carried out. Configurations

performed in IPv6 PIM view are effective to all interfaces, while configurations performed in interface view are effective to the current interface only. The system gives priority to configurations made in interface view. Configurations made in IPv6 PIM view are used only if the corresponding configurations have not been carried out in interface view.

Related commands: **pim ipv6 timer hello**.

Examples # Set the global hello interval to 40 seconds.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] timer hello 40
```

timer join-prune (IPv6 PIM view)

Syntax **timer join-prune** *interval*

undo timer join-prune

View IPv6 PIM view

Parameters *interval*: Join/prune interval in seconds.

Description Use the **timer join-prune** command to configure the join/prune interval globally.

Use the **undo timer join-prune** command to restore the system default.

By default, the join/prune interval is 60 seconds.

Related commands: **pim ipv6 timer join-prune**.

Examples # Set the global join/prune interval to 80 seconds.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] timer join-prune 80
```

51 UDP HELPER CONFIGURATION COMMANDS

debugging udp-helper

Syntax **debugging udp-helper** { **event** | **packet** [**receive** | **send**] }

undo debugging udp-helper { **event** | **packet** [**receive** | **send**] }

View User view

Parameter **event**: Enables event debugging for UDP Helper.

packet: Enables packet debugging for UDP Helper.

receive: Enables incoming packet debugging for UDP Helper.

send: Enables outgoing packet debugging for UDP Helper.

Description Use the **debugging udp-helper** command to enable UDP Helper debugging.

Use the **undo debugging udp-helper** command to disable UDP Helper debugging.

By default, UDP Helper debugging is disabled.

Table 258 Description on major fields of the debugging udp-helper event command

Field	Description
TTL Exceed!	The TTL timer expires.
Dest Ip(Num) is not routable or the packet is from the device itself.	The packet will not be processed because no outbound interface is found or the packet is sent out of the local device itself.
Pointer of the route table outer interface is NULL!	The pointer of the outbound interface of the found routing entry is null.
Making MBUF continuous failed	Fails to arrange MBUF space.
Fail to input the message to the queue, maybe it's already full. The return code is : *number*	Writing the message failed, possibly because the queue is full. The error code *number* is returned.
Receive invalid DHCP packet	An invalid DHCP packet is received.
Receive a dhcp REQUEST packet	A DHCP request packet is received.
Receive a dhcp RESPONSE packet	A DHCP response packet is received.
UNIT *number* is not in Fabric Discard the dhcp RESPONSE packet	The unit with the Unit ID *number* is not in the Fabric, and the DHCP response packet is discarded.

Table 258 Description on major fields of the debugging udp-helper event command

Field	Description
Cannot find the saved xid of the dhcp RESPONSE packet	The saved xid value cannot be found, and the DHCP response packet is discarded.
Discard the dhcp RESPONSE packet	
Convert xid to saved xid	Convert xid and save it.
Send the packet to udp module in DHCP case.	Send DHCP UDP packets to the UDP module.
Self UNIT is MASTER UNIT	The local unit is the Master Unit, which sends DHCP response packets to the UDP module.
Send dhcp RESPONSE packet to udp module	
Self UNIT is SLAVE UNIT	The local unit is the Slave Unit, which sends DHCP response packets to the Master Unit with the ID *number* for processing.
Send dhcp RESPONSE packet to MASTER UNIT : *number*	

Table 259 Description on major fields of the debugging udp-helper packet command

Field	Description
Dest Ip	Destination IP address.
Source Ip	Source IP address.
Dest Port	Destination port number.
New Dest Ip	New destination IP address of the packet after being forwarded through UDP Helper.
Intercept a UDP packet.	A UDP packet is intercepted.
Copy the packet and send it to the UDP module.	Copy a packet and send the original packet to the UDP module.
New Dest Ip *ip-address*	Forward a packet to the destination server with the new destination IP address *ip-address*.
Forward the packet to destination server	
Send the packet to udp module without relay.	Send a packet to the UDP module directly without relaying.

Example # Configure port 520 to forward packets to the server at 2.2.2.2 and enable packet debugging for UDP Helper.

```
<Sysname> system-view
[Sysname] udp-helper enable
[Sysname] udp-helper port 520
[Sysname] interface Vlan-interface 20
[Sysname-Vlan-interface20] udp-helper server 2.2.2.2
[Sysname-Vlan-interface20] return
<Sysname> debugging udp-helper packet
*Aug 11 08:20:46:00 2005 Sysname UDPH/7/UDPHelper_Pkt:
Dest Ip(1.1.1.255)    Source Ip(1.1.1.5)    Dest Port(520)
 Prompt: Intercept a UDP packet.
```

// A UDP packet is received, in which the source IP address is 1.1.1.5, the destination IP address is 1.1.1.255, and the destination port number is 520.

```
*Aug 11 08:20:46:01 2005 Sysname UDPH/7/UDPHelper_Pkt:
Dest Ip(1.1.1.255)    Source Ip(1.1.1.5)    Dest Port(520)
 Prompt: Copy the packet and send it to the UDP module.
```

// Copy the packet and send it to the UDP module. In the original packet, the source IP address is 1.1.1.5, the destination IP address is 1.1.1.255, and the destination port number is 520.

```
*Aug 11 08:20:46:02 2005 Sysname UDPH/7/UDPHelper_Pkt:
Dest Ip(1.1.1.255)    Source Ip(1.1.1.5)    Dest Port(520)
New Dest Ip(2.2.2.2)
 Prompt: Forward the packet to destination server
```

// Forward the packet to the destination server at 2.2.2.2. In the packet, the source IP address is 1.1.1.5, the destination IP address is 1.1.1.255, and the destination port number is 520.

display udp-helper server

Syntax **display udp-helper server** [**interface** *interface-type interface-number*]

View Any view

Parameter **interface** *interface-type interface-number*: Specifies an interface by interface type and interface number.

Description Use the **display udp-helper server** command to display the information of forwarded UDP packets on the specified interface or all interfaces.

If *interface-type interface-number* is not specified, this command displays the information of forwarded UDP packets on all interfaces.

Example # Display the information of forwarded UDP packets on the interface VLAN-interface 1.

```
<Sysname> display udp-helper server interface vlan-interface 1
Interface name      Server address      Packets sent
Vlan-interface1     192.1.1.2           0
```

The information above shows that the IP address of the destination server corresponding to the interface VLAN-interface 1 is 192.1.1.2, and that no packets are forwarded to the destination server.

reset udp-helper packet

Syntax **reset udp-helper packet**

View User view

Parameter None

Description Use the **reset udp-helper packet** command to clear the statistics of UDP packets forwarded.

Related command: **display udp-helper serve**.

Example # Clear the statistics of the forwarded UDP packets.

```
<Sysname> reset udp-helper packet
```

udp-helper enable

Syntax **udp-helper enable**

undo udp-helper enable

View System view

Parameter None

Description Use the **udp-helper enable** command to enable UDP Helper.

Use the **undo udp-helper enable** command to disable UDP Helper.

By default, UDP Helper is disabled.

Example # Enable UDP Helper

```
<Sysname> system-view
[Sysname] udp-helper enable
```

udp-helper port

Syntax **udp-helper port** { *port-number* | **dns** | **netbios-ds** | **netbios-ns** | **tacacs** | **tftp** | **time** }

undo udp-helper port { *port-number* | **dns** | **netbios-ds** | **netbios-ns** | **tacacs** | **tftp** | **time** }

View System view

Parameter *port-number*: UDP port number with which packets need to be forwarded, in the range of 1 to 65535 (except 67 and 68).

dns: Forwards DNS data packets. The corresponding UDP port number is 53.

netbios-ds: Forwards NetBIOS data packets. The corresponding UDP port number is 138.

netbios-ns: Forwards NetBIOS name service data packets. The corresponding UDP port number is 137.

tacacs: Forwards terminal access controller access control system (TACACS) data packet. The corresponding UDP port number is 49.

tftp: Forwards TFTP data packets. The corresponding UDP port number is 69.

time: Forwards time service data packets. The corresponding UDP port number is 37.

Description Use the **udp-helper port** command to enable the forwarding of packets with the specified UDP port number.

Use the **undo udp-helper port** command to remove the configured UDP port numbers.

By default, the UDP Helper enabled device forwards broadcast packets with the default six UDP destination port numbers 69, 53, 37, 137, 138 and 49. The configured UDP port numbers (including the default UDP port numbers) will all be removed if UDP Helper is disabled.

Example # Forward broadcast packets with the UDP destination port number 100.

```
<Sysname> system-view
[Sysname] udp-helper port 100
```

udp-helper server

Syntax **udp-helper server** *ip-address*

undo udp-helper server [*ip-address*]

View VLAN interface view

Parameter *ip-address*: IP address of the destination server.

Description Use the **udp-helper server** command to specify the destination server which UDP packets need to be forwarded to.

Use the **undo udp-helper server** command to remove the destination server.

No destination server is configured by default.

By default, you can configure up to 20 destination servers on an interface.

Note that you will remove all the destination servers on an interface if you carry out the **undo udp-helper server** command without the *ip-address* argument.

Related command: **display udp-helper server**.

Example # Specify the IP address of the UDP destination server as 192.1.1.2 on the interface VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] udp-helper server 192.1.1.2
```

52 DHCP SERVER CONFIGURATION COMMANDS

bims-server

Syntax **bims-server ip** *ip-address* [**port** *port-number*] **sharekey** *key*

undo bims-server

View DHCP address pool view

Parameters **ip** *ip-address*: Specifies an IP address for the BIMS server.

port *port-number*: Specifies a port number for the BIMS server.

sharekey *key*: Specifies a shared key for the BIMS server, which is a string of 1 to 16 characters.

Description Use the **bims-server** command to specify the IP address, port number, and shared key of the BIMS server in the DHCP address pool for the client.

Use the **undo bims-server** command to remove BIMS server information assigned from the DHCP address pool to the DHCP client.

By default, no BIMS server information is specified.

If you execute the **bims-server** command repeatedly, the latest configuration will overwrite the previous one.

Related commands: **dhcp server ip-pool**.

Examples # Specify the IP address 1.1.1.1, port number 80, shared key aabbcc of the BIMS server in DHCP address pool 0 for the client.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] bims-server ip 1.1.1.1 port 80 sharekey aabbcc
```

bootfile-name

Syntax **bootfile-name** *bootfile-name*

undo bootfile-name

View DHCP address pool view

Parameters *bootfile-name*: Boot file name, a string of 1 to 63 characters.

Description Use the **bootfile-name** command to specify a bootfile name in the DHCP address pool for the client.

Use the **undo bootfile-name** command to remove the specified bootfile name assigned from the DHCP address pool to the DHCP client.

By default, no bootfile name is specified.

If you execute the **bootfile-name** command repeatedly, the latest configuration will overwrite the previous one.

Examples # Specify the bootfile name aaa in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] bootfile-name aaa
```

debugging dhcp server

Syntax **debugging dhcp server** { **all** | **error** | **event** | **packet** }

undo debugging dhcp server { **all** | **error** | **event** | **packet** }

View User view

Parameters **all**: Enables/disables all debugging options on the DHCP server.

error: Enables/disables error debugging on the DHCP server. Errors include those occurring when the DHCP server processes DHCP packets or allocates addresses.

event: Enables/disables event debugging on the DHCP server. Events include address allocation and ping detection timeout.

packet: Enables/disables DHCP packet debugging. Packets include the packets that the DHCP server has received and sent, and the ping packets sent for the purpose of detection and the received response packets.

Description Use the **debugging dhcp server** command to enable debugging on the DHCP server.

Use the **undo debugging dhcp server** command to disable debugging on the DHCP server.

By default, debugging is disabled on the DHCP server.

Table 260 Description on fields of the debugging dhcp server packet command

Field	Description
Rx/Tx	Receive or transmit
Interface *InterfaceName*	Receiving interface
Message type: *MessageType*	Content of the first byte of the DHCP message. That is, the operation type of a DHCP message, namely request or reply.
Hardware Type: *HardwareType*	Hardware type of the DHCP client
Hardware Address Length: *HardwareAddressLength*	Length of the DHCP client's hardware address
Hops: *Hops*	Number of relay agents a DHCP message passed
Transaction ID: *TransactionID*	A random number, uniquely identifying an address allocation requested by the DHCP client
Seconds: *Seconds*	Number of seconds that has elapsed since the DHCP client began address acquisition
Broadcast Flag: *BroadcastFlag*	DHCP broadcast flag ■ 1: Broadcast ■ 0: Unicast.
Client IP Address: *ClientIPAddress*	IP address of the DHCP client
Your IP Address: *YourIPAddress*	IP address that the DHCP server assigns to the client
Server IP Address: *ServerIPAddress*	IP address of the DHCP server
Gateway IP Address: *GatewayIPAddress*	IP address of the DHCP relay agent
Client Hardware Address: *ClientHardwareAddress*	Hardware address of the DHCP client
Server Host Name: *ServerHostName*	Host name of the DHCP server.
Boot File Name: *BootFileName*	Boot file name of the DHCP server
DHCP message type: *DHCPmessagetype*	DHCP message type, including ■ DHCP Discover ■ DHCP Offer ■ DHCP Request ■ DHCP Decline ■ DHCP ACK ■ DHCP NAK ■ DHCP Release ■ DHCP Inform

Table 261 Description on fields of the debugging dhcp server event command

Field	Description
DHCPServer:	Identifies DHCP server event
operation	DHCP server operation

Examples # Enable all the debugging options on the DHCP server.

```
<Sysname> debugging dhcp server all
<Sysname> terminal debugging
```

// All the debugging options on the DHCP server are enabled.

```
<Sysname>
*0.263828 server DHCPS/8/DHCPS_DEBUG_COMMON:
 Checking for expired lease
```

// The DHCP server periodically checks whether there is any expired lease.

```
*0.278312 server DHCPS/8/DHCPS_DEBUG_COMMON:
DHCPServer: Receive DHCPDISCOVER from 00e0.fc14.1601-Vlan-interface2
 through 22.0.0.1
*0.278312 server DHCPS/8/DHCPS_DEBUG_PACKET:
Rx, interface Vlan-interface1
    Message type: request
    Hardware Type: 1, Hardware Address Length: 6
    Hops: 1, Transaction ID: 4281385283
    Seconds: 0, Broadcast Flag: 0
    Client IP Address: 0.0.0.0    Your IP Address: 0.0.0.0
    Server IP Address: 0.0.0.0    Gateway IP Address: 22.0.0.1
    Client Hardware Address: 00e0-fc14-1601
    Server Host Name: Not Configured, Boot File Name: Not Configured
    DHCP message type: DHCP Discover
```

// The DHCP server receives a DHCP-DISCOVER message.

```
*0.278312 server DHCPS/8/DHCPS_DEBUG_COMMON:
DHCPServer: Sending ICMP ECHO to target IP: 22.0.0.1
*0.278312 server DHCPS/8/DHCPS_DEBUG_COMMON:
DHCPServer: Assign Free Lease from global pool.
```

// The DHCP server assigns a temporary lease with the IP address 22.0.0.1 from the global address pool to the client. Before assigning, the DHCP server checks whether the IP address is currently in use by sending ICMP messages.

```
*0.278406 server DHCPS/8/DHCPS_DEBUG_COMMON:
DHCPServer: ICMP ECHOREPLY received from Client IP 22.0.0.1
*0.278406 server DHCPS/8/DHCPS_DEBUG_COMMON:
DHCPServer: Create timeout timer for ICMP
```

// The DHCP server receives a response from a client with the IP address 22.0.0.1, which implies this IP address is in use.

```
*0.278406 server DHCPS/8/DHCPS_DEBUG_COMMON:
DHCPServer: Sending ICMP ECHO to target IP: 22.0.0.2
```

// The DHCP server assigns another IP address 22.0.0.2 and probes by sending ICMP messages.

```
*0.278406 server DHCPS/8/DHCPS_DEBUG_COMMON:
DHCPServer: Assign Free Lease from global pool.
*0.279016 server DHCPS/8/DHCPS_DEBUG_COMMON:
DHCPServer: ICMP Timeout!
*0.279016 server DHCPS/8/DHCPS_DEBUG_COMMON:
```

```
DHCPServer: ICMP detecting finished. The target IP can be used for d
hcp allocation.
```

// No response is received from 22.0.0.2 after the timer expires, which indicates this IP address is assignable.

```
*0.279016 server DHCPS/8/DHCPS_DEBUG_PACKET:
Tx, interface Vlan-interface1
    Message type: reply
    Hardware Type: 1, Hardware Address Length: 6
    Hops: 0, Transaction ID: 4281385283
    Seconds: 0, Broadcast Flag: 0
    Client IP Address: 0.0.0.0    Your IP Address: 22.0.0.2
    Server IP Address: 0.0.0.0    Gateway IP Address: 22.0.0.1
    Client Hardware Address: 00e0-fc14-1601
    Server Host Name: Not Configured, Boot File Name: Not Configured
    DHCP message type: DHCP Offer
```

// The DHCP server sends a DHCP-OFFER message and assigns the IP address 22.0.0.2 to the DHCP client.

```
*0.279016 server DHCPS/8/DHCPS_DEBUG_COMMON:
DhcpServer: Send DHCPOFFER to 00e0.fc14.1601-Vlan-interface2 Offer I
P=> 22.0.0.2 through 22.0.0.1
*0.279172 server DHCPS/8/DHCPS_DEBUG_COMMON:
DHCPServer: Receive DHCPREQUEST from 00e0.fc14.1601-Vlan-interface2
through 22.0.0.1
*0.279172 server DHCPS/8/DHCPS_DEBUG_PACKET:
Rx, interface Vlan-interface1
    Message type: request
    Hardware Type: 1, Hardware Address Length: 6
    Hops: 1, Transaction ID: 2294688324
    Seconds: 0, Broadcast Flag: 0
    Client IP Address: 0.0.0.0    Your IP Address: 0.0.0.0
    Server IP Address: 0.0.0.0    Gateway IP Address: 22.0.0.1
    Client Hardware Address: 00e0-fc14-1601
    Server Host Name: Not Configured, Boot File Name: Not Configured
    DHCP message type: DHCP Request
```

// The DHCP server receives a DHCP-REQUEST message.

```
*0.279172 server DHCPS/8/DHCPS_DEBUG_COMMON:
DHCPServer: Acknowledge the DHCPREQUEST message!
*0.279172 server DHCPS/8/DHCPS_DEBUG_PACKET:
Tx, interface Vlan-interface1
    Message type: reply
    Hardware Type: 1, Hardware Address Length: 6
    Hops: 0, Transaction ID: 2294688324
    Seconds: 0, Broadcast Flag: 0
    Client IP Address: 0.0.0.0    Your IP Address: 22.0.0.2
    Server IP Address: 0.0.0.0    Gateway IP Address: 22.0.0.1
    Client Hardware Address: 00e0-fc14-1601
    Server Host Name: Not Configured, Boot File Name: Not Configured
    DHCP message type: DHCP Ack

*0.279172 server DHCPS/8/DHCPS_DEBUG_COMMON:
```

```
DhcpServer: Send DHCPACK to 00e0.fc14.1601-Vlan-interface2 Offer IP=
> 22.0.0.2 through 22.0.0.1
```

// The DHCP server sends a DHCP-ACK message.

dhcp enable

Syntax **dhcp enable**

undo dhcp enable

View System view

Parameters None

Description Use the **dhcp enable** command to enable DHCP.

Use the **undo dhcp enable** command to disable DHCP.

By default, DHCP is disabled.

You need to enable DHCP before performing DHCP server and relay agent configurations.

Examples # Enable DHCP.

```
<Sysname> system-view
[Sysname] dhcp enable
```

dhcp select server global-pool

Syntax **dhcp select server global-pool** [**subaddress**]

undo dhcp select server global-pool subaddress

View VLAN interface view

Parameters **subaddress**: Supports subaddress allocation. That is, the DHCP server and clients are on the same network segment, and the server allocates IP addresses from the address pool containing the network segment of the first subaddress if several subaddresses exist.

Description Use the **dhcp select server global-pool** command to enable specified interface(s) to operate in DHCP address pool mode. After the interface receives a DHCP request, the DHCP server will allocate an IP address from the address pool.

Use the **undo dhcp select server global-pool subaddress** command to cancel the support for subaddress allocation.

By default, the DHCP server is enabled on an interface.

Examples # Enable the DHCP server on VLAN interface 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp select server global-pool
```

dhcp server detect

Syntax **dhcp server detect**

undo dhcp server detect

View System view

Parameters None

Description Use the **dhcp server detect** command to enable unauthorized DHCP server detection.

Use the **undo dhcp server detect** command to disable the function.

By default, the function is disabled.

Examples # Enable unauthorized DHCP server detection.

```
<Sysname> system-view
[Sysname] dhcp server detect
```

dhcp server forbidden-ip

Syntax **dhcp server forbidden-ip** *low-ip-address* [*high-ip-address*]

undo dhcp server forbidden-ip *low-ip-address* [*high-ip-address*]

View System view

Parameters *low-ip-address*: Start IP address of the IP address range to be excluded from dynamic allocation.

high-ip-address: End IP address of the IP address range to be excluded from dynamic allocation. The end IP address must have a higher sequence than the start one.

Description Use the **dhcp server forbidden-ip** command to exclude IP addresses from dynamic allocation.

Use the **undo dhcp server forbidden-ip** command to remove the configuration.

By default, all IP addresses in DHCP address pools are assignable.

When you use the **undo dhcp server forbidden-ip** command to remove the configuration to exclude an IP address from dynamic assignment, the specified address/address range must be consistent with the one specified by the **dhcp server forbidden-ip** command. If you have configured to exclude an address range from dynamic assignment, you need to specify an address range in the **undo dhcp server forbidden-ip** command instead of specifying one IP address.

Related commands: **dhcp server ip-pool** and **network**.

Examples # Exclude the IP address range 10.110.1.1 to 10.110.1.63 from dynamic allocation.

```
<Sysname> system-view
[Sysname] dhcp server forbidden-ip 10.110.1.1 10.110.1.63
```

dhcp server ip-pool

Syntax **dhcp server ip-pool** *pool-name*

undo dhcp server ip-pool *pool-name*

View System view

Parameters *pool-name*: Global address pool name, which is a unique pool identifier, a string of 1 to 35 characters.

Description Use the **dhcp server ip-pool** command to create a DHCP address pool and enter its view. If the pool was created, you will directly enter its view.

Use the **undo dhcp server ip-pool** command to remove specified DHCP address pool.

By default, no DHCP address pool is created.

Related commands: **dhcp enable**.

Examples # Create the DHCP address pool identified by 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
```

dhcp server ping packets

Syntax **dhcp server ping packets** *number*

undo dhcp server ping packets

View System view

Parameters *number*: Number of ping packets. 0 means no ping operation.

Description Use the **dhcp server ping packets** command to specify the maximum number of ping packets on the DHCP server.

Use the **undo dhcp server ping packets** command to restore the default.

The number defaults to 1.

Examples # Specify the maximum number of ping packets as 1.

```
<Sysname> system-view
[Sysname] dhcp server ping packets 10
```

dhcp server ping timeout

Syntax **dhcp server ping timeout** *milliseconds*

undo dhcp server ping timeout

View System view

Parameters *milliseconds*: Response timeout value for ping packets in milliseconds. 0 means no ping operation.

Description Use the **dhcp server ping timeout** command to configure response timeout time of the ping packet on the DHCP server.

Use the **undo dhcp server ping timeout** command to restore the default.

The time defaults to 500.

Examples # Specify the response timeout time as 1000ms.

```
<Sysname> system-view
[Sysname] dhcp server ping timeout 1000
```

dhcp server relay information enable

Syntax **dhcp server relay information enable**

undo dhcp server relay information enable

View System view.

Parameters None

Description Use the **dhcp server relay information enable** command to enable the DHCP server to support option 82.

Use the **undo dhcp server relay information enable** command to disable the option 82 support on the DHCP server.

By default, the DHCP server supports Option 82.

Examples # Disable the option 82 support on the DHCP server.

```
<Sysname> system-view
[Sysname] undo dhcp server relay information enable
```

display dhcp server conflict

Syntax **display dhcp server conflict** { **all** | **ip** *ip-address* }

View Any view

Parameters **all**: Specifies all IP addresses.

ip-address: IP address

Description Use the **display dhcp server conflict** command to display information about IP address conflicts.

Related commands: **reset dhcp server conflict**.

Examples # Display information about all IP address conflicts.

```
<Sysname> display dhcp server conflict all
Address             Discover Time
10.110.1.2         Jan 11 2003 11:57:07
```

Table 262 Description on fields of the display dhcp server conflict command

Field	Description
Address	Conflicted IP address
Discover Time	Time when the conflict was discovered

display dhcp server expired

Syntax **display dhcp server expired** { **ip** *ip-address* | **pool** [*pool-name*] | **all** }

View Any view

Parameters **ip** *ip-address*: Displays the lease expiration information of a specified IP address.

pool [*pool-name*]: Displays the lease expiration information of a specified address pool. The *pool name* is a string of 1 to 35 characters. If the *pool name* is not specified, the lease expiration information of all address pools is displayed.

all: Displays the lease expiration information of all DHCP address pools.

Description Use the **display dhcp server expired** command to display the lease expiration information of specified DHCP address pool(s) or an IP address.

DHCP will assign these expired IP addresses to DHCP clients after all addresses have been assigned.

Examples # Display information about lease expirations in all DHCP address pools.

```
<Sysname> display dhcp server expired all
Global pool:
IP address    Client-identifier/    Lease expiration           Type
                   Hardware address
1.1.1.4        0001-0001-0003        Feb 21 2006 18:07:26 PM   Release
1.1.1.5        0001-0001-0004        Feb 21 2006 18:07:26 PM   Release
--- total 2 entry ---
```

Table 263 Description on fields of the display dhcp server expired command

Field	Description
Global pool	Information about lease expiration of a DHCP global address pool
IP address	Expired IP addresses
Client-identifier/Hardware address	IDs or MACs of clients whose IP addresses were expired
Lease expiration	The lease expiration time
Type	Types of lease expirations. Currently, this field is set to Release.

display dhcp server forbidden-ip

Syntax **display dhcp server forbidden-ip**

View Any view

Parameters None

Description Use the **display dhcp server forbidden-ip** command to display IP addresses excluded from dynamic allocation in DHCP address pool.

Examples # Display IP addresses excluded from dynamic allocation in the DHCP address pool.

```
<Sysname> display dhcp server forbidden-ip
IP Range from 1.1.1.1              to  1.1.1.1
IP Range from 2.2.2.2              to  2.2.2.5
```

display dhcp server free-ip

Syntax **display dhcp server free-ip**

View Any view

Parameters None

Description Use the **display dhcp server free-ip** command to display information about assignable IP addresses.

Examples # Display information about assignable IP addresses.

```
<Sysname> display dhcp server free-ip
IP Range from 10.0.0.0             to  10.0.0.255
```

display dhcp server ip-in-use

Syntax **display dhcp server ip-in-use** { **ip** *ip-address* | **pool** [*pool-name*] | **all** }

View Any view

Parameters **ip** *ip-address*: Displays the binding information of a specified IP address.

pool [*pool-name*]: Displays the binding information of a specified address pool. The *pool name* is a string of 1 to 35 characters. If no *pool name* is specified, the binding information of all address pools is displayed.

all: Displays the binding information of all DHCP address pools.

Description Use the **display dhcp server ip-in-use** command to display the binding information of DHCP address pool(s) or an IP address.

Related commands: **reset dhcp server ip-in-use**.

Examples # Display the binding information of all DHCP address pools.

```
<Sysname> display dhcp server ip-in-use all
Global pool:
IP address    Client-identifier/    Lease expiration        Type
                   Hardware address
10.1.1.1       0016-EC41-4D4C        NOT Used                  Manual
--- total 1 entry ---
```

Table 264 Description on fields of the display dhcp server ip-in-use command

Field	Description
Global pool	Binding information of a DHCP global address pool
IP address	Bound IP address
Client-identifier/Hardware address	Client's ID or MAC of the binding
Lease expiration	Lease expiration time
Type	Binding types, including Manual, Auto:OFFERED and Auto:COMMITTED. ■ Manual: Static binding ■ Auto:OFFERED: The binding sent in the DHCP-OFFER message from the server to the client. ■ Auto:COMMITTED: The binding sent in the DHCP-ACK message from the server to the client.

display dhcp server statistics

Syntax **display dhcp server statistics**

View Any view

Parameters None

Description Use the **display dhcp server statistics** command to display the statistics of the DHCP server.

Related commands: **reset dhcp server statistics**.

Examples # Display the statistics on the DHCP server.

```
<Sysname> display dhcp server statistics
    Global Pool:
     Pool Number:           5
     Binding
      Auto:             0
      Manual:               1
      Expire:               0
    BOOTP Request:          7
     DHCPDISCOVER:          1
     DHCPREQUEST:           4
     DHCPDECLINE:           0
     DHCPRELEASE:           1
     DHCPINFORM:            0
     BOOTPREQUEST:          1
    BOOTPREPLY:         5
     DHCPOFFER:         1
     DHCPACK:               3
     DHCPNAK:               0
     BOOTPREPLY:            1
    Bad Messages:           0
```

Table 265 Description on fields of the display dhcp server statistics command

Field	Description
Global Pool	Statistics of a DHCP global address pool
Pool Number	The number of address pools
Auto	The number of dynamic bindings
Manual	The number of static bindings
Expire	The number of expired bindings
BOOTP Request: 7 DHCPDISCOVER: 1 DHCPREQUEST: 4 DHCPDECLINE: 0 DHCPRELEASE: 1 DHCPINFORM: 0 BOOTPREQUEST: 1	The number of DHCP requests sent from DHCP clients to the DHCP server.

Table 265 Description on fields of the display dhcp server statistics command

Field	Description
BOOTP Reply: 5 DHCPOFFER: 1 DHCPACK: 3 DHCPNAK: 0 Bad Messages: 0 BOOTPREPLY: 1	The number of DHCP replies sent from the DHCP server to DHCP clients.
Bad Messages	The number of erroneous messages

display dhcp server tree

Syntax **display dhcp server tree** { **pool** [*pool-name*] | **all** }

View Any view

Parameters **pool** [*pool-name*]: Displays the tree organization information of a specified address pool. The *pool name* is a string of 1 to 35 characters. If no *pool name* is specified, the tree organization information of all address pools will be displayed.

all: Displays the tree organization information of all DHCP address pools.

Description Use the **display dhcp server tree** command to display the tree organization information of DHCP address pool(s).

Examples # Display the tree organization information of all DHCP address pools.

```
<Sysname> display dhcp server tree all
Global pool:

Pool name: 0
static-bind ip-address 10.10.1.2 mask 255.0.0.0
 static-bind mac-address 00e0-00fc-0001
 PrevSibling node:0
 expired 1 0 0

Pool name: 1
network 192.168.8.0 mask 255.255.255.0
 gateway-list 10.110.1.99
 dns-list 10.1.1.254
 domain-name mydomain.com
 nbns-list 10.12.1.99
 netbios-type b-node
 expired 1 2 3
tftp-server domain-name aaa
tftp-server ip-address 10.1.1.1
```

Table 266 Description on fields of the display dhcp server tree command

Field	Description
Global pool	Information of a global address pool

Table 266 Description on fields of the display dhcp server tree command

Field	Description
Pool name	Address pool name
network	Network segment for address allocation
static-bind ip-address 10.10.1.2 mask 255.0.0.0	The IP address and MAC address of the static binding
static-bind mac-address 00e0-00fc-0001	
Sibling node	Sub-node of the current node. The node in the output may be one of the following types: ■ Child node: The child node (subnet segment) address pool of the current node ■ Parent node: The parent node (nature network segment) address pool of the current node ■ Sibling node: The latter sibling node of the current node (another subnet of the same nature network). The earlier the sibling node is configured, the higher selection priority the sibling node has. ■ PrevSibling node: The previous sibling node of the current node
option	Self-defined DHCP options
expired	The lease duration, in the format of day, hour, and minute
gateway-list	Gateway assigned to the DHCP client
dns-list	DNS server assigned to the DHCP client
domain-name	Domain name specified for the DHCP client
nbns-list	WINS server assigned to the DHCP client
netbios-type	NetBIOS node type assigned to the DHCP client
tftp-server domain-name	TFTP server name assigned to the DHCP client
tftp-server ip-address	TFTP server IP address assigned to the DHCP client

dns-list

Syntax **dns-list** *ip-address*&<1-8>

undo dns-list { *ip-address* | **all** }

View DHCP address pool view

Parameters *ip-address*&<1-8>: DNS server IP address. &<1-8> means you can specify up to eight DNS server addresses separated by spaces.

all: Specifies all DNS server addresses to remove.

Description Use the **dns-list** command to specify DNS server addresses in a DHCP global address pool.

Use the **undo dns-list** command to remove DNS server addresses from a DHCP global address pool.

By default, no DNS server address is specified.

If you repeatedly use the **dns-list** command, the latest configuration will overwrite the previous one.

Related commands: **dhcp server ip-pool**.

Examples # Specify the DNS server address 10.1.1.254 for the DHCP client in DHCP global address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] dns-list 10.1.1.254
```

domain-name

Syntax **domain-name** *domain-name*

undo domain-name

View DHCP address pool view

Parameters *domain-name*: DHCP client domain name to be specified in a DHCP global address pool, a string of 1 to 50 characters.

Description Use the **domain-name** command to specify the DHCP client domain name in a DHCP global address pool.

Use the **undo domain-name** command to remove the domain name assigned from a DHCP global address pool to the DHCP client.

No domain name is specified by default.

Related commands: **dhcp server ip-pool**.

Examples # Specify the client domain name as mydomain.com in DHCP global address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] domain-name mydomain.com
```

expired

Syntax **expired** { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** }

undo expired

View DHCP address pool view

Parameters **day** *day*: Specifies the number of days.

hour *hour*: Specified the number of hours.

minute *minute*: Specifies the number of minutes.

unlimited: Specifies the infinite duration, which is actually 136 years.

Description Use the **expired** command to specify the lease duration in a DHCP global address pool.

Use the **undo expired** command to restore the default lease duration in a DHCP global address pool.

The lease duration defaults to one day.

Note that if the lease duration you specified is beyond the year 2106, the system regards the lease as expired.

Related commands: **dhcp server ip-pool**.

Examples # Specify the lease duration as one day, two hours and three minutes in DHCP global address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] expired day 1 hour 2 minute 3
```

gateway-list

Syntax **gateway-list** *ip-address*&<1-8>

undo gateway-list { *ip-address* | **all** }

View DHCP address pool view

Parameters *ip-address*&<1-8>: Gateway IP address. &<1-8> means you can specify up to eight gateway addresses separated by spaces.

all: Specifies all gateway IP addresses to be removed.

Description Use the **gateway-list** command to specify gateway address(es) in a DHCP global address pool.

Use the **undo gateway-list** command to remove gateway address(es) specified for the DHCP client from a DHCP global address pool.

By default, no gateway address is specified.

If you use the **gateway-list** command repeatedly, the latest configuration will overwrite the previous one.

Examples # Specify the gateway address 10.110.1.99 in DHCP global address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] gateway-list 10.110.1.99
```

nbns-list

Syntax **nbns-list** *ip-address*&<1-8>

undo nbns-list { *ip-address* | **all** }

View DHCP address pool view

Parameters *ip-address*&<1-8>: WINS server IP address. &<1-8> means you can specify up to eight WINS server addresses separated by spaces.

all: Specifies all WINS server addresses to be removed.

Description Use the **nbns-list** command to specify WINS server address(es) in a DHCP global address pool.

Use the **undo nbns-list** command to remove WINS server address(es) assigned from a DHCP global address pool to the DHCP client.

By default, no WINS server address is specified.

If you use the **nbns-list** command repeatedly, the latest configuration will overwrite the previous one.

Related commands: **dhcp server ip-pool** and **netbios-type**.

Examples # Specify WINS server address 10.12.1.99 in DHCP global address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] nbns-list 10.12.1.99
```

netbios-type

Syntax **netbios-type** { **b-node** | **h-node** | **m-node** | **p-node** }

undo netbios-type

View DHCP address pool view

Parameters **b-node**: Broadcast node. A b-node client sends the destination name in a broadcast message. The destination returns the name-to-IP mapping to the client after receiving the message.

p-node: Peer-to-peer node. A p-node client sends the destination name in a unicast message to the WINS server, and the WINS server returns the mapping to the client.

m-node: Mixed node, a combination of a b-node first and p-node second. An m-node client broadcasts the destination name, if there is no response, and then unicasts the destination name to the WINS server to get the mapping.

h-node: Hybrid node, a combination of a p-node first and b-node second. An h-node is a p-node with the peer-to-peer communication mechanism. An h-node client unicasts the destination name to the WINS server, if there is no response, and then broadcasts it to get the mapping from the destination.

Description Use the **netbios-type** command to specify the client NetBIOS node type in a DHCP global address pool.

Use the **undo netbios-type** command to remove the client NetBIOS node type assigned from a DHCP global address pool to the DHCP client.

By default, no NetBIOS node type is specified.

Related commands: **dhcp server ip-pool** and **nbns-list**.

Examples # Specify the NetBIOS node type as b-node in DHCP global address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] netbios-type b-node
```

network

Syntax **network** *ip-address* [*mask-length* | **mask** *mask*]

undo network

View DHCP address pool view

Parameters *ip-address*: IP address range for dynamic allocation. If no mask length and mask is specified, the natural mask will be used.

mask-length: Mask length.

mask *mask*: Specifies the IP address network mask, in dotted decimal format.

Description Use the **network** command to specify the IP address range for dynamic allocation in a DHCP global address pool.

Use the **undo network** command to remove the specified address range.

No IP address range is specified by default.

Note that you can specify only one network segment for each DHCP global address pool. If you use the **network** command repeatedly, the latest configuration will overwrite the previous one.

Related commands: **dhcp server ip-pool** and **dhcp server forbidden-ip**.

Examples # Specify 192.168.8.0/24 as the address range for dynamic allocation in DHCP global address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] network 192.168.8.0 mask 255.255.255.0
```

option

Syntax **option** *code* { **ascii** *ascii-string* | **hex** *hex-string*&<1-16> | **ip-address** *ip-address*&<1-8> }

undo option *code*

View DHCP address pool view

Parameters *code*: Self-defined option number.

ascii *ascii-string*: Specifies an ASCII string with 1 to 63 characters.

hex *hex-string*&<1-16>: Specifies hex digit strings. &<1-16> indicates you can specify up to 16 hex digit strings, separated by spaces. Each string contains 2, 4, 6 or 8 hex digits. The device currently supports total 128 hex digits, not including spaces.

ip-address *ip-address*&<1-8>: Specifies IP addresses. &<1-8> indicates you can specify up to eight IP addresses, separated by spaces.

Description Use the **option** command to configure a self-defined DHCP option in a DHCP global address pool.

Use the **undo option** command to remove a self-defined DHCP option from a DHCP global address pool.

The **option** command is not configured by default.

If you use the **option** command repeatedly, the latest configuration will overwrite the previous one.

Related commands: **dhcp server ip-pool**.

Examples # Configure the hex digits 0x11 and 0x22 for the self-defined DHCP option 100 in DHCP global address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] option 100 hex 11 22
```

reset dhcp server conflict

Syntax **reset dhcp server conflict** { **all** | **ip** *ip-address* }

View User view

Parameters **ip** *ip-address*: Clears the conflict statistics of a specified IP address.

all: Clears the statistics of all IP addresses that conflict.

Description Use the **reset dhcp server conflict** command to clear statistics of IP address conflict(s).

Related commands: **display dhcp server conflict**.

Examples # Clears the statistics of all IP address conflicts.

```
<Sysname> reset dhcp server conflict all
```

reset dhcp server ip-in-use

Syntax **reset dhcp server ip-in-use** { **ip** *ip-address* | **pool** [*pool-name*] | **all** }

View User view

Parameters **all**: Clears the IP address dynamic binding information of all DHCP address pools.

ip *ip-address*: Clears the dynamic binding information of a specified IP address.

pool [*pool-name*]: Clears the dynamic binding information of a specified address pool. The *pool name* is a string of 1 to 35 characters. If no *pool name* is specified, the dynamic binding information of all address pools is cleared.

Description Use the **reset dhcp server ip-in-use** command to clear dynamic IP address binding information.

Related commands: display dhcp server ip-in-use

Examples # Clear the binding information of IP address 10.110.1.1.

```
<Sysname> reset dhcp server ip-in-use ip 10.110.1.1
```

reset dhcp server statistics

Syntax **reset dhcp server statistics**

View User view

Parameters None

Description Use the **reset dhcp server statistics** command to clear the statistics of the DHCP server.

Related commands: **display dhcp server statistics**.

Examples # Clear the statistics of the DHCP server.

```
<Sysname> reset dhcp server statistics
```

static-bind client-identifier

Syntax **static-bind client-identifier** *client-identifier*

undo static-bind client-identifier

View DHCP address pool view

Parameters *client-identifier*: The client ID of a static binding, a string with 4 to 160 characters in the format H-H-H..., each H indicates 4 hex digits except the last H indicates 2 or 4 hex digits. For example, aabb-cccc-dd is a valid ID, while aabb-c-dddd and aabb-cc-dddd are both invalid.

Description Use the **static-bind client-identifier** command to specify the client ID of a static binding in a DHCP address pool.

Use the **undo static-bind client-identifier** command to remove the client ID of a static binding from a DHCP address pool.

By default, no client ID is specified.

Note that:

- Use the **static-bind client-identifier** command together with the **static-bind ip-address** command to accomplish a static binding configuration.
- If you use the **static-bind client-identifier** or **static-bind mac-address** command repeatedly, the latest configuration will overwrite the previous one.

Related commands: **dhcp server ip-pool**, **static-bind ip-address**, and **static-bind mac-address**.

Examples # Bind the client ID aaaa-bbbb to the IP address 10.1.1.1 with the mask 255.255.255.0 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] static-bind ip-address 10.1.1.1 mask 255.255.255.0
[Sysname-dhcp-pool-0] static-bind client-identifier aaaa-bbbb
```

static-bind ip-address

Syntax **static-bind ip-address** *ip-address* [*mask-length* | **mask** *mask*]

undo static-bind ip-address

View DHCP address pool view

Parameters *ip-address*: IP address of a static binding, if no mask and mask length is specified, the natural mask is used.

mask-length: Mask length of the IP address, that is, the number of ones in the mask.

mask *mask*: Specifies the IP address mask, in dotted decimal format.

Description Use the **static-bind ip-address** command to specify an IP address in a DHCP address pool for a static binding.

Use the **undo static-bind ip-address** command to remove the statically bound IP address.

By default, no IP address is statically bound in a DHCP address pool.

Note that:

- Use the **static-bind ip-address** command together with the **static-bind mac-address** or **static-bind client-identifier** command to accomplish a static binding configuration.
- If the statically bound address is an interface address of the DHCP server, the static binding does not take effect.
- If you use the **static-bind ip-address** command repeatedly, the latest configuration will overwrite the previous one.

Related commands: **dhcp server ip-pool**, **static-bind client-identifier** and **static-bind mac-address**.

Examples # Bind the client MAC address 0000-e03f-0305 to the IP address 10.1.1.1 with the mask 255.255.255.0 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] static-bind ip-address 10.1.1.1 mask 255.255.255.0
[Sysname-dhcp-pool-0] static-bind mac-address 0000-e03f-0305
```

static-bind mac-address

Syntax **static-bind mac-address** *mac-address*

undo static-bind mac-address

View DHCP address pool view

Parameters *mac-address*: The MAC address of a static binding, in the format H-H-H.

Description Use the **static-bind mac-address** command to statically bind a MAC address to an IP address in a DHCP address pool.

Use the **undo static-bind mac-address** command to remove the statically bound MAC address..

By default, no MAC address is statically bound.

Note that:

- Use the **static-bind mac-address** command together with the **static-bind ip-address** command to complete a static binding configuration.
- If you use the **static-bind mac-address** or **static-bind client-identifier** command repeatedly, the latest configuration will overwrite the previous one.

Relate command: **dhcp server ip-pool**, **static-bind client-identifier** and **static-bind ip-address.**

Examples # Bind the client MAC address 0000-e03f-0305 to the IP address 10.1.1.1 with the mask 255.255.255.0 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] static-bind ip-address 10.1.1.1 mask 255.255.255.0
[Sysname-dhcp-pool-0] static-bind mac-address 0000-e03f-0305
```

tftp-server domain-name

Syntax **tftp-server domain-name** *domain-name*

undo tftp-server domain-name

View DHCP address pool view

Parameters *domain-name*: TFTP server name, a string of 1 to 63 characters.

Description Use the **tftp-server domain-name** command to specify a TFTP server name in a DHCP global address pool.

Use the **undo tftp-server domain-name** command to remove the TFTP server name from a DHCP global address pool.

By default, no TFTP server name is specified.

Using the **tftp-server domain-name** command repeatedly will overwrite the previous configuration.

Examples # Specify the TFTP server name as aaa in DHCP global address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] tftp-server domain-name aaa
```

tftp-server ip-address

Syntax **tftp-server ip-address** *ip-address*

undo tftp-server ip-address

View DHCP address pool view

Parameters *ip-address:* TFTP server IP address.

Description Use the **tftp-server ip-address** command to specify the TFTP server IP address in a DHCP global address pool.

Use the **undo tftp-server ip-address** command to remove the TFTP server IP address from a DHCP global address pool.

By default, no TFTP server address is specified.

Using the **tftp-server ip-address** command repeatedly will overwrite the previous configuration.

Examples # Specify the TFTP server address 10.1.1.1 in DHCP global address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] tftp-server ip-address 10.1.1.1
```

53 DHCP RELAY AGENT CONFIGURATION COMMANDS

debugging dhcp relay

Syntax **debugging dhcp relay** { **all** | **error** | **event** | **packet** [**client mac** *mac-address*] }

undo debugging dhcp relay { **all** | **error** | **event** | **packet** [**client mac** *mac-address*] }

View User view

Parameters **all**: Enables/disables all debugging options on the DHCP relay agent.

error: Enables/disables error debugging on the DHCP relay agent.

event: Enables/disables event debugging on the DHCP relay agent.

packet: Enables/disables packet debugging on the DHCP relay agent.

client mac *mac-address*: Enables/disables packet debugging on a DHCP client. The *mac-address* argument specifies the MAC address of a DHCP client, in the format of H-H-H.

Description Use the **debugging dhcp relay** command to enable debugging on the DHCP relay agent.

Use the **undo debugging dhcp server** command to disable debugging on the DHCP relay agent.

Examples # Enable packet debugging on the DHCP relay agent.

```
<Sysname> debugging dhcp relay packet
<Sysname> terminal debugging
<Sysname>
*0.230094 relay DHCPR/8/DHCPR_DEBUG_EVENT:
 Begin to deal with DHCP Discover packet.
*0.230094 relay DHCPR/8/DHCPR_DEBUG_PKTRXTX:
Rx, DHCP request packet, interface Vlan-interface2
*0.230094 relay DHCPR/8/DHCPR_DEBUG_PACKET:
From client to server(Server-group 0):
    Message type: request
    Hardware Type: 1, Hardware Address Length: 6
    Hops: 1, Transaction ID: 4281385283
    Seconds: 0, Broadcast Flag: 1
    Client IP Address: 0.0.0.0    Your IP Address: 0.0.0.0
    Server IP Address: 0.0.0.0    Gateway IP Address: 22.0.0.1
    Client Hardware Address: 00e0-fc14-1601
    Server Host Name: Not Configured, Boot File Name: Not Configured
```

```
    DHCP message type: DHCP Discover
*0.230094 relay DHCPR/8/DHCPR_DEBUG_RELAYPKT:
Pkt Sent: send request interface Vlan-interface22, dest IP: 11.0.0.1,
         CHardAddr: 00e0.fc14.1601, server-group: 0
```

// The DHCP relay agent receives a DHCP-DISCOVER message from the DHCP client, and then forwards the message to the DHCP server at 11.0.0.1 in DHCP server group 0.

```
*0.230891 relay DHCPR/8/DHCPR_DEBUG_EVENT:
 Begin to deal with DHCP Offer packet.
*0.230891 relay DHCPR/8/DHCPR_DEBUG_PKTRXTX:
Rx, DHCP reply packet, interface Vlan-interface22

*0.230891 relay DHCPR/8/DHCPR_DEBUG_PACKET:
From server to client(Server-group 0):
    Message type: reply
    Hardware Type: 1, Hardware Address Length: 6
    Hops: 0, Transaction ID: 2294688324
    Seconds: 0, Broadcast Flag: 1
    Client IP Address: 0.0.0.0    Your IP Address: 22.0.0.2
    Server IP Address: 0.0.0.0    Gateway IP Address: 22.0.0.1
    Client Hardware Address: 00e0-fc14-1601
    Server Host Name: Not Configured, Boot File Name: Not Configured
    DHCP message type: DHCP Offer

*0.230891 relay DHCPR/8/DHCPR_DEBUG_RELAYPKT:
Pkt Sent: send reply interface Vlan-interface22, dest IP: 255.255.255.255,
         CHardAddr: 00e0.fc14.1601, server-group: 0
```

// The DHCP relay agent receives a DHCP-OFFER message from the DHCP server, and then broadcasts the message.

```
*0.230969 relay DHCPR/8/DHCPR_DEBUG_EVENT:
 Begin to deal with DHCP Request packet.
*0.230969 relay DHCPR/8/DHCPR_DEBUG_PKTRXTX:
Rx, DHCP request packet, interface Vlan-interface22

*0.230969 relay DHCPR/8/DHCPR_DEBUG_PACKET:
From client to server(Server-group 0):
    Message type: request
    Hardware Type: 1, Hardware Address Length: 6
    Hops: 1, Transaction ID: 2294688324
    Seconds: 0, Broadcast Flag: 1
    Client IP Address: 0.0.0.0    Your IP Address: 0.0.0.0
    Server IP Address: 0.0.0.0    Gateway IP Address: 22.0.0.1
    Client Hardware Address: 00e0-fc14-1601
    Server Host Name: Not Configured, Boot File Name: Not Configured
    DHCP message type: DHCP Request

*0.230969 relay DHCPR/8/DHCPR_DEBUG_RELAYPKT:
Pkt Sent: send request interface Vlan-interface22, dest IP: 11.0.0.1,
         CHardAddr: 00e0.fc14.1601, server-group: 0
```

// The DHCP relay agent receives a DHCP-REQUEST message from the DHCP client, and then forwards the message to the DHCP server at 11.0.0.1.

```
*0.231063 relay DHCPR/8/DHCPR_DEBUG_EVENT:
 Begin to deal with DHCP Ack packet.
*0.231063 relay DHCPR/8/DHCPR_DEBUG_PKTRXTX:
Rx, DHCP reply packet, interface Vlan-interface22

*0.231063 relay DHCPR/8/DHCPR_DEBUG_PACKET:
From server to client(Server-group 0):
```

```
    Message type: reply
    Hardware Type: 1, Hardware Address Length: 6
    Hops: 0, Transaction ID: 2294688324
    Seconds: 0, Broadcast Flag: 1
    Client IP Address: 0.0.0.0    Your IP Address: 22.0.0.2
    Server IP Address: 0.0.0.0    Gateway IP Address: 22.0.0.1
    Client Hardware Address: 00e0-fc14-1601
    Server Host Name: Not Configured, Boot File Name: Not Configured
    DHCP message type: DHCP Ack

*0.231063 relay DHCPR/8/DHCPR_DEBUG_RELAYPKT:
Pkt Sent: send reply interface Vlan-interface22, dest IP: 255.255.255.255,
         CHardAddr: 00e0.fc14.1601, server-group: 0
```

// The DHCP relay agent receives a DHCP-ACK response from the DHCP server, and then broadcasts the message.

Table 267 Description on fields of the debugging dhcp relay packet command

Field	Description
From client to server(Server-group 0)	Information that the DHCP client sends to the DHCP server (in DHCP server group 0).
Message type	Content of the first byte of the DHCP message. That is, the operation type of a DHCP message, namely request or reply.
Hardware Type	Hardware address type of the DHCP client, where 1 indicates Ethernet type.
Hardware Address Length	Length of the DHCP client's hardware address
Hops	Number of hops a DHCP message traveled
Transaction ID	A random number uniquely identifying an address allocation request by a DHCP client
Seconds	Number of seconds that has elapsed since the DHCP message is sent. It is filled by the DHCP client.
Broadcast Flag	Broadcast flag ■ 1: Broadcast ■ 0: Unicast
Client IP Address	IP address of the DHCP client
Your IP Address	IP address that the DHCP server assigns to the client
Server IP Address	IP address of the DHCP server
Gateway IP Address	IP address of the DHCP relay agent
Client Hardware Address	MAC address of the DHCP client
Server Host Name	Host name of the DHCP server.
Boot File Name	Boot file name

Table 267 Description on fields of the debugging dhcp relay packet command

Field	Description
DHCP message type	DHCP message type, including ■ DHCP Discover ■ DHCP Offer ■ DHCP Request ■ DHCP Decline ■ DHCP ACK ■ DHCP NAK ■ DHCP Release ■ DHCP Inform

dhcp relay address-check

Syntax **dhcp relay address-check** { **enable** | **disable** }

View VLAN interface view

Parameters **enable**: Enables IP address match checking on the relay agent.

disable: Disables IP address match checking on the relay agent.

Description Use the **dhcp relay address-check** command to configure IP address match checking on the relay agent.

By default, the function is disabled.

Examples # Enable IP address match checking on the DHCP relay agent.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp relay address-check enable
```

dhcp relay information enable

Syntax **dhcp relay information enable**

undo dhcp relay information enable

View VLAN interface view

Parameters None

Description Use the **dhcp relay information enable** command to enable the relay agent to support option 82.

Use the **undo dhcp relay information enable** command to disable option 82 support.

By default, option 82 support is disabled on DHCP relay agent.

Examples # Enable option 82 support on the relay agent.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp relay information enable
```

dhcp relay information format

Syntax **dhcp relay information format** { **normal** | **verbose** [**node-identifier** { **mac** | **sysname** | **user-defined** *node-identifier* }] }

undo dhcp relay information format [**verbose node-identifier**]

View VLAN interface view

Parameters **normal**: Specifies the normal padding format.

verbose: Specifies the verbose padding format.

node-identifier { **mac** | **sysname** | **user-defined** *node-identifier* }: Specifies access node identifier.

- **mac** indicates using MAC address as the node identifier.
- **sysname** indicates using the device name of a node as the node identifier.
- **user-defined** *node-identifier* indicates using a specified character string as the node identifier, in which *node-identifier* is a string with 1 to 50 characters.

By default, the node MAC address is used as the node identifier.

Description Use the **dhcp relay information format** command to specify a padding format for option 82.

Use the **undo dhcp relay information format** command to restore the default padding format.

The option 82 padding format defaults to **normal**.

- *Using the **undo dhcp relay information format** command without the keyword **verbose node-identifier** restores the default **normal** padding format, or with the keyword **verbose node-identifier** restores the **mac** mode of the **verbose** padding format.*
- *If configuring the handling strategy of the DHCP relay agent as **replace**, you need to configure a padding format of option 82. If the handling strategy is keep or drop, you need not configure any padding format.*

- *If sub-option 1 (node identifier) of Option 82 is padded with the device name (sysname) of a node, the device name must contain no spaces. Otherwise, the DHCP relay agent will drop the message.*

Examples # Specify the verbose padding format for option 82.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp relay information format verbose
```

dhcp relay information strategy

Syntax **dhcp relay information strategy** { **drop | keep | replace** }

undo dhcp relay information strategy

View VLAN interface view

Parameters **drop**: Specifies to drop messages containing option 82.

keep: Specifies to forward messages containing option 82 without any change.

replace: Specifies to forward messages containing option 82 after replacing the original option 82 with the option 82 padded in the specified padding format.

Description Use the **dhcp relay information strategy** command to configure DHCP relay agent handling strategy for messages containing option 82.

Use the **undo dhcp relay information strategy** command to restore the default handling strategy.

The handling strategy for messages containing option 82 defaults to **replace**.

Examples # Configure the DHCP relay agent handling strategy for messages containing option 82 as **keep**.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp relay information strategy keep
```

dhcp relay release ip

Syntax **dhcp relay release ip** *client-ip*

View System view

Parameters *client-ip*: DHCP client IP address.

Description Use the **dhcp relay release ip** command to send a release request to a specified DHCP server or server groups for releasing a specified client IP address.

In system view, the relay agent will send a release request to the DHCP server corresponding to the interfaces working in DHCP relay agent mode.

Examples # Send a release request to the DHCP server for releasing the IP address 1.1.1.1 that was obtained by the client.

```
<Sysname> system-view
[Sysname] dhcp relay release ip 1.1.1.1
```

dhcp relay security static

Syntax **dhcp relay security static** *ip-address mac-address*

undo dhcp relay security { *ip-address* | **all** | **dynamic** | **static** }

View System view

Parameters *ip-address*: Client IP address for creating a static binding.

mac-address: Client MAC address for creating a static binding, in the format H-H-H.

all: Specifies all entries of client IP-to-MAC bindings to be removed.

dynamic: Specifies entries of dynamic client IP-to-MAC bindings to be removed.

static: Specifies entries of manual client IP-to-MAC bindings to be removed.

Description Use the **dhcp relay security static** command to configure a manual IP-to-MAC binding on the relay agent.

Use the **undo dhcp relay security** command to remove specified entries of client IP-to-MAC bindings from the relay agent.

No manual IP-to-MAC binding is configured on the DHCP relay agent by default.

Related commands: **display dhcp relay security**.

Examples # Configure a static binding between IP address 1.1.1.1 to MAC address 0005-5d02-f2b3.

```
<Sysname> system-view
[Sysname] dhcp relay security static 1.1.1.1 0005-5d02-f2b3
```

dhcp relay security tracker

Syntax **dhcp relay security tracker** { *interval* | **auto** }

undo dhcp relay security tracker [*interval*]

View System view

Parameters **auto**: Specifies the **auto** refreshing interval, which is the value of 60 seconds divided by the number of binding entries. Thus, the more entries, the shorter interval, but the shortest interval is no less than 500 ms.

interval: Refreshing interval in seconds, in the range of 1 to 120.

Description Use the **dhcp relay security tracker** command to set a refreshing interval at which the relay agent contacts the DHCP server for refreshing dynamic bindings.

Use the **undo dhcp relay security tracker** command to restore the default interval.

The default handshake interval is **auto**, the value of 60 seconds divided by the number of binding entries.

A large number of binding entries may result in a slow refreshing speed, so you are recommended to use the default refreshing interval.

Examples # Set the handshake interval as 100 seconds.

```
<Sysname> system-view
[Sysname] dhcp relay security tracker 100
```

dhcp relay server-detect

Syntax **dhcp relay server-detect**

undo dhcp relay server-detect

View System view

Parameters None

Description Use the **dhcp relay server-detect** command to enable unauthorized DHCP server detection.

Use the **undo dhcp relay server-detect** command to disable unauthorized DHCP server detection.

By default, unauthorized DHCP server detection is disabled.

Examples # Enable unauthorized DHCP server detection.

```
<Sysname> system-view
[Sysname] dhcp relay server-detect
```

dhcp relay server-group

Syntax **dhcp relay server-group** *group-* **ip** *ip-address*

undo dhcp relay server-group *group-id* [**ip** *ip-address*]

View System view

Parameters *group-id*: DHCP server group number.

ip-address: DHCP server IP address.

Description Use the **dhcp relay server-group** command to specify a DHCP server for a DHCP server group.

Use the **undo dhcp relay server-group** command to remove a DHCP server from a DHCP server group, if no **ip** *ip-address* is specified, all servers in the DHCP server group and the server group itself will be removed.

By default, no DHCP server is specified for a DHCP server group.

Note that:

- If a server group has been correlated to multiple interfaces, you need to cancel these correlations before deleting the server group.
- The IP address of any DHCP server and any interface's IP address of the DHCP relay agent cannot be in the same network segment. Otherwise, the client may fail to obtain an IP address.

Related commands: **display dhcp relay server-group**.

Examples # Specify DHCP server 1.1.1.1 for DHCP server group 1 on the relay agent.

```
<Sysname> system-view
[Sysname] dhcp relay server-group 1 ip 1.1.1.1
```

dhcp relay server-select

Syntax **dhcp relay server-select** *group-id*

undo dhcp relay server-select

View VLAN interface view

Parameters *group-id*: DHCP server group number to be correlated. The specified server group must be an existing group containing at least a DHCP server.

Description Use the **dhcp relay server-select** command to correlate specified interface(s) to a specified DHCP server group.

Use the **undo dhcp relay server-select** command to remove a configured correlation.

By default, no DHCP server group is correlated with an interface on the relay agent.

Note that an interface on the relay agent can only be correlated to one DHCP server group, and a newly configured correlation overwrites the previous one. If the server group in the new correlation does not exist, the new configuration will not work. The interface still maintains the previous correlation.

Examples # Correlate VLAN interface 1 to DHCP server group 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp relay server-select 1
```

dhcp select relay

Syntax **dhcp select relay**

undo dhcp select relay

View VLAN interface view

Parameters None

Description Use the **dhcp select relay** command to enable the relay agent on the current interface, specified or all interfaces. Upon receiving requests from an enabled interface, the relay agent will forward these requests to outside DHCP servers for IP address allocation.

Use the **undo dhcp select relay** command to restore the default on interface(s).

After DHCP is enabled, the DHCP server is enabled on an interface by default. That is, upon receiving a client's request from the interface, the DHCP server allocates an IP address from the DHCP address pool to the client.

Examples # Enable the DHCP relay agent on the interface Vlan-inteface1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp select relay
```

display dhcp relay

Syntax **display dhcp relay** { **interface** *interface-type interface-number* | **all** }

View Any view

Parameters **interface** *interface-type interface-number*: Displays information of the DHCP server group that a specified interface corresponds to.

all: Displays information of DHCP server groups that all interfaces correspond to.

Description Use the **display dhcp relay** command to display information about DHCP server groups correlated to an interface or all interfaces.

Examples # Display information about DHCP server groups correlated to all interfaces.

```
[Sysname] display dhcp relay all
    Interface name            Server-group
    Vlan-interface22                  2
```

Table 268 Description on fields of the display dhcp relay all command

Field	Description
Interface name	Interface name
Server-group	DHCP server group number correlated to the interface.

display dhcp relay security

Syntax **display dhcp relay security** [**dynamic** | **static** | *ip-address*]

View Any view

Parameters **dynamic**: Displays information about dynamic bindings.

static: Displays information about static bindings.

ip-address: Displays the binding information of an IP address.

Description Use the **display dhcp relay security** command to display information about bindings of DHCP relay agents. If no parameter is specified, information about all bindings will be displayed.

Examples # Display information about all bindings.

```
[Sysname] display dhcp relay security
IP Address      MAC Address     Type
 10.1.1.1       00e0-0000-0001  Static
 10.1.1.5       00e0-0000-0002  Static
---   2 dhcp-security item(s) found   ---
```

Table 269 Description on fields of the display dhcp relay security command

Field	Description
IP Address	Client IP address
MAC Address	Client MAC address
Type	Type of binding, including dynamic and static

display dhcp relay security statistics

Syntax **display dhcp relay security statistics**

View Any view

Parameters None

Description Use the **display dhcp relay security statistics** command to display statistics information about bindings of DHCP relay agents.

Examples # Display statistics about client address binding entries.

```
<Sysname> display dhcp relay security statistics
Static Items      :2
Dynamic Items     :2
Temporary Items   :2
All Items          :6
```

Table 270 Description on fields of the display dhcp relay security statistics command

Field	Description
Static Items	Static client address binding items
Dynamic Items	Dynamic client address binding items
Temporary Items	Temporary client address binding items
All Items	All client address binding items

display dhcp relay security tracker

Syntax **display dhcp relay security tracker**

View Any view

Parameters None

Description Use the **display dhcp relay security tracker** command to display the interval for refreshing dynamic bindings on the relay agent.

Examples # Display the interval for refreshing dynamic bindings on the relay agent.

```
[Sysname] display dhcp relay security tracker
Current tracker interval: 10s (Specified by user)
```

The interval is 10 seconds.

display dhcp relay server-group

Syntax **display dhcp relay server-group** { *group-id* | **all** }

View Any view

Parameters *group-id*: Displays the information of the specified DHCP server group.

all: Displays the information of all DHCP server groups.

Description Use the **display dhcp relay server-group** command to display the configuration information of a specified or all DHCP server groups.

Examples # Display IP addresses of DHCP servers in DHCP server group 1.

```
<Sysname> display dhcp relay server-group 1
    No.             Group IP
    1               10.1.1.1
    2               10.1.1.2
```

Table 271 Description on fields of the display dhcp relay server-group command

Field	Description
Server-group	DHCP server group number
Group IP	IP address in the server group

display dhcp relay statistics

Syntax **display dhcp relay statistics** [**server-group** { *group-id* | **all** }]

View Any view

Parameters *group-id*: Number of a server group about which to display DHCP packet statistics.

all: Specifies all server groups about which to display DHCP packet statistics. Information for each group will be displayed.

Description Use the **display dhcp relay statistics** command to display DHCP packet statistics related to a specified or all DHCP server groups, which includes number of error packets, number of DHCP packets received from the client, number of DHCP packets received from the server, number of DHCP packets sent to the server, and number of DHCP packets sent to the client (including unicast packets and broadcast packets).

Note that if no parameter (**server-group** and **all)** is specified, all DHCP packet statistics on the relay agent will be displayed.

Examples # Display all DHCP packet statistics on the relay agent.

```
<Sysname> display dhcp relay statistics
     Bad packets received:                  0
     DHCP packets received from clients:    20
         DHCPDISCOVER packets received:     10
         DHCPREQUEST packets received:      10
         DHCPINFORM packets received:       0
         DHCPRELEASE packets received:      0
```

```
        DHCPDECLINE packets received:      0
        BOOTPREQUEST packets received:     0
    DHCP packets received from servers:    20
        DHCPOFFER packets received:        10
        DHCPACK packets received:          10
        DHCPNAK packets received:          0
        BOOTPREPLY packets received:       0
    DHCP packets relayed to servers:       0
        DHCPDISCOVER packets relayed:      0
        DHCPREQUEST packets relayed:       0
        DHCPINFORM packets relayed:        0
        DHCPRELEASE packets relayed:       0
        DHCPDECLINE packets relayed:       0
        BOOTPREQUEST packets relayed:      0
    DHCP packets relayed to clients:      0
        DHCPOFFER packets relayed:         0
        DHCPACK packets relayed:           0
        DHCPNAK packets relayed:           0
```

Table 272 Field descriptions of the display dhcp relay statistics command

Field	Description
Bad packets received	Number of error packets received by the DHCP relay agent
DHCP packets received from clients	Number of DHCP packets that the DHCP relay agent receives from the client
DHCP packets received from servers	Number of DHCP packets that the DHCP relay agent receives from the server
DHCP packets relayed to servers	Number of packets that the DHCP relay agent sent to the server
DHCP packets relayed to clients	Number of packets that the DHCP relay agent sent to the client
DHCP packets sent to servers	Number of DHCP packets that the DHCP relay agent sent to the server. The packets include those that the DHCP relay agent forwarded to server and those that the DHCP relay agent sent to the server.
DHCP packets sent to clients	Number of DHCP packets that the DHCP relay agent sent to the client. The packets include those that the DHCP relay agent forwarded to client and those that the DHCP relay agent sent to the client. (Currently, the switch operating as DHCP relay agent will not send DHCP packets to clients.)

Display DHCP packet statistics related to every server group on the relay agent.

```
<Sysname> display dhcp relay statistics server-group all
DHCP relay server-group           #2
     Packet type               Packet number
 Client -> Server:
     DHCPDISCOVER                 5
     DHCPREQUEST                  5
     DHCPINFORM                   0
     DHCPRELEASE                  0
     DHCPDECLINE                  0
     BOOTPREQUEST                 0
 Server -> Client:
     DHCPOFFER                    5
     DHCPACK                      5
```

```
     DHCPNAK                        0
     BOOTPREPLY                     0

DHCP relay server-group             #3
     Packet type                Packet number
 Client -> Server:
     DHCPDISCOVER                   5
     DHCPREQUEST                    5
     DHCPINFORM                     0
     DHCPRELEASE                    0
     DHCPDECLINE                    0
     BOOTPREQUEST                   0
 Server -> Client:
     DHCPOFFER                      5
     DHCPACK                        5
     DHCPNAK                        0
     BOOTPREPLY                    0
```

Table 273 Description on fields of the display dhcp relay statistics server-group command

Field	Description
DHCP relay server-group	DHCP server group
Packet type	DHCP packet type
Packet number	Number of packets received by the DHCP relay agent
Client -> Server	DHCP packets that the DHCP relay agent received from the client
Server -> Client	DHCP packets that the DHCP relay agent received from the server

reset dhcp relay statistics

Syntax **reset dhcp relay statistics** [**server-group** *group-id*]

View User view

Parameters **server-group** *group-id*: Specifies a server group about which to remove statistics from the relay agent.

Description Use the **reset dhcp relay statistics** command to remove statistics from the relay agent.

If no **server-group** is specified, all statistics will be removed from the relay agent.

Related commands: **display dhcp relay statistics**.

Examples # Remove all statistics from the DHCP relay agent.

```
<Sysname> reset dhcp relay statistics
```

54 DNS CONFIGURATION COMMANDS

debugging dns

Syntax **debugging dns**

undo debugging dns

View User view

Parameters None

Description Use the **debugging dns** command to enable debugging for dynamic domain name resolution.

Use the **undo debugging dns** command to disable debugging.

By default, debugging for dynamic domain name resolution is disabled.

Examples # Enable debugging for dynamic domain name resolution.

```
<Sysname> debugging dns
succeed in making DNS packet for name aabbcc.com
```

// A packet querying for domain name aabbcc.com is generated.

```
send the packet to 172.16.1.1 DNS server for 1 times
```

// The query packet is sent for the first time to the DNS server at 172.16.1.1.

```
receive a right answer from server 172.16.1.1
```

// A correct response is received from the server at 172.16.1.1.

```
query timeout
```

// No response is received, and the query times out.

display dns domain

Syntax **display dns domain** [**dynamic**]

View Any view

Parameters **dynamic**: Displays the domain name suffixes dynamically obtained through DHCP or other protocols.

Description Use the **display dns domain** command to display the domain name suffixes.

Related commands: **dns domain**.

Examples # Display domain name suffixes.

```
<Sysname> display dns domain
Type:
  D:Dynamic    S:Static

No.     Type    Domain-name
1       S       com
```

Table 274 Description on fields of display dns domain command

Field	Description
No	Sequence number
Type	Type of domain name suffix: S represents a statically configured domain name suffix, and D represents a domain name suffix obtained dynamically through DHCP.
Domain-name	Domain name suffix

display dns dynamic-host

Syntax **display dns dynamic-host**

View Any view

Parameters None

Description Use the **display dns dynamic-host** command to display the information in the dynamic domain name resolution cache.

Examples # Display the information in the dynamic domain name resolution cache.

```
<Sysname> display dns dynamic-host
No.  Domain-name            Ip Address          TTL
1    www.baidu.com          202.108.249.134     63000
2    www.yahoo.akadns.net   66.94.230.39        24
3    www.hotmail.com        207.68.172.239      3585
4    www.eyou.com           61.136.62.70        3591
```

Table 275 Description on the field of the display dns dynamic-host command

Field	Description
No	Sequence number
Domain-name	Domain name
Ip Address	IP address for the corresponding domain name

Table 275 Description on the field of the display dns dynamic-host command

Field	Description
TTL	Time a mapping can be stored in the cache (seconds).

*The domain-name field in the **display dns dynamic-host** command contains 21 characters at most. If a resolved domain name consists of more than 21 characters, only the first 21 characters are displayed.*

display dns server

Syntax **display dns server** [**dynamic**]

View Any view

Parameters **dynamic**: Displays the DNS server information dynamically obtained through DHCP or other protocols

Description Use the **display dns server** command to display the DNS server information.

Related commands: **dns server**.

Examples # Display the DNS server information.

```
<Sysname> display dns server
Type:
  D:Dynamic    S:Static

IPv4 DNS Servers :
Domain-server Type  IP Address
     1        S     169.254.65.125

IPv6 DNS Servers :
Domain-server Type IPv6 Address                          (Interface Name)
     1        S    FE01:9A2::1
     2        S    FE80::3                                GE4/2/4
```

Table 276 Description on fields of the display dns server command

Field	Description
Domain-server	Sequence number of the DNS server. Configured automatically by the device, starting from 1. Servers with IPv4 or IPv6 addresses are numbered respectively.
IP Address	IPv4 address of the DNS server
IPv6 Address	IPv6 address of the DNS server
Interface Name	Only displayed when the DNS server is configured with an IPv6 address.

For details about IPv6 DNS, refer to "DNS Configuration Commands" on page 939.

display ip host

Syntax **display ip host**

View Any view

Parameters None

Description Use the **display ip host** command to display the host names and corresponding IP addresses in the static DNS database.

Examples # Display the host names and corresponding IP addresses in the static DNS database.

```
<Sysname> display ip host
Host            Age     Flags       Address
My          0       static      1.1.1.1
Aa          0       static      2.2.2.4
```

Table 277 Description on fields of the display ip host command

Field	Description
Host	Host name
Age	Time to live. 0 means that a static mapping will never age out.
	You can only manually remove the mappings between host names and IP addresses.
Flags	Indicates the type of mappings between host names and IP addresses, static or dynamic.
	Static represents static domain name resolution.
Address	Host IP addresses

dns domain

Syntax **dns domain** *domain-name*

undo dns domain [*domain-name*]

View System view

Parameters *domain-name*: DNS suffix, a case-insensitive string consisting of 1 to 238 characters. A DNS suffix may include letters, digits, hyphens (-), underscores (_), and dots (.).

*You can use the **dns domain** command to configure a DNS suffix with the maximum length of 238 characters. Since a valid DNS suffix is a character string separated by dots, with each separated part (label) containing no more than 63 characters, any part exceeding this length may result in failure to generate packets.*

Description Use the **dns domain** command to configure a DNS suffix. The system can automatically add corresponding suffix to the domain name you entered for resolution, so you can just enter the name part of the domain name.

Use the **undo dns domain** command to delete a DNS suffix or all DNS suffixes.

No DNS suffix is configured by default.

You can configure a maximum of 10 DNS suffixes. You must enter a suffix name before deleting it. Otherwise, all the statically configured suffixes are deleted.

Related commands: **display dns domain**.

Examples # Configure com as a DNS suffix.

```
[Sysname] dns domain com
```

dns resolve

Syntax **dns resolve**

undo dns resolve

View System view

Parameters None

Description Use the **dns resolve** command to enable dynamic domain name resolution.

Use the **undo dns resolve** command to disable dynamic domain name resolution.

Dynamic domain name resolution is disabled by default.

Examples # Enable dynamic domain name resolution.

```
[Sysname] dns resolve
```

dns server

Syntax **dns server** *ip-address*

undo dns server [*ip-address*]

View System view

Parameters *ip-address*: IP address of the DNS server.

Description Use the **dns server** command to configure an IP address for the DNS server.

Use the **undo dns server** to remove the IP address.

No IP address is configured for the DNS server by default.

You can configure a maximum of six DNS servers.

Related commands: **display dns server**.

Examples # Configure 172.16.1.1 for the DNS server.

```
[Sysname] dns server 172.16.1.1
```

ip host

Syntax **ip host** *hostname ip-address*

undo ip host *hostname* [*ip-address*]

View System view

Parameters *Hostname*: Host name, consisting of 1 to 20 characters, including case-insensitive letters, numbers, hyphens (-), or dots (.). The host name must include at least one letter.

ip-address: IP address of the specified host in dotted decimal notation.

Description Use the **ip host** command to create a mapping between host name and IP address in the static resolving list.

Use the **undo ip host** command to remove the mapping.

No mappings are created by default.

You can configure only one mapping between IP address and host name. For example, a mapping configured last time will overwrite the previous one if there is any.

Related commands: **display ip host**.

Examples # Configure the IP address 10.110.0.1 for a host named aaa.

```
[Sysname] ip host aaa 10.110.0.1
```

reset dns dynamic-host

Syntax **reset dns dynamic-host**

View User view

Parameters None

Description Use the **reset dns dynamic-host** command to clear the information in the dynamic domain name cache.

Related commands: **display dns dynamic-host**.

Examples # Clear the information in the dynamic domain name cache.

```
<Sysname> reset dns dynamic-host
```

55 IPv4-Based VRRP Configuration Commands

debugging vrrp packet

Syntax **debugging vrrp packet** [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]

undo debugging vrrp packet [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]

View User view

Parameters **interface** *interface-type interface-number:* Enables packet debugging for a specified interface, where *interface-type* indicates the interface type and *interface-number* indicates the interface number.

vrid *virtual-router-id*: Enables packet debugging for a standby group on a specified interface, where *virtual-router-id* indicates the standby group number.

Description Use the **debugging vrrp packet** command to enable debugging for sending and receiving VRRP packets.

Use the **undo debugging vrrp packet** command to disable debugging for sending and receiving VRRP packets.

By default, debugging for sending and receiving VRRP packets is disabled.

Note that if debugging globally for sending and receiving VRRP packets is disabled and debugging for an interface or a standby group is enabled, the interface or the standby group can still output debugging information and you must use the **undo** command to disable the debugging. Disabling of global debugging does not disable debugging for a specific interface or standby group.

Examples # Enable debugging for sending and receiving VRRP packets to debug all packets received on and sent from all the virtual standby groups on the device.

```
<Sysname> debugging vrrp packet
*0.649641 router a VRRP/7/DebugPacket:
IPv4 Vlan-interface2 | Virtual Router 1:receiving from 1.1.1.3, vers
ion = 2, type =1, priority = 120, count ip addrs = 1, timer = 1, aut
h type is no, checksum = 61796
IPv4 Vlan-interface2 | Virtual Router 1:sending from 1.1.1.2, versio
n = 2, type = 1,priority = 120, count ip addrs = 1, timer = 1, auth
type is no, checksum = 61725
```

Enable debugging for sending and receiving all VRRP packets on Vlan-interface3.

```
<Sysname> debugging vrrp packet interface Vlan-interface 3
*0.715203 router b VRRP/7/DebugPacket:
IPv4 Vlan-interface3 | Virtual Router 1:sending from 2.2.2.3, versio
n = 2, type = 1,priority = 100, count ip addrs = 1, timer = 1, auth
type is no, checksum = 63245
```

Table 278 Field descriptions of the debugging vrrp packet command

Field	Description
interface-name (Vlan-interface2)	Specified interface to send or receive VRRP packets
VRID (Virtual Router 1)	Virtual standby group number corresponding to the state change
Packet Action (receiving from)	VRRP packets sent or received
IpAddress (1.1.1.3)	IP address of the sending interface
version	VRRP version number, with that of IPv4 being version 2 and that of IPv6 being version 3
type	Type of the VRRP packet. Only one VRRP packet type is present, that is, VRRP advertisement.
priority	Priority of the switch sending VRRP packets in the virtual standby group
count ip addrs	Number of IP addresses contained in the virtual standby group
timer	Interval for sending advertisements
auth type	Authentication type for the virtual standby group
checksum	16-bit checksum

debugging vrrp state

Syntax **debugging vrrp state**

undo debugging vrrp state

View User view

Parameters None

Description Use the **debugging vrrp state** command to enable VRRP state debugging.

Use the **undo debugging vrrp state** command to disable VRRP state debugging.

By default, VRRP state debugging is disabled.

Examples # Enable VRRP state debugging.

```
<Sysname> debugging vrrp state
*0.982485 router a VRRP/7/DebugState:
IPv4 Vlan-interface2 | Virtual Router 1 :  BACKUP --> INITIALIZE
```

Table 279 Field descriptions of the debugging vrrp state command

Field	Description
interface-name (Vlan-interface2)	Interface to which the standby group in state change belongs
VRID (Virtual Router 1)	Virtual standby group number corresponding to the state change
state change (BACKUP --> INITIALIZE)	Standby group state change information, indicating state change from backup to initialize in this example

display vrrp

Syntax **display vrrp** [**verbose**] [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]

View Any view

Parameters **verbose:** Displays detailed state information of VRRP.

interface *interface-type interface-number*: Displays VRRP state information of the specified interface. *interface-type interface-number* specifies an interface by its type and number.

vrid *virtual-router-id*: Displays state information of the specified VRRP group. *virtual-router-id* specifies a standby group by its group number.

Description Use the **display vrrp** command to display the state information of VRRP.

If you do not specify **verbose**, only the brief state information of VRRP is displayed.

If you specify both interface and standby group, only the state information of the specified standby group is displayed; if you only specify an interface, the state information of all the standby groups on the interface is displayed; if you specify neither, the state information of all the standby groups on the device is displayed.

Examples # Display brief information about all standby groups on the device.

```
<Sysname> display vrrp verbose
IPv4 Standby Information:
 Run Method      : VIRTUAL-MAC
 Virtual IP Ping : Enable
 Interface       : Vlan-interface100
 VRID            : 1                    Adver. Timer    : 1
 Admin Status    : UP                   State           : Master
 Config Pri      : 100                  Run Pri         : 100
 Preempt Mode    : YES                  Delay Time      : 0
 Auth Type       : NONE
 Track IF        : Vlan-interface200    Pri Reduced     : 10
 Virtual IP      : 10.10.10.2
 Virtual MAC     : 0000-5e00-0101
 Master IP       : 10.10.10.1
```

Table 280 Field descriptions of the display vrrp command

Field	Description
Run Method	Current VRRP running mode, real MAC or virtual MAC
Virtual IP Ping	Whether you can ping the virtual IP address of the standby group
Interface	Interface to which the standby group belongs
VRID	Number of the standby group
Adver. Timer	VRRP advertisement interval
Admin Status	Administrative state: UP or DOWN
State	Status of the switch in the standby group, master, backup, or initialize
Config Pri	Configured priority
Run Pri	Running priority
Preempt Mode	Preemption mode
Delay Time	Preemption delay
Auth Type	Authentication type
Track IF	The interface to be tracked. It is displayed only after the execution of the **vrrp vrid track** command.
Pri Reduced	The priority value that is reduced when the interface being tracked is down. It is displayed only after the execution of the **vrrp vrid track** command.
Virtual IP	Virtual IP addresses of the standby group
Virtual MAC	Virtual MAC address corresponding to the virtual IP address of the standby group. It is displayed only when the switch is in the state of master.
Master IP	Primary IP address of the interface to which the switch in the state of master belongs

display vrrp statistics

Syntax **display vrrp statistics** [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]

View Any view

Parameters **interface** *interface-type interface-number*: Displays VRRP statistics of the specified interface. *interface-type interface-number* specifies an interface by its type and number.

vrid *virtual-router-id*: Displays statistics of the specified VRRP group. *virtual-router-id* specifies a standby group by its group number.

Description Use the **display vrrp statistics** command to display statistics about VRRP.

If you specify both interface and standby group, only the statistics about the specified standby group are displayed; if you only specify an interface, the statistics about all the standby groups on the interface are displayed; if you specify neither, the statistics about all the standby groups on the device are displayed.

Examples # Display the statistics about all standby groups.

```
<Sysname> display vrrp statistics
Interface              : Vlan-interface100
 VRID                  : 1
 Version               : 2
 CheckSum Errors       : 16         Version Errors                : 0
 Invalid Type Pkts Rcvd : 0         Advertisement Interval Errors : 0
 IP TTL Errors         : 0          Auth Failures                 : 0
 Invalid Auth Type     : 0          Auth Type Mismatch            : 0
 Packet Length Errors  : 0          Address List Errors           : 0
 Become Master         : 1          Priority Zero Pkts Rcvd       : 0
 Advertise Rcvd        : 16         Priority Zero Pkts Sent       : 0
 Advertise Sent        : 40
 Interface             : Vlan-interface200
 VRID                  : 105
 Version               : 2
 CheckSum Errors       : 0          Version Errors                : 0
 Invalid Type Pkts Rcvd : 0         Advertisement Interval Errors : 0
 IP TTL Errors         : 0          Auth Failures                 : 0
 Invalid Auth Type     : 0          Auth Type Mismatch            : 0
 Packet Length Errors  : 0          Address List Errors           : 0
 Become Master         : 0          Priority Zero Pkts Rcvd       : 0
 Advertise Rcvd        : 0          Priority Zero Pkts Sent       : 0
 Advertise Sent        : 30
Global statistics
 CheckSum Errors       : 16
 Version Errors        : 0
 VRID Errors           : 20
```

Table 281 Field descriptions of the display vrrp statistics command

Field	Description
Interface	Interface to which the standby group belongs
VRID	Number of the standby group
Version	VRRP version
CheckSum Errors	Number of packets with checksum errors
Version Errors	Number of packets with version errors
Invalid Type Pkts Rcvd	Number of packets with incorrect packet type
Advertisement Interval Errors	Number of packets with advertisement interval errors
IP TTL Errors	Number of packets with TTL errors
Auth Failures	Number of packets with authentication failures
Invalid Auth Type	Number of packets with authentication failures due to invalid authentication types
Auth Type Mismatch	Number of packets with authentication failures due to mismatching authentication types
Packet Length Errors	Number of packets with VRRP packet length errors
Address List Errors	Number of packets with virtual IP address list errors
Become Master	Number of times that the switch worked as the master
Priority Zero Pkts Rcvd	Number of received advertisements with the priority of 0

Table 281 Field descriptions of the display vrrp statistics command

Field	Description
Advertise Rcvd	Number of received advertisements
Advertise Sent	Number of advertisements sent
Global statistics	Statistics about all standby groups
CheckSum Errors	Total number of packets with checksum errors
Version Errors	Total number of packets with version errors
VRID Errors	Total number of packets with VRID errors

reset vrrp statistics

Syntax **reset vrrp statistics** [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]

View User view

Parameters **interface** *interface-type interface-number*: Clears VRRP statistics of a specified interface. *interface-type interface-number* specifies an interface by its type and number.

vrid *virtual-router-id*: Clears VRRP statistics of the specified standby group. *virtual-router-id* specifies a standby group by its group number.

Description Use the **reset vrrp statistics** command to clear VRRP statistics.

If you specify both the interface and standby group, the statistics about the specified standby group on the specified interface are cleared; if you specify only the interface, the statistics about all the standby groups on the interface are cleared; if you specify neither, the statistics about all the standby groups on the device are cleared.

Examples # Clear the statistics about all the standby groups on the device.

```
<Sysname> reset vrrp statistics
```

vrrp vrid authentication-mode

Syntax **vrrp vrid** *virtual-router-id* **authentication-mode** { **md5** | **simple** } *key*

undo vrrp vrid *virtual-router-id* **authentication-mode**

View VLAN interface view

Parameters **simple**: Plain text authentication mode.

md5: Authentication header (AH) authentication using the MD5 algorithm.

key: Authentication key, case sensitive. When **simple** authentication applies, the authentication key is in plain text with a length of 1 to 8 characters. When **md5** authentication applies, the authentication key is in MD5 cipher text or in plain text and the length of the key depends on its input format. If the key is input in plain text, its length is 1 to 8 characters, such as 1234567; if the key is input in ciphertext, its length must be 24 characters, such as _(TT8F]Y5SQ=^Q‘MAF4<1!!.

Description Use the **vrrp vrid authentication-mode** command to configure authentication mode and authentication key for the VRRP standby groups to send and receive VRRP packets.

Use the **undo vrrp vrid authentication-mode** command to restore the default.

By default, authentication is disabled.

Note that:

- Before executing the command, create a standby group on an interface and configure the virtual IP address of the standby group.
- You may configure different authentication types and authentication keys for the standby groups on an interface. However, the members of the same standby group must use the same authentication mode and authentication key.

Examples # Set the authentication mode and authentication key for VRRP standby group 1 on interface Vlan-interface2 to send and receive VRRP packets.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.1
[Sysname-Vlan-interface2] vrrp vrid 1 authentication-mode simple Sysname
```

vrrp method

Syntax **vrrp method** { **real-mac** | **virtual-mac** }

undo vrrp method

View System view

Parameters **real-mac**: Associates the real MAC address of the interface with the virtual IP address of the standby group.

virtual-mac: Associates the virtual MAC address with the virtual IP address of the standby group.

Description Use the **vrrp method** command to set the mappings between the MAC addresses and the virtual IP addresses of the standby groups.

Use the **undo vrrp method** command to restore the default.

By default, the virtual MAC address of the standby group is associated with the virtual IP address.

Note that you must configure the mapping between the virtual MAC address and the virtual IP address before configuring a standby group. Otherwise, your configuration will fail.

Examples # Associate the virtual IP address of the standby group with the real MAC address of the interface.

```
<Sysname> system-view
[Sysname] vrrp method real-mac
```

vrrp ping-enable

Syntax **vrrp ping-enable**

undo vrrp ping-enable

View System view

Parameters None

Description Use the **vrrp ping-enable** command to enable users to ping the virtual IP addresses of standby groups.

Use the **undo vrrp ping-enable** command to disable the virtual IP addresses of standby groups from being pinged.

By default, the virtual IP addresses of standby groups can be pinged.

Perform this configuration before configuring a standby group.

Examples # Enable users to ping the virtual IP addresses of standby groups.

```
<Sysname> system-view
[Sysname] vrrp ping-enable
```

vrrp un-check ttl

Syntax **vrrp un-check ttl**

undo vrrp un-check ttl

View VLAN interface view

Parameters None

Description Use the **vrrp un-check ttl** command to disable TTL check on VRRP packets.

Use the **undo vrrp un-check ttl** command to enable TTL check on VRRP packets.

By default, TTL check on VRRP packets is enabled.

Note that:

Before executing the command, create a standby group on an interface and configure the virtual IP address of the standby group.

Examples # Disable TTL check on VRRP packets.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.1
[Sysname-Vlan-interface2] vrrp un-check ttl
```

vrrp vrid preempt-mode

Syntax **vrrp vrid** *virtual-router-id* **preempt-mode** [**timer delay** *delay-value*]

undo vrrp vrid *virtual-router-id* **preempt-mode** [**timer delay**]

View VLAN interface view

Parameters *virtual-router-id*: VRRP standby group number.

timer delay: Sets preemption delay. In preemption mode, if you configure a preemption delay, the standby group member in the backup state will wait for the specified period of time before becoming the master.

delay-value: Preemption delay, in seconds. In preemption mode, if *delay-value* is configured, the Backup becomes the Master in *delay-value* time. It defaults to 0 seconds.

Description Use the **vrrp vrid preempt-mode** command to enable preemption on the switch and configure its preemption delay in the specified standby group.

Use the **undo vrrp vrid preempt-mode** command to disable preemption on the switch in the specified standby group.

Use the **undo vrrp vrid preempt-mode timer delay** command to restore the default preemption delay, that is, zero seconds.

The default mode is immediate preemption without delay.

On an instable network, the standby group member in the backup state may not normally receive the packets from the master member due to network congestion, resulting in frequent master/backup state transition of the standby group members. Preemption delay is introduced to solve this problem. With a preemption delay set, if the backup member does not receive the packet from the master member duly, it waits for a period to see whether it can receive any packet from the master. If the specified period elapses but it still receives no packet from the master, it becomes the master.

Note that:

- Before executing the command, create a standby group on an interface and configure the virtual IP address of the standby group.
- If the switch in the standby group works in non-preemption mode, the delay period changes to zero seconds automatically.

Examples # Enable preemption on the switch in VRRP standby group 1, and set the preemption delay to five seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5
```

vrrp vrid priority

Syntax **vrrp vrid** *virtual-router-id* **priority** *priority-value*

undo vrrp vrid *virtual-router-id* **priority**

View VLAN interface view

Parameters *virtual-router-id*: VRRP standby group number.

priority-value: Priority value of the switch in the specified standby group, with a higher number indicating a higher priority.

Description Use the **vrrp vrid priority** command to configure the priority of the switch in the specified standby group.

Use the **undo vrrp vrid priority** command to restore the default.

By default, the priority of a switch in a standby group is 100.

- Before executing the command, create a standby group on an interface and configure the virtual IP address of the standby group.
- In VRRP, the role that a switch plays in a standby group depends on its priority. A higher priority means that the switch is more likely to become the master. Note that priority 0 is reserved for special use and 255 for the IP address owner.
- If the switch is the IP address owner, its priority is always 255. Therefore, it will be the master so long as it is functioning normally.

Examples # Set the priority of standby group 1 on interface Vlan-interface2 to 150.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.1
[Sysname-Vlan-interface2] vrrp vrid 1 priority 150
```

vrrp vrid timer advertise

Syntax **vrrp vrid** *virtual-router-id* **timer advertise** *adver-interval*

undo vrrp vrid *virtual-router-id* **timer advertise**

View VLAN interface view

Parameters *virtual-router-id*: VRRP standby group number.

adver-interval: Interval at which the master in the specified standby group sends VRRP advertisements. It ranges from 1 to 255 seconds.

Description Use the **vrrp vrid timer advertise** command to configure the Adver_Timer of the specified standby group.

Use the **undo vrrp vrid timer advertise** command to restore the default.

By default the Adver_Timer is 1 second.

The Adver_Timer controls the interval at which the master sends VRRP packets.

Note that:

- Before executing the command, create a standby group on an interface and configure the virtual IP address of the standby group.
- Switches in the same VRRP standby group must use the same Adver_Timer setting.

Examples # Set the master in standby group 1 to send VRRP advertisements at intervals of five seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.1
[Sysname-Vlan-interface2] vrrp vrid 1 timer advertise 5
```

vrrp vrid track

Syntax **vrrp vrid** *virtual-router-id* **track interface** *interface-type interface-number* [**reduced** *priority-reduced*]

undo vrrp vrid *virtual-router-id* **track** [**interface** *interface-type interface-number*]

View VLAN interface view

Parameters *virtual-router-id*: VRRP standby group number.

interface-type interface-number: Specifies an interface to be tracked by its type and number.

priority-reduced: Value by which the priority decrements. If it is not specified, the default 10 applies.

Description Use the **vrrp vrid track** command to configure to track the specified interface.

Use the **undo vrrp vrid track** command to disable tracking the specified interface.

By default, no interface is being tracked.

Note that:

- Before executing the command, create a standby group on an interface and configure the virtual IP address of the standby group.
- When the switch is the owner of the IP address, you cannot perform the configuration.
- When the status of the tracked interface turns from down to up, the corresponding switch restores its priority automatically.
- At present, the interface specified in this command can only be a VLAN interface for Switch 8800s.

Examples # On interface Vlan-interface2, set the interface to be tracked as Vlan-interface1, making the priority of standby group 1 on interface Vlan-interface2 decrement by 50 when Vlan-interface1 goes down.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.1
[Sysname-Vlan-interface2] vrrp vrid 1 track interface vlan-interface
 1 reduced 50
```

vrrp vrid virtual-ip

Syntax **vrrp vrid** *virtual-router-id* **virtual-ip** *virtual-address*

undo vrrp vrid *virtual-router-id* [**virtual-ip** *virtual-address*]

View VLAN interface view

Parameters *virtual-router-id*: VRRP standby group number.

virtual-address: Virtual IP address.

Description Use the **vrrp vrid virtual-ip** command to create a standby group the first time that you add a virtual IP address or add a virtual IP address to it after that.

Use the **undo vrrp vrid** *virtual-router-id* command to remove a standby group.

Use the **undo vrrp vrid** *virtual-router-id* **virtual-ip** *virtual-address* command to remove a virtual IP address from a standby group.

By default, no standby group is created.

Note that:

- The system removes a standby group after you delete all the virtual IP addresses in it.
- The virtual IP address of the standby group cannot be 0.0.0.0, 255.255.255.255, loopback address, non A/B/C address and other illegal IP addresses such as 0.0.0.1.
- Only when the configured virtual IP address and the interface IP address belong to the same segment and are legal host addresses can the standby group operate normally; otherwise. the state of the standby group is always **Initialize**.

Examples # Create standby group 1 and set its virtual IP address to 10.10.10.10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp vrid 1 virtual-ip 10.10.10.10
```

56 IPv6-Based VRRP Configuration Commands

debugging vrrp ipv6 packet

Syntax **debugging vrrp ipv6 packet** [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]

undo debugging vrrp ipv6 packet [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]

View User view

Parameters **interface** *interface-type interface-number:* Enables packet debugging for a specified interface, where *interface-type* indicates the interface type and *interface-number* indicates the interface number.

vrid *virtual-router-id*: Enables packet debugging for a standby group on a specified interface, where *virtual-router-id* indicates the standby group ID.

Description Use the **debugging vrrp ipv6 packet** command to enable debugging for sending and receiving VRRP packets.

Use the **undo debugging vrrp ipv6 packet** command to disable debugging for sending and receiving VRRP packets.

By default, debugging for sending and receiving VRRP packets is disabled.

Note that

Examples # Enable debugging for sending and receiving VRRP packets and debug all packets received on and sent from all the virtual standby groups on the device.

```
<Sysname> debugging vrrp ipv6 packet
<Sysname> terminal debugging
0.7344453 Sysname-wvrp VRRP/7/DebugPacket:

 IPv6 Vlan-interface2 | Virtual Router 10:receiving from FE80::2, ve
rsion = 3, type = 1, priority = 100, count ip addrs = 1, timer = 100
, auth type is simple text, checksum = 34932
```

Enable debugging for sending and receiving all VRRP packets on Vlan-interface3.

```
<Sysname> debugging vrrp ipv6 packet interface Vlan-interface 2
*0.7501140 Sysname-wvrp VRRP/7/DebugPacket:
```

```
 IPv6 Vlan-interface2 | Virtual Router 10:receiving from FE80::2, ve
rsion = 3, type = 1, priority = 100, count ip addrs = 1, timer = 100
, auth type is simple text, checksum = 34932
```

Table 282 Field descriptions of the debugging vrrp ipv6 packet command

Field	Description
interface-name (Vlan-interface2)	Specified interface to send or receive VRRP packets
VRID (Virtual Router 1)	Virtual standby group number corresponding to the state change
Packet Action (receiving from)	VRRP packets sent or received
IpAddress (fe80::7)	IPv6 address of the sending interface
version	VRRP version number, with that of IPv4 being version 2 and that of IPv6 being version 3
type	Type of the VRRP packet. Only one VRRP packet type is present, that is, VRRP advertisement.
priority	Priority of the switch sending VRRP packets in the virtual standby group
count ip addrs	Number of IPv6 addresses contained in the virtual standby group
timer	Interval for sending advertisement packets
auth type	Authentication type for the virtual standby group
checksum	16-bit checksum

debugging vrrp ipv6 state

Syntax **debugging vrrp ipv6 state**

undo debugging vrrp ipv6 state

View User view

Parameters None

Description Use the **debugging vrrp ipv6 state** command to enable VRRP state debugging.

Use the **undo debugging vrrp ipv6 state** command to disable VRRP state debugging.

By default, VRRP state debugging is disabled.

Examples # Enable VRRP state debugging.

```
<Sysname> debugging vrrp ipv6 state
*0.7757984 Sysname-wvrp VRRP/7/DebugState:
 IPv6 Vlan-interface2 | Virtual Router 10 :  BACKUP --> MASTER
```

Table 283 Field descriptions of the debugging vrrp ipv6 state command

Field	Description
interface-name (Vlan-interface2)	Interface to which the standby group in state change belongs

Table 283 Field descriptions of the debugging vrrp ipv6 state command

Field	Description
VRID (Virtual Router 1)	Virtual standby group number corresponding to the state change
state change (BACKUP --> INITIALIZE)	Standby group state change information, indicating state change from backup to initialize in this example

display vrrp ipv6

Syntax **display vrrp ipv6** [**verbose**] [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]

View Any view

Parameters **verbose:** Displays detailed state information of VRRP.

interface *interface-type interface-number*: Displays VRRP state information of the specified interface. *interface-type interface-number* specifies an interface by its type and number.

vrid *virtual-router-id*: Displays state information of the specified VRRP group. *virtual-router-id* specifies a standby group by its group number.

Description Use the **display vrrp ipv6** command to display the state information of VRRP for IPv6.

If you do not specify **verbose**, only the brief state information of VRRP is displayed.

If you specify both interface and standby group, only the state information of the specified standby group is displayed; if you only specify an interface, the state information of all the standby groups on the interface is displayed; if you specify neither, the state information of all the standby groups on the device is displayed.

Examples # Display detailed information about all standby groups on the device.

```
<Sysname>display vrrp ipv6 verbose
IPv6 Standby Information:
 Run Method      : VIRTUAL-MAC
 Virtual IP Ping : Enable
 Interface       : Vlan-interface100
 VRID            : 1                    Adver. Timer    : 100
 Admin Status    : UP                   State           : Master
 Config Pri      : 100                  Run Pri         : 100
 Preempt Mode    : YES                  Delay Time      : 0
 Auth Type       : NONE
 Track IF        : Vlan-interface200    Pri Reduced     : 10
 Virtual IP      : FE80::1
 Virtual MAC     : 0000-5e00-0201
 Master IP       : FE80::20F:E2FF:FE49:8060
```

Table 284 Field descriptions of the display vrrp ipv6 command

Field	Description
Run Method	Current VRRP running mode, real MAC or virtual MAC
Virtual IP Ping	Whether you can ping the virtual IPv6 address
Interface	Interface to which the standby group belongs
VRID	Number of the standby group
Adver. Timer	VRRP advertisement interval in centiseconds
Admin Status	Administrative state: UP or DOWN
State	Status of the switch in the standby group, master, backup, or initialize
Virtual IP	Virtual IPv6 address
Config Pri	Configured priority
Run Pri	Running priority
Preempt Mode	Preemption mode
Delay Time	Preemption delay
Auth Type	Authentication type
Track IF	The interface to be tracked. It is displayed only after the execution of the **vrrp ipv6 vrid track** command.
Pri Reduced	The priority value that is reduced when the interface being tracked is down. It is displayed only after the execution of the **vrrp ipv6 vrid track** command.
Virtual IP	Virtual IPv6 addresses of the standby group
Virtual MAC	Virtual MAC address corresponding to the virtual IPv6 address of the standby group. It is displayed only when the switch is in the state of master.
Master IP	Primary IPv6 address of the interface to which the switch in the state of master belongs

display vrrp ipv6 statistics

Syntax **display vrrp ipv6 statistics** [**interfac**e *interface-type interface-number* [**vrid** *virtual-router-id*]]

View Any view

Parameters **interface** *interface-type interface-number*: Displays VRRP statistics information of the specified interface. *interface-type interface-number* specifies an interface by its type and number.

vrid *virtual-router-id*: Displays statistics information of the specified VRRP group. *virtual-router-id* specifies a standby group by its group number.

Description Use the **display vrrp ipv6 statistics** command to display statistics about VRRP for IPv6.

If you specify both interface and standby group, only the statistics about the specified standby group are displayed; if you only specify an interface, the statistics about all the standby groups on the interface are displayed; if you specify neither, the statistics about all the standby groups on the device are displayed.

Examples # Display the statistics about all standby groups for IPv6.

```
<Sysname> display vrrp ipv6 statistics
 Interface              : Vlan-interface100
 VRID                   : 80
 Version                : 3
 CheckSum Errors        : 0          Version Errors                 : 0
 Invalid Type Pkts Rcvd : 0          Advertisement Interval Errors  : 0
 Hot Limit Errors       : 0          Auth Failures                  : 0
 Invalid Auth Type      : 0          Auth Type Mismatch             : 0
 Packet Length Errors   : 0          Address List Errors            : 0
 Become Master          : 1          Priority Zero Pkts Rcvd        : 0
 Advertise Rcvd         : 0          Priority Zero Pkts Sent        : 0
 Advertise Sent         : 20

 Interface              : Vlan-interface200
 VRID                   : 10
 Version                : 3
 CheckSum Errors        : 0          Version Errors                 : 0
 Invalid Type Pkts Rcvd : 0          Advertisement Interval Errors  : 0
 Hot Limit Errors       : 0          Auth Failures                  : 0
 Invalid Auth Type      : 0          Auth Type Mismatch             : 0
 Packet Length Errors   : 0          Address List Errors            : 0
 Become Master          : 1          Priority Zero Pkts Rcvd        : 0
 Advertise Rcvd         : 0          Priority Zero Pkts Sent        : 0
 Advertise Sent         : 30

 Global statistics
 CheckSum Errors        : 0
 Version Errors         : 0
 VRID Errors            : 1439
```

Table 285 Field descriptions of the display vrrp ipv6 statistics command

Field	Description
Interface	Interface to which the standby group belongs
VRID	Number of the standby group
Version	VRRP version
CheckSum Errors	Number of packets with checksum errors
Version Errors	Number of packets with version errors
Invalid Type Pkts Rcvd	Number of packets with incorrect packet type
Advertisement Interval Errors	Number of packets with advertisement interval errors
Hot Limit Errors	Number of packets with Hot Limit errors
Auth Failures	Number of packets with authentication failures
Invalid Auth Type	Number of packets with authentication failures due to invalid authentication types
Auth Type Mismatch	Number of packets with authentication failures due to mismatching authentication types
Packet Length Errors	Number of packets with VRRP packet length errors
Address List Errors	Number of packets with virtual IPv6 address list errors

Table 285 Field descriptions of the display vrrp ipv6 statistics command

Field	Description
Become Master	Number of times that the switch worked as the master
Priority Zero Pkts Rcvd	Number of received advertisements with the priority of 0
Advertise Rcvd	Number of received advertisements
Advertise Sent	Number of advertisements sent
Global statistics	Statistics about all standby groups
CheckSum Errors	Total number of packets with checksum errors
Version Errors	Total number of packets with version errors
VRID Errors	Total number of packets with VRID errors

reset vrrp ipv6 statistics

Syntax **reset vrrp ipv6 statistics** [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]

View User view

Parameters **interface** *interface-type interface-number*: Clears VRRP statistics of a specific interface. *interface-type interface-number* specifies an interface by its type and number.

vrid *virtual-router-id*: Clears VRRP statistics of the specified standby group. *virtual-router-id* specifies a standby group by its group number, in the range 1 to 255.

Description Use the **reset vrrp ipv6 statistics** command to clear VRRP statistics.

If you specify both the interface and standby group, the statistics about the specified standby group on the specified interface are cleared; if you specify only the interface, the statistics about all the standby groups on the interface are cleared; if you specify neither, the statistics about all the standby groups on the device are cleared.

Examples # Clear the statistics about all the standby groups on the device.

```
<Sysname> reset vrrp ipv6 statistics
```

vrrp ipv6 vrid authentication-mode

Syntax **vrrp ipv6 vrid** *virtual-router-id* **authentication-mode simple** *key*

undo vrrp ipv6 vrid *virtual-router-id* **authentication-mode**

View VLAN interface view

Parameters *virtual-router-id*: VRRP standby group number, in the range 1 to 255.

simple: Sets the authentication mode to plain text authentication.

key: Authentication key of 1 to 8 case-sensitive characters in plain text.

Description Use the **vrrp ipv6 vrid** *virtual-router-id* **authentication-mode simple** *key* command to configure authentication mode and authentication key for the VRRP standby groups to send and receive VRRP packets.

Use the **undo vrrp ipv6 vrid** *virtual-router-id* **authentication-mode** command to restore the default.

By default, authentication is disabled.

Note that:

- Before executing the command, create a standby group on an interface and configure the virtual IP address of the standby group.
- You may configure different authentication types and authentication keys for the standby groups on an interface. However, the members of the same standby group must use the same authentication mode and authentication key.

Examples # Set the authentication mode and authentication key for VRRP standby group 10 on interface Vlan-interface2 to send and receive VRRP packets.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp ipv6 vrid 10 virtual-ip fe80::2 link-local
[Sysname-Vlan-interface2]vrrp ipv6 vrid 10 authentication-mode simple test
```

vrrp ipv6 method

Syntax **vrrp ipv6 method** { **real-mac** | **virtual-mac** }

undo vrrp ipv6 method

View System view

Parameters **real-mac**: Associates the real MAC address of the interface with the virtual IPv6 address of the standby group.

virtual-mac: Associates the virtual MAC address with the virtual IPv6 address of the standby group.

Description Use the **vrrp ipv6 method** command to set the mappings between the MAC addresses and the virtual IPv6 addresses of the standby groups.

Use the **undo vrrp ipv6 method** command to restore the default mapping.

By default, the virtual MAC address of the standby group is associated with the virtual IP address.

Configure the mapping between the virtual MAC address and the virtual IPv6 address before configuring a standby group. Otherwise, your configuration will fail.

Examples # Associate the virtual IP address of the standby group with the real MAC address of the routing interface.

```
<Sysname> system-view
[Sysname] vrrp ipv6 method real-mac
```

vrrp ipv6 ping-enable

Syntax **vrrp ipv6 ping-enable**

undo vrrp ipv6 ping-enable

View System view

Parameters None

Description Use the **vrrp ipv6 ping-enable** command to enable users to ping the virtual IPv6 addresses of standby groups.

Use the **undo vrrp ipv6 ping-enable** command to disable the virtual IPv6 addresses of standby groups from being pinged.

By default, the virtual IP addresses of standby groups can be pinged.

Perform this configuration before configuring a standby group.

Examples # Enable users to ping the virtual IPv6 addresses of standby groups.

```
<Sysname> system-view
[Sysname] vrrp ipv6 ping-enable
```

vrrp ipv6 vrid preempt-mode

Syntax **vrrp ipv6 vrid** *virtual-router-id* **preempt-mode** [**timer delay** *delay-value*]

undo vrrp ipv6 vrid *virtual-router-id* **preempt-mode** [**timer delay**]

View VLAN interface view

Parameters *virtual-router-id*: Virtual router ID or VRRP standby group number.

timer delay: Sets preemption delay. In preemption mode, if you configure a preemption delay, the standby group member in the backup state will wait for the specified period of time before becoming the master.

delay-value: Preemption delay, in seconds. In preemption mode, if *delay-value* is configured, the Backup becomes the Master in *delay-value* time. It defaults to 0 seconds.

Description Use the **vrrp ipv6 vrid preempt-mode** command to configure preemption on the switch and configure its preemption delay in the specified standby group.

Use the **undo vrrp ipv6 vrid preempt-mode** command to disable preemption on the router in the specified standby group.

Use the **undo vrrp ipv6 vrid preempt-mode timer delay** command to restore the default preemption delay, that is, zero seconds.

The default mode is immediate preemption without delay.

If you set the router in the standby group to work in non-preemption mode, the delay period changes to zero seconds automatically.

On an instable network, the standby group member in the backup state may not normally receive the packets from the master member due to network congestion, resulting in frequent master/backup state transition of the standby group members. Preemption delay is introduced to solve this problem. With a preemption delay set, if the backup member does not receive the packet from the master member duly, it waits for a period to see whether it can receive any packet from the master. If the specified period elapses but it still receives no packet from the master, it becomes the master.

Note that:

- Before executing the command, create a standby group on an interface and configure the virtual IPv6 address of the standby group.
- If the switch in the standby group works in non-preemption mode, the delay period changes to zero seconds automatically.

Examples # Enable preemption on the device and set the preemption delay to five seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp ipv6 vrid 80 virtual-ip fe80::2 link-local
[Sysname-Vlan-interface2] vrrp ipv6 vrid 80 preempt-mode timer delay 5
```

vrrp ipv6 vrid priority

Syntax **vrrp ipv6 vrid** *virtual-router-id* **priority** *priority-value*

undo vrrp ipv6 vrid *virtual-router-id* **priority**

View VLAN interface view

Parameters *virtual-router-id*: VRRP standby group number.

priority-value: Priority value of the router in the specified standby group, with a higher number indicating a higher priority.

Description Use the **vrrp ipv6 vrid priority** command to configure the priority of the switch in the specified standby group.

Use the **undo vrrp ipv6 vrid priority** command to restore the default.

By default, the priority of a switch in a standby group is 100.

- Before executing the command, create a standby group on an interface and configure the virtual IPv6 address of the standby group.
- In VRRP, the role that a switch plays in a standby group depends on its priority. A higher priority means that the switch is more likely to become the master. Note that priority 0 is reserved for special use and 255 for the IP address owner.
- If the switch is the IP address owner, its priority is always 255. Therefore, it will be the master so long as it is functioning normally.

Examples # Set the priority of standby group 1 on interface Vlan-interface2 to 150.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::2 link-local
[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 priority 150
```

vrrp ipv6 vrid timer advertise

Syntax **vrrp ipv6 vrid** *virtual-router-id* **timer advertise** *adver-interval*

undo vrrp ipv6 vrid *virtual-router-id* **timer advertise**

View VLAN interface view

Parameters *virtual-router-id*: VRRP standby group number.

adver-interval: Interval at which the master in the specified standby group sends VRRP advertisements, in centiseconds.

Description Use the **vrrp ipv6 vrid timer advertise** command to configure the Adver_Timer of the specified standby group.

Use the **undo vrrp ipv6 vrid timer advertise** command to restore the default.

By default the Adver_Timer is 100 centiseconds.

The Adver_Timer controls the interval at which the master sends VRRP packets.

- Before executing the command, create a standby group on an interface and configure the virtual IPv6 address of the standby group.
- Routers in the same VRRP standby group must use the same Adver_Timer setting.

Examples # Set the master in standby group 1 to send VRRP advertisements at intervals of 500 centiseconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::2 link-local
[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 timer advertise 500
```

vrrp ipv6 vrid track

Syntax **vrrp ipv6 vrid** *virtual-router-id* **track interface** *interface-type interface-number* [**reduced** *priority-reduced*]

undo vrrp ipv6 vrid *virtual-router-id* **track** [**interface** *interface-type interface-number*]

View VLAN interface view

Parameters *virtual-router-id*: VRRP standby group number.

interface *interface-type interface-number*: Specifies an interface by its type and number.

priority-reduced: Value by which the priority decrements. If it is not specified, the default 10 applies.

Description Use the **vrrp ipv6 vrid track** command to configure to track the specified interface.

Use the **undo vrrp ipv6 vrid track** command to disable tracking the specified interface.

By default, no interface is being tracked.

Note that:

- Before executing the command, create a standby group on an interface and configure the virtual IPv6 address of the standby group.
- When the switch is the owner of the IP address, you cannot perform the configuration.
- When the status of the tracked interface turns from down to up, the corresponding switch restores its priority automatically.
- At present, the interface specified in this command can only be a VLAN interface for Switch 8800s.

Examples # On interface Vlan-interface2, set the interface to be tracked as Vlan-interface1, making the priority of standby group 1 on interface Vlan-interface2 decrement by 50 when Vlan-interface1 goes down.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
```

```
[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 track interface vlan-inte
rface 1 reduced 50
```

vrrp ipv6 vrid virtual-ip

Syntax **vrrp ipv6 vrid** *virtual-router-id* **virtual-ip** *virtual-address* [**link-local**]

undo vrrp ipv6 vrid *virtual-router-id* [**virtual-ip** *virtual-address* [**link-local**]]

View VLAN interface view

Parameters *virtual-router-id*: VRRP standby group number.

virtual-address: Virtual IPv6 address.

link-local: Indicates that the virtual IPv6 address of the standby group is a link local address.

Description Use the **vrrp ipv6 vrid virtual-ip link-local** command to create a standby group and assign the first virtual IPv6 address to the specified standby group. The first virtual IPv6 address assigned to a standby group must be a link local address and only one such address is allowed in a standby group.

Use the **vrrp ipv6 vrid virtual-ip** command to add a virtual IPv6 address to a standby group.

Use the **undo vrrp ipv6 vrid** command to remove a standby group.

Use the **undo vrrp ipv6 vrid** *virtual-router-id* **virtual-ip** *virtual-address* [**link-local**] command to remove a virtual IPv6 address from a standby group.

After you remove all virtual IPv6 addresses, the standby group is automatically removed. Note that the first address assigned to the group must be removed the last.

By default, no standby group is created.

Examples # Create standby group 1, and configure its virtual IPv6 address as fe80::10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
```

57 GR CONFIGURATION COMMANDS

enable link-local-signaling

Syntax **enable link-local-signaling**

undo enable link-local-signaling

View OSPF view

Parameters None

Description **Use the enable link-local-signaling command to enable the use of the Link-Local Signaling (LLC) in originated OSPF packets.**

Use the undo enable link-local-signaling command to disable the use of Link-Local Signaling in originated OSPF packets.

By default, the use of the Link-Local Signaling for OSPF is disabled.

Examples # Enable the Link-Local Signaling for OSPF process 1.

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] enable link-local-signaling
```

enable out-of-band-resynchronization

Syntax **enable out-of-band-resynchronization**

undo enable out-of-band-resynchronization

View OSPF view

Parameters None

Description **Use the enable out-of-band-resynchronization command to enable the use of out-of-band resynchronization (OOB-Resynch) in originated OSPF packets.**

Use the undo enable out-of-band-resynchronization command to disable the use of out-of-band resynchronization in originated OSPF packets.

By default, the use of out-of-band resynchronization is disabled.

*Enable the OSPF link-local signaling before enabling OSPF out-of-band resynchronization. Refer to the **enable link-local-signaling** command on page 973 for enabling link-local signaling of OSPF.*

Examples # Enable the out-of-band resynchronization for OSPF process 1.

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] enable link-local-signaling
[Sysname-ospf-1] enable out-of-band-resynchronization
```

graceful-restart (BGP view)

Syntax **graceful-restart**

undo graceful-restart

View BGP view

Parameters None

Description Use the **graceful-restart** command to enable BGP Graceful Restart Capability.

Use the **undo graceful-restart** command to disable BGP Graceful Restart Capability.

By default, BGP Graceful Restart Capability is disabled.

*A GR Restarter can still maintain its forwarding state in the address family it belongs and sends the End-of-RIB marker during execution of the **graceful-restart** command. However, during restart, the GR Restarter does not necessarily maintain its forwarding state.*

Examples # Enable Graceful Restart for BGP process 100.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] graceful-restart
```

graceful-restart (OSPF view)

Syntax **graceful-restart**

undo graceful-restart

View OSPF view

Parameters None

Description **Use the graceful-restart command to enable OSPF Graceful Restart Capability.**

Use the undo graceful-restart command to disable OSPF Graceful Restart Capability.

By default, OSPF Graceful Restart Capability is disabled.

Note that:

Before enabling GR Capability for OSPF, enable OSPF LLS (link local signaling) and OOB (out of band resynchronization) first.

Related commands: **enable link-local-signaling**, **enable out-of-band-resynchronization**.

Examples # Enable Graceful Restart for OSPF process 1.

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] enable link-local-signaling
[Sysname-ospf-1] enable out-of-band-resynchronization
[Sysname-ospf-1] graceful-restart
```

graceful-restart help

Syntax **graceful-restart help** { *acl-number* | **prefix** *prefix-list* }

View OSPF view

Parameters *acl-number*: The basic or advanced ACL number.

prefix *prefix-list*: The name of the specified address prefix list, in the range of 1 to 19 characters.

Description **Use the graceful-restart help command to configure for which OSPF neighbors the current device can serve as a GR Helper. (The routers can be specified by the ACL or the IP Prefix list.)**

By default, the device can serve as a GR Helper for any OSPF neighbor.

Note that:

Before executing this command, enable OSPF LLS (link local signaling) and OOB (out of band resynchronization) first.

Related commands: **enable link-local-signaling**, **enable out-of-band-resynchronization**.

Examples # Configure OSPF 1 to act as a GR Helper for OSPF neighbors defined in the ACL 2001 (supposing ACL 2001 has already existed).

```
<Sysname> system-view
[Sysname] ospf 1
```

```
[Sysname-ospf-1] enable link-local-signaling
[Sysname-ospf-1] enable out-of-band-resynchronization
[Sysname-ospf-1] graceful-restart help 2001
```

graceful-restart suppress-sa

Syntax **graceful-restart suppress-sa**

undo graceful-restart suppress-sa

View IS-IS view

Parameters None

Description **Use the graceful-restart suppress-sa command to set the SA (Suppress-Advertisement) bit during restart.**

Use the undo graceful-restart suppress-sa command to clear the SA bit.

By default, the SA bit is cleared during restart.

Note that:

- For a switch that has restarted its routing protocol, copies of LSPs generated by this router during the previous operation may still exist in the LSP databases of other switches in the network.
- Copies of LSPs in the LSP databases in other switches which may look "newer" than LSPs generated by the restarting switch after it initializes LSP fragment sequence numbers. This may result in temporary blackholes until new LSPs are regenerated and copies of them are flooded using higher sequence numbers upon completion of the restarting process.
- These blackholes can be avoided if the neighbors of the restarting switch suppress advertising the adjacency relationship with the restarting switch until the latter has flooded its latest LSPs.

Examples # Set the SA bit in Graceful Restart.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] graceful-restart suppress-sa
```

graceful-restart timer neighbor-liveness

Syntax **graceful-restart timer neighbor-liveness** *timer*

undo graceful-restart timer neighbor-liveness

View MPLS LDP view

Parameters *timer*: Specifies the LDP GR Helper life time, in seconds.

Description Use the **graceful-restart timer neighbor-liveness** command to configure the LDP GR Helper life time.

Use the **undo graceful-restart timer neighbor-liveness** command to restore the default GR Helper life time.

By default, the LDP GR Helper life time is 60 seconds.

To modify the GR Helper life time may cause the reestablishment of the original session. As a result, the LSP based on this session will be removed and needs to be rebuilt.

Examples # Configure the LDP Neighbor Liveliness Time as 100 seconds.

```
<Sysname> system-view
[Sysname] mpls ldp
[Sysname-mpls-ldp] graceful-restart timer neighbor-liveness 100
```

graceful-restart timer reconnect

Syntax **graceful-restart timer reconnect** *timer*

undo graceful-restart timer reconnect

View MPLS LDP view

Parameters *timer*: Specifies the FT Reconnect Time, in the range of 60 to 300 seconds.

Description Use the **graceful-restart timer reconnect** command to configure the FT Reconnect Time.

Use the **undo graceful-restart timer reconnect** command to restore the default FT Reconnect Time.

By default, the FT Reconnect Time is 300 seconds.

- *FT Reconnect Time defines the maximum time that the Stale label status will be preserved by the LSR after the TCP connection failure.*

- *To modify the FT Reconnect Time may cause the reestablishment of the original session. As a result, the LSP based on this session will be removed and needs to be rebuilt.*

Examples # Configure the FT Reconnect Time as 100 seconds.

```
<Sysname> system-view
[Sysname] mpls ldp
[Sysname-mpls-ldp] graceful-restart timer reconnect 100
```

graceful-restart timer recovery

Syntax **graceful-restart timer recovery** *timer*

undo graceful-restart timer recovery

View MPLS LDP view

Parameters *timer*: Specifies LDP Recovery Time, in the range 3 to 300 seconds.

Description Use the **graceful-restart timer recovery** command to configure the maximum Recovery Time.

Use the **undo graceful-restart timer recovery** command to restore the default Recovery Time.

By default, the LDP Recovery Time is 300 seconds.

- *Recovery time defines the maximum time that the Stale label state will be kept by LSR after a TCP reconnection.*
- *To modify the Recovery time may cause the reestablishment of the original session. As a result, the LSP based on this session will be removed and needs to be rebuilt.*

Examples # Configure the Recovery time as 45 seconds.

```
<Sysname> system-view
[Sysname] mpls ldp
[Sysname-mpls-ldp] graceful-restart timer recovery 45
```

graceful-restart timer restart

Syntax **graceful-restart timer restart** *timer*

undo graceful-restart timer restart

View BGP view

Parameters *timer*: Specifies the time taken to reestablish a session between the GR Restarter and the GR Helper, in seconds.

Description Use the **graceful-restart timer restart** command to configure the maximum time taken by the peers to reestablish a BGP session.

Use the **undo graceful-restart timer restart** command to restore the default.

By default, the maximum time taken by the peers to reestablish a BGP session is 150 seconds.

Examples # Configure the maximum time taken by the peers to reestablish a BGP session as 300 seconds.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] graceful-restart timer restart 300
```

graceful-restart timer wait-for-rib

Syntax **graceful-restart timer wait-for-rib** *timer*

undo graceful-restart timer wait-for-rib

View BGP view

Parameters *timer*: Specifies the time to wait for the End-of-RIB, in seconds.

Description Use the **graceful-restart timer wait-for-rib** command to configure the time to wait for the End-of-RIB.

Use the **undo graceful-restart timer wait-for-rib** command to restore the default.

By default, the time to wait for the End-of-RIB is 180 seconds.

- *After a BGP session has been successfully (re)established, the End-of-RIB marker will be received in the time specified by this command.*
- *It is intended to speed up route convergence.*

Examples # Configure the time to wait for the End-of-RIB as 100 seconds.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] graceful-restart timer wait-for-rib 100
```

reset ospf process graceful-restart

Syntax **reset ospf** [*process-id*] **process graceful-restart**

View User view

Parameters *process-id*: Specifies OSPF process ID.

Description **Use the reset ospf process graceful-restart command to restart an OSPF GR process with a specified ID.**

Examples # Restart OSPF process 100 to trigger GR.

```
<Sysname> reset ospf 100 process graceful-restart
```

58 COMMON CONFIGURATION COMMANDS

display time-range

Syntax **display time-range** { *time-name* | **all** }

View Any view

Parameters *time-name*: Time range name comprising 1 to 32 characters. It is case insensitive and must start with an English letter. To avoid confusion, this name cannot be all.

all: All existing time ranges.

Description Use the **display time-range** command to display the configuration and state of a specified or all time ranges.

A time range is active if the system time falls into its range, and if otherwise, inactive.

Examples # Display the configuration and state of time range trname.

```
[Sysname] display time-range trname
Current time is 10:45:15 4/14/2005 Thursday
Time-range : trname ( Inactive )
from 08:00 12/1/2005 to 23:59 12/31/2100
```

Table 286 Field descriptions of the display time-range command

Field	Description
Current time	Current system time
Time-range	The configuration and state of time range, such as time range name, its activated state, and start time and ending time.

time-range

Syntax **time-range** *time-name* { *start-time* **to** *end-time days* [**from** *time1 date1*] [**to** *time2 date2*] | **from** *time1 date1* [**to** *time2 date2*] | **to** *time2 date2* }

undo time-range *time-name* [*start-time* **to** *end-time days* [**from** *time1 date1*] [**to** *time2 date2*] | **from** *time1 date1* [**to** *time2 date2*] | **to** *time2 date2*]

View System view

Parameters *time-name*: Time range name comprising 1 to 32 characters. It is case insensitive and must start with an English letter. To avoid confusion, this name cannot be all.

start-time: Start time of a periodic time range, in *hh***:***mm* format as 24-hour time, where *hh* is hours and *mm* is minutes. Its value ranges from 00:00 to 23:59.

end-time: End time of the periodic time range, in *hh***:***mm* format as 24-hour time, where *hh* is hours and *mm* is minutes. Its value ranges from 00:00 to 24:00. The end time must be greater than the start time.

days: Indicates on which day or days of the week the periodic time range is valid. You may specify multiple values, in words or in digits, separated by spaces, for this argument, but make sure that they do not overlap. These values can take one of the following forms:

- A digit in the range 0 to 6, respectively for Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday.
- Week in words, that is, **Mon**, **Tue**, **Wed**, **Thu**, **Fri**, **Sat**, or **Sun**.
- **working-day** for Monday through Friday.
- **off-day** for Saturday and Sunday.
- **daily** for seven days of a week.

from *time1 date1*: Indicates the start time and date of an absolute time range. The *time1* argument specifies the time of the day in *hh***:***mm* format as 24-hour time, where *hh* is hours and *mm* is minutes. Its value ranges from 00:00 to 23:59. The *date1* argument specifies a date in *MM***/***DD***/***YYYY* or *YYYY***/***MM***/***DD* format, where *MM* is the month of the year in the range 1 to 12, DD is the day of the month in the range 1 to 31, and YYYY is the year in the usual Gregorian calendar in the range 1970 to 2100. If not specified, the start time is the earliest time available from the system, namely, 01/01/1970 00:00:00 AM.

to *time2 date2*: Indicates the end time and date of the absolute time range. The format of the *time2* argument is the same as that of the *time1* argument, but its value ranges from 00:00 to 24:00. The end time must be greater than the start time. If not specified, the end time is the maximum time available from the system, namely, 12/31/2100 24:00:00 PM. The format and value range of the *date2* argument are the same as those of the *date1* argument.

Description Use the **time-range** command to create a time range.

Use the **undo time-range** command to remove a time range.

You may create a maximum of 256 time ranges.

A time range can be one of the following:

- Periodic time range created using the **time-range** *time-name start-time* **to** *end-time days* command. A time range thus created recurs periodically on the day or days of the week.
- Absolute time range created using the **time-range** *time-name* { **from** *time1 date1* [**to** *time2 date2*] | **to** *time2 date2* } command. Unlike a periodic time range, a time range thus created does not recur.

- Compound time range created using the **time-range** *time-name start-time* **to** *end-time days* { **from** *time1 date1* [**to** *time2 date2*] | **to** *time2 date2* } command. A time range thus created recurs on the day or days of the week only within the specified period. For example, to create a time range that is active from 12:00 to 14:00 on Wednesdays between January 1, 2004 00:00 and December 31, 2004 23:59, you may use the **time-range test 12:00 to 14:00 wednesday from 00:00 01/01/2004 to 23:59 12/31/2004** command.
- By default, up to 256 time ranges are available.

You may create individual time ranges identified with the same name. They are regarded as one time range whose active period is the result of ORing periodic ones, ORing absolute ones, and ANDing periodic and absolute ones.

Examples # Create an absolute time range named **test**, setting it to become active from 00:00 on January 1, 2003.

```
<Sysname> system-view
[Sysname] time-range test from 0:0 2003/1/1
```

Create a compound time range named **test**, setting it to be active between 8:00 to 18:00 during working days.

```
<Sysname> system-view
[Sysname] time-range test 8:00 to 18:00 working-day
```

Create a periodic time range named **test**, setting it to be active between 14:00 and 18:00 on Saturday and Sunday.

```
<Sysname> system-view
[Sysname] time-range test 14:00 to 18:00 off-day
```

59 IPv4 ACL Configuration Commands

acl (System view)

Syntax **acl number** *acl-number* [**match-order** { **auto** | **config** }]

undo acl { **all | number** *acl-number* }

View System view

Parameters **number**: Defines a numbered access control list (ACL).

acl-number: IPv4 ACL number in the range 2000 to 5999, where:

- 2000 to 2999 for basic IPv4 ACLs
- 3000 to 3999 for advanced IPv4 ACLs
- 4000 to 4999 for Ethernet frame header ACLs
- 5000 to 5999 for user-defined ACLs

match-order: Sets the order in which ACL rules are matched.

- **auto**: Performs depth-first match.
- **config**: Performs matching against rules in the order in which they are configured.

all: All IPv4 ACLs.

Description Use the **acl** command to enter IPv4 ACL view. If the ACL does not exist, it is created first.

Use the **undo acl** command to remove a specified or all IPv4 ACLs.

By default, the match order is **config**.

Note that:

- The match order for user-defined ACLs can only be **config**.
- You can also use this command to modify the match order of an existing IPv4 ACL but only when it is empty.

Examples # Create IPv4 ACL 2000.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000]
```

description (for IPv4)

Syntax **description** *text*

undo description

View Basic IPv4 ACL view, advanced IPv4 ACL view, Ethernet frame header ACL view, user-defined ACL view

Parameters *text*: ACL description, a case-sensitive string of 1 to 127 characters.

Description Use the **description** command to create an IPv4 ACL description to describe the purpose of the ACL for example.

Use the **undo description** command to remove the ACL description.

Examples # Define the description of IPv4 ACL 2000.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] description This acl is used in eth 0
```

Define the description of IPv4 ACL 3000.

```
<Sysname> system-view
[Sysname] acl number 3000
[Sysname-acl-adv-3000] description This acl is used in eth 0
```

Define the description of IPv4 ACL 4000.

```
<Sysname> system-view
[Sysname] acl number 4000
[Sysname-acl-ethernetframe-4000] description This acl is used in eth 0
```

Define the description of IPv4 ACL 5000.

```
<Sysname> system-view
[Sysname] acl number 5000
[Sysname-acl-user-5000] description This acl is used in eth 0
```

display acl

Syntax **display acl** { *acl-number* | **all** }

View Any view

Parameters *acl-number*: IPv4 ACL number in the range 2000 to 5999, where:

- 2000 to 2999 for basic IPv4 ACLs
- 3000 to 3999 for advanced IPv4 ACLs
- 4000 to 4999 for Ethernet frame header ACLs
- 5000 to 5999 for user-defined ACLs

all: All IPv4 ACLs.

Description Use the **display acl** command to display information about the specified or all IPv4 ACLs.

This command displays ACL rules in the order in which the system compares a packet against them.

Examples # Display information about ACL 2001.

```
<Sysname> display acl 2001
Basic acl  2001, named flow, 1 rules,
Acl's step is 5
 rule 5 permit source 1.1.1.1 0 (5 times matched)
 rule 5 comment This rule is used in eth 1
```

Table 287 Field descriptions of the display acl command

Field	Description
Basic acl 2001	The displayed information is about the basic IPv4 ACL 2001.
1 rule	The ACL contains one rule.
Acl's step is 5	The rules in this ACL are numbered in the step of 5.
5 times matched	Five matches for the rule. Only ACL matches performed by software are counted.
	This field appears as long as one match is found.
rule 5 comment This rule is used in eth 1	The description of ACL rule 5 is "This rule is used in eth 1."

reset acl counter

Syntax **reset acl counter** { *acl-number* | **all** }

View User view

Parameters *acl-number*: IPv4 ACL number in the range 2000 to 4999, where:

- 2000 to 2999 for basic IPv4 ACLs
- 3000 to 3999 for advanced IPv4 ACLs
- 4000 to 4999 for Ethernet frame header ACLs

all: All IPv4 ACLs except for user-defined ACLs.

Description Use the **reset acl counter** command to clear statistics about specified or all IPv4 ACLs except for user-defined ACLs.

Examples # Clear statistics about IPv4 ACL 2001.

```
<Sysname> reset acl counter 2001
```

rule (in basic ACL view)

Syntax **rule** [*rule-id*] { **deny** | **permit** } [**fragment** | **logging** | **source** { *sour-addr sour-wildcard* | **any** } | **time-range** *time-name* | **vpn-instance** *vpn-instance-name*] *

undo rule *rule-id* [**fragment** | **logging** | **source** | **time-range** | **vpn-instance**] *

View Basic ACL view

Parameters *rule-id*: ACL rule number in the range 0 to 65534.

deny: Defines a deny statement to drop matched packets.

permit: Defines a permit statement to allow matched packets to pass.

fragment: Indicates that the rule applies only to non-first fragments. Without this keyword, the rule applies to both fragments and non-fragments

logging: Specifies to log matched packets. The log provides information about ACL rule number, whether packets are permitted or dropped, upper layer protocol that IP carries, source/destination address, source/destination port number, and number of packets.

source { *sour-addr sour-wildcard* | **any** }: Specifies a source address. The *sour-addr sour-wildcard* argument specifies a source IP address in dotted decimal notation. Setting the wildcard to a zero indicates a host address. The **any** keyword indicates any source IP address.

time-range *time-name:* Specifies the time range in which the rule takes effect. The *time-name* argument specifies a time range name with 1 to 32 characters. It is case insensitive and must start with an English letter. To avoid confusion, this name cannot be all.

vpn-instance *vpn-instance-name:* Specifies a VPN instance. The *vpn-instance-name* argument is a case-insensitive string of 1 to 31 characters.

Description Use the **rule** command to create an IPv4 ACL rule or modify the rule if it has existed.

Use the **undo rule** command to remove an IPv4 ACL rule or parameters from the rule.

With the **undo rule** command, if no parameters are specified, the entire ACL rule is removed; if other parameters are specified, only the involved information is removed.

You will fail to create or modify a rule if its permit/deny statement is exactly the same as another rule. In addition, if the ACL match order is set to **auto** rather than **config**, you cannot modify ACL rules.

When defining ACL rules, you need not assign them IDs. The system can automatically assign rule IDs starting with 0 and increasing in certain rule numbering steps. A rule ID thus assigned is greater than the current highest rule ID. For example, if the rule numbering step is 5 and the current highest rule ID is 28, the next rule will be numbered 30.

You may use the **display acl** command to verify rules configured in an ACL. If the match order for this ACL is **auto**, rules are displayed in the depth-first match order rather than by rule number.

Examples # Create a rule to deny packets with the source IP address 1.1.1.1.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule deny source 1.1.1.1 0
```

rule (in advanced ACL view)

Syntax **rule** [*rule-id*] { **deny** | **permit** } *protocol* [**destination** { *dest-addr dest-wildcard* | **any** } | **destination-port** *operator port1* [*port2*] | **dscp** *dscp* | **established** | **fragment** | **icmp-type** { *icmp-type icmp-code* | *icmp-message* } | **logging** | **precedence** *precedence* | **reflective** | **source** { *sour-addr sour-wildcard* | **any** } | **source-port** *operator port1* [*port2*] | **time-range** *time-name* | **tos** *tos* | **vpn-instance** *vpn-instance-name*] *

undo rule *rule-id* [**destination | destination-port | dscp | fragment** | **icmp-type | logging** | **precedence | reflective | source | source-port** | **time-range** | **tos** | **vpn-instance**] *

View Advanced ACL view

Parameters *rule-id*: ACL rule number in the range 0 to 65534.

deny: Defines a deny statement to drop matched packets.

permit: Defines a permit statement to allow matched packets to pass.

protocol: Protocol carried by IP. It can be a number in the range 0 to 255, or in words, **gre** (47), **icmp** (1), **igmp** (2), **ipinip** (4), **ospf** (89), **tcp** (6), **udp** (17).

Table 288 Parameters for advanced IPv4 ACL rules

Parameter	Function	Description
source { *sour-addr sour-wildcard* | **any** }	Specifies a source address.	The *sour-addr sour-wildcard* argument specifies a source IP address in dotted decimal notation. Setting the wildcard to a zero indicates a host address. The **any** keyword indicates any source IP address.
destination { *dest-addr dest-wildcard* | **any** }	Specifies a destination address.	The *dest-addr dest-wildcard* argument specifies a destination IP address in dotted decimal notation. Setting the *dest-wildcard* to a zero indicates a host address. The **any** keyword indicates any destination IP address.
precedence *precedence*	Specifies an IP precedence value.	The *precedence* argument can be a number in the range 0 to 7, or in words, **routine**, **priority**, **immediate**, **flash**, **flash-override**, **critical**, **internet**, or **network**.
tos *tos*	Specifies a ToS preference.	The *tos* argument can be a number in the range 0 to 15, or in words, **max-reliability** (2), **max-throughput** (4), **min-delay** (8), **min-monetary-cost** (1), or **normal** (0).
dscp *dscp*	Specifies a DSCP priority.	The *dscp* argument can be a number in the range 0 to 63, or in words, **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs6**, **cs7**, **default**, or **ef**.
logging	Specifies to log matched packets.	The log provides information about ACL rule number, whether packets are permitted or dropped, upper layer protocol that IP carries, source/destination address, source/destination port number, and number of packets.
reflective	Specifies the rule to be reflective.	A rule with the **reflective** keyword can be defined only for TCP, UDP, or ICMP packets and its statement can only be **permit**.
vpn-instance *vpn-instance-name*	Specifies a VPN instance.	The *vpn-instance-name* argument is a case-insensitive string of 1 to 31 characters.
fragment	Indicates that the rule applies only to non-first fragments.	With this keyword not provided, the rule is effective to both non-fragments and fragments.

Table 288 Parameters for advanced IPv4 ACL rules

Parameter	Function	Description
time-range *time-name*	Specifies the time range in which the rule can take effect.	The *time-name* argument comprises 1 to 32 characters. It is case insensitive and must start with an English letter. To avoid confusion, this name cannot be all.

If the *protocol* argument is set to **tcp** or **udp**, you may define the parameters in the following table.

Table 289 TCP/UDP-specific parameters for advanced IPv4 ACL rules

Parameter	Function	Description
source-port *operator port1* [*port2*]	Defines a UDP or TCP source port against which UDP or TCP packets are matched.	The *operator* argument can be **lt** (lower than), **gt** (greater than), **eq** (equal to), **neq** (not equal to), and **range** (inclusive range). *port1, port2*: TCP or UDP port number, represented by a number in the range 0 to 65535. TCP port number can be represented in words as follows: **chargen** (19), **bgp** (179), **cmd** (514), **daytime** (13), **discard** (9), **domain** (53), **echo** (7), **exec** (512), **finger** (79), **ftp** (21), **ftp-data** (20), **gopher** (70), **hostname** (101), **irc** (194), **klogin** (543), **kshell** (544), **login** (513), **lpd** (515), **nntp** (119), **pop2** (109), **pop3** (110), **smtp** (25), **sunrpc** (111), **tacacs** (49), **talk** (517), **telnet** (23), **time** (37), **uucp** (540), **whois** (43), or **www** (80). UDP port number can be represented in words as follows: **biff** (512), **bootpc** (68), **bootps** (67), **discard** (9), **dns** (53), **dnsix** (90), **echo** (7), **mobilip-ag** (434), **mobilip-mn** (435), **nameserver** (42), **netbios-dgm** (138), **netbios-ns** (137), **netbios-ssn** (139), **ntp** (123), **rip** (520), **snmp** (161), **snmptrap** (162), **sunrpc** (111), **syslog** (514), **tacacs-ds** (65), **talk** (517), **tftp** (69), **time** (37), **who** (513), **xdmcp** (177).
destination-port *operator port1* [*port2*]	Defines a UDP or TCP destination port against which UDP or TCP packets are matched.	

Table 289 TCP/UDP-specific parameters for advanced IPv4 ACL rules

Parameter	Function	Description
established	Defines the rule for TCP connection packets.	A keyword specific to TCP. On a router, With this keyword, the rule matches the TCP connection packets with the ACK or RST flag. The use and availability of this keyword on switches may vary.

If the *protocol* argument is set to **icmp**, you may define the parameters in the following table.

Table 290 Parameters for advanced IPv4 ACL rules

Parameter	Function	Description
icmp-type { *icmp-type* *icmp-code* | *icmp-message* }	Specifies the ICMP message type and code.	The *icmp-type* argument ranges from 0 to 255. The *icmp-code* argument ranges from 0 to 255. The *icmp-message* argument specifies a message name.

The following table provides the ICMP messages that you can specify in advanced IPv4 ACL rules.

Table 291 ICMP messages and their codes

ICMP message	Type	Code
echo	8	0
echo-reply	0	0
fragmentneed-DFset	3	4
host-redirect	5	1
host-tos-redirect	5	3
host-unreachable	3	1
information-reply	16	0
information-request	15	0
net-redirect	5	0
net-tos-redirect	5	2
net-unreachable	3	0
parameter-problem	12	0
port-unreachable	3	3
protocol-unreachable	3	2
reassembly-timeout	11	1
source-quench	4	0
source-route-failed	3	5
timestamp-reply	14	0
timestamp-request	13	0

Table 291 ICMP messages and their codes

ICMP message	Type	Code
ttl-exceeded	11	0

Description Use the **rule** command to define or modify an IPv4 ACL rule. If the rule does not exist, it is created first.

Use the **undo rule** command to remove an ACL rule or parameters from the rule.

With the **undo rule** command, if no parameters are specified, the entire ACL rule is removed; if other parameters are specified, only the involved information is removed.

You will fail to create or modify a rule if its permit/deny statement is exactly the same as another rule. In addition, if the ACL match order is set to **auto** rather than **config**, you cannot modify ACL rules.

When defining ACL rules, you need not assign them IDs. The system can automatically assign rule IDs starting with 0 and increasing in certain rule numbering steps. A rule ID thus assigned is greater than the current highest rule ID. For example, if the rule numbering step is five and the current highest rule ID is 28, the next rule will be numbered 30. For detailed information about step, refer to the **step** command.

You may use the **display acl** command to verify rules configured in an ACL. If the match order for this ACL is **auto**, rules are displayed in the depth-first order rather than by rule number.

Examples # Define a rule to permit the TCP packets to pass with the destination port 80 sent from 129.9.0.0 to 202.38.160.0.

```
<Sysname> system-view
[Sysname] acl number 3101
[Sysname-acl-adv-3101] rule permit tcp source 129.9.0.0 0.0.255.255
destination 202.38.160.0 0.0.0.255 destination-port eq 80
```

rule (in Ethernet frame header ACL view)

Syntax **rule** [*rule-id*] { **deny** | **permit** } [**cos** *vlan-pri* | **dest-mac** *dest-addr dest-mask* | **lsap** *lsap-code lsap-wildcard* | **source-mac** *sour-addr source-mask* | **time-range** *time-name* | **type** *type-code type-wildcard*] *

undo rule *rule-id*

View Ethernet frame header ACL view

Parameters *rule-id*: ACL rule number in the range 0 to 65534.

deny: Defines a deny statement to drop matched packets.

permit: Defines a permit statement to allow matched packets to pass.

cos *vlan-pri:* Defines a 802.1p priority. The *vlan-pri* argument takes a value in the range 0 to 7; or its equivalent in words, **best-effort**, **background**, **spare**, **excellent-effort**, **controlled-load**, **video**, **voice**, or **network-management**.

dest-mac *dest-addr dest-mask:* Specifies a destination MAC address range. The *dest-addr* and *dest-mask* arguments indicate a destination MAC address and mask in xxxx-xxxx-xxxx format.

lsap *lsap-code lsap-wildcard:* Defines the DSAP and SSAP fields in the LLC encapsulation. The *lsap-code* argument is a 16-bit hexadecimal number indicating frame encapsulation. The *lsap-wildcard* argument is a 16-bit hexadecimal number indicating the wildcard of the LSAP code.

source-mac *sour-addr source-mask:* Specifies a source MAC address range. The *sour-addr* and *sour-mask* arguments indicate a source MAC address and mask in xxxx-xxxx-xxxx format.

time-range *time-name:* Specifies the time range in which the rule can take effect. The *time-name* argument comprises 1 to 32 characters. It is case insensitive and must start with an English letter. To avoid confusion, this name cannot be all.

type *type-code type-wildcard:* Defines a link layer protocol. The *type-code* argument is a 16-bit hexadecimal number indicating frame type. It is corresponding to the type-code field in Ethernet_II and Ethernet_SNAP frames. The *type-wildcard* argument is a 16-bit hexadecimal number indicating the wildcard.

The use of this parameter depends on the hardware chip of your device.

Description Use the **rule** command to create an ACL rule or modify the rule if it has existed.

Use the **undo rule** command to remove an ACL rule.

You will fail to create or modify a rule if its permit/deny statement is exactly the same as another rule. In addition, if the ACL match order is set to **auto** rather than **config**, you cannot modify ACL rules.

When defining ACL rules, you need not assign them IDs. The system can automatically assign rule IDs, starting with 0 and increasing in certain rule numbering steps. A rule ID thus assigned is greater than the current highest rule ID. For example, if the rule numbering step is five and the current highest rule ID is 28, the next rule will be numbered 30. For detailed information about step, refer to the **step** command.

You may use the **display acl** command to verify rules configured in an ACL. If the match order for this ACL is **auto**, rules are displayed in the depth-first order rather than by rule number.

CAUTION:

- *When you define an Ethernet frame header ACL, do not set the type-code argument to 0800, 86DD, 8847, 8848 or 8100.*
- *For the default flow template to be used, the destination mask corresponding to the **type** keyword must be FFFF.*

Examples # Create a rule to deny packets with the 802.1p priority of 3.

```
<Sysname> system-view
[Sysname] acl number 4000
[Sysname-acl-ethernetframe-4000] rule deny cos 3
```

rule (in user-defined ACL view)

Syntax **rule** [*rule-id*] { **deny** | **permit** } [{ { **ipv4 | ipv6 | l2 | l4 | l5** } *rule-string rule-mask offset* }&<1-8>] [**time-range** *time-name*]

undo rule *rule-id*

View User-defined ACL view

Parameters *rule-id*: ACL rule number in the range 0 to 65534.

deny: Defines a deny statement to drop matched packets.

permit: Defines a permit statement to allow matched packets to pass.

ipv4: Sets the offset from the beginning of the IPv4 header.

ipv6: Sets the offset from the beginning of the IPv6 header.

l2: Sets the offset from the beginning of the Layer 2 frame header.

l4: Sets the offset from the beginning of the Layer 4 header.

l5: Sets the offset from the beginning of the Layer 5 header.

rule-string: Defines a match pattern in hexadecimal format. Its length must be a multiple of two.

rule-mask: Defines a match pattern mask in hexadecimal format. Its length must be the same as that of the match pattern.

offset: The offset in bytes at which the match operation begins.

&<1-8>: Indicates that up to eight match patterns can be defined in the rule.

time-range *time-name*: Specifies the time range in which the rule can take effect. The *time-name* argument is a case-insensitive string of 1 to 32 characters. The name must begin with an English letter and cannot be all to avoid confusion.

Description Use the **rule** command to create an IPv4 ACL rule.

Use the **undo rule** command to remove an IPv4 ACL rule.

You will fail to create a user-defined ACL rule if its permit/deny statement is exactly the same as another rule. However, you can modify a user-defined ACL rule.

When defining user-defined ACL rules, you need not assign them IDs. The system can automatically assign rule IDs starting with 0 and increasing in rule numbering steps of five. A rule ID thus assigned is greater than the current highest rule ID. For example, if the current highest rule ID is 28, the next rule will be numbered 30. For detailed information about step, refer to the **step** command.

You may use the **display acl** command to verify rules configured in an ACL.

Examples # Create ACL 5500.

```
<Sysname> system-view
[Sysname] acl number 5500
[Sysname-acl-user-5500] rule 0 permit l2 0806 ffff 20 time-range t1
[Sysname-acl-user-5500] display acl 5500
User defined ACL  5500, 1 rule,
Acl's step is 5
 rule 0 permit l2 0806 ffff 20 time-range t1 (Active)
```

rule comment (for IPv4)

Syntax **rule** *rule-id* **comment** *text*

undo rule *rule-id* **comment**

View Basic IPv4 ACL view, advanced IPv4 ACL view, Ethernet frame header ACL view, user-defined ACL view

Parameters *rule-id*: IPv4 ACL rule number in the range 0 to 65534.

text: IPv4 ACL rule description, a case-sensitive string of 1 to 127 characters.

Description Use the **rule comment** command to create or modify an ACL rule description, for example to describe the purpose of the ACL rule or the parameters it contains.

You will fail to do that if the specified rule does not exist.

Use the **undo rule comment** command to remove the ACL rule description.

By default, no rule description is created.

Examples # Create a rule in ACL 2000 and define the rule description.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule 0 deny source 1.1.1.1 0
[Sysname-acl-basic-2000] rule 0 comment This rule is used in eth 1
```

Create a rule in ACL 3000 and define the rule description.

```
<Sysname> system-view
[Sysname] acl number 3000
[Sysname-acl-adv-3000] rule 0 permit ip source 1.1.1.1 0
[Sysname-acl-adv-3000] rule 0 comment This rule is used in eth 1
```

Create a rule in ACL 4000 and define the rule description.

```
<Sysname> system-view
[Sysname] acl number 4000
[Sysname-acl-ethernetframe-4000] rule 0 deny cos 3
[Sysname-acl-ethernetframe-4000] rule 0 comment This rule is used in eth 1
```

Create a rule in ACL 5000 and define the rule description.

```
<Sysname> system-view
[Sysname] acl number 5000
[Sysname-acl-user-5000] rule 0 permit l2 14 20 10
[Sysname-acl-user-5000] rule 0 comment This rule is used in eth 1
```

step (for IPv4)

Syntax **step** *step-value*

undo step

View Basic IPv4 ACL view, advanced IPv4 ACL view, Ethernet frame header ACL view

Parameters *step-value*: IPv4 ACL rule numbering step, in the range 1 to 20.

Description Use the **step** command to set a rule numbering step.

Use the **undo step** command to restore the default.

By default, rule numbering step is five.

When defining rules in an IPv4 ACL, you do not necessarily assign them numbers. The system can do this automatically in steps. For example, if the default step applies, rules you created are automatically numbered 0, 5, 10, 15, and so on. One benefit of rule numbering step is that it allows you to insert new rules between existing ones as needed. For example, after creating four rules numbered 0, 5, 10, 15 in an ACL configured with the step of five, you can still insert a rule numbered 1.

Any step change can result in renumbering. For example, after you change the step in the above example from five to two, the rules are renumbered 0, 2, 4, 6, and 8.

Note that even if the current step is the default, performing the **undo step** command can still result in rule renumbering. Suppose that ACL 3001 adopts the default numbering step and contains two rules numbered 0 and 5. After you insert rule 1 and rule 3, the rules are numbered 0, 1, 3, and 5. If you perform the **undo step** command, they will be renumbered 0, 5, 10, and 15.

Examples # Set the rule numbering step to 2 for IPv4 ACL 3101.

```
<Sysname> system-view
[Sysname] acl number 3101
[Sysname-acl-basic-3101] step 2
```

60 IPv6 ACL Configuration Commands

acl ipv6

Syntax **acl ipv6 number** *acl6-number* [**match-order** { **auto** | **config** }]

undo acl ipv6 { **all** | **number** *acl6-number* }

View System view

Parameters *acl6-number*: IPv6 ACL number. It is a value in one of the following ranges:

- 2000 to 2999 for basic IPv6 ACLs
- 3000 to 3999 for advanced IPv6 ACLs

match-order: Sets the order in which ACL rules are matched.

- **auto**: Performs depth-first match.
- **config**: Performs matching against rules in the order in which they are configured.

all: All IPv6 ACLs.

Description Use the **acl ipv6** command to enter IPv6 ACL view. If the ACL does not exist, it is created first.

Use the **undo acl ipv6** command to remove a specified or all IPv6 ACLs.

By default, the match order is **config**.

You can also use this command to modify the match order of an existing IPv6 ACL but only when it is empty.

Examples # Create ACL 2000.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000]
```

description (for IPv6)

Syntax **description** *text*

undo description

View Basic IPv6 ACL view, advanced IPv6 ACL view

Parameters *text*: ACL description, a case-sensitive string of 1 to 127 characters.

Description Use the **description** command to create an IPv6 ACL description, to describe the purpose of the ACL for example.

Use the **undo description** command to remove the IPv6 ACL description.

Examples # Create a description for IPv6 ACL 2000.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] description This acl is used in eth 0
```

Create a description for IPv6 ACL 3000.

```
<Sysname> system-view
[Sysname] acl ipv6 number 3000
[Sysname-acl6-adv-3000] description This acl is used in eth 0
```

display acl ipv6

Syntax **display acl ipv6** { *acl6-number* | **all** }

View Any view

Parameters *acl6-number*: IPv6 ACL number. It is a value in one of the following ranges:

- 2000 to 2999 for basic IPv6 ACLs
- 3000 to 3999 for advanced IPv6 ACLs

all: All IPv6 ACLs.

Description Use the **display acl ipv6** command to display information about the specified or all IPv6 ACLs.

The output will be displayed in matching order.

Examples # Display information about IPv6 ACL 2001.

```
<Sysname> display acl ipv6 2001
Basic IPv6 ACL  2001, 1 rule,
Acl's step is 5
rule 0 permit source 1::2/128 (5 times matched)
rule 0 comment This rule is used in eth 1
```

Table 292 Field descriptions of the display acl ipv6 command

Field	Description
Basic IPv6 ACL 2001	The displayed information is about the basic IPv6 ACL 2001.
1 rule	The ACL contains one rule.
Acl's step is 5	The rules in this ACL are numbered in steps of 5.
5 times matched	Five matches for the rule. Only ACL matches performed by software are counted.
	The field appears as long as one match is found.
rule 0 comment This rule is used in eth 1	The description of ACL rule 5 is "This rule is used in eth 1."

reset acl ipv6 counter

Syntax **reset acl ipv6 counter** { *acl6-number* | **all** }

View User view

Parameters *acl6-number*: IPv6 ACL number. It is a value in one of the following ranges:

- 2000 to 2999 for basic IPv6 ACLs
- 3000 to 3999 for advanced IPv6 ACLs

all: All basic and advanced IPv6 ACLs.

Description Use the **reset acl ipv6 counter** command to clear statistics about specified or all basic and advanced IPv6 ACLs.

Examples # Clear the statistics about IPv6 ACL 2001.

```
<Sysname> reset acl ipv6 counter 2001
```

rule (in basic IPv6 ACL view)

Syntax **rule** [*rule-id*] { **deny** | **permit** } [**fragment** | **logging** | **source** { *ipv6-address prefix-length* | *ipv6-address/prefix-length* **| any** } | **time-range** *time-name*] *

undo rule *rule-id* [**fragment** | **logging** | **source** | **time-range**] *

View Basic IPv6 ACL view

Parameters *rule-id*: IPv6 ACL rule number in the range 0 to 65534.

deny: Defines a deny statement to drop matched packets.

permit: Defines a permit statement to allow matched packets to pass.

fragment: Indicates that the rule applies only to non-first fragments. The rule applies to both fragments and non-fragments without this keyword.

logging: Specifies to log matched packets. The log provides information about ACL rule number, whether packets are permitted or dropped, upper layer protocol that IP carries, source/destination address, source/destination port number, and number of packets.

source { *ipv6-address prefix-length* | *ipv6-address/prefix-length* | **any** }: Specifies a source address. The *ipv6-address* and *prefix-length* arguments specify a source IPv6 address, and its address prefix length in the range 1 to 128. The **any** keyword indicates any IPv6 source address.

time-range *time-name:* Specifies the time range in which the rule takes effect. The *time-name* argument specifies a time range name with 1 to 32 characters. It is case insensitive and must start with an English letter. To avoid confusion, this name cannot be all.

Description Use the **rule** command to create an IPv6 ACL rule or modify the rule if it has existed.

Use the **undo rule** command to remove an IPv6 ACL rule or parameters from the rule.

With the **undo rule** command, if no parameters are specified, the entire ACL rule is removed; if other parameters are specified, only the involved information is removed.

You will fail to create or modify a rule if its permit/deny statement is exactly the same as another rule. In addition, if the ACL match order is set to **auto** rather than **config**, you cannot modify ACL rules.

When defining ACL rules, you need not assign them IDs. The system can automatically assign rule IDs starting with 0 and increasing in certain rule numbering steps. A rule ID thus assigned is greater than the current highest rule ID. For example, if the rule numbering step is five and the current highest rule ID is 28, the next rule will be numbered 30.

You may use the **display acl ipv6** command to verify rules configured in an ACL. If the match order for this IPv6 ACL is **auto**, rules are displayed in the depth-first match order rather than by rule number.

Examples # Create rules in IPv6 ACL 2000.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule permit source 2030:5060::9050/64
[Sysname-acl6-basic-2000] rule 8 deny source fe80:5060::8050/96
```

rule (in advanced IPv6 ACL view)

Syntax **rule** [*rule-id*] { **deny** | **permit** } *protocol* [**destination** { *dest dest-prefix* | *dest/dest-prefix* | **any** } | **destination-port** *operator port1* [*port2*] | **dscp** *dscp* |

fragment | **icmpv6-type** { *icmpv6-type icmpv6-code* | *icmpv6-message* } | **logging** | **source** { *source source-prefix* | *source/source-prefix* **| any** } | **source-port** *operator port1* [*port2*] | **time-range** *time-name*] *

undo rule *rule-id* [**destination | destination-port** | **dscp | fragment** | **icmpv6-type | logging** | **source | source-port** | **time-range**] *

View Advanced IPv6 ACL view

Parameters *rule-id*: IPv6 ACL rule number in the range 0 to 65534.

deny: Defines a deny statement to drop matched packets.

permit: Defines a permit statement to allow matched packets to pass.

protocol: Protocol carried on IP. It can be a number in the range 0 to 255, or in words, **gre** (47), **icmpv6** (58), **ipv6-ah** (51), **ipv6-esp** (50), **ospf** (89), **tcp** (6), **udp** (17).

Table 293 Match criteria and other rule information for advanced IPv6 ACL rules

Parameter	Function	Description
source { *source source-prefix* | *source/source-prefix* | **any** }	Specifies a source IPv6 address.	The *source* and *source-prefix* arguments specify an IPv6 source address and its prefix length in the range 1 to 128. The **any** keyword indicates any IPv6 source address.
destination { *dest dest-prefix* | *dest/dest-prefix* | **any** }	Specifies a destination IPv6 address.	The *dest* and *dest-prefix* arguments specify a destination IPv6 address, and its prefix length in the range 1 to 128. The **any** keyword indicates any IPv6 destination address.
dscp *dscp*	Specifies a DSCP preference	The *dscp* argument can be a number in the range 0 to 63, or in words, **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs6**, **cs7**, **default**, or **ef**.
logging	Specifies to log matched packets	The log provides information about ACL rule number, whether packets are permitted or denied, protocol that IP carries, source/destination address, source/destination port number, and number of packets.
fragment	Indicates that the rule applies only to non-first fragments	With this keyword not provided, the rule is effective to both non-fragments and fragments.

Table 293 Match criteria and other rule information for advanced IPv6 ACL rules

Parameter	Function	Description
time-range *time-name*	Specifies the time range in which the rule can take effect.	The time-name argument comprises 1 to 32 characters. It is case insensitive and must start with an English letter. To avoid confusion, this name cannot be all.

If the *protocol* argument is set to **tcp** or **udp,** you may define the parameters in the following table.

Table 294 TCP/UDP-specific match criteria for advanced IPv6 ACL rules

Parameter	Function	Description
source-port *operator port1* [*port2*]	Defines the source port in the UDP/TCP packet.	The *operator* argument can be **lt** (lower than), **gt** (greater than), **eq** (equal to), or **range** (inclusive range). The *port1* and *port2* arguments each specify a TCP or UDP port, represented by a number in the range 0 to 65535. TCP port number can be represented in words as follows: **chargen** (19), **bgp** (179), **cmd** (514), **daytime** (13), **discard** (9), **domain** (53), **echo** (7), **exec** (512), **finger** (79), **ftp** (21), **ftp-data** (20), **gopher** (70), **hostname** (101), **irc** (194), **klogin** (543), **kshell** (544), **login** (513), **lpd** (515), **nntp** (119), **pop2** (109), **pop3** (110), **smtp** (25), **sunrpc** (111), **tacacs** (49), **talk** (517), **telnet** (23), **time** (37), **uucp** (540), **whois** (43), or **www** (80). UDP port number can be represented in words as follows: **biff** (512), **bootpc** (68), **bootps** (67), **discard** (9), **dns** (53), **dnsix** (90), **echo** (7), **mobilip-ag** (434), **mobilip-mn** (435), **nameserver** (42), **netbios-dgm** (138), **netbios-ns** (137), **netbios-ssn** (139), **ntp** (123), **rip** (520), **snmp** (161), **snmptrap** (162), **sunrpc** (111), **syslog** (514), **tacacs-ds** (65), **talk** (517), **tftp** (69), **time** (37), **who** (513), **xdmcp** (177).
destination-port *operator port1* [*port2*]	Defines the destination port in the UDP/TCP packet.	

If the *protocol* argument is set to **ICMPv6**, you may define the parameters in the following table.

Table 295 ICMPv6-specific match criteria for advanced IPv6 ACL rules

Parameter	Function	Description
icmpv6-type { *icmpv6-type icmpv6-code* | *icmpv6-message* }	Specifies the ICMPv6 message type and code	The *icmpv6-type* argument ranges from 0 to 255. The *icmpv6-code* argument ranges from 0 to 255. The *icmpv6-message* argument specifies a message name.

The following table provides the ICMPv6 messages that you can specify in advanced IPv6 ACL rules.

Table 296 Available ICMPv6 messages

ICMPv6 message	Type	Code
redirect	137	0
echo-request	128	0
echo-reply	129	0
err-Header-field	4	0
frag-time-exceeded	3	1
hop-limit-exceeded	3	0
host-admin-prohib	1	1
host-unreachable	1	3
neighbor-advertisement	136	0
neighbor-solicitation	135	0
network-unreachable	1	0
packet-too-big	2	0
port-unreachable	1	4
router-advertisement	134	0
router-solicitation	133	0
unknown-ipv6-opt	4	2
unknown-next-hdr	4	1

Description

Use the **rule** command to create an IPv6 ACL rule or modify the rule if it has existed.

Use the **undo rule** command to remove an IPv6 ACL rule or parameters from the rule.

With the **undo rule** command, if no parameters are specified, the entire ACL rule is removed; if other parameters are specified, only the involved information is removed.

You will fail to create or modify a rule if its permit/deny statement is exactly the same as another rule. In addition, if the ACL match order is set to **auto** rather than **config**, you cannot modify ACL rules.

When defining ACL rules, you need not assign them IDs. The system can automatically assign rule IDs, starting with 0 and increasing in certain rule numbering steps. A rule ID thus assigned is greater than the current highest rule ID. For example, if the rule numbering step is 5 and the current highest rule ID is 28, the next rule will be numbered 30.

You may use the **display acl ipv6** command to verify rules configured in an IPv6 ACL. If the match order for this IPv6 ACL is **auto**, rules are displayed in the depth-first match order rather than by rule number.

Examples # Create a rule in IPv6 ACL 3000, permitting the TCP packets with the source address 2030:5060::9050/64 to pass.

```
<Sysname> system-view
[Sysname] acl ipv6 number 3000
[Sysname-acl6-adv-3000] rule permit tcp source 2030:5060::9050/64
```

rule comment (for IPv6)

Syntax **rule** *rule-id* **comment** *text*

undo rule *rule-id* **comment**

View Basic IPv6 ACL view, advanced IPv6 ACL view

Parameters *rule-id*: IPv6 ACL rule number in the range 0 to 65534.

text: IPv6 ACL rule description, a case-sensitive string of 1 to 127 characters.

Description Use the **rule comment** command to create or modify a description for an existing IPv6 ACL rule, for example to describe the purpose of the ACL rule or its attributes.

Use the **undo rule comment** command to remove the IPv6 ACL rule description.

By default, no rule description is created.

Examples # Define a rule in IPv6 ACL 2000 and create a description for the rule.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule 0 permit source 2030:5060::9050/64
[Sysname-acl6-basic-2000] rule 0 comment This rule is used in eth 1
```

Define a rule in IPv6 ACL 3000 and create a description for the rule.

```
<Sysname> system-view
[Sysname] acl ipv6 number 3000
[Sysname-acl6-adv-3000] rule 0 permit tcp source 2030:5060::9050/64
[Sysname-acl6-adv-3000] rule 0 comment This rule is used in eth 1
```

step (for IPv6)

Syntax **step** *step-value*

undo step

View Basic IPv6 ACL view, advanced IPv6 ACL view

Parameters *step-value*: The step in which the rules in the IPv6 ACL is numbered. By default, it is in the range 1 to 20 at the step of 5.

Description Use the **step** command to set a rule numbering step for the IPv6 ACL.

Use the **undo step** command to restore the default.

When defining rules in an IPv6 ACL, you do not necessarily assign them numbers. The system can do this automatically in steps. For example, if the default step applies, rules you created are numbered 0, 5, 10, 15, and so on automatically.

One benefit of rule numbering step is that it allows you to insert new rules between existing ones as needed. For example, after creating four rules numbered 0, 5, 10, 15 in an ACL configured with the step of 5, you can still insert a rule numbered 1.

Any step change can result in renumbering. For example, after you change the step in the above example from 5 to 2, the rules are renumbered 0, 2, 4, 6, and 8.

Note that even if the current step is the default, performing the **undo step** command can still result in rule renumbering. Suppose that IPv6 ACL 3001 adopts the default numbering step and contains two rules numbered 0 and 5. After you insert rule 1 and rule 3, the rules are numbered 0, 1, 3, and 5. If you perform the **undo step** command, they will be renumbered 0, 5, 10, and 15.

Examples # Set the rule numbering step to 2 for IPv6 ACL 2000.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] step 2
```

Set the rule numbering step to 2 for IPv6 ACL 3000.

```
<Sysname> system-view
[Sysname] acl ipv6 number 3000
[Sysname-acl6-adv-3000] step 2
```

61 FLOW TEMPLATE CONFIGURATION COMMANDS

display flow-template user-defined

Syntax **display flow-template user-defined** [*flow-template-name*]

View Any view

Parameters *flow-template-name*: Flow template name, a case-insensitive string of 1 to 31 characters.

Description Use the **display flow-template user-defined** command to display the configuration of the specified or all user-defined flow templates.

Examples # Display the configuration of all user-defined flow templates.

```
<Sysname> display flow-template user-defined
user-defined flow template: basic
 name:f1, index:1, total reference counts:1
 fields: ip-protocol fragments ip-precedence

user-defined flow template: extend
 name:f2, index:2, total reference counts:0
 fields: start 22 33 l2 55 66

user-defined flow template: basic
 name:f3, index:3, total reference counts:1
 fields: tos
```

Table 297 Field descriptions of display flow-template user-defined

Field	Description
user-defined flow template	Type of the user-defined flow template: basic or extend
name	Name of the flow template
index	Index of the flow template
total reference counts	Total number of the times that the flow template is referenced.
fields	Fields included in the flow template

display flow-template interface

Syntax **display flow-template interface** [*interface-type interface-number*]

View Any view

Parameters *interface-type interface-number*: Specifies an interface by its type and number.

Description Use the **display flow-template interface** command to display information about the user-defined flow template applied to the specified interface or all the interfaces.

Examples # Display information about the flow templates applied to all interfaces.

```
<Sysname> display flow-template interface
Interface: Ethernet1/0
user-defined flow template: basic
 name:f1, index:1, total reference counts:1
 fields: ip-protocol fragments ip-precedence
Interface: Ethernet1/1
user-defined flow template: basic
 name:f3, index:3, total reference counts:1
 fields: tos
```

Table 298 Field descriptions of display flow-template interface

Field	Description
Interface	Interface where the flow template is referenced
user-defined flow template	Type of the user-defined flow template: basic or extend
name	Name of the flow template
index	Index of the flow template
total reference counts	Reference count for the flow templates
fields	Fields included in the flow template

flow-template

Syntax **flow-template** *flow-template-name*

undo flow-template

View Interface view, port group view

Parameters *flow-template-name*: Flow template name, a case-insensitive string of 1 to 31 characters

Description Use the **flow-template** command to reference a flow template on current interface or port group.

Use the **undo flow-template** command to remove the referenced flow template from the interface or port group.

Note that on an interface you can reference only one flow template.

Examples # Reference flow template f1 on Ethernet 1/1/1.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1/1
[Sysname-Ethernet1/1/1] flow-template f1
```

Remove the referenced flow template on Ethernet 1/1/1.

```
[Sysname-Ethernet1/1/1] undo flow-template
```

Reference flow template f1 on port group 1.

```
<Sysname> system-view
[Sysname] link-aggregation group 1 mode manual
[Sysname] interface ethernet 1/1/2
[Sysname-Ethernet1/1/2] port link-aggregation group 1
[Sysname-Ethernet1/1/2] interface ethernet 1/1/3
[Sysname-Ethernet1/1/3] port link-aggregation group 1
[Sysname-Ethernet1/1/3] quit
[Sysname] port-group aggregation 1
[Sysname-port-group-aggregation-1] flow-template f1
```

flow-template basic

Syntax **flow-template** *flow-template-name* **basic** { **customer-vlan-id** | **dip** | **dipv6** | **dmac** | **dport** | **dscp** | **ethernet-protocol** | **fragments** | **icmp-code** | **icmp-type** | **icmpv6-code** | **icmpv6-type** | **ip-precedence** | **ip-protocol** | **ipv6-dscp** | **ipv6-fragment** | **ipv6-protocol** | **service-cos** | **service-vlan-id** | **sip** | **sipv6** | **smac** | **sport** | **tcp-flag** | **tos** } *

undo flow-template { **all** | **name** *flow-template-name* }

View System view

Parameters *flow-template-name*: Flow template name, a case-insensitive string of 1 to 31 characters.

basic: Sets the type of the flow template to basic.

customer-vlan-id: Customer VLAN ID.

dip: Destination IP address.

dipv6: Destination IPv6 address.

dmac: Destination MAC address.

dport: Destination Layer 4 port.

dscp: Differentiated service code point (DSCP) field in the IP header.

ethernet-protocol: Protocol type field in the Ethernet frame header.

fragments: Fragments field in the IP header.

icmp-code: ICMP code field.

icmp-type: ICMP type field.

icmpv6-code: IPv6 code field.

Icmpv6-type: IPv6 type field.

ip-precedence: Precedence field in the IP header.

ip-protocol: Protocol type field in the IP header.

ipv6-dscp: DSCP field in the IPv6 header.

ipv6-fragments: IPv6 fragments flag.

ipv6-protocol: Protocol type in the IPv6 header.

service-cos: Specifies the service provider 802.1p COS field.

service-vlan-id: Service provider VLAN ID.

sip: Source IP address.

sipv6: Source IPv6 address.

smac: Source MAC address.

sport: Source Layer 4 port.

tcp-flag: Flags field.

tos: ToS field.

all: All flow templates.

Description Use the **flow-template basic** command to create a basic flow template.

Use the **undo flow-template** command to remove the specified or all flow templates.

When removing templates, make sure that they are not referenced on interfaces. Otherwise, your removing attempt will fail.

Examples # Create a basic flow template.

```
<Sysname> system-view
[Sysname] flow-template f1 basic dip smac ip-protocol tcp-flag
```

Remove flow template f1.

```
[Sysname] undo flow-template name f1
```

Remove all flow templates.

```
[Sysname] undo flow-template all
```

flow-template extend

Syntax **flow-template** *flow-template-name* **extend** { **ipv4** *offset-max-value length-max-value* | **ipv6** *offset-max-value length-max-value* | **l2** *offset-max-value length-max-value* | **l4** *offset-max-value length-max-value* | **l5** *offset-max-value length-max-value* } *

undo flow-template { **all** | **name** *flow-template-name* }

View System view

Parameters *flow-template-name*: Flow template name, a case-insensitive string of 1 to 31 characters.

extend: Sets the type of the flow template to extend.

ipv4: Sets the offset from the beginning of the IPv4 header.

ipv6: Sets the offset from the beginning of the IPv6 header.

l2: Sets the offset from the beginning of the Layer 2 frame header.

l4: Sets the offset from the beginning of the Layer 4 header.

l5: Sets the offset from the beginning of the Layer 5 header.

offset-max-value: The maximum offset relative to the referential location.

length-max-value: The maximum comparing length.

all: Specifies to remove all flow templates.

Description Use the **flow-template extend** command to create an extended flow template. If no offset type is specified, the **start** keyword applies.

Use the **undo flow-template** command to remove the specified or all flow templates.

When removing templates, make sure that they are not referenced on interfaces. Otherwise, your removing attempt will fail.

Examples # Create an extended flow template.

```
<Sysname> system-view
[Sysname] flow-template f2 extend l2 3 10 ipv4 5 8
```

Remove flow template f2.

```
[Sysname] undo flow-template name f2
```

Remove all flow templates.

```
[Sysname] undo flow-template all
```

62 TRAFFIC SHAPING CONFIGURATION COMMANDS

display qos gts interface

Syntax **display qos gts interface** [*interface-type interface-number*]

View Any view

Parameters *interface-type interface-number*: Specifies an interface by its type and number.

Description Use the **display qos gts interface** command to view parameter configuration and statistics information of generic traffic shaping (GTS) on an interface or all interfaces.

If no interface is specified, GTS configuration and statistics information of all interfaces is displayed.

Examples # Display the GTS parameter configuration information and statistic information on all the interfaces.

```
<Sysname> display qos gts interface
Interface: Ethernet1/1/1
Rule(s): If-match any
 CIR 10000 (kbps), CBS 100000 (byte)
 Rule(s): If-match queue  2
 CIR 10000 (kbps), CBS 400000 (byte)
```

Table 299 Field descriptions of the display qos gts command

Filed	Description
Interface	Interface name, consisting of interface type and interface number
Rule(s)	Matching rules
CIR	Committed information rate, in kbps
CBS	Committed burst size, that is, the depth of the token bucket holding burst traffic, in bytes

qos gts

Syntax **qos gts** { **any** | **queue** *queue-number* } **cir** *committed-information-rate* [**cbs** *committed-burst-size*]

undo qos gts { **any** | **queue** *queue-number* }

View Ethernet interface view, port group view

Parameters **any**: Specifies to perform traffic shaping (TS) for all the IP data packets.

queue *queue-number*: Specifies to perform TS for data packets in a queue identified by the *queue-number* argument.

cir *committed-information-rate*: Committed information rate.

cbs *committed-burst-size*: Committed burst size, which must be the multiple of 4000. The default CBS value is expressed in the formula MIN (cir*62.5, 16000000), that is, the minimum value of cir*62.5 and 16000000.

*If the **cbs** keyword is not specified in this command, the system calculates the CBS value using the formula cir*62.5 if cir*62.5 is smaller than 16000000. Because CBS must be the multiple of 4000, the system adjusts the calculation result of cir*62.5 automatically if the calculation result is not the multiple of 4000.*

Description Use the **qos gts** command to set TS parameters for traffic of a particular class or all the traffic and start TS.

Use the **undo qos gts** command to cancel the TS parameters set for traffic of a particular class or all the traffics.

Use the **qos gts any** command to set TS parameters for all the traffics.

Use the **qos gts queue** command to set TS parameters for the traffic in a particular queue.

By default, a port is not configured with any TS parameter.

Related commands: **acl**.

*CIR and CBS must satisfy the following formula: **cbs** >= **cir** * 62.5.*

Examples # Perform TS for all the packets on Ethernet 6/1/1. The normal traffic rate (that is, CIR) is 200 kbps, and CBS is 50000 bytes.

```
<Sysname> system-view
[Sysname] interface ethernet6/1/1
[Sysname-Ethernet6/1/1] qos gts any cir 200 cbs 50000
```

63 QoS Policy Class Defining Commands

display traffic classifier

Syntax **display traffic classifier user-defined** [*tcl-name*]

View Any view

Parameters **user-defined**: User-defined class.

tcl-name: Class name.

Description Use the **display traffic classifier** command to view the information about the user-defined classes.

Examples # Display the information about user-defined classes.

```
<Sysname> display traffic classifier user-defined
User Defined Classifier Information:
 Classifier: USER1
 Operator: AND
  Rule(s) : if-match ip-precedence 5

 Classifier: database
  Operator: AND
  Rule(s) : if-match acl 3131
            if-match inbound-interface Ethernet4/1/1
```

Table 300 Field descriptions of the display traffic classifier user-defined command

Field	Description
User Defined Classifier Information	Class type: user-defined
Classifier	Class name and the class content (of multiple types)
Operator	Logical relationship between classification rules
Rule	Classification rule

if-match

Syntax **if-match** *match-criteria*

undo if-match *match-criteria*

View Class view

Parameters *match-criteria*: Match rules of a class. The values are as shown in Table 301:

Table 301 Values of match rules of a class

Value	Description
acl { **IPv6** | *acl-numbe*r }	Define ACL matching rules The *acl-number* argument is the number of an ACL, which is in the range of 2000 to 5999 for IPv4 ACLs and in the range of 2000 to 3999 for IPv6 ACLs.
dscp *dscp-list*	Define DSCP matching rules The *dscp-list* argument is the list of DSCP values and up to eight DSCP values can be input. The DSCP value is in the range 0 to 63.
destination-mac *mac-address*	Define destination MAC address matching rules
dot1p *dot1p-id*	Define dot1p matching rules
ip-precedence *ip-precedence-list*	Define IP precedence matching rules The *ip-precedence-list* argument is the list of ip-precedence values and up to eight ip precedence values can be input. The ip-precedence value is in the range of 0 to 7.
protocol *protocol-name*	Define protocol matching rules The *protocol-name* argument can be IP, IPv6 or bittorrent.
customer-vlan-id { *vlan-id-list* | *vlan-id1* **to** *vlan-id2* }	Define customer network VLAN ID matching rules The *vlan-id-list* argument is the list of VLAN IDs and up to eight VLAN IDs can be input. The *vlan-id1* **to** *vlan-id2* argument-keyword combination represents a VLAN ID range, where the *vlan-id1* argument must be smaller than the *vlan-id2* argument.
source-mac *mac-address*	Define source MAC address matching rules
service-vlan-id { *vlan-id-list* | *vlan-id1* **to** *vlan-id2* }	Define service provider network VLAN ID matching rules The *vlan-id-list* argument is the list of VLAN IDs and up to eight VLAN IDs can be input. The *vlan-id1* **to** *vlan-id2* argument-keyword combination represents a VLAN ID range, where the *vlan-id1* argument must be smaller than the *vlan-id2* argument.

Description Use the **if-match** command to define matching rules for packets.

Use the **undo if-match** command to delete the existing matching rules.

When defining the rules, take the following into consideration:

1 Define ACL matching rules

- If the ACL referenced in a class is not created, the matching rule cannot be applied to the hardware.
- A class can reference the same ACL by the ACL name and the ACL number respectively.

2 Define destination MAC address matching rules

- The destination MAC address matching rules are only meaningful for the outbound policies on Ethernet ports.
- For a class, you can configure multiple commands which cannot be overwritten.

3 Define source MAC address matching rules

- The source MAC address matching rules are only meaningful for the inbound policies on Ethernet ports.
- For a class, you can configure multiple commands which cannot be overwritten.

4 Define DSCP matching rules

- For a class, you can configure multiple commands which cannot be overwritten. The DSCP values specified by them are automatically arranged in ascending order. Only when the specified DSCP values are identical with those in the rule (sequence may be different) can the command be deleted.
- You may configure up to eight DSCP values in one command. If multiple DSCPs of the same value are specified, the system regards them as one. Relation between different DSCP values is "OR".

5 Define IP precedence matching rules

- When the command is configured, the IP precedence values are arranged automatically in ascending order.
- You may configure up to eight IP precedence values in one command. If multiple IP precedences of the same value are specified, the system regards them as one. Relation between different IP precedence values is "OR".

6 Define customer network VLAN ID matching rules and service provider network VLAN ID matching rules

- For a class, you can configure multiple commands which cannot be overwritten. When the command is configured, the *vlan-id* values are arranged automatically in ascending order. Only when the specified VLAN ID values are identical with those in the rule (sequence may be different) can the command be deleted.
- You may configure multiple VLAN ID values in one command. If multiple VLAN IDs of the same value are specified, the system regards them as one. Relation between different VLAN IDs is "OR".

Related commands: **traffic classifier**.

Examples # Define a matching rule to match IP packets for class 1.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match protocol ip
```

Define a matching rule for class 1 to match packets with the destination MAC address 0050-ba27-bed3.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match destination-mac 0050-ba27-bed3
```

Define a matching rule for class 2 to match packets with the source MAC address 0050-ba27-bed2.

```
<Sysname> system-view
[Sysname] traffic classifier class2
[Sysname-classifier-class2] if-match source mac 0050-ba27-bed2
```

Define a matching rule for class 1 to match IPv6 ACL 3101.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match ipv6 acl 3101
```

Define a matching rule for class 1 to match packets with IP precedence 1 or 6.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match ip-precedence 1 6
```

Define a matching rule for class 1 to match packets with the customer VLAN ID 1, 6, or 9.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match customer-vlan-id 1 6 9
```

traffic classifier

Syntax **traffic classifier** *tcl-name* [**operator** { **and** | **or** }]

undo traffic classifier *tcl-name*

View System view

Parameters **and**: Specifies the relationship between the rules in the class as logic AND (that is, the packet that matches all the rules belongs to this class).

or: Specifies the relationship between the rules in the class as logic OR (that is, the packet that matches any one of the rules belongs to this class).

tcl-name: Class name.

Description Use the **traffic classifier** command to define a class and enter the class view.

Use the **undo traffic classifier** command to delete a class.

By default, the relationship between the rules in a class is logic AND.

Related commands: **qos policy**, **qos apply policy**, and **classifier behavior**.

Examples # Define a class named **class1**.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1]
```

64 QoS Policy Traffic Behavior Defining Commands

accounting

Syntax **accounting**

undo accounting

View Traffic behavior view

Parameters None

Description Use the **accounting** command to configure the accounting action for a traffic behavior.

Use the **undo accounting** command to cancel the accounting action configured for a traffic behavior.

Related commands: **qos policy**, **traffic behavior**, and **classifier behavior**.

Examples # Configure the accounting action for the traffic behavior **database**.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] accounting
```

car

Syntax **car cir** *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]] [**pir** *peak-information-rate*] [**red** *action*]

undo car

View Traffic behavior view

Parameters **cir** *committed-information-rate*: Committed information rate in kbps, that is, the average traffic rate.

cbs *committed-burst-size*: Committed burst size, number of bits that can be sent in each interval. By default, the CBS is MAX (cir*62.5, 1875), which means the maximum number of cir*62.5 and 1875.

ebs *excess-burst-size*: Excessive burst size. It defaults to 0.

pir *peak information rate*: Peak information rate in kbps.

red: Action conducted to packets when traffic of packets does not conform to the CIR. By default, the action of **red** is **discard**.

action: Action conducted on a packet, including the following types:

- **discard**: Drops the packet.
- **pass**: Transmits the packet.

Description Use the **car** command to configure traffic policing for a traffic behavior.

Use the **undo car** command to cancel traffic policing configured for a traffic behavior.

If this command is configure for a traffic behavior multiple times, the new command overwrites the previous one.

Related commands: **qos policy**, **traffic behavior**, and **classifier behavior**.

CIR, CBS, EBS, and PIR must satisfy the following formulas:

- ***cbs*** *>=* ***cir*** ** 62.5*
- ***ebs*** *>=* ***pir*** ** 50ms*
- ***pir*** *>=* ***cir***

Examples # Configure traffic policing for the traffic behavior **database**. The following traffic policing parameters are adopted: CIR is 200 kbps; EBS is 50000 bytes; when the traffic rate exceeds 200 kbps, the packets are dropped.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] car cir 200 cbs 50000 ebs 0 red discard
```

display traffic behavior

Syntax **display traffic behavior user-defined** [*behavior-name*]

View Any view

Parameters **user-defined**: User-defined traffic behavior.

behavior-name: Behavior name. If it is not specified, the information of all the traffic behaviors is displayed.

Description Use the **display traffic behavior** command to display the information of the specific traffic behavior.

Examples # Display information of all the user-defined traffic behaviors.

```
<Sysname> display traffic behavior user-defined
  User Defined Behavior Information:
    Behavior: test1
      Accounting Enable
      Committed Access Rate:
        CIR 20000 (kbps), CBS 300000 (byte), EBS 100 (byte), PIR 25000 (kbps)
        Red Action: discard
      Filter enable : permit
      Marking:
        Remark dot1p COS 2
    Behavior: test2
      Accounting Enable
      Committed Access Rate:
        CIR 10000 (kbps), CBS 250000 (byte), EBS 100 (byte), PIR 25000 (kbps)
        Red Action: discard
      Filter enable : deny
      Marking:
        Remark dot1p COS 2
```

Table 302 Field descriptions of the display traffic behavior user-defined command

Field	Description
User Defined Behavior Information	Behavior type: user-defined
Behavior	Behavior name and the behavior content (of multiple types)
Accounting enable	The accounting action is enabled for the traffic behavior
Committed Access Rate	Information about rate limiting
Red Action	Action conducted to packets nonconforming to CIR
Filter enable	The traffic filtering action is configure for the traffic behavior
Marking	Information about priority marking

filter

Syntax **filter** { **deny** | **permit** }

undo filter

View Traffic behavior view

Parameters **deny**: Discards the packet.

permit: Transmits the packet.

Description Use the **filter** command to configure the traffic filtering action for a traffic behavior.

Use the **undo filter** command to cancel the traffic filtering action configured for a traffic behavior.

Examples # Configure the traffic filtering action for the traffic behavior **database**.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] filter deny
```

nest

Syntax **nest top-most vlan-id** *vlan-id-value*

undo nest

View Traffic behavior view

Parameters *vlan-id-value*: VLAN ID of the outer VLAN tag.

Description Use the **nest** command to configure the action of creating an outer VLAN tag for a traffic behavior.

Use the **undo nest** command to cancel the action of creating an outer VLAN tag configured for the traffic behavior.

Note that:

- A policy configured with the action of creating an outer VLAN tag can be applied to only the ingress direction of an interface.
- If this command is executed multiple times, the new command overwrites the previous one.

Related commands: **qos policy**, **traffic behavior**, **classifier behavior**.

Examples # Configure the action of creating outer VLAN tag 657 for traffic behavior **be1**.

```
<Sysname> system-view
[Sysname] traffic behavior be1
[Sysname-behavior-be1] nest top-most vlan-id 657
```

primap

Syntax **primap pre-defined** { **dscp-lp** | **dscp-dp** | **dscp-dot1p** | **dscp-dscp** | **color+dscp-dscp** | **color+dscp-dp** | **color+dscp-lp** | **color+dscp-dot1p** | **color+lp-dot1p** }

undo primap pre-defined { **dscp-lp** | **dscp-dp** | **dscp-dot1p** | **dscp-dscp** | **color+dscp-dscp** | **color+dscp-dp** | **color+dscp-lp** | **color+dscp-dot1p** | **color+lp-dot1p** }

View Traffic behavior view

Parameters **pre-defined**: Pre-defined priority mapping table.

dscp-lp: DSCP-to-local-precedence mapping table.

dscp-dp: DSCP-to-drop-precedence mapping table.

dscp-dot1p: DSCP-to-802.1p-precedence mapping table.

dscp-dscp: DSCP-to-DSCP mapping table.

color+dscp-dscp: Colored DSCP-to-DSCP mapping table.

color+dscp-dp: Colored DSCP-to-drop-precedence mapping table.

color+dscp-lp: Colored DSCP-to-local-precedence mapping table.

color+dscp-dot1p: Colored DSCP-to-802.1p-precedence mapping table.

color+lp-dot1p: Colored local-precedence-to-801.p-precedence mapping table.

Description Use the **primap** command to configure the action of obtaining other precedence values through the corresponding priority mapping table for a traffic behavior.

Use the **undo primap** command to cancel the action of obtaining other precedence values through the corresponding priority mapping table configured for a behavior. Note that a colored priority mapping table must be used in conjunction with the **car** command.

Related commands: **display qos map-table**.

Examples # Obtain the local precedence values for packets through the DSCP-to-local-precedence mapping table.

```
<Sysname> system-view
[Sysname] traffic behavior behavior1
[Sysname-behavior-behavior1] primap pre-defined dscp-dp
```

redirect

Syntax **redirect** { **cpu** | **interface** *interface-type interface-number* | **next-hop** { *ipv4-add* [*ipv4-add*] | *ipv6-add* [*interface-type interface-number*] [*ipv6-add* [*interface-type interface-number* | **link-aggregation group** *group-number*]] } }

undo redirect

View Traffic behavior view

Parameters **cpu**: Redirects traffic to CPU.

interface: Redirects traffic to specified interface.

next-hop: Redirects traffic to the next hop.

interface-type interface-number: Specifies an interface by its type and number.

ipv4-add: Next hop IPv4 address.

ipv6-add: Next hop IPv6 address. If the IPv6 address is a local address, an interface must be configured for the next hop IPv6 address; otherwise, an interface need not be configured for the next hop IPv6 address.

link-aggregation: Redirects traffic to a link aggregation group.

group *group-number*: Group number of a link aggregation group.

Description User the **redirect** command to configure the traffic redirecting action for a traffic behavior.

User the **undo redirect** command to cancel the traffic redirecting action configured for a traffic behavior.

CAUTION:

- *When the traffic redirecting action is configured, if the outgoing interface to be redirected to is bound to an NAT virtual interface, packets sent from this outgoing interface are redirected to the L3+NAT module, thus resulting in traffic redirecting failure.*
- *The policy routing function can be implemented through configuring the action of redirecting traffic to the next hop.*
- *Two next hop addresses can be configured for the action of redirecting traffic to the next hop, with one address being the primary next hop address and the other being the secondary next hop address. The traffic is redirected to the primary next hop address if the primary next hop address exists; otherwise, the traffic is redirected to the secondary next hop address.*
- *The device can only operate as follows: with the traffic redirected to the next hop address, if neither the primary next hop address nor the secondary next hop address exists, the device drops these packets.*

Examples # Configure the action of redirecting traffic to Ethernet 1/1/1 for the traffic behavior **database**.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] redirect interface ethernet1/1/1
```

remark service-vlan-id

Syntax **remark service-vlan-id** *vlan-id-value*

undo remark service-vlan-id

View Traffic behavior view

Parameters *vlan-id-value*: Service provider network VLAN ID of the packets. This argument ranges from 1 to 4094.

Description Use the **remark service-vlan-id** command to configure the action of marking the service provider network VLAN ID of the packets for a traffic behavior.

Use the **undo remark atm-clp** command to cancel the action of marking the service provider network VLAN ID of the packets configured for a traffic behavior.

Related commands: **qos policy**, **traffic behavior**, and **classifier behavior**.

Examples # Mark the packets with the service provider network VLAN ID 2.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark service-vlan-id 2
```

remark dot1p

Syntax **remark dot1p** *8021p*

undo remark dot1p

View Traffic behavior view

Parameters *8021p*: Remarked 802.1p priority value, in the range 0 to 7.

Description Use the **remark dot1p** command to configure the 802.1p priority value of the remarked packet.

Use the **undo remark dot1p** command to remove the 802.1p priority value from the remarked packet.

Related commands: **qos policy**, **traffic behavior**, and **classifier behavior**.

Examples # Set the 802.1p priority value of the remarked packet to 2.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark dot1p 2
```

remark drop-precedence

Syntax **remark drop-precedence** *drop-precedence-value*

undo remark drop-precedence

View Traffic behavior view

Parameters *drop-precedence-value*: Drop precedence value to be marked, in the range of 0 to 2.

Description Use the **remark drop-precedence** command to configure the action of marking the drop precedence of packets.

Use the **undo remark drop-precedence** command to cancel the action of marking the drop precedence of packets.

Related commands: **qos policy**, **traffic behavior**, and **classifier behavior**.

Examples # Mark the packets with drop precedence 2.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark drop-precedence 2
```

remark dscp

Syntax **remark dscp** *dscp-value*

undo remark dscp

View Traffic behavior view

Parameters *dscp-value*: DSCP value, in the range 0 to 63, which can be any of these keywords as follows:

Table 303 DSCP keywords and values

Keyword	DSCP value (binary)	DSCP value (decimal)
default	000000	0
af11	001010	10
af12	001100	12
af13	001110	14
af21	010010	18
af22	010100	20
af23	010110	22
af31	011010	26
af32	011100	28
af33	011110	30
af41	100010	34
af42	100100	36
af43	100110	38
cs1	001000	8
cs2	010000	16
cs3	011000	24
cs4	100000	32
cs5	101000	40
cs6	110000	48
cs7	111000	56

Table 303 DSCP keywords and values

Keyword	DSCP value (binary)	DSCP value (decimal)
ef	101110	46

Description Use the **remark dscp** command to set a remarked DSCP value for IP packets belonging to the class.

Use the **undo remark dscp** command to disable DSCP remark.

Related commands: **qos policy**, **traffic behavior**, **classifier behavior**.

Examples # Remark the DSCP of the IP packets belonging to the class to 6.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark dscp 6
```

remark local-precedence

Syntax **remark local-precedence** *local-precedence*

undo remark local-precedence

View Traffic behavior view

Parameters *local-precedence*: Local precedence value to be marked, in the range of 0 to 7.

Description Use the **remark local-precedence** command to configure the action of marking the local precedence of packets.

Use the **undo remark local-precedence** command to cancel the action of marking the local precedence of packets.

Related commands: **qos policy**, **traffic behavior**, and **classifier behavior**.

Examples # Mark packets with the local precedence 2.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark local-precedence 2
```

traffic behavior

Syntax **traffic behavior** *behavior-name*

undo traffic behavior *behavior-name*

View System view

Parameters *behavior-name*: Behavior name.

Description Use the **traffic behavior** command to define a traffic behavior and enter the behavior view.

Use the **undo traffic behavior** command to delete a traffic behavior.

Related commands: **qos policy**, **qos apply policy**, and **classifier behavior**.

Examples # Define a traffic behavior named behavior1.

```
<Sysname> system-view
[Sysname] traffic behavior behavior1
[Sysname-behavior-behavior1]
```

65 QoS Policy Defining Commands

classifier behavior

Syntax **classifier** *tcl-name* **behavior** *behavior-name*

undo classifier *tcl-name*

View Policy view

Parameters *tcl-name*: Name of a defined class.

behavior-name: Name of a defined traffic behavior.

Description Use the **classifier behavior** command to specify the behavior for the class in the policy.

Use the **undo classifier** command to remove the application of the class in the policy.

Each class in the policy can only be associated with one behavior.

Related commands: **qos policy**.

Examples # Specify the behavior test for the class database in the policy user1.

```
<Sysname> system-view
[Sysname] qos policy user1
[Sysname-qospolicy-user1] classifier database behavior test
[Sysname-qospolicy-user1]
```

display qos policy

Syntax **display qos policy user-defined** [*policy-name* [**classifier** *tcl-name*]]

View Any view

Parameters **user-defined**: Policy pre-defined by the user.

policy-name: Policy name. If it is not specified, the configuration information of all the user-defined policies is displayed.

tcl-name: Class name in the policy.

Description Use the **display qos policy** command to display the configuration information of the specified class or all the classes and associated behaviors in the user-defined policy or all policies.

Examples # Display the configuration information of the specified class or all the classes and associated behaviors in the user-defined policy.

```
<Sysname> display qos policy user-defined
  User Defined QoS Policy Information:

  Policy: default
  Policy: user1
   Classifier: class1
     Behavior: test
      Accounting Enable
      Committed Access Rate:
        CIR 20000 (kbps), CBS 300000 (byte), EBS 100 (byte), PIR 25000 (kbps
)
        Red Action: discard
      Filter enable : permit
      Marking:
        Remark dot1p COS 2
```

Table 304 Field descriptions of the display qos policy command

Field	Description
Policy	Policy name
Classifier	Class name. Multiple classes may exist in a policy, each corresponding with a behavior and multiple matching rules. For details, refer to the **traffic classifier** command on page 1020.
Behavior	The behavior in a policy that corresponds with a class. Each behavior can have multiple matching rules. For details, refer to the **traffic behavior** command on page 1029.
Accounting enable	The traffic statistics action is configured for the traffic behavior
Committed Access Rate	Information about rate limiting
Red Action	Action conducted to packets nonconforming to CIR (that is, red packets)
Filter enable	The traffic filtering action is configure for the traffic behavior
Marking	Information about priority marking

display qos policy interface

Syntax **display qos policy interface** [*interface-type interface-number*] [**inbound** | **outbound**]

View Any view

Parameters *interface-type interface-number*: Specifies an interface by its type and number.

inbound: Inbound direction.

outbound: Outbound direction.

Description Use the **display qos policy interface** command to view the configuration and operating state about the policy on the specified interface.

Examples # Display the configuration and operating state about the policy on Ethernet 4/1/1.

```
<Sysname> display qos policy interface ethernet 4/1/1

  Interface: Ethernet4/1/1

  Direction: Inbound

  Policy: test1
   Classifier: cl1
     Operator: AND
     Rule(s) : If-match acl 2345
     Behavior: be1
      Committed Access Rate:
        CIR 10 (kbps), CBS 10000 (byte), EBS 0 (byte)
        Red Action: discard
        Green : 0(Bytes)
        Yellow: 0(Bytes)
        Red   : 0(Bytes)
```

Table 305 Field descriptions of the display qos policy interface command

Field	Description
Interface	Interface name, consisting of interface type and interface number
Direction	Specifies the direction that the policy is applied to the interface.
Policy	Name of the policy applied to the interface
Classifier	Classification rules and corresponding configurations in the policy
Operator	Logical relationship between classification rules
Rule(s)	Classification rules of class
Behavior	Name and configuration information of the behavior. Refer to related command of behavior.
Committed Access Rate	Information about rate limiting
CIR	Committed information rate in kbps
CBS	Committed burst size, i.e. the depth of the token bucket holding burst traffic, in bytes
EBS	Excess burst size, in bytes
Red	Traffic statistics information about red traffic
Green	Traffic statistics information about green traffic
Yellow	Traffic statistics information about yellow traffic

qos apply policy

Syntax **qos apply policy** *policy-name* { **inbound** | **outbound** }

undo qos apply policy { **inbound** | **outbound** }

View Interface view, port group view

Parameters **inbound**: Inbound direction.

outbound: Outbound direction.

policy-name: Policy name.

Description Use the **qos apply policy** command to apply associated policy to the interface.

Use the **undo qos apply policy** command to delete the associated policy from the interface.

To successfully apply the policy to the interface, you must make sure that the sum of bandwidth specified for the AF and EF classes in the policy is smaller than the available bandwidth of the interface. You can modify the available bandwidth of the current interface. If the sum of their bandwidth still exceeds that modified value, the policy will be deleted.

For a policy to be applied in the inbound direction, it cannot contain classes associated with traffic behaviors specified using **gts**.

Configured in interface view, the setting is effective on the current interface only; configured in port group view, the setting is effective on all the ports in the port group.

Examples # Apply the policy USER1 in the outbound direction of Ethernet 1/1/1.

```
<Sysname> system-view
[Sysname] interface ethernet1/1/1
[Sysname-Ethernet1/1/1] qos apply policy USER1 outbound
```

qos policy

Syntax **qos policy** *policy-name*

undo qos policy *policy-name*

View System view

Parameters **policy** *policy-name*: Policy name.

Description Use the **qos policy** command to define a policy and enter policy view.

Use the **undo qos policy** command to delete a policy.

The policy cannot be deleted if it is applied on an interface. It is necessary to remove application of the policy on the current interface before deleting it via the **undo qos policy** command.

Related commands: **classifier behavior** and **qos apply policy**.

Examples # Define a policy named as USER1.

```
<Sysname> system-view
[Sysname] qos policy user1
[Sysname-qospolicy-user1]
```

66 HARDWARE-BASED CONGESTION MANAGEMENT CONFIGURATION COMMANDS

display qos sp

Syntax **display qos sp interface** [*interface-type interface-number*]

View Any view

Parameters *interface-type*: Interface type.

interface-number: Interface number.

Description Use the **display qos sp interface** command to display the strict priority (SP) queuing configuration on an interface.

If no interface is specified, the SP queuing configuration information on all the interfaces is displayed.

Related commands: **qos sp**.

Examples # Display the SP queuing configuration information on Ethernet 1/1/1/.

```
<Sysname> display qos sp interface ethernet 1/1/1
Output queue: Strict-priority queue
```

Table 306 Field descriptions of the display qos sp interface command

Field	Description
Output queue	Type of the current output queue
Strict-priority queue	Adopt the SP queuing mechanism for queue scheduling

qos sp

Syntax **qos sp**

undo qos sp

View Ethernet interface view, port group view

Parameters None

Description Use the **qos sp** command to configure SP queuing on a port.

Use the **undo qos sp** command to restore the default queuing algorithm on the port.

Configured in interface view, the setting is effective on the current interface only; configured in port group view, the setting is effective on all the ports in the port group.

Related commands: **display qos sp interface**.

Examples # Adopt SP queuing for queue scheduling on Ethernet 6/1/1.

```
<Sysname> system-view
[Sysname] interface ethernet6/1/1
[Sysname-Ethernet6/1/1] qos sp
```

display qos wrr interface

Syntax **display qos wrr interface** [*interface-type interface-number*]

View Any view

Parameters *interface-type*: Interface type.

interface-number: Interface number.

Description Use the **display qos wrr interface** command to display the weighted round robin (WRR) queuing configuration on an interface.

If no interface is specified, the WRR queuing configuration on all the interfaces is displayed.

Related commands: **qos wrr**.

Examples # Display the WRR queuing configuration information on Ethernet 6/1/1.

```
<Sysname> display qos wrr interface ethernet 6/1/1
Interface: Ethernet6/1/1
Output queue:   Weighted round robin queue
Queue ID    Group   Weight
-------------------------------------------
0                2       100
1                1       1
2                1       1
3                1       1
4                1       1
5                1       1
6                1       1
7                1       1
```

Table 307 Field descriptions of the display qos wrr interface command

Field	Description
Interface	Interface name consisting of interface type and interface number.

Table 307 Field descriptions of the display qos wrr interface command

Field	Description
Output queue	Type of the current output queue
Queue ID	Queue ID
Group	ID of the group that the current queue belongs to By default, all the queues belong to group 1.
Weight	Weight of a queue during queue scheduling

qos wrr

Syntax **qos wrr**

undo qos wrr

View Ethernet interface view, port group view

Parameters None

Description Use the **qos wrr** command to enable WRR queuing on a port.

Use the **undo qos wrr** command to disable WRR queuing on a port.

Configured in interface view, the setting is effective on the current interface only; configured in port group view, the setting is effective on all the ports in the port group.

Before configuring WRR, make sure that you have used the **qos wrr** command to enable WRR queuing on a port.

Examples # Enable WRR queuing on Ethernet 1/1/1.

```
<Sysname> system-view
[Sysname] interface ethernet1/1/1
[Sysname-Ethernet1/1/1] qos wrr
```

qos wrr group

Syntax **qos wrr** *queue-id* **group** { { **1** | **2** } **weight** *schedule-value* | **sp** }

undo qos wrr

View Ethernet interface view, port group view

Parameters *queue-id*: Queue ID, in the range of 0 to 7.

1 | **2** : Specifies the WRR priority group a queue belongs to. All queues belong to group 1 by default. The **group 1** keyword indicates that a queue belongs to WRR

priority group 1, and the **group 2** keyword indicates that a queue belongs to WRR priority group 2.

For group-based WRR queuing, all the queues adopt the mix of WRR queue scheduling algorithm and the SP queue scheduling algorithm. You can allocate an output queue to WRR priority queue group 1, WRR priority queue group 2, or SP queue group as required. Queues are scheduled as follows: each group selects a candidate queue according to its own queue scheduling algorithm, and then the three candidate queues are scheduled using the SP algorithm.

sp: Indicates that the queue belongs to WRR priority group 0 (that is, the SP queue).

weight *schedule-value*: Scheduling weight value of a queue. The **weight** keyword indicates that the weight of a queue is calculated based on the queue length.

Description Use the **qos wrr group** command to configure or modify WRR queuing parameters.

Use the **undo qos wrr** command to restore the default queuing algorithm on the port.

If you configure a queue on a port as a WRR queue, the current port adopts the WRR queue scheduling algorithm. The queues which are not configured adopt the default WRR scheduling weight value and belong to the default WRR priority group.

Configured in interface view, the setting is effective on the current interface only; configured in port group view, the setting is effective on all the ports in the port group.

Related commands: **display qos wrr interface**.

Examples # Enable the WRR queue scheduling algorithm on Ethernet 1/1/1, set the scheduling weight value of queue 0 to 100, and allocate queue 0 to group 1.

```
<Sysname> system-view
[Sysname] interface ethernet1/1/1
[Sysname-Ethernet1/1/1] qos wrr
[Sysname-Ethernet1/1/1] qos wrr 0 group 1 weight 100
```

67 PRIORITY MAPPING CONFIGURATION COMMANDS

display qos map-table

Syntax **display qos map-table** [**dot1p-lp** | **dot1p-dp** | **dscp-lp** | **dscp-dp** | **dscp-dot1p** | **dscp-dscp** | **exp-rpr** | **dot1p-rpr** | **ippre-rpr** | **green+dscp-dscp** | **yellow+dscp-dscp** | **red+dscp-dscp** | **green+dscp-dp** | **yellow+dscp-dp** | **red+dscp-dp** | **green+dscp-lp** | **yellow+dscp-lp** | **red+dscp-lp** | **green+dscp-dot1p** | **yellow+dscp-dot1p** | **red+dscp-dot1p** | **green+lp-dot1p** | **yellow+lp-dot1p** | **red+lp-dot1p**]

View Any view

Parameters **dot1p-lp**: 802.1p-precedence-to-local-precedence mapping table.

dot1p-dp: 802.1p-precedence-to-drop-precedence mapping table.

dscp-lp: DSCP-to-local-precedence mapping table.

dscp-dp: DSCP-to-drop-precedence mapping table.

dscp-dot1p: DSCP-to-802.1p-precedence mapping table.

dscp-dscp: DSCP-to-DSCP mapping table.

exp-rpr: EXP-to-RPR-precedence mapping table.

dot1p-rpr: 802.1p-precedence-to-RPR-precedence mapping table.

ippre-rpr: IP-precedence-to-RPR-precedence mapping table.

green+dscp-dscp: DSCP-to-DSCP mapping table for green packets.

yellow+dscp-dscp: DSCP-to-DSCP mapping table for yellow packets.

red+dscp-dscp: DSCP-to-DSCP mapping table for red packets.

green+dscp-dp: DSCP-to-drop-precedence mapping table for green packets.

yellow+dscp-dp: DSCP-to-drop-precedence mapping table for yellow packets.

red+dscp-dp: DSCP-to-drop-precedence mapping table for red packets.

green+dscp-lp: DSCP-to-local-precedence mapping table for green packets.

yellow+dscp-lp: DSCP-to-local-precedence mapping table for yellow packets.

red+dscp-lp: DSCP-to-local-precedence mapping table for red packets.

green+dscp-dot1p: DSCP-to-802.1p-precedence mapping table for green packets.

yellow+dscp-dot1p: DSCP-to-802.1p-precedence mapping table for yellow packets.

red+dscp-dot1p: DSCP-to-802.1p-precedence mapping table for red packets.

green+lp-dot1p: Local-precedence-to-802.1p-precedence mapping table for green packets.

yellow+lp-dot1p: Local-precedence-to-802.1p-precedence mapping table for yellow packets.

red+lp-dot1p: Local-precedence-to-802.1p-precedence mapping table for red packets.

Description Use the **display qos map-table** command to display the configuration of a specific priority mapping table.

If the table type is not specified, the configuration information of all mapping tables is displayed.

Related commands: qos map-table.

Examples # Display the configuration information of the 802.1p-precedence-to-drop-precedence mapping table.

```
<Sysname> display qos map-table dot1p-dp
MAP-TABLE NAME: dot1p-dp   TYPE: pre-define
IMPORT  :  EXPORT
   0    :    0
   1    :    0
   2    :    0
   3    :    0
   4    :    0
   5    :    0
   6    :    0
   7    :    0
```

Table 308 Field descriptions of the display qos map-table command

Field	Description
MAP-TABLE NAME	Name of the mapping table
TYPE	Type of the mapping table
IMPORT	Import entry of the mapping table
EXPORT	Export entry of the mapping table

qos map-table

Syntax **qos map-table** { **dot1p-lp** | **dot1p-dp** | **dscp-lp** | **dscp-dp** | **dscp-dot1p** | **dscp-dscp** | **exp-rpr** | **dot1p-rpr** | **ippre-rpr** | **green+dscp-dscp** | **yellow+dscp-dscp** | **red+dscp-dscp** | **green+dscp-dp** | **yellow+dscp-dp** | **red+dscp-dp** | **green+dscp-lp** | **yellow+dscp-lp** | **red+dscp-lp** | **green+dscp-dot1p** | **yellow+dscp-dot1p** | **red+dscp-dot1p** | **green+lp-dot1p** | **yellow+lp-dot1p** | **red+lp-dot1p** }

View System view

Parameters **dot1p-lp**: 802.1p-precedence-to-local-precedence mapping table.

dot1p-dp: 802.1p-precedence-to-drop-precedence mapping table.

dscp-lp: DSCP-to-local-precedence mapping table.

dscp-dp: DSCP-to-drop-precedence mapping table.

dscp-dot1p: DSCP-to-802.1p-precedence mapping table.

dscp-dscp: DSCP-to-DSCP mapping table.

exp-rpr: EXP-to-RPR-precedence mapping table.

dot1p-rpr: 802.1p-precedence-to-RPR-precedence mapping table.

ippre-rpr: IP-precedence-to-RPR-precedence mapping table.

green+dscp-dscp: DSCP-to-DSCP mapping table for green packets.

yellow+dscp-dscp: DSCP-to-DSCP mapping table for yellow packets.

red+dscp-dscp: DSCP-to-DSCP mapping table for red packets.

green+dscp-dp: DSCP-to-drop-precedence mapping table for green packets.

yellow+dscp-dp: DSCP-to-drop-precedence mapping table for yellow packets.

red+dscp-dp: DSCP-to-drop-precedence mapping table for red packets.

green+dscp-lp: DSCP-to-local-precedence mapping table for green packets.

yellow+dscp-lp: DSCP-to-local-precedence mapping table for yellow packets.

red+dscp-lp: DSCP-to-local-precedence mapping table for red packets.

green+dscp-dot1p: DSCP-to-802.1p-precedence mapping table for green packets.

yellow+dscp-dot1p: DSCP-to-802.1p-precedence mapping table for yellow packets.

red+dscp-dot1p: DSCP-to-802.1p-precedence mapping table for red packets.

green+lp-dot1p: Local-precedence-to-802.1p-precedence mapping table for green packets.

yellow+lp-dot1p: Local-precedence-to-802.1p-precedence mapping table for yellow packets.

red+lp-dot1p: Local-precedence-to-802.1p-precedence mapping table for red packets.

Description Use the **qos map-table** command to enter the specified priority mapping table view.

Related commands: **display qos map-table**.

Examples # Enter 802.1p-precedence-to-drop-precedence mapping table view.

```
<Sysname> system-view
[Sysname] qos map-table dot1p-dp
[Sysname-maptbl-dot1p-dp]
```

import

Syntax **import** *import-value-list* **export** *export-value*

undo import { *import-value-list* | **all** }

View Priority mapping table view

Parameters *import-value-list*: Input parameters of a mapping table. Up to seven values can be input for a mapping table.

export-value: Output parameters of a mapping table.

all: Deletes all parameters in this mapping table.

Description Use the **import** command to configure the parameters in the specified priority mapping table to define a mapping rule or a group of mapping rules.

Use the **undo import** command to delete the mapping entries corresponding to specified mapping index. The deleted entries are restored to the default.

Related commands: display qos map-table.

Examples # Configure the parameters in the 802.1p-precedence-to-drop-precedence mapping table, with both 802.1p precedence 4 and 802.1p precedence 5 mapped to drop precedence 1.

```
<Sysname> system-view
[Sysname] qos map-table dot1p-dp
[Sysname-maptbl-dot1p-dp] import 4 5 export 1
```

qos priority

Syntax **qos priority** *priority-value*

undo qos priority

View Ethernet interface view, port group view

Parameters *priority-value*: Port priority value, in the range 0 to 7.

Description Use the **qos priority** command to configure the port priority of the current port.

Use the **undo qos priority** command to restore the port priority of the current port to the default value.

Configured in interface view, the setting is effective on the current interface only; configured in port group view, the setting is effective on all the ports in the port group.

By default, the port priority of a port is 0.

Examples # Set the port priority of Ethernet 1/1/1 to 2.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1/1
[Sysname-Ethernet1/1/1] qos priority 2
```

display qos trust interface

Syntax **display qos trust interface** [*interface-type interface-number*]

View Any view

Parameters *interface-type*: Interface type.

interface-number: Interface number.

Description Use the **display qos trust interface** command to display the information about the port priority trust mode of a port.

If no port is specified, the port priority trust mode information of all the ports is displayed.

Examples # Display the information about the port priority trust mode of Ethernet 1/1/1/.

```
<Sysname> display qos trust interface ethernet 1/1/1
Interface: Ethernet1/1/1
Port priority trust information
Port priority :0
Port priority trust type :  dot1p
```

Table 309 Field descriptions of the display qos trust interface command

Field	Description
Interface	Interface name, consisting of interface type and interface number
Port priority	Port priority
Port priority trust type	Port priority trust mode

qos trust dot1p

Syntax **qos trust dot1p**

undo qos trust

View Ethernet interface view, port group view

Parameters None

Description Use the **qos trust dot1p** command to set to trust 802.1p precedence on a port.

Use the **undo qos trust dot1p** command to restore the default.

By default, 802.1p precedence is not trusted on a port.

Configured in interface view, the setting is effective on the current interface only; configured in port group view, the setting is effective on all the ports in the port group.

Examples # Configure to trust the 802.1p precedence carried in packets on Ethernet 1/1/1.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1/1
[Sysname-Ethernet1/1/1] qos trust dot1p
```

68 CONGESTION AVOIDANCE WRED TABLE CONFIGURATION COMMANDS

display qos wred interface

Syntax **display qos wred interface** [*interface-type interface-number*]

View Any view

Parameters *interface-type*: Interface type.

interface-number: Interface number.

Description Use the **display qos wred interface** command to view weighed random early detection (WRED) configuration and statistics information of an interface.

If no interface is specified, WRED table configuration and statistics information of all interfaces is displayed.

Examples # Display WRED table configuration and statistics information of Ethernet 1/1/1.

```
<Sysname> display qos wred interface ethernet 1/1/1
Interface: Ethernet1/1/1
 Current WRED configuration:
 Applied WRED table name: table1
```

Table 310 Field descriptions of the display qos wred interface command

Field	Description
Interface	Interface name, consisting of interface type and interface number
Current WRED configuration	Current WRED configuration, that is, the applied WRED table

display qos wred table

Syntax **display qos wred table** [*table-name*]

View Any view

Parameters *table-name*: Name of the WRED table to be displayed.

Description Use the **display qos wred table** command to display the configuration information about a specific WRED table.

If no WRED table name is specified, the configuration information about all the WRED tables is displayed.

Examples # Display the configuration information about all the tables of the switch.

```
<Sysname> display qos wred table
Table Name: zhou
Table Type: Queue based WRED
QID:  gmin  gmax  gprob  ymin  ymax  yprob  rmin  rmax  rprob  exponent
------------------------------------------------------------------------
 0    76    134     1    33     66     1    11     23     1      9
 1    85    143     1    37     75     1    13     27     1      9
 2    95    153     1    42     85     1    16     32     1      9
 3   104    162     1    47     94     1    18     37     1      9
 4   114    172     1    52    104     1    21     42     1      9
 5   124    182     1    57    114     1    23     47     1      9
 6   133    191     1    61    123     1    25     51     1      9
 7   143    201     1    66    133     1    28     56     1      9

Table Name: table1
Table Type: Queue based WRED
QID:  gmin  gmax  gprob  ymin  ymax  yprob  rmin  rmax  rprob  exponent
------------------------------------------------------------------------
 0    76    134     1    33     66     1    11     23     1      9
 1    85    143     1    37     75     1    13     27     1      9
 2    15     50   100    15     50   100    15     50   100      9
 3   104    162     1    47     94     1    18     37     1      3
 4   114    172     1    52    104     1    21     42     1      9
 5   124    182     1    57    114     1    23     47     1      9
 6   133    191     1    61    123     1    25     51     1      9
 7   143    201     1    66    133     1    28     56     1      9
```

Table 311 Field descriptions of the display qos wred table command

Field	Description
Table name	WRED table name
Table type	WRED table type
QID	Queue ID
gmin	Lower threshold for green packets
gmax	Upper threshold for green packets
gprob	Maximum drop probability for green packets
ymin	Lower threshold for yellow packets
ymax	Upper threshold for yellow packets
yprob	Maximum drop probability for yellow packets
rmin	Lower threshold for red packets
rmax	Upper threshold for red packets
rprob	Maximum drop probability for red packets
exponent	Exponent used for calculating average queue length

qos wred

Syntax **qos wred queue table** *table-name*

undo qos wred table *table-name*

View System view

Parameters **table** *table-name*: Specifies the table name.

Description Use the **qos wred** command to create a WRED table and enter WRED table view.

Use the **undo qos wred table** command to delete the global WRED table.

By default, no global WRED table exists.

A WRED table being used cannot be deleted.

Related commands: **qos wfq**, **qos wred**, and **display qos wred interface**.

Examples # Create queue-based WRED table **table1**.

```
<Sysname> system-view
[Sysname] qos wred queue table table1
[Sysname-wred-table-table1]
```

---

queue

Syntax **queue** *queue-value* [**drop-level** *drop-level*] **low-limit** *low-limit* **high-limit** *high-limit* [**discard-probability** *discard-prob*]

undo queue { *queue-value* | **all** }

View WRED table view

Parameters *queue-value*: Queue ID.

drop-level *drop-level*: Drop level. If the **drop-level** *drop-level* keyword-argument combination is not specified, the parameters configured subsequently apply to packets of all drop levels in the specific queue.

low-limit *low-limit*: Lower threshold for the priority WRED table. The lower threshold is 10 by default.

high-limit *high-limit*: Upper threshold for the priority WRED table. The upper threshold is 30 by default.

discard-probability *discard-prob*: Denominator of drop probability. Each drop level has an independent drop probability denominator. The *discard-prob* argument is 10 by default.

Description Use the **queue** command to edit the content of the queue-based WRED table.

Use the **undo queue** command to restore the content of the WRED table to the default.

By default, a global queue-based WRED table has a set of applicable default parameters. Therefore, there are no default values for the parameters during editing. As long as no value is specified, the default values keep unchanged.

Related commands: **qos wred** (in system view).

Examples # Modify the drop parameter for packets of drop level 1 in queue 1 of the global queue-based WRED table **queue-table1**.

```
<Sysname> system-view
[Sysname] qos wred queue table queue-table1
[Sysname-wred-table-queue-table1]
[Sysname-wred-table-queue-table1] queue 1 drop-level 1 low-limit 10
high-limit 20 discard-probability 30
[Sysname-wred-table-queue-table1]
```

queue weighting-constant

Syntax **queue** *queue-value* **weighting-constant** *exponent*

undo queue *queue-value* **weighting-constant**

View WRED table view

Parameters *queue-value*: Queue ID.

weighting-constant *exponent*: Exponent used for calculating the average queue length. This argument defaults to 9.

Description Use the **queue weighting-constant** command to set the exponent used for calculating the average queue length for a queue-based WRED table.

Use the **undo queue weighting-constant** command to restore the default value.

Related commands: **qos wred**.

Examples # Set the exponent used for calculating the average queue length to 6 for the queue-based WRED table **queue-table1**.

```
<Sysname> system-view
[Sysname] qos wred queue table queue-table1
[Sysname-wred-table-queue-table1] queue 1 weighting-constant 12
[Sysname-wred-table-queue-table1]
```

apply

qos wred

Syntax **qos wred apply** *table-name*

undo qos wred apply

View Ethernet interface view, port group view

Parameters *table-name*: Name of a global WRED table.

Description Use the **qos wred apply** command to apply a global WRED table to a port.

Use the **undo qos wred apply** command to restore the default drop mode (that is, tail drop) on the port. This command also cancels the application of the WRED table to the port.

By default, a port adopts tail drop.

Configured in interface view, the setting is effective on the current interface only; configured in port group view, the setting is effective on all the ports in the port group.

Related commands: **display qos wred interface**, **display qos wred table**, and **qos wred table**.

Examples # Apply the queue-based WRED table **queue-table1** to Ethernet 1/1/1/.

```
<Sysname> system-view
[Sysname] interface ethernet1/1/1
[Sysname-Ethernet1/1/1] qos wred apply queue-table1
```

69 AGGREGATION CAR CONFIGURATION COMMANDS

qos car aggregative

Syntax **qos car** *car-name* **aggregative cir** *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]] [**pir** *peek-information-rate*] [**red** *action*]

undo qos car *car-name*

View System view

Parameters *car-name*: Name of an aggregation CAR.

aggregative: Specifies that the global CAR is aggregative. Only the aggregation CAR is supported currently.

cir *committed-information-rate*: Committed information rate (CIR) in kbps.

cbs *committed-burst-size*: Committed burst size, which must be the multiple of 4000. The default CBS value is expressed in the formula MIN (cir*62.5, 16000000), that is, the minimum value of cir*62.5 and 16000000.

ebs *excess-burst-size*: Excess burst size in bytes. This argument defaults to 0.

pir *peak-information-rate*: Peak information rate in kbps.

red *action*: Specifies the action conducted for red packets, whose traffic is not conforming to CIR.

The *action* argument can be:

- **discard**: Drops the packet.
- **pass**: Forwards the packet.

Description Use the **qos car aggregative** command to configure an aggregation CAR.

Use the **undo qos car aggregative** command to cancel the aggregation CAR configuration.

An aggregation CAR takes effect after it is applied to an interface or it is referenced in a policy.

CIR, CBS, EBS, and PIR must satisfy the following formulas:

- ***cbs*** >= ***cir*** * *62.5*
- ***ebs*** >= ***pir*** * *50ms*
- ***pir*** >= ***cir***

Examples # Configure CAR parameters for the aggregation CAR as follows: CIR is 200, CBS is 2000, and the action for red packets is **discard**.

```
<Sysname> system-view
[Sysname] qos car aggcar-1 aggregative cir 200 cbs 2000 red discard
```

car name

Syntax **car name** *car-name*

undo car

View Traffic behavior view

Parameters **name** *car-name*: Name of an aggregation CAR.

Description Use the **car name** *car-name* command to configure an aggregation CAR action for a traffic behavior.

Use the **undo car** command to remove the traffic policing action of a traffic behavior.

Examples # Configure the aggregation CAR action **aggcar-1** for the traffic behavior **be1**.

```
<Sysname> system-view
[Sysname] traffic behavior be1
[Sysname-behavior-be1] car name aggcar-1
```

display qos car name

Syntax **display qos car name** [*car-name*]

View Any view

Parameters *car-name*: Name of an aggregation CAR.

Description Use the **display qos car name** command to display the CAR configuration and statistics information of a specific aggregation CAR.

Examples # Display the configuration information of aggregation CAR **aggcar-1**.

```
<Sysname> display qos car name aggcar-1
Name: aggcar-1
  Mode: aggregative
  CIR 100(kbps)  CBS: 10000(byte)  EBS: 100000(byte)
  Red Action: discard
  Green packet 2300(Bytes)
  Yellow packet 0(Bytes)
  Red packet 4500(Bytes)
```

Table 312 Field descriptions of the display qos car name command

Field	Description
Name: aggcar-1	Name of the traffic policing action
Mode: aggregative	Type of the traffic policing action
CIR 200(Kbps) CBS: 2000(Bits) EBS: 0(Bits)	Traffic policing parameters
Red Action: discard	Action conducted to red packets
Green packet	Action conducted to green packets
Yellow packet	Traffic statistics about yellow packets
Red packet	Traffic statistics about red packets

reset qos car name

Syntax **reset qos car name** [*car-name*]

View User view

Parameters *car-name*: Name of an aggregation CAR. If this argument is not specified, this command clears the statistics about all the aggregation CARs.

Description Use the **reset qos car name** command to clear the statistics about the specific aggregation CAR.

Examples # Clear the statistics about the aggregation CAR **aggcar-1**.

```
<Sysname> reset qos car name aggcar-1
```

70 VLAN POLICY CONFIGURATION COMMANDS

display qos vlan-policy

Syntax **display qos vlan-policy** { **name** *policy-name* | **vlan** [*vlan-id*] } [**slot** *slot-id*]

View Any view

Parameters **name** *policy-name*: Specifies to display the information about the VLAN policy identified by the *policy-name* argument.

vlan *vlan-id*: Specifies to display VLAN policies applied to the VLAN identified by the *vlan-id* argument.

slot-id: Specifies to display the information about the VLAN policies applied to VLANs on the module residing in the specific slot. If this argument is not specified, the information about VLAN policies applied to the Fabric is displayed; if this argument is specified, the information about VLAN policies applied to the specific module is displayed.

Description Use the **display qos vlan-policy** command to display the information about a specific VLAN policy.

Examples # Display the information about VLAN policy **test**.

```
<Sysname> display qos vlan-policy name test
Policy test
    Vlan 34: inbound (active)
    Vlan 38: outbound (active)
```

Table 313 Field descriptions of the display qos vlan-policy command

Field	Description
Policy test	Name of the QoS policy
Vlan 34	ID of the VLAN referencing the QoS policy
Inbound (Active)	Apply the QoS policy to the incoming packets of the VLAN
	The Active field indicates that the VLAN policy is active
Outbound (Active)	Apply the QoS policy to the outgoing packets of the VLAN
	The Active field indicates that the VLAN policy is active

qos vlan-policy

Syntax **qos vlan-policy** *policy-name* **vlan** *vlan-id-list* { **inbound** | **outbound** }

undo qos vlan-policy vlan *vlan-id-list* { **inbound** | **outbound** }

View System view

Parameters *policy-name*: Policy name.

vlan-id-list: VLAN ID list, which may be expressed in the form of *vlan-id* **to** *vlan-id*. The *vlan-id* argument is the ID of a VLAN. You can input multiple discontinuous VLAN IDs. For Switch 8800s, up to eight VLAN IDs can be input.

inbound: Applies the QoS policy to the incoming packets of the specific VLANs.

outbound: Applies the QoS policy to the outgoing packets of the specific VLANs.

Description Use the **qos vlan-policy** command to apply the QoS policy to the specific VLANs.

Use the **undo qos vlan-policy** command to cancel the QoS policy applied to the specific VLANs.

A QoS policy can be applied in the following two ways:

- Port-based application: a QoS policy is applied to the incoming packets or outgoing packets of a port.
- VLAN-based application: a QoS policy is applied to all the traffic of a VLAN.

A QoS policy applied to all the traffic of a VLAN is also known as a VLAN policy.

Examples # Apply the VLAN policy **test** to the incoming packets of VLAN 200, VLAN 300, VLAN 400, VLAN 500, VLAN 600, VLAN 700, VLAN 800, and VLAN 900.

```
<Sysname> system-view
[Sysname] qos vlan-policy test vlan 200 300 400 500 600 700 800 900 inbound
```

reset qos vlan-policy

Syntax **reset qos vlan-policy** [**vlan** *vlan-id*]

View User view

Parameters *vlan-id*: ID of a VLAN.

Description Use the **reset qos vlan-policy** command to clear the statistics information about the VLAN policies applied to a VLAN.

Examples # Clear the statistics information about the VLAN policies applied to VLAN 2.

```
<Sysname> reset qos vlan-policy vlan 2
```

71 TRAFFIC MIRRORING CONFIGURATION COMMANDS

display qos policy user-defined

Syntax **display qos policy user-defined** [*policy-name* [**classifier** *tcl-name*]]

View Any view

Parameters *policy-name*: Policy name.

tcl-name: Traffic classification rule name in a policy.

Description Use the **display qos policy user-defined** command to display the configuration information about a user-defined policy.

Examples # Display the configuration information about the user-defined QoS policy **test**.

```
<Sysname> display qos policy user-defined test
  User Defined QoS Policy Information:

  Policy: test
   Classifier: test
     Behavior: test
      Mirror enable:
        Mirror type: interface
        Mirror destination: Ethernet3/1/1
```

Table 314 Field descriptions of the display qos policy user-defined command

Field	Description
Policy	QoS policy name
Classifier	Traffic classification rule name
Behavior	Traffic behavior name
Mirror enable	Traffic mirroring is enabled
Mirror type	Traffic mirroring type
Mirror destination	Destination of traffic mirroring

display traffic behavior user-defined

Syntax **display traffic behavior user-defined** [*behavior-name*]

View Any view

Parameters *behavior-name*: Traffic behavior name.

Description Use the **display traffic behavior user-defined** command to display the configuration information about a user-defined traffic behavior.

Examples # Display the configuration information about the user-defined traffic behavior **test**.

```
<Sysname> display traffic behavior user-defined test
  User Defined Behavior Information:
    Behavior: test
      Mirror enable:
        Mirror type: interface
        Mirror destination: Ethernet3/1/1
```

Table 315 Field descriptions of the display traffic behavior user-defined command

Field	Description
Behavior	Traffic behavior name
Mirror enable	Traffic mirroring is enabled
Mirror type	Traffic mirroring type
Mirror destination	Destination of traffic mirroring

mirror-to cpu

Syntax **mirror-to cpu**

undo mirror-to cpu

View Traffic behavior view

Parameters **cpu**: Mirrors traffic to the CPU.

Description Use the **mirror-to cpu** command to configure the action of mirroring traffic to the CPU for a traffic behavior.

Use the **undo mirror-to cpu** command to cancel the action of mirroring traffic to the CPU for a traffic behavior.

By default, the action of mirroring traffic to the CPU is not configured for a traffic behavior.

In a traffic behavior, the action of mirroring traffic to a port is mutually exclusive with the action of mirroring traffic to the CPU.

Examples # Configure the action of mirroring traffic to the CPU for the traffic behavior **test**.

```
<Sysname> system-view
[Sysname] traffic behavior test
[Sysname-behavior-test] mirror-to cpu
```

mirror-to interface

Syntax **mirror-to interface** *interface-type interface-number*

undo mirror-to interface *interface-type interface-number*

View Traffic behavior view

Parameters *interface-type interface-number*: Type and number of the destination interface of traffic mirroring.

Description Use the **mirror-to interface** command to configure the action of mirroring traffic to a specific port for a traffic behavior.

Use the **undo mirror-to interface** command to cancel the action of mirroring traffic to a specific port configured for a traffic behavior.

By default, the action of mirroring traffic to a specific port is not configured for a traffic behavior.

Note that:

- In a traffic behavior, the action of mirroring traffic to a port is mutually exclusive with the action of mirroring traffic to the CPU.
- If this command is executed multiple times, the new command overwrites the previous command.

Examples # Configure the action of mirroring traffic to Ethernet 1/1/1 for the traffic behavior **test**.

```
<Sysname> system-view
[Sysname] traffic behavior test
[Sysname-behavior-test] mirror-to interface ethernet 1/1/1
```

72 EACL CONFIGURATION COMMANDS

Interface eacl

Syntax **interface eacl** *interface-number*

View System view

Parameters *interface-number*: Interface number.

Description Use the **interface eacl** command to enter EACL service subinterface view.

Currently, only the Switch 8800 3C17542 modules support EACL service subinterface view.

Examples # Enter EACL service subinterface view.

```
<Sysname> system-view
[Sysname] interface eacl 8/0/1.1
```

qos binding

Syntax **qos binding interface** *interface-type interface-number*

undo qos binding

View EACL service subinterface view

Parameters *interface-type interface-number*: Type and number of the interface to be bound to. Currently, only virtual VLAN interfaces are available.

Description Use the **qos binding** command to bind an EACL service subinterface to a specific layer-3 interface.

Use the **undo qos binding** command to cancel the binding.

An EACL service interface is bijective with a layer-3 interface, that is, an EACL service subinterface can be bound to only one layer-3 interface and a layer-3 interface can be bound to only one EACL service subinterface too.

Examples # Bind EACL service subinterface EACL 8/0/1.1 to the virtual interface of VLAN 100.

```
<Sysname> system-view
[Sysname] interface eacl 8/0/1.1
[Sysname-EACL8/0/1.1] qos binding interface vlan-interface 100
```

73 OUTBOUND TRAFFIC STATISTICS CONFIGURATION COMMANDS

qos traffic-counter outbound

Syntax **qos traffic-counter outbound** { **counter0** | **counter1** } **slot** *slot-num* [**interface** *interface-type interface-number* | **vlan** *vlan-id* | **local-precedence** *lp-value* | **drop-priority** *dp-value*] *

undo qos traffic-counter outbound { **counter0** | **counter1** } **slot** *slot-num*

View System view

Parameters **outbound**: Counter for outbound traffic statistics.

counter0: Counter 0.

counter1: Counter 1.

slot-num: Number of the slot where the module resides.

interface-type interface-number: Type and number of the interface to be bound. Currently, Ethernet ports, POS interfaces, and RPR interfaces are supported.

vlan-id: VLAN ID, in the range of 1 to 4094.

lp-value: Local precedence value, in the range of 0 to 7.

dp-value: Drop precedence, in the range of 0 to 2.

Description Use the **qos traffic-counter outbound** command to enable the outbound traffic statistics function and specify the type of outbound traffic.

Use the **undo qos traffic-counter outbound** command to disable the outbound traffic statistics function.

By default, the outbound traffic statistics function is disabled on a module.

A module provides two counters for outbound traffic statistics. The monitored object can be an interface, a VLAN, a local precedence value, or a drop precedence value.

- If no interface is specified, the outbound traffic of all the interfaces on the module is monitored.
- If no VLAN is specified, the outbound traffic of all the VLANs is monitored.
- If no local precedence value is specified, the outbound traffic is monitored regardless of the local precedence.
- If no drop precedence value is specified, the outbound traffic is monitored regardless of the drop precedence.

- *After the **qos traffic-counter outbound** command is used to reset the monitored object for a module, the counter is rest automatically.*
- *For the outbound traffic statistics function configured on XP4B, XP4CA, and D modules, the monitored object of the counter cannot be an interface.*

Examples # Enable counter 0 in slot 4 to collect statistics information about the outbound traffic of Ethernet 1/1/1.

```
<Sysname> system-view
[Sysname] qos traffic-counter outbound counter0 slot 4 interface Ethernet1/1/1
```

display qos traffic-counter outbound

Syntax **display qos traffic-counter outbound** { **counter0** | **counter1** } **slot** *slot-num*

View Any view

Parameters **outbound**: Counter for outbound traffic statistics.

counter0: Counter 0.

counter1: Counter 1.

slot-num: Number of the slot where the module resides.

Description Use the **display qos traffic-counter** command to display the outbound traffic statistics information collected by the counter and display the configuration information of the counter.

Examples # Display the statistics information about the outbound traffic of the module in slot 4.

```
<Sysname> display qos traffic-counter outbound counter0 slot 4
Slot 4 outbound counter0 mode:
  Interface: all
  VLAN: all
  Local precedence: all
  Drop priority: all

 The outgoing packets:
  Unicast: 0 packets
  Multicast: 0 packets
  Broadcast: 0 packets
```

```
                        packets: 0 packets
  Bridge egr             TxQ filtered packets(Due to TxQ congestion): 0 packets
ess filtered
```

Table 316 Field descriptions of the display qos traffic-counter outbound command

Field	Description
Slot 4 outbound counter0 mode	Monitored object of a counter on the module used for outbound traffic statistics
Interface	Interfaces whose outbound traffic information the counter collects
VLAN	VLANs whose outbound traffic information the counter collects
Local precedence	Local precedence values whose outbound traffic information the counter collects
Drop priority	Drop precedence values whose outbound traffic information the counter collects
The outgoing packets	The number of outgoing packets
Unicast	The number of unicast packets
Multicast	The number of multicast packets
Broadcast	The number of broadcast packets
Bridge egress filtered packets	The number of packets filtered in the egress direction of the bridge
TxQ filtered packets(Due to TxQ congestion)	The number of packets filtered due to congestion in the TxQ

reset qos traffic-counter outbound

Syntax **reset qos traffic-counter outbound** { **counter0** | **counter1** } **slot** *slot-num*

View User view

Parameters **outbound**: Counter for outbound traffic statistics.

counter0: Counter 0.

counter1: Counter 1.

slot-num: Number of the slot where the module resides.

Description Use the **reset qos traffic-counter outbound** command to clear the outbound traffic statistics information collected by a counter.

Examples # Clear the outbound traffic statistics information collected by counter 0 on the module in slot 4.

```
<Sysname> reset qos traffic-counter outbound counter0 slot 4
```

74 AAA CONFIGURATION COMMANDS

access-limit

Syntax **access-limit** { **disable** | **enable** *max-user-number* }

undo access-limit

View ISP domain view

Parameters **disable**: Specifies that the system do not limit the number of accessing users in the current ISP domain.

enable *max-user-number*: Maximum number of accessing users in the current ISP domain. The valid range varies by device, in the range 1 to 2048.

Description Use the **access-limit enable** command to set the maximum number of accessing users allowed by an ISP domain.

Use the **undo access-limit** or **access-limit disable** command to remove the limitation.

By default, there is no limit to the amount of supplicants in an ISP domain.

As the supplicants may compete for network resources, setting a proper limit to the amount of accessing users helps in providing a reliable system performance.

Examples # Set a limit of 500 supplicants for ISP domain aabbcc.net.

```
<Sysname> system-view
[Sysname] domain aabbcc.net
[Sysname-isp-aabbcc.net] access-limit enable 500
```

accounting default

Syntax **accounting default** { **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }

undo accounting default

View ISP domain view

Parameters *hwtacacs-scheme-name*: HWTACACS scheme name, a string of 1 to 32 characters.

local: Performs local accounting.

none: Does not perform any accounting.

radius-scheme-name: RADIUS scheme name, a string of 1 to 32 characters.

Description Use the **accounting default** command to specify the default accounting scheme for all types of users.

Use the **undo accounting default** command to restore the default.

By default, the accounting scheme is **local**.

Note that:

- The accounting scheme specified with the **accounting default** command is for all types of users and has a priority lower than that for a specific access mode.
- Local accounting is only for managing the local user connection number; it does not provide the statistics function. The local user connection number management is only for local accounting; it does not affect local authentication and authorization.
- With the access mode of login, accounting is not supported for FTP services.

Related commands: **authentication default**, **authorization default**.

Examples # Configure the default ISP domain system to use the local accounting scheme for all types of users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] accounting default local
```

Configure the default ISP domain system to use RADIUS accounting scheme rd for all types of users and to use the local accounting scheme as the backup scheme. Note that the scheme rd must already exist. For configuration of the scheme, refer to the **radius scheme** command on page 1113.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] accounting default radius-scheme rd local
```

Configure the default ISP domain **system** to use the default accounting scheme for all types of users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] undo accounting default
```

accounting lan-access

Syntax **accounting lan-access** { **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }

undo accounting lan-access

View ISP domain view

Parameters **local**: Performs local accounting.

none: Does not perform any accounting.

radius-scheme-name: RADIUS scheme name, a string of 1 to 32 characters.

Description Use the **accounting lan-access** command to specify the accounting scheme for LAN access users.

Use the **undo accounting lan-access** command to remove the accounting scheme.

Related commands: **accounting default**.

Examples # Configure the default ISP domain system to use the local accounting scheme for LAN access users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system]accounting lan-access local
```

Configure the default ISP domain system to use RADIUS accounting scheme rd for LAN access users and to use the local accounting scheme as the backup scheme. Note that the scheme rd must already exist. For configuration of the scheme, refer to the **radius scheme** command on page 1113.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] accounting lan-access radius-scheme rd local
```

Configure the default ISP domain **system** to remove the configured accounting scheme for LAN access users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] undo accounting lan-access
```

accounting login

Syntax **accounting login** { **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }

undo accounting login

View ISP domain view

Parameters *hwtacacs-scheme-name*: HWTACACS scheme name, a string of 1 to 32 characters.

local: Performs local accounting.

none: Does not perform any accounting.

radius-scheme-name: RADIUS scheme name, a string of 1 to 32 characters.

Description Use the **accounting login** command to specify the accounting scheme for login users.

Use the **undo accounting login** command to remove the accounting scheme for login users.

Related commands: **accounting default**.

Examples # Configure the default ISP domain system to use the local accounting scheme for login users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] accounting login local
```

Configure the default ISP domain system to use RADIUS accounting scheme rd for login users and to use the local accounting scheme as the backup scheme. Note that the scheme rd must already exist. For configuration of the scheme, refer to the **radius scheme** command on page 1113.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] accounting login radius-scheme rd local
```

Configure the default ISP domain **system** to remove the configured accounting scheme for login users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] undo accounting login
```

accounting optional

Syntax **accounting optional**

undo accounting optional

View ISP domain view

Parameters None

Description Use the **accounting optional** command to enable the accounting optional feature.

Use the **undo accounting optional** command to disable the feature.

By default, the feature is disabled.

Note that:

- With the **accounting optional** command configured, a user that will be disconnected otherwise can use the network resources even when there is no available accounting server or the communication with the current accounting server fails. This command is normally used when authentication is required but accounting is not.
- If you configure the **accounting optional** command for a domain, the device does not send real-time accounting updates or stop-accounting requests for users of the domain any more.

Examples # Enable the accounting optional feature for users in domain aabbcc.net.

```
<Sysname> system-view
[Sysname] domain aabbcc.net
[Sysname-isp-aabbcc.net] accounting optional
```

accounting ppp

Syntax **accounting ppp** { **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }

undo accounting ppp

View ISP domain view

Parameters *hwtacacs-scheme-name*: HWTACACS scheme name, a string of 1 to 32 characters.

local: Performs local accounting.

none: Does not perform any accounting.

radius-scheme-name: RADIUS scheme name, a string of 1 to 32 characters.

Description Use the **accounting ppp** command to specify the accounting scheme for PPP users.

Use the **undo accounting ppp** command to remove the accounting scheme for PPP users.

Related commands: **accounting default**.

Examples # Configure the default ISP domain system to use the local accounting scheme for PPP users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] accounting ppp local
```

Configure the default ISP domain system to use RADIUS accounting scheme rd for PPP users and to use the local accounting scheme as the backup scheme. Note that the scheme rd must already exist. For configuration of the scheme, refer to the **radius scheme** command on page 1113.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] accounting ppp radius-scheme rd local
```

Configure the default ISP domain **system** to remove the configured accounting scheme for PPP users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] undo accounting ppp
```

attribute

Syntax **attribute** { **access-limit** *max-user-number* | **idle-cut** *minute* | **ip** *ip-address* | **location** { **nas-ip** *ip-address* **port** *slot-number subslot-number port-number* | **port** *slot-number subslot-number port-number* } | **mac** *mac-address* | **vlan** *vlan-id* } *

undo attribute { **access-limit** | **idle-cut** | **ip** | **location** | **mac** | **vlan** }*

View Local user view

Parameters **access-limit** *max-user-number*: Specifies the maximum number of users that can log in using the current username at a time, which ranges from 1 to 1024.

idle-cut *minute*: Configures the idle cut function. The idle cut period ranges from 1 to 120, in minutes.

ip *ip-address*: Specifies the IP address of the user. The **attribute ip** command only applies to authentications that support IP address passing, such as 802.1x. If you configure the command to authentications that do not support IP address passing, such as MAC address authentication, the local authentication will fail.

location: Specifies the port binding attribute of the user.

nas-ip *ip-address*: Specifies the IP address of the port of the remote access server bound by the user. *ip-address* specifies an IP address in dotted decimal notation. The default is 127.0.0.1, that is, the device itself. This keyword and argument combination is required only when the user is bound to a remote port.

port *slot-number subslot-number port-number*: Specifies the port to which the user is bound. The value of *slot-number* and *subslot-number* both range from 0 to 15. The value of *port-number* ranges from 0 to 255. The ports bounded are determined by port number, regardless of port type.

mac *mac-address*: Specifies the MAC address of the user in the format of *H-H-H.*

vlan *vlan-id*: Specifies the VLAN to which the user belongs. The *vlan-id* argument is an integer in the range 1 to 4094.

Description Use the **attribute** command to set some of the attributes for a LAN access user.

Use the **undo attribute** command to remove the configuration.

The **idle-cut** command in user interface view applies to lan-access users only.

Related commands: **display local-user**.

Examples # Set the IP address of user **user1** to 10.110.50.1.

```
<Sysname> system-view
[Sysname] local-user user1
[Sysname-luser-user1] attribute ip 10.110.50.1
```

authentication default

Syntax **authentication default** { **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }

undo authentication default

View ISP domain view

Parameters *hwtacacs-scheme-name*: HWTACACS scheme name, a string of 1 to 32 characters.

local: Performs local authentication.

none: Does not perform any authentication.

radius-scheme-name: RADIUS scheme name, a string of 1 to 32 characters.

Description Use the **authentication default** command to specify the authentication scheme for all types of users.

Use the **undo authentication default** command to restore the default for all types of users.

By default, the authentication scheme is **local**.

The authentication scheme specified with the **authentication default** command is for all types of users and has a priority lower than that for a specific access mode.

Related commands: **authorization default**, **accounting default**.

Examples # Configure the default ISP domain system to use the local authentication scheme for all types of users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authentication default local
```

Configure the default ISP domain system to use RADIUS authentication scheme rd for all types of users and to use the local authentication scheme as the backup scheme. Note that the scheme rd must already exist. For configuration of the scheme, refer to the **radius scheme** command on page 1113.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authentication default radius-scheme rd local
```

Configure the default ISP domain **system** to use the default authentication scheme for all types of users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] undo authentication default
```

authentication lan-access

Syntax **authentication lan-access** { **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }

undo authentication lan-access

View ISP domain view

Parameters **local**: Performs local authentication.

none: Does not perform any authentication.

radius-scheme-name: RADIUS scheme name, a string of 1 to 32 characters.

Description Use the **authentication lan-access** command to specify the authentication scheme for LAN access users.

Use the **undo authentication login** command to remove the authentication scheme for LAN access users.

Related commands: **authentication default**.

Examples # Configure the default ISP domain system to use the local authentication scheme for LAN access users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authentication lan-access local
```

Configure the default ISP domain system to use RADIUS authentication scheme rd for LAN access users and to use the local authentication scheme as the backup scheme. Note that the scheme rd must already exist. For configuration of the scheme, refer to the **radius scheme** command on page 1113.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authentication lan-access radius-scheme rd local
```

Configure the default ISP domain **system** to remove the configured authentication scheme for LAN access users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] undo authentication lan-access
```

authentication login

Syntax **authentication login** { **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }

undo authentication login

View ISP domain view

Parameters *hwtacacs-scheme-name*: HWTACACS scheme name, a string of 1 to 32 characters.

local: Performs local authentication.

none: Does not perform any authentication.

radius-scheme-name: RADIUS scheme name, a string of 1 to 32 characters.

Description Use the **authentication login** command to specify the authentication scheme for login users.

Use the **undo authentication login** command to remove the authentication scheme for login users.

Related commands: **authentication default**.

Examples # Configure the default ISP domain system to use the local authentication scheme for login users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authentication login local
```

Configure the default ISP domain system to use RADIUS authentication scheme rd for login users and to use the local authentication scheme as the backup scheme. Note that the scheme rd must already exist. For configuration of the scheme, refer to the **radius scheme** command on page 1113.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authentication login radius-scheme rd local
```

Configure the default ISP domain **system** to remove the configured authentication scheme for login users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] undo authentication login
```

authentication ppp

Syntax **authentication ppp** { **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }

undo authentication ppp

View ISP domain view

Parameters *hwtacacs-scheme-name*: HWTACACS scheme name, a string of 1 to 32 characters.

local: Performs local authentication.

none: Does not perform any authentication.

radius-scheme-name: RADIUS scheme name, a string of 1 to 32 characters.

Description Use the **authentication ppp** command to specify the authentication scheme for PPP users.

Use the **undo authentication ppp** command to remove the authentication scheme for PPP users.

Related commands: **authentication default**.

Examples # Configure the default ISP domain system to use the local authentication scheme for PPP users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authentication ppp local
```

Configure the default ISP domain system to use RADIUS authentication scheme rd for PPP users and to use the local authentication scheme as the backup scheme. Note that the scheme rd must already exist. For configuration of the scheme, refer to the **radius scheme** comman on page 1113.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authentication ppp radius-scheme rd local
```

Configure the default ISP domain **system** to remove the configured authentication scheme for PPP users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] undo authentication ppp
```

authorization command

Syntax **authorization command hwtacacs-scheme** *hwtacacs-scheme-name*

undo authorization command

View ISP domain view

Parameters *hwtacacs-scheme-name*: HWTACACS scheme name, a string of 1 to 32 characters.

Description Use the **authorization command** command to specify the authorization scheme for command line users.

Use the **undo authorization command** command to remove the authorization scheme for command line users.

Related commands: **authorization default**.

Examples # Configure the default ISP domain system to use HWTACACS authorization scheme hw for command line users. Note that the scheme hw must already exist. For configuration of the scheme, refer to the **hwtacacs scheme** command on page 1131.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authorization command hwtacacs-scheme hw
```

authorization default

Syntax **authorization default** { **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }

undo authorization default

View ISP domain view

Parameters *hwtacacs-scheme-name*: HWTACACS scheme name, a string of 1 to 32 characters.

local: Performs local authorization.

none: Does not perform any authorization. In this case, an authenticated user is automatically authorized with the default right.

radius-scheme-name: RADIUS scheme name, a string of 1 to 32 characters.

Description Use the **authorization default** command to specify the authorization scheme for all types of users.

Use the **undo authorization default** command to restore the default for all types of users.

By default, the authorization scheme for all types of users is **local**.

Note that:

- The authorization scheme specified with the **authorization default** command is for all types of users and has a priority lower than that for a specific access mode.
- RADIUS authorization is special in that it takes effect only when the RADIUS authorization scheme is the same as the RADIUS authentication scheme. In addition, if a RADIUS authorization fails, the error message returned to the NAS says that the server is not responding.

Related commands: **authentication default**, **accounting default**.

Examples # Configure the default ISP domain system to use the local authorization scheme for all types of users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authorization default local
```

Configure the default ISP domain system to use RADIUS authorization scheme rd for all types of users and to use the local authorization scheme as the backup scheme. Note that the scheme rd must already exist. For configuration of the scheme, refer to the **radius scheme** command on page 1113.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authorization default radius-scheme rd local
```

Configure the default ISP domain **system** to use the default authorization scheme for all types of users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] undo authorization default
```

authorization lan-access

Syntax **authorization lan-access** { **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }

undo authorization lan-access

View ISP domain view

Parameters **local**: Performs local authorization.

none: Does not perform any authorization. In this case, an authenticated user is automatically authorized with the default right.

radius-scheme-name: RADIUS scheme name, a string of 1 to 32 characters.

Description Use the **authorization lan-access** command to specify the authorization scheme for LAN access users.

Use the **undo authorization lan-access** command to remove the authorization scheme for LAN access users.

Related commands: **authorization default**.

Examples # Configure the default ISP domain system to use the local authorization scheme for LAN access users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system]authorization lan-access local
```

Configure the default ISP domain system to use RADIUS authorization scheme rd for LAN access users and to use the local authorization scheme as the backup scheme. Note that the scheme rd must already exist. For configuration of the scheme, refer to the **radius scheme** command on page 1113.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authorization lan-access radius-scheme rd local
```

Configure the default ISP domain **system** to remove the configured authorization scheme for LAN access users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] undo authorization lan-access
```

authorization login

Syntax **authorization login** { **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }

undo authorization login

View ISP domain view

Parameters *hwtacacs-scheme-name*: HWTACACS scheme name, a string of 1 to 32 characters.

local: Performs local authorization.

none: Does not perform any authorization. In this case, an authenticated user is automatically authorized with the default right.

radius-scheme-name: RADIUS scheme name, a string of 1 to 32 characters.

Description Use the **authorization login** command to specify the authorization scheme for login users.

Use the **undo authorization login** command to remove the authorization scheme for login users.

Related commands: **authorization default**.

Examples # Configure the default ISP domain system to use the local authorization scheme for login users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authorization login local
```

Configure the default ISP domain system to use RADIUS authorization scheme rd for login users and to use the local authorization scheme as the backup scheme. Note that the scheme rd must already exist. For configuration of the scheme, refer to the **radius scheme** command on page 1113.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authorization login radius-scheme rd local
```

Configure the default ISP domain **system** to remove the configured authorization scheme for login users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] undo authorization login
```

authorization ppp

Syntax **authorization ppp** { **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }

undo authorization ppp

View ISP domain view

Parameters *hwtacacs-scheme-name*: HWTACACS scheme name, a string of 1 to 32 characters.

local: Performs local authorization.

none: Does not perform any authorization. In this case, an authenticated user is automatically authorized with the default right.

radius-scheme-name: RADIUS scheme name, a string of 1 to 32 characters.

Description Use the **authorization ppp** command to specify the authorization scheme for PPP users.

Use the **undo authorization ppp** command to remove the authorization scheme for PPP users.

Related commands: **authorization default**.

Examples # Configure the default ISP domain system to use the local authorization scheme for PPP users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system]authorization ppp local
```

Configure the default ISP domain system to use RADIUS authorization scheme rd for PPP users and to use the local authorization scheme as the backup scheme. Note that the scheme rd must already exist. For configuration of the scheme, refer to the **radius scheme** command on page 1113.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authorization ppp radius-scheme rd local
```

Configure the default ISP domain **system** to remove the configured authorization scheme for PPP users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] undo authorization ppp
```

cut connection

Syntax **cut connection** { **access-type** { **dot1x** | **mac-authentication** } | **all** | **domain** *isp-name* | **interface** *interface-type interface-number* | **ip** *ip-address* | **mac** *mac-address* | **ucibindex** *ucib-index* | **user-name** *user-name* | **vlan** *vlan-id* } [**slot** *slot-number*]

View System view

Parameters **access-type** { **dot1x** | **mac-authentication** }: Specifies user connections according to the type of access. **dot1x** specifies all 802.1x user connections, and **mac-authentication** specifies all MAC authentication user connections.

all: Specifies all user connections.

domain *isp-name*: Specifies all user connections of an ISP domain. The *isp-name* argument refers to the name of an existing ISP domain and is a string of 1 to 24 characters.

interface *interface-type interface-number*: Specifies all user connections of an interface.

ip *ip-address*: Specifies all user connections of an IP address specified by *ip-address*.

mac *mac-address*: Specifies the user connection of a MAC address specified by *mac-address.* The MAC address must be in the format of *H-H-H.*

vlan *vlan-id*: Specifies all user connections of a VLAN specified by *vlan-id*. The VLAN ID ranges from 1 to 4094.

user-name *user-name*: Specifies a user connection by user name.

ucibindex *ucib-index*: Specifies a user connection by connection index.

slot *slot-number*: Specifies a connection on a slot.

Description Use the **cut connection** command to tear down the specified connecitons forcibly.

This command is effective to lan-access users of service-type only. You cannot cut the connections of Telnet, FTP, and SSH users with this command.

Related commands: display connection, service-type

Examples # Tear down all connections in ISP domain aabbcc.net.

```
<Sysname> system-view
[Sysname] cut connection domain aabbcc.net
```

display connection

Syntax **display connection** [**access-type** { **dot1x** | **mac-authentication** } | **domain** *isp-name* | **interface** *interface-type interface-number* | **ip** *ip-address* | **mac** *mac-address* | **ucibindex** *ucib-index* | **user-name** *user-name* | **vlan** *vlan-id*] [**slot** *slot-number*]

View Any view

Parameters **access-type** { **dot1x** | **mac-authentication** }: Specifies user connections by access type. **dot1x** specifies all 802.1x user connections, and **mac-authentication** specifies all MAC authentication user connections.

domain *isp-name*: Specifies user connections by ISP domain. *isp-name* specifies an ISP domain name and is a string of 1 to 24 characters. The specified ISP domain must already exist.

interface *interface-type interface-number*: Specifies user connections by interface number.

ip *ip-address*: Specifies user connections by IP address.

mac *mac-address*: Specifies user connections by MAC address. The MAC address must be in the format of *H-H-H.*

ucibindex *ucib-index*: Specifies a user connection by connection index.

user-name *user-name*: Specifies user connection by user name.

vlan *vlan-id*: Specifies user connections by VLAN ID. The VLAN ID ranges from 1 to 4094.

slot *slot-number*: Specifies user connections by slot number ..

Description Use the **display connection** command to display information about specified or all AAA user connections.

If no parameters are specified in the command, the system displays the information about all AAA user connections.

This command does not apply to FTP user connections.

Related commands: **cut connection**.

Examples # Display information about all AAA user connections.

```
<Sysname> display connection
Total 0 connection(s) matched ,0 listed.
```

display domain

Syntax **display domain** [*isp-name*]

View Any view

Parameters *isp-name*: Name of an existing ISP domain, a string of 1 to 24 characters. The specified ISP domain must already exist.

Description Use the **display domain** command to display the configuration information of a specified ISP domain.

By default, the system displays the configuration information about all ISP domains if no ISP domain is specified.

Related commands: **access-limit**, **domain**, **state**.

Examples # Display the configuration information of all ISP domains.

```
<Sysname> display domain
0  Domain = aabbcc
   State = Active
   Access-limit = Disable
   Accounting method = Required
   Default authentication scheme      : local
   Default authorization scheme       : local
   Default accounting scheme          : local
   Lan-access authentication scheme   : radius=test, local
   Lan-access authorization scheme    : hwtacacs=hw, local
   Lan-access accounting scheme       : local
   Domain User Template:
   Idle-cut = Disable
   Self-service = Disable

1  Domain = system
   State = Active
   Access-limit = Disable
   Accounting method = Required
   Default authentication scheme      : local
   Default authorization scheme       : local
   Default accounting scheme          : local
   Domain User Template:
   Idle-cut = Disable
   Self-service = Disable

Default Domain Name: system
Total 2 domain(s)
```

Table 317 Field descriptions of the display domain command

Field	Description
Domain	Domain name
State	Status of the domain (active or block)
Access-limit	Access limit (disabled or enabled)
Accounting method	Accounting method (either required or optional)
Default authentication scheme	Default authentication scheme
Default authorization scheme	Default authorization scheme
Default accounting scheme	Default accounting scheme
Authentication scheme	Authentication scheme
Authorization scheme	Authentication scheme
Accounting scheme	Accounting scheme
Domain User Template	Template for users in the domain
Idle-cut	Whether idle cut is enabled
Self-service	Whether self service is enabled
Total 2 domain(s).	Two ISP domains in total

display local-user

Syntax **display local-user** [**domain** *isp-name* | **idle-cut** { **disable** | **enable** } | **service-type** { **ftp** | **lan-access** | **ppp** | **ssh** | **telnet** | **terminal** } | **state** { **active** | **block** } | **user-name** *user-name* | **vlan** *vlan-id*] [**slot** *slot-number*]

View Any view

Parameters **domain** *isp-name*: Specifies local users by ISP domain. *isp-name* specifies an ISP domain name. The specified ISP domain must already exist.

idle-cut { **disable** | **enable** }: Specifies local users with the idle-cut function disabled or enabled.

disable indicates that users are not allowed to enable idle-cut, and **enable** indicates that users are allowed to enable idle-cut.

service-type: Specifies local users by user type. **ftp** refers to users using FTP, **lan-access** refers to users accessing the network through an Ethernet, such as 802.1x users; **pad** refers to users using x.25 PAD; **ppp** refers to users using PPP; **ssh** refers to users using SSH; **telnet** refers to users using Telnet; **terminal** refers to users logging in through the console port, AUX port, or Asyn port.

state { **active** | **block** }: Specifies local users by state. A local user in the state of active can access network services, while a local user in the state of blocked cannot.

user-name *user-name*: Specifies a local user by username.

vlan *vlan-id*: Specifies local users by VLAN ID. The VLAN ID ranges from 1 to 4094.

slot *slot-number*: Specifies local users by slot number.

Description Use the **display local-user** command to display information about specified or all local users.

Related commands: **local-user**.

Examples # Display the information on the local user named "abc" on the interface module of Slot 1.

```
<Sysname> display local-user user-name abc slot 1
Slot:  1
The contents of local user abc:
 State:                    Active
 ServiceType:              lan-access
 Idle-cut:                 Disable
 Access-limit:             Enable           Current AccessNum: 0
 Bind location:            2.2.2.2/3/2/255 (NAS/SLOT/SUBSLOT/PORT)
 Vlan ID:                  Disable
 IP address:               Disable
 MAC address:              Disable
 Password-Aging:           Enable(90 day(s))
 Password-Length:          Enable(10 characters)
```

```
 Password-Composition:     Enable(1 type(s),  1 character(s) per type)
Total 1 local user(s) matched.
```

Table 318 Field descriptions of display local-user (for centralized device)

Field	Description
Slot	Slot number
State	Status of the local user, active or block
ServiceType	Service types that the user can use (ftp, lan-access, pad, ssh, telnet, terminal)
Idle-cut	Whether idle cut is enabled
Access-limit	Accessing user connection limit
Current AccessNum	Number of users currently accessing network services
Bind location	Whether bound with a port
VLAN ID	VLAN to which the user belongs
IP address	IP address of the user
MAC address	MAC address of the user
Password-Aging	Aging time of the local user password
Password-Length	Minimum length of the local user password
Password-Composition	Password composition policy of the local user
Total 1 local user(s) matched	1 local user in total

domain

Syntax **domain** *isp-name*

undo domain *isp-name*

View System view

Parameters *isp-name*: ISP domain name, a case-insensitive string of 1 to 24 characters that cannot contain any slash (/), colon (:), asterisk (*), question mark (?), less-than sign (<), greater-than sign (>), or @.

Description Use the **domain** *isp-name* command to create an ISP domain or enter ISP domain view.

Use the **domain default** command to specify the default ISP domain and enter ISP domain view.

Use the **undo domain** command to remove an ISP domain.

By default, the system uses the domain of system. You can view its settings by executing the **display domain** command.

If the specified ISP domain does not exist, the system will create a new ISP domain. All the ISP domains are in the active state when they are created.

Related commands: **state**, **display domain**.

Examples # Create ISP domain aabbcc.net, and enter ISP domain view.

```
<Sysname> system-view
[Sysname] domain aabbcc.net
New Domain added.
[Sysname-isp-aabbcc.net]
```

domain default

Syntax **domain default** { **disable** | **enable** *isp-name* }

View System view

Parameters **disable:** Disables the configured default ISP domain.

enable: Enables the configured default ISP domain.

isp-name: Name of the ISP.

Description Use the **domain default** command to manually configure the system default ISP domain.

By default, the default domain is named "system".

Note that:

- There must be only one default ISP domain.
- When configure a default domain, this domain must have existed.
- The default domain configured cannot be deleted unless you cancel it as a default domain first.

Related commands: **state**, **display domain**.

Examples # Create a new ISP domain named aabbcc.net, and configure it as the default ISP domain.

```
<Sysname> system-view
[Sysname] domain aabbcc.net
[Sysname-isp-aabbcc.net] quit
[Sysname] domain default enable aabbcc.net
```

idle-cut

Syntax **idle-cut** { **disable** | **enable** *minute* }

View ISP domain view

Parameters **disable**: Disables the idle cut function.

enable: Enables the idle cut function.

minute: Allowed idle duration in minutes, in the range 1 to 120.

Description Use the **idle-cut** command to enable or disable the idle cut function.

By default, the function is disabled.

Related commands: **domain**.

Examples # Enable the idle cut function and set the idle threshold to 50 minutes for ISP domain aabbcc.net.

```
<Sysname> system-view
[Sysname] domain aabbcc.net
[Sysname-isp-aabbcc.net] idle-cut enable 50
```

ip pool

Syntax **ip pool** *pool-number low-ip-address* [*high-ip-address*]

undo ip pool *pool-number*

View System view/ISP domain view

Parameters *pool-number*: Address pool number, in the range 0 to 99.

low-ip-address and *high-ip-address*: Start and end IP addresses of the address pool. Up to 1024 addresses are allowed for an address pool. If you do not specify the end IP address, there will be only one IP address in the pool, namely the start IP address.

Description Use the **ip pool** command to configure a local address pool for assigning addresses to PPP users.

Use the **undo ip pool** command to delete a local address pool.

By default, no local IP address pool is configured.

- Configure an IP address pool in system view and use the **remote address** command in interface view to assign IP addresses from the pool to PPP users.
- You can also configure an IP address pool in ISP domain view for assigning IP addresses to the PPP users in the ISP domain. This applies to the scenario where an interface serves a great amount of PPP users but the address resources are inadequate. For example, an Ethernet interface running PPPoE can accommodate up to 4095 users. However, only one address pool with up to 1024 addresses can be configured on its virtual template (VT). This is obviously far from what is required. To address the issue, you can configure address pools for ISP domains and assign addresses from them to the PPP users by domain.

Examples # Configure the local IP address pool 0 with the address range of 129.102.0.1 to 129.102.0.10.

```
<Sysname> system-view
[Sysname] domain aabbcc.net
[Sysname-isp-aabbcc.net] ip pool 0 129.102.0.1 129.102.0.10
```

level

Syntax **level** *level*

undo level

View Local user view

Parameters *level*: Priority level for the user, which can be 0 for visit level, 1 for monitor level, 2 for system level, and 3 for manage level. A smaller number means a lower priority.

Description Use the **level** command to set the priority level of a user.

Use the **undo level** command to restore the default.

By default, the user priority is 0.

Note that:

- If you specify not to perform authentication or use password authentication, the level of the commands that a user can use after logging in depends on the priority of the user interface. For details about the authentication, refer to the **authentication-mode** on command page 67.
- If you specify an authentication method that requires the username and password, the level of the commands that a user can use after logging in depends on the priority of the user. For an SSH user using RSA public key authentication, the commands that can be used depend on the level configured on the user interface.

Related commands: **local-user**.

Examples #Set the level of user user1 to 3.

```
<Sysname> system-view
[Sysname] local-user user1
[Sysname-luser-user1] level 3
```

local-user

Syntax **local-user** *user-name*

undo local-user { *user-name* | **all** [**service-type** { **ftp** | **lan-access** | **ppp** | **ssh** | **telnet** | **terminal** }] }

View System view

Parameters *user-name*: Name for the local user, a case-sensitive string of 1 to 80 characters that cannot contain any forward slash (/), colon (:), asterisk (*), question mark (?), less-than sign (<), and greater-than sign (>). In addition, the @ sign can be used only once in one username, and the username part before the @ sign (that is, the user ID) cannot be more than 55 characters. Note that a username cannot be a, al, or all.

all: Specifies all users.

service-type: Specifies the type of users. **ftp** specifies FTP users, **lan-access** specifies LAN access users (Ethernet access users mainly, like 802.1x users), **ppp** specifies PPP users, **ssh** specifies SSH users, **telnet** specifies Telnet users, and **terminal** specifies terminal users that gain access through the Console port, AUX port or Asyn port.

Description Use the **local-user** command to add a local user and enter local user view.

Use the **undo local-user** command to remove the specified local users.

By default, no local user is configured.

Related commands: display local-user, service-type.

Examples # Add a local user named user1.

```
<Sysname> system-view
[Sysname] local-user user1
[Sysname-luser-user1]
```

local-user password-display-mode

Syntax **local-user password-display-mode** { **auto** | **cipher-force** }

undo local-user password-display-mode

View System view

Parameters **auto**: Displays the password of an accessing user based on the configuration of the user by using the **password** command.

cipher-force: Displays the passwords of all accessing users in cipher text.

Description Use the **local-user password-display-mode** command to set the password display mode for all local users.

Use the **undo local-user password-display-mode** command to restore the default.

The default mode is **auto**.

With the **cipher-force** mode, the password of any local user is always displayed in cipher text, even if you specify in the **password** command to display the password in simple text.

Related commands: **display local-user**, **password**.

Examples # Specify to display the passwords of all accessing users in cipher text.

```
[Sysname] local-user password-display-mode cipher-force
```

password (Local user view)

Syntax **password** { **cipher** | **simple** } *password*

undo password

View Local user view

Parameters **cipher**: Specifies to display the password in cipher text.

simple: Specifies to display the password in simple text.

password: Password for the local user. In simple text, it must be a string of 1 to 63 characters that contains no blank space, for example, aabbcc. In cipher text, it must be a string of 24, 32, 44, 56, 64, 76, or 88 characters, for example, _(TT8F]Y5SQ=^Q'MAF4<1!!. With the **simple** keyword, you must specify the password in simple text. With the **cipher** keyword, you can specify the password in either simple or cipher text.

Description Use the **password** command to configure a password for a local user.

Use the **undo password** command to delete the password of a local user.

Note that with the **local-user password-display-mode cipher-force** command configured, the password is always displayed in cipher text, regardless of the configuration of the **password** command.

Related commands: **display local-user**.

Examples # Set the password of user1 to 20030422 and specify to display the password in plain text.

```
<Sysname> system-view
[Sysname] local-user user1
[Sysname-luser-user1] password simple 20030422
```

self-service-url

Syntax **self-service-url** { **disable** | **enable** *url-string* }

undo self-service-url

View ISP domain view

Parameters *url-string*: URL of the self-service server for changing a user password, a string of 1 to 64 characters that starts with http:// and cannot contain any question mark.

Description Use the **self-service-url enable** command to enable the self-service server localization function.

Use the **self-service-url disable** command or the **undo self-service-url** command to disable the self-service server localization function.

By default, the function is disabled.

Note that:

- A self-service RADIUS server, for example, CAMS, is required for the self-service server localization function. With the self-service function, a user can manage and control his or her accounting information or module number. A server with self-service software is a self-service server.
- After you configure the **self-service-url enable** command, a user can locate the self-service server by selecting [Service/Change Password] from the 802.1x client. The client software automatically launches the default browser, IE or Netscape, and opens the URL page of the self-service server for changing the user password. A user can change his or her password through the page.
- Only authenticated users can select [Service/Change Password] from the 802.1x client. The option is gray and unavailable for unauthenticated users.

Examples # Enable the self-service server localization function and specify the URL of the self-service server for changing user password to http://10.153.89.94/selfservice/modPasswd1x.jsp|userName for the default ISP domain system.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] self-service-url enable http://10.153.89.94/sel
fservice/modPasswd1x.jsp|userName
```

service-type

Syntax **service-type** { **lan-access** | { **ssh** | **telnet** | **terminal** }* [**level** *level*] }

undo service-type { **lan-access** | { **ssh** | **telnet** | **terminal** }* }

View Local user view

Parameters **lan-access**: Authorizes the user to use the Ethernet to access the network. The user can be, for example, an 802.1x user.

ssh: Authorizes the user to use the SSH service.

telnet: Authorizes the user to use the Telnet service.

terminal: Authorizes the user to use the terminal service, allowing the user to login from the console, AUX or Asyn port.

level *level*: Sets the user level of a Telnet, terminal, or SSH user. The *level* argument is in the range 0 to 3 and defaults to 0.

Description Use the **service-type** command to specify the service types that a user can use.

Use the **undo service-type** command to delete one or all service types configured for a user.

By default, a user is authorized with no service.

Related commands: **service-type ppp** and **service-type ftp**.

Examples # Authorize user user1 to use the Telnet service.

```
<Sysname> system-view
[Sysname] local-user user1
[Sysname-luser-user1] service-type telnet
```

service-type ftp

Syntax **service-type ftp**

undo service-type ftp

View Local user view

Parameters None

Description Use the **service-type ftp** command to authorize a user to use the FTP service.

Use the **undo service-type ftp** command to disable a user from using the FTP service.

By default, no service is authorized to a user and anonymous access to FTP service is not allowed. If you authorize a user to use the FTP service but do not specify a directory that the user can access, the user can access the root directory of the device by default.

Related commands: **work-directory**, **service-type**, **service-type ppp**.

Examples # Authorize a user to use the FTP service.

```
<Sysname> system-view
[Sysname] local-user user1
[Sysname-luser-user1] service-type ftp
```

service-type ppp

Syntax **service-type ppp** [**call-number** *call-number* [**:** *subcall-number*] | **callback-nocheck** | **callback-number** *callback-number*]

undo service-type ppp [**call-number** | **callback-nocheck** | **callback-number**]

View Local user view

Parameters **callback-number** *callback-number*: Specifies a callback number, which must be less than 64 bytes.

[: *subcall-number*]: Specifies the sub-caller number. The total length of the caller number and the sub-caller number must be less than 62 bytes.

callback-nocheck: Enables the PPP user callback without authentication feature.

call-number *call-number*: Specifies a caller number for ISDN user authentication, which must be less than 64 bytes.

Description Use the **service-type ppp** command to authorize a user to use the PPP service and configure the callback attribute and caller number of the user.

Use the **undo service-type ppp** command to restore their default settings.

By default, no service is authorized to a user; if the PPP service is authorized, callback without authentication is enabled, no callback number is specified, and the system does not authenticate the caller number of ISDN users.

Related commands: **service-type** and **service-type ftp**.

Examples # Authorize a user to use the PPP service and enable the callback without authentication feature.

```
<Sysname> system-view
[Sysname] local-user user1
[Sysname-luser-user1] service-type ppp callback-nocheck
```

state (ISP domain view/local user view)

Syntax **state** { **active** | **block** }

View ISP domain view/local user view

Parameters **active**: Places the current ISP domain or local user in the active state, allowing the users in the current ISP domain or the current local user to request network services.

block: Places the current ISP domain or local user in the blocked state, preventing users in the current ISP domain or the current local user from requesting network services.

Description Use the **state** command to configure the status of the current ISP domain or local user.

By default, an ISP domain is active when created. So does a local user.

By blocking an ISP domain, you disable users of the domain that are offline from requesting network services. Note that the online users are not affected.

By blocking a user, you disable the user from requesting network services. No other users are affected.

Related commands: **domain**.

Examples # Place the current ISP domain aabbcc.net to the state of "block".

```
<Sysname> system-view
[Sysname] domain aabbcc.net
[Sysname-isp-aabbcc.net] state block
```

Place the current user user1 to the state of blocked.

```
<Sysname> system-view
[Sysname] domain aabbcc.net
[Sysname-user-user1] state block
```

work-directory

Syntax **work-directory** *directory-name*

undo work-directory

View Local user view

Parameters *directory-name*: Name of the directory that FTP/SFTP users are authorized to access, a string of 1 to 135 characters.

Description Use the **work-directory** command to specify the directory accessible to FTP/SFTP users.

Use the **undo work-directory** command to restore the default.

By default, FTP/SFTP users can access the root directory of the device.

Note that:

- The specified directory accessible to users must exist. Otherwise, the system will give an error prompt.
- If you delete a directory accessible to FTP/SFTP users, FTP/SFTP users will not be able to access this directory.

- *In active/standby mode, if the directory specified by the active module is not available on the standby module, you may fail to log into the system or cannot perform normal operation subsequent to successful login after active/standby switchover occurs.*
- *If the current working directory specified by FTP/SFTP contains a slot number of the standby module, you will fail to log into the system after active/standby switchover occurs. Therefore, it is recommended that the specified working directory should contain no slot number information.*

Examples # Specify the directory accessible to FTP/SFTP users.

```
<Sysname> system-view
[Sysname] local-user user1
[Sysname-user-user1] work-directory cf:
```

75 RADIUS CONFIGURATION COMMANDS

data-flow-format (RADIUS scheme view)

Syntax **data-flow-format** { **data** { **byte** | **giga-byte** | **kilo-byte** | **mega-byte** } | **packet** { **giga-packet** | **kilo-packet** | **mega-packet** | **one-packet** } }*

undo data-flow-format { **data** | **packet** }

View RADIUS scheme view

Parameters **data**: Specifies the unit of data.

byte: Specifies bytes as unit.

giga-byte: Specifies Gigabytes as unit.

kilo-byte: Specifies Kilobytes as unit.

mega-byte: Specifies Megabytes as unit.

packet: Specifies the unit of packets.

giga-packet: Specifies Giga-packets as unit.

kilo-packet: Specifies Kilo-packets as unit.

mega-packet: Specifies Mega-packets as unit.

one-packet: Specifies packets as unit.

Description Use the **data-flow-format** command to configure the unit of data sent to the RADIUS server. Use the **undo data-flow-format** command to restore the default.

By default, the unit of data is byte, and the unit of packets is one-packet.

Related commands: **display radius**.

Examples # Configure the unit of data sent to the RADIUS server as kilobyte, and configure the unit of packets sent to the RADIUS server as kilo-packet.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] data-flow-format data kilo-byte packet kilo-packet
```

debugging radius packet

Syntax **debugging radius packet** [**slot** *slot-number*]

undo debugging radius packet [**slot** *slot-number*]

View User view

Parameters **packet**: Enables debugging for packets.

slot *slot-number*: Specifies the module in a slot.

Description Use the **debugging radius** command to enable debugging for RADIUS.

Use the **undo debugging radius** command to disable debugging for RADIUS.

By default, debugging is disabled for RADIUS.

Examples # Enable debugging for RADIUS.

```
<Sysname> debugging radius packet
```

display local-server statistics

Syntax **display local-server statistics**

View Any view

Parameters None

Description Use the **display local-server statistics** command to display the statistics of the local RADIUS authentication server.

Related commands: **local-server**.

Examples # Display the statistics of the local RADIUS authentication server.

```
<Sysname> display local-server statistics
The localserver packet statistics:
Receive:                30          Send:                   30
Discard:                0           Receive Packet Error:   0
Auth Receive:           10          Auth Send:              10
Acct Receive:           20          Acct Send:              20
```

radius

display

Syntax **display radius** [*radius-scheme-name*] [**slot** *slot-number*]

View Any view

Parameters *radius-scheme-name*: Specifies a RADIUS scheme name, a string of 1 to 32 characters.

slot *slot-number*: Specifies the module in a slot.

Description Use the **display radius** command to display the configuration information of all RADIUS schemes or a specified RADIUS scheme.

Note: *If you do not specify a RADIUS scheme name, the system displays configuration information of all RADIUS schemes.*

Related commands: **radius scheme**.

Examples # Configure the configuration information of all RADIUS schemes.

```
<Sysname> display radius
------------------------------------------------------------------
SchemeName  = system
  Index = 0                          Type=extended
  Primary Auth IP  = 127.0.0.1       Port= 1645   State= active
  Primary Acct IP  = 127.0.0.1       Port= 1646   State= active
  Second  Auth IP  = 0.0.0.0         Port= 1812   State= block
  Second  Acct IP  = 0.0.0.0         Port= 1813   State= block
  Auth Server Encryption Key = Not configured
  Acct Server Encryption Key = Not configured
  Interval for timeout(second)                          = 3
  Retransmission times for timeout                      = 3
  Interval for realtime accounting(minute)              = 12
  Retransmission times of realtime-accounting packet    = 5
  Retransmission times of stop-accounting packet        = 500
  Quiet-interval(min)                                   = 5
  Username format                                       = without-domain
  Data flow unit                                        = Byte
  Packet unit                                           = one


------------------------------------------------------------------
Total 1 RADIUS scheme(s).
```

display radius statistics

Syntax **display radius statistics** [**slot** *slot-number*]

View Any view

Parameters **slot** *slot-number*: Displays the statistics of RADIUS packets on the module of the specified slot.

Description Use the **display radius statistics** command to display statistics about RADIUS packets.

Related commands: **radius scheme**.

Examples # Display statistics about RADIUS packets.

```
<Sysname> display radius statistics
Slot  1:state statistic(total=2048):
     DEAD=2048     AuthProc=0        AuthSucc=0
AcctStart=0         RLTSend=0         RLTWait=0
 AcctStop=0          OnLine=0            Stop=0
 StateErr=0

Received and Sent packets statistic:
Sent PKT total  :0        Received PKT total:0
RADIUS received packets statistic:
Code= 2,Num=0       ,Err=0
Code= 3,Num=0       ,Err=0
Code= 5,Num=0       ,Err=0
Code=11,Num=0       ,Err=0

Running statistic:
RADIUS received messages statistic:
Normal auth request             , Num=0       , Err=0       , Succ=0
EAP auth request                , Num=0       , Err=0       , Succ=0
Account request                 , Num=0       , Err=0       , Succ=0
Account off request             , Num=0       , Err=0       , Succ=0
PKT auth timeout                , Num=0       , Err=0       , Succ=0
PKT acct_timeout                , Num=0       , Err=0       , Succ=0
Realtime Account timer          , Num=0       , Err=0       , Succ=0
PKT response                    , Num=0       , Err=0       , Succ=0
Session ctrl pkt                , Num=0       , Err=0       , Succ=0
Normal author request           , Num=0       , Err=0       , Succ=0
RADIUS sent messages statistic:
Auth accept                     , Num=0
Auth reject                     , Num=0
EAP auth replying               , Num=0
Account success                 , Num=0
Account failure                 , Num=0
Server ctrl req                 , Num=0
RecError_MSG_sum:0        SndMSG_Fail_sum :0
Timer_Err       :0        Alloc_Mem_Err   :0
State Mismatch  :0        Other_Error     :0

No-response-acct-stop packet =0
Discarded No-response-acct-stop packet for buffer overflow =0
```

Table 319 Field descriptions of display radius statistics command

Field	Description
state statistic(total=2,048)	state statistic (total=2,048)
DEAD	The state of idle

Table 319 Field descriptions of display radius statistics command

Field	Description
AuthProc	The state of waiting for authentication
AuthSucc	The state of authenticated
AcctStart	The state of accounting start
RLTSend	The state of sending real-time accounting packets
RLTWait	The state of waiting for real-time accounting
AcctStop	The state of accounting waiting stopped
OnLine	The state of online
Stop	The state of stop
Received and Sent packets statistic	Number of packets sent and received
Sent PKT total	Number of packets sent
Received PKT total	Number of packets received
RADIUS received packets statistic	Statistic of packets received by RADIUS
Code	Type of packet
Num	Total number of packets
Err	Number of error packets
Running statistic	Statistics of running packets
RADIUS received messages statistic	Number of messages received by RADIUS
Normal auth request	Number of normal authentication requests
EAP auth request	Number of EAP authentication requests
Account request	Number of accounting requests
Account off request	Number of stop-accounting requests
PKT auth timeout	Number of authentication timeout packets
PKT acct_timeout	Number of accounting timeout packets
Realtime Account timer	Number of realtime accounting requests
PKT response	Number of PKT responses
Session ctrl pkt	Number of session control packets
Normal author request	Number of normal authorization packets
Succ	Number of successful packets
RADIUS sent messages statistic	Number of messages that have been sent by RADIUS
Auth accept	Number of accepted authentication packets
Auth reject	Number of rejected authentication packets
EAP auth replying	Number of replying packets of EAP authentication
Account success	Number of accounting succeeded packets
Account failure	Number of accounting failed packets
Server ctrl req	Number of server control requests
RecError_MSG_sum	Number of received packets in error
SndMSG_Fail_sum	Number of packets that failed to be sent out
Timer_Err	Number of timer errors
Alloc_Mem_Err	Number of memory errors
State Mismatch	Number of errors for mismatching status

Table 319 Field descriptions of display radius statistics command

Field	Description
Other_Error	Number of errors of other types
No-response-acct-stop packet	Number of times that no response was received for stop-accounting packets
Discarded No-response-acct-stop packet for buffer overflow	Number of stop-accounting packets that were buffered but then discarded due to full memory

display stop-accounting-buffer (Any view)

Syntax **display stop-accounting-buffer** { **radius-scheme** *radius-scheme-name* | **session-id** *session-id* | **time-range** *start-time stop-time* | **user-name** *user-name* } [**slot** *slot-number*]

View Any view

Parameters **radius-scheme** *radius-scheme-name*: Displays information about the buffered stop-accounting requests of the specified RADIUS scheme. *radius-scheme-name*: Specifies a RADIUS scheme name, a string of 1 to 32 characters.

session-id *session-id*: Displays information about the buffered stop-accounting requests of the specified session. *session-id* specifies a session ID, a string of 1 to 50 characters.

time-range *start-time stop-time*: Displays information about the buffered stop-accounting requests in the specified time range. *start-time* specifies the start time of a time range, and *stop-time* specifies the end time of a time range. They are in the format of hh:mm:ss- mm/dd/yyyy or *hh:mm:ss-yyyy/mm/dd*. If this argument is specified, the system will display information about the buffered stop-accounting requests in the time range from *start-time* to *stop-time*.

user-name *user-name*: Displays information about the buffered stop-accounting requests of the specified user name.

slot *slot-number*: Displays information about the stop-accounting requests on the module of the specified slot.

Description Use the **display stop-accounting-buffer** command to display information about the stop-accounting requests buffered in the device by scheme, session ID, time range, user name, or slot.

*If receiving no response after sending a stop-accounting request to a RADIUS server, the device buffers the request and retransmits it. You can use the **retry stop-accounting** command to set the number of allowed transmission attempts.*

Related commands: **reset stop-accounting-buffer**, **stop-accounting-buffer enable**, **retry stop-accounting**.

Examples # Display information about the buffered stop-accounting requests from 0:0:0 to 23:59:59 on August 31, 2002.

```
<Sysname> display stop-accounting-buffer time-range 0:0:0-08/31/2002
 23:59:59-08/31/2002
 Slot  1:
Total 0 record(s) Matched
```

key (RADIUS scheme view)

Syntax **key** { **accounting** | **authentication** } *string*

undo key { **accounting** | **authentication** }

View RADIUS scheme view

Parameters **accounting**: Sets the shared key for RADIUS accounting packets.

authentication: Sets the shared key for RADIUS authentication/authorization packets.

string: Shared key, a case-sensitive string of 1 to 16 characters.

Description Use the **key** command to set the shared key for RADIUS authentication/authorization or accounting packets.

Use the **undo key** command to restore the default.

By default, no shared key is configured.

Note that: You must ensure that the same shared key is set on the device and the RADIUS server.

Related commands: **display radius**.

Examples # Set the shared key for authentication/authorization packets to hello for RADIUS scheme radius1.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] key authentication hello
```

Set the shared key for accounting packets to ok for RADIUS scheme radius1.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] key accounting ok
```

local-server

Syntax **local-server nas-ip** *ip-address* **key** *password*

undo local-server nas-ip *ip-address*

View System view

Parameters **nas-ip** *ip-address*: Sets the IP address of the network access server for the local RADIUS server, in dotted decimal notation.

key *password*: Sets the shared key of the local RADIUS server. *password* specifies a key, a string of 1 to 16 characters.

Description Use the **local-server** command to set related parameters for a local RADIUS server. Use the **undo local-server** command to remove a configured local RADIUS server.

By default, no parameters are configured for local RADIUS servers.

Note that:

- When the authentication function of the local RADIUS server is used, the number of the UDP port for authentication/authorization must be 1645, and the number of the UDP port for accounting must be 1646.
- The shared key configured using the **local server** command must be consistent with that for authentication/authorization or accounting packets configured using the **key** { **accounting** | **authentication** } command in RADIUS scheme view.
- The device supports a maximum of 16 local RADIUS servers including the default local RADIUS server.

Related commands: **radius scheme**, **state**.

Examples # Set the IP address of the network access server for the local RADIUS server to 10.110.1.2, and set the shared key to **aabbcc.**

```
<Sysname> system-view
[Sysname] local-server nas-ip 10.110.1.2 key aabbcc
```

nas-ip (RADIUS scheme view)

Syntax **nas-ip** *ip-address*

undo nas-ip

View RADIUS scheme view

Parameters *ip-address*: IP address in dotted decimal notation. It must be an address of the device and cannot be all 0s address, all 1s address, a class D address, a class E address or a loopback address.

Description Use the **nas-ip** command to set the IP address for the device to use as the source address of the RADIUS packets to be sent to the server.

Use the **undo nas-ip** command to remove the configuration.

By default, the source IP address of a packet sent to the server is the IP address of the outbound port.

Note that:

- Specifying a source address for the RADIUS packets to be sent to the server can avoid the situation where the packets sent back by the RADIUS server cannot reach the device as the result of a physical interface failure. The address of a loopback interface is recommended.
- The **nas-ip** command in RADIUS scheme view is only for the current RADIUS scheme, while the **radius nas-ip** command in system view is for all RADIUS schemes. However, the **nas-ip** command in RADIUS scheme view overwrites the configuration of the **radius nas-ip** command.

Related commands: **radius nas-ip**.

Examples # Set the IP address for the device to use as the source address of the RADIUS packets to 10.1.1.1.

```
<Sysname> system-view
[Sysname] radius scheme test1
[Sysname-radius-test1] nas-ip 10.1.1.1
```

primary accounting (RADIUS scheme view)

Syntax **primary accounting** *ip-address* [*port-number*]

undo primary accounting

View RADIUS scheme view

Parameters *ip-address*: IP address of the primary accounting server.

port-number: UDP port number of the primary accounting server, which ranges from 1 to 65535.

Description Use the **primary accounting** command to configure the IP address and UDP port of the primary RADIUS accounting server.

Use the **undo primary accounting** command to restore the defaults.

By default, the default IP address is 0.0.0.0, and the default port number 1813.

Note that

- The IP address of the primary accounting server must differ from that of the secondary accounting server. Otherwise, the system will prompt that the configuration fails.
- For the primary accounting server used by the default scheme **system**, the IP address is 127.0.0.1, and the port number is 1646.

Related commands: **key**, **radius scheme**, **state**.

Examples # Set the IP address of the primary accounting server for RADIUS scheme radius1 to 10.110.1.2 and the UDP port of the server to 1813.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] primary accounting 10.110.1.2 1813
```

primary authentication (RADIUS scheme view)

Syntax **primary authentication** *ip-address* [*port-number*]

undo primary authentication

View RADIUS scheme view

Parameters *ip-address*: IP address of the primary authentication/authorization server.

port-number: UDP port number of the primary authentication/authorization server, which ranges from 1 to 65535.

Description Use the **primary authentication** command to configure the IP address and UDP port of the primary RADIUS authentication/authorization server.

Use the **undo primary authentication** command to restore the defaults.

By default, the default IP address is 0.0.0.0, and the default port number 1812.

Note that:

- After creating a RADIUS scheme, you are supposed to configure the IP address and UDP port of each RADIUS server (primary/secondary authentication/authorization or accounting server). The configuration of RADIUS servers is at your discretion except that there must be at least one authentication/authorization server and one accounting server. Besides, ensure that the RADIUS service port settings on the device are consistent with the port settings on the RADIUS servers.
- The IP addresses of the primary and secondary authentication/authorization servers cannot be the same. Otherwise, the configuration fails.
- For the primary authentication server used by the default scheme **system**, the IP address is 127.0.0.1, and the port number is 1645.

Related commands: **key**, **radius scheme**, **state**.

Examples # Set the IP address of the primary authentication/authorization server for RADIUS scheme radius1 to 10.110.1.1 and the UDP port of the server to 1812.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] primary authentication 10.110.1.1 1812
```

radius nas-ip

Syntax **radius nas-ip** *ip-address*

undo radius nas-ip

View System view

Parameters *ip-address*: IP address in dotted decimal notation. It must be an address of the device and cannot be all 0s address, all 1s address, a class D address, a class E address or a loopback address.

Description Use the **radius nas-ip** command to set the IP address for the device to use as the source address of the RADIUS packets to be sent to the server.

Use the **undo radius nas-ip** command to remove the configuration.

By default, the source IP address of a packet sent to the server is the IP address of the outbound port.

Note that:

- Specifying a source address for the RADIUS packets to be sent to the server can avoid the situation where the packets sent back by the RADIUS server cannot reach the device as the result of a physical interface failure.
- If you configure the command for more than one time, the last configuration takes effect.
- The **nas-ip** command in RADIUS scheme view is only for the current RADIUS scheme, while the **radius nas-ip** command in system view is for all RADIUS schemes. However, the **nas-ip** command in RADIUS scheme view overwrites the configuration of the **radius nas-ip** command.

Related commands: **nas-ip**.

Examples # Set the IP address for the device to use as the source address of the RADIUS packets to 129.10.10.1.

```
<Sysname> system-view
[Sysname] radius nas-ip 129.10.10.1
```

radius scheme

Syntax **radius scheme** *radius-scheme-name*

undo radius scheme *radius-scheme-name*

View System view

Parameters *radius-scheme-name*: RADIUS scheme name, a case-insensitive string of 1 to 32 characters.

It cannot be the first n characters of "statistics" (n ranges from 1 to 10). Otherwise, the system will associate it with the **display radius statistics** command (for displaying the statistics of RADIUS packets) when you execute the **display radius** command (for displaying the configuration of a RADIUS scheme).

Description Use the **radius scheme** command to create a RADIUS scheme and enter RADIUS scheme view.

Use the **undo radius scheme** command to delete a RADIUS scheme.

By default, the system has created a RADIUS scheme named "system".

Note that:

- For the RADIUS scheme named "system", the attributes are of default configuration. You can view the settings of the default scheme **system** by executing the **display radius** command.
- The RADIUS protocol is configured scheme by scheme. Every RADIUS scheme must at least specify the IP addresses and UDP ports of the RADIUS authentication/authorization/accounting servers and the parameters necessary for a RADIUS client to interact with the servers.
- A RADIUS scheme can be referenced by more than one ISP domain at the same time.
- The **undo radius scheme** command can be used to remove a specified RADIUS scheme, but not the default RADIUS scheme. You cannot remove a RADIUS scheme when the RADIUS scheme is used by an online user.

Related commands: **key**, **retry realtime-accounting**, **timer realtime-accounting**, **stop-accounting-buffer enable**, **retry stop-accounting**, **server-type**, **state**, **user-name-format**, **retry**, **display radius**, **display radius statistics**.

Examples # Create a RADIUS scheme named radius1 and enter RADIUS scheme view.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1]
```

radius trap

Syntax **radius trap** { **accounting-server-down** | **authentication-server-down** }

undo radius trap { **accounting-server-down** | **authentication-server-down** }

View System view

Parameters **accounting-server-down**: RADIUS trap for accounting servers.

authentication-server-down: RADIUS trap for authentication servers.

Description Use the **radius trap** command to enable the RADIUS trap function.

Use the **undo radius trap** command to disable the function.

By default, the RADIUS trap function is disabled.

Note that:

- If a NAS sends an accounting or authentication request to the RADIUS server but gets no response, the NAS retransmits the request. With the RADIUS trap function enabled, when the NAS transmits the request for half of the specified maximum number of transmission attempts, it sends a trap message; when the NAS transmits the request for the specified maximum number, it sends another trap message.
- If the specified maximum number of transmission attempts is odd, the half of the number refers to the smallest integer greater than the half of the number.

Examples # Enable the RADIUS trap function for accounting servers.

```
<Sysname> system-view
[Sysname] radius trap accounting-server-down
```

Disable the RADIUS trap function when the RADIUS accounting server gives no response.

```
[Sysname] undo radius trap accounting-server-down
```

reset local-server statistics

Syntax **reset local-server statistics**

View User view

Parameters None

Description Use the **reset local-server statistics** command to clear the statistics of the local server.

Related commands: **display local-server statistics**.

Examples # Clear the statistics of the local server.

```
<Sysname> reset local-server statistics
```

reset radius statistics

Syntax **reset radius statistics** [**slot** *slot-number*]

View User view

Parameters **slot** *slot-number*: Specifies the slot where the interface module is inserted.

Description Use the **reset radius statistics** command to clear RADIUS statistics.

Related commands: **display radius**.

Examples # Clear RADIUS statistics.

```
<Sysname> reset radius statistics
```

reset stop-accounting-buffer (User view)

Syntax **reset stop-accounting-buffer** { **radius-scheme** *radius-scheme-name* | **session-id** *session-id* | **time-range** *start-time stop-time* | **user-name** *user-name* } [**slot** *slot-number*]

View User view

Parameters **radius-scheme** *radius-scheme-name*: Clears the buffered stop-accounting requests of the specified RADIUS scheme. *radius-scheme-name* specifies a RADIUS scheme name, a string of 1 to 32 characters.

session-id *session-id*: Clears the buffered stop-accounting requests of the specified session. *session-id* specifies a session by its ID, a string of 1 to 50 characters.

time-range *start-time stop-time*: Clears the buffered stop-accounting requests in the specified time range. *start-time* specifies the start time of a time range, and *stop-time* specifies the end time of a time range. They are in the format of hh:mm:ss- mm/dd/yyyy or *hh:mm:ss-yyyy/mm/dd*.

user-name *user-name*: Clears the buffered stop-accounting requests of the specified user name.

slot *slot-number*: Clears the buffered stop-accounting requests of the module on the specified slot.

Description Use the **reset stop-accounting-buffer** command to clear the buffered stop-accounting requests, which get no responses.

Related commands: **stop-accounting-buffer enable**, **retry stop-accounting**, **display stop-accounting-buffer**.

Examples # Clear the buffered stop-accounting requests for user user0001@aabbcc.net.

```
<Sysname> reset stop-accounting-buffer user-name user0001@aabbcc.net
```

Clear the buffered stop-accounting requests in the time range from 0:0:0 to 23:59:59 on August 31, 2002.

```
<Sysname> reset stop-accounting-buffer time-range 0:0:0-08/31/2002 2
3:59:59-08/31/2002
```

retry

Syntax **retry** *retry-times*

undo retry

View RADIUS scheme view

Parameters *retry-times*: Maximum number of retransmission attempts, in the range 1 to 20.

Description Use the **retry** command to set the maximum number of RADIUS retransmission attempts.

Use the **undo retry** command to restore the default.

The default value for the *retry-times* argument is 3.

Note that the maximum number of retransmission attempts multiplied by the RADIUS server response timeout period cannot be greater than 75.

*The maximum number of retransmission attempts configured using the **retry** command is the sum of retransmission attempts of all RADIUS servers. If you configure active/standby RADIUS servers, the number of retransmission attempts of the first RADIUS server is the half of the sum.*

Related commands: **radius scheme**, **timer response-timeout**.

Examples # Set the maximum number of RADIUS request transmission attempts to 5 for RADIUS scheme radius1.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] retry 5
```

retry realtime-accounting

Syntax **retry realtime-accounting** *retry-times*

undo retry realtime-accounting

View RADIUS scheme view

Parameters *retry-times*: Maximum number of accounting request transmission attempts. It ranges from 1 to 255 and defaults to 5.

Description Use the **retry realtime-accounting** command to set the maximum number of accounting request transmission attempts.

Use the **undo retry realtime-accounting** command to restore the default.

Note that:

- A RADIUS server usually checks whether a user is online by a timeout timer. If it receives from the NAS no real-time accounting packet for a user in the timeout period, it considers that there may be line or device failure and stops accounting for the user. This may happen when some unexpected failure occurs. In this case, the NAS is required to disconnect the user in accordance. This is done by the maximum number of accounting request transmission attempts. Once the limit is reached but the NAS still receives no response, the NAS disconnects the user.
- Suppose that the RADIUS server response timeout period is 3 seconds (set with the **timer response-timeout** command), the timeout retransmission attempts is 3 (set with the **retry** command), and the real-time accounting interval is 12 minutes (set with the **timer realtime-accounting** command), and the maximum number of accounting request transmission attempts is 5 (set with the **retry realtime-accounting** command). In such a case, the device generates an accounting request every 12 minutes, and retransmits the request when receiving no response within 3 seconds. The accounting is deemed unsuccessful if no response is received within 3 requests. Then the device sends a request every 12 minutes, and if for 5 times it still receives no response, the device will cut the user connection.

Related commands: **radius scheme**, **timer realtime-accounting**.

Examples # Set the maximum number of accounting request transmission attempts to 10 for RADIUS scheme radius1.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname -radius-radius1] retry realtime-accounting 10
```

retry stop-accounting (RADIUS scheme view)

Syntax **retry stop-accounting** *retry-times*

undo retry stop-accounting

View RADIUS scheme view

Parameters *retry-times*: Maximum number of stop-accounting request transmission attempts. It ranges from 10 to 65,535 and defaults to 500.

Description Use the **retry stop-accounting** command to set the maximum number of stop-accounting request transmission attempts.

Use the **undo retry stop-accounting** command to restore the default.

- Suppose that the RADIUS server response timeout period is 3 seconds (set with the **timer response-timeout** command), the timeout retransmission attempts is 5 (set with the **retry** command), and the maximum number of stop-accounting request transmission attempts is 20 (set with the **retry stop-accounting** command). This means that for each stop-accounting request, if the device receives no response within 3 seconds, it will initiate a new request. If still no responses are received within 5 renewed requests, the stop-accounting request is deemed unsuccessful. Then the device will temporarily store the request in the device and resend a request and repeat the whole process described above. Only when 20 consecutive attempts fail will the device discard the request.

Related commands: **reset stop-accounting-buffer**, **radius scheme**, **display stop-accounting-buffer**.

Examples # Set the maximum number of stop-accounting request transmission attempts to 1,000 for RADIUS scheme radius1.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] retry stop-accounting 1000
```

secondary accounting (RADIUS scheme view)

Syntax **secondary accounting** *ip-address* [*port-number*]

undo secondary accounting

View RADIUS scheme view

Parameters *ip-address*: IP address of the secondary accounting server, in dotted decimal notation. The default is 0.0.0.0.

port-number: UDP port number of the secondary accounting server, which ranges from 1 to 65535 and defaults to 1813.

Description Use the **secondary accounting** command to configure the IP address and UDP port of the secondary RADIUS accounting server.

Use the **undo secondary accounting** command to restore the defaults.

The IP addresses of the primary and secondary accounting servers cannot be the same. Otherwise, the configuration fails.

Related commands: **key**, **radius scheme**, **state**.

Examples # Set the IP address of the secondary accounting server for RADIUS scheme radius1 to 10.110.1.1 and the UDP port of the server to 1813.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] secondary accounting 10.110.1.1 1813
```

secondary authentication (RADIUS scheme view)

Syntax **secondary authentication** *ip-address* [*port-number*]

undo secondary authentication

View RADIUS scheme view

Parameters *ip-address*: IP address of the secondary authentication/authorization server, in dotted decimal notation. The default is 0.0.0.0.

port-number: UDP port number of the secondary authentication/authorization server, which ranges from 1 to 65535 and defaults to 1812.

Description Use the **secondary authentication** command to configure the IP address and UDP port of the secondary RADIUS authentication/authorization server.

Use the **undo secondary authentication** command to restore the defaults.

Note that the IP addresses of the primary and secondary authentication/authorization servers cannot be the same. Otherwise, the configuration fails.

Related commands: **key**, **radius scheme**, **state**.

Examples # Set the IP address of the secondary authentication/authorization server for RADIUS scheme radius1 to 10.110.1.2 and the UDP port of the server to 1812.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] secondary authentication 10.110.1.2 1812
```

server-type

Syntax **server-type** { **extended** | **standard** }

undo server-type

View RADIUS scheme view

Parameters **extended**: Specifies the extended RADIUS server (generally CAMS), which requires the RADIUS client and RADIUS server to interact according to the procedures and packet formats provisioned by the private RADIUS protocol.

standard: Specifies the standard RADIUS server, which requires the RADIUS client end and RADIUS server to interact according to the regulation and packet format of the standard RADIUS protocol (RFC 2138/2139 or newer).

Description Use the **server-type** command to specify the RADIUS server type supported by the device.

Use the **undo server-type** command to restore the default.

By default, the supported RADIUS server type is **standard**.

For the default scheme named "system", the type of its RADIUS server is **extended**.

Related commands: **radius scheme**.

Examples # Set the RADIUS server type of RADIUS scheme radius1 to "extended".

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] server-type extended
```

state (RADIUS scheme view)

Syntax **state** { **primary** | **secondary** } { **accounting** | **authentication** } { **active** | **block** }

View RADIUS scheme view

Parameters **primary**: Sets the status of the primary RADIUS server.

secondary: Sets the status of the secondary RADIUS server.

accounting: Sets the status of the RADIUS accounting server.

authentication: Sets the status of the RADIUS authentication/authorization server.

active: Sets the status of the RADIUS server to **active**, namely the normal operation state.

block: Sets the status of the RADIUS server to **block**.

Description Use the **state** command to set the status of a RADIUS server.

By default, every RADIUS server configured with an IP address in the RADIUS scheme is in the state of active.

Note that:

- When a primary server, authentication/authorization server or accounting server, fails, the device automatically turns to the secondary server. After the status of a primary server stays blocked for a period specified by the **timer**

quiet command, the device tries to communicate with the primary server. If the primary server has resumed, the device turns to use the primary server and stops communicating with the secondary server. In this case, the status of the primary server is active again and the status of the secondary server remains the same.

- If both the primary server and the secondary server are in the state of active or blocked, the device sends the packets only to the primary server.

Related commands: **radius scheme**, **primary authentication**, **secondary authentication**, **primary accounting**, **secondary accounting**.

Examples # Set the status of the secondary server in RADIUS scheme radius1 to active.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] state secondary authentication active
```

stop-accounting-buffer enable (RADIUS scheme view)

Syntax **stop-accounting-buffer enable**

undo stop-accounting-buffer enable

View RADIUS scheme view

Parameters None

Description Use the **stop-accounting-buffer enable** command to enable the device to buffer stop-accounting requests getting no responses.

Use the **undo stop-accounting-buffer enable** command to disable the device from buffering stop-accounting requests getting no responses.

By default, the device is enabled to buffer stop-accounting requests getting no responses.

Since stop-accounting requests affect the charge to users, a NAS must make its best effort to send every stop-accounting request to the RADIUS accounting servers. For each stop-accounting request getting no response in the specified period of time, the NAS buffers and resends the packet until it receives a response or the number of transmission retries reaches the configured limit. In the latter case, the NAS discards the packet.

Related commands: **reset stop-accounting-buffer**, **radius scheme**, **display stop-accounting-buffer**.

Examples # In RADIUS scheme radius1, enable the device to buffer the stop-accounting requests getting no responses.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] stop-accounting-buffer enable
```

timer quiet (RADIUS scheme view)

Syntax **timer quiet** *minutes*

undo timer quiet

View RADIUS scheme view

Parameters *minutes*: Primary server quiet period, in minutes. It ranges from 1 to 255 and defaults to 5.

Description Use the **timer quiet** command to set the quiet timer for the primary server, that is, the period during which the status of the primary server stays blocked before resuming the active state.

Use the **undo timer quiet** command to restore the default.

By default, the quiet timer of the primary server is 5 minutes.

Related commands: **display radius**.

Examples # Set the quiet timer for the primary server to 10 minutes.

```
<Sysname> system-view
[Sysname] radius scheme test1
[Sysname-radius-test1] timer quiet 10
```

timer realtime-accounting (RADIUS scheme view)

Syntax **timer realtime-accounting** *minutes*

undo timer realtime-accounting

View RADIUS scheme view

Parameters *minutes*: Real-time accounting interval in minutes, must be a multiple of 3 and in the range 3 to 60, with the default value being 12.

Description Use the **timer realtime-accounting** command to set the real-time accounting interval.

Use the **undo timer realtime-accounting** command to restore the default.

Note that:

- For real-time accounting, a NAS must transmit the accounting information of online users to the RADIUS accounting server periodically. This command is for setting the interval.
- The setting of the real-time accounting interval somewhat depends on the performance of the NAS and the RADIUS server: a shorter interval requires higher performance. You are therefore recommended to adopt a longer interval when there are a large number of users (more than 1000, inclusive). The following table lists the recommended ratios of the interval to the number of users.

Table 320 Recommended ratios of the accounting interval to the number of users

Number of users	Real-time accounting interval (minute)
1 to 99	3
100 to 499	6
500 to 999	12
1000 or more	15 or more

Related commands: **retry realtime-accounting**, **radius scheme**.

Examples # Set the real-time accounting interval to 51 minutes for RADIUS scheme radius1.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] timer realtime-accounting 51
```

timer response-timeout (RADIUS scheme view)

Syntax **timer response-timeout** *seconds*

undo timer response-timeout

View RADIUS scheme view

Parameters *seconds*: RADIUS server response timeout period in seconds. It ranges from 1 to 10 and defaults to 3.

Description Use the **timer response-timeout** command to set the RADIUS server response timeout timer.

Use the **undo timer** command to restore the default.

Note that:

- If a NAS receives no response from the RADIUS server in a period of time after sending a RADIUS request (authentication/authorization or accounting request), it has to resend the request so that the user has more opportunity to obtain the RADIUS service. The NAS uses the RADIUS server response timeout timer to control the transmission interval.

- A proper value for the RADIUS server response timeout timer can help improve the system performance. Set the timer based on the network conditions.
- The maximum total number of all types of retransmission attempts multiplied by the RADIUS server response timeout period cannot be greater than 75.

Related commands: **radius scheme**, **retry**.

Examples # Set the RADIUS server response timeout timer to 5 seconds for RADIUS scheme radius1.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] timer response-timeout 5
```

user-name-format (RADIUS scheme view)

Syntax **user-name-format** { **with-domain** | **without-domain** }

View RADIUS scheme view

Parameters **with-domain**: Includes the ISP domain name in the username sent to the RADIUS server.

without-domain: Excludes the ISP domain name from the username sent to the RADIUS server.

Description Use the **user-name-format** command to specify the format of the username to be sent to a RADIUS server.

By default, the ISP domain name is included in the username.

For the default scheme named "system", its user names contain no ISP domain name.

Note that:

- A username is generally in the format of userid@isp-name, of which isp-name is used by the device to determine the ISP domain to which a user belongs. Some earlier RADIUS servers, however, cannot recognize a username including an ISP domain name. Before sending a username including a domain name to such a RADIUS server, the device must remove the domain name. This command is thus provided for you to decide whether to include a domain name in a username to be sent to a RADIUS server.
- If a RADIUS scheme defines that the username is sent without the ISP domain name, do not apply the RADIUS scheme to more than one ISP domain, thus avoiding the confused situation where the RADIUS server regards two users in different ISP domains but with the same userid as one.

Related commands: **radius scheme**.

Examples # Specify the device to include the domain name in the username sent to the RADIUS servers for the RADIUS scheme radius1.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] user-name-format without-domain
```

76 HWTACACS CONFIGURATION COMMANDS

data-flow-format (HWTACACS scheme view)

Syntax **data-flow-format** { **data** { **byte** | **giga-byte** | **kilo-byte** | **mega-byte** } | **packet** { **giga-packet** | **kilo-packet** | **mega-packet** | **one-packet** } }*

undo data-flow-format { **data** | **packet** }

View HWTACACS scheme view

Parameters **data**: Specifies the unit for data flows, which can be byte, kilobyte, megabyte, or gigabyte.

packet: Specifies the unit for data packets, which can be one-packet, kilo-packet, mega-packet, or giga-packet.

Description Use the **data-flow-format** command to specify the unit for data flows or packets to be sent to a HWTACACS server.

Use the **undo data-flow-format** command to restore the default.

By default, the unit for data flows is **byte** and that for data packets is **one-packet**.

Related commands: **display hwtacacs**.

Examples # Define HWTACACS scheme hwt1 to send data flows and packets destined for the HWTACACS server in kilobytes and kilo-packets.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] data-flow-format data kilo-byte
[Sysname-hwtacacs-hwt1] data-flow-format packet kilo-packet
```

debugging hwtacacs

Syntax **debugging hwtacacs** { **all** | **error** | **event** | **message** | **receive-packet** | **send-packet** } [**slot** *slot-number*]

undo debugging hwtacacs { **all** | **error** | **event** | **message** | **receive-packet** | **send-packet** } [**slot** *slot-number*]

View User view

Parameters **all**: Turns on/off all types of debugging for HWTACACS.

error: Turns on/off error debugging.

event: Turns on/off event debugging.

message: Turns on/off message debugging.

receive-packet: Turns on/off debugging for received packets.

send-packet: Turns on/off debugging for sent packets.

slot *slot-number*: Turns on/off debugging for the module in a specified slot.

Description Use the **debugging hwtacacs** command to enable debugging for HWTACACS.

Use the **undo debugging hwtacacs** command to disable debugging for HWTACACS.

By default, debugging is disabled for HWTACACS.

Examples # Enable debugging for HWTACACS.

```
<Sysname> debugging hwtacacs event
```

display hwtacacs

Syntax **display hwtacacs** [*hwtacacs-scheme-name* [**statistics** [**slot** *slot-number*]]]

View Any view

Parameters *hwtacacs-scheme-name*: Displays the HWTACACS configuration of the specified scheme.

statistics: Displays complete statistics about the HWTACACS server.

slot *slot-number*: Displays the HWTACACS information about the module in a specified slot.

Description Use the **display hwtacacs** command to display configuration information or statistics of the specified or all HWTACACS schemes.

Related commands: **hwtacacs scheme**.

Examples # Display configuration information about HWTACACS scheme gy.

```
<Sysname> disp
lay hwtacacs g
y
```

```
  ------------------------------------------------------------------------
HWTACACS-server template name       : gy
  Primary-authentication-server     : 172.31.1.11:49
  Primary-authorization-server      : 172.31.1.11:49
  Primary-accounting-server         : 172.31.1.11:49
  Secondary-authentication-server   : 0.0.0.0:0
  Secondary-authorization-server    : 0.0.0.0:0
  Secondary-accounting-server       : 0.0.0.0:0



  Current-authentication-server     : 172.31.1.11:49
  Current-authorization-server      : 172.31.1.11:49
  Current-accounting-server         : 172.31.1.11:49
  NAS-IP-address                    : 0.0.0.0
  key authentication                : 790131
  key authorization                 : 790131
  key accounting                    : 790131
  Quiet-interval(min)               : 5
  Realtime-accounting-interval(min) : 12
  Response-timeout-interval(sec)    : 5
  Acct-stop-PKT retransmit times    : 100
  Domain-included                   : Yes
  Data traffic-unit                 : B
  Packet traffic-unit               : one-packet
  ------------------------------------------------------------------------
```

display stop-accounting-buffer (Any view)

Syntax **display stop-accounting-buffer** { **hwtacacs-scheme** *hwtacacs-scheme-name* | **session-id** *session-id* | **time-range** *start-time stop-time* | **user-name** *user-name* } [**slot** *slot-number*]

View Any view

Parameters **hwtacacs-scheme** *hwtacacs-scheme-name*: Displays information about the buffered stop-accounting requests of the specified HWTACACS scheme.

session-id *session-id*: Displays information about the buffered stop-accounting requests of the specified session. *session-id* specifies a session by its ID, a string of 1 to 50 characters.

time-range *start-time stop-time*: Displays information about the buffered stop-accounting requests in the specified time range. *start-time* specifies the start time of a time range, and *stop-time* specifies the end time of a time range. They are in the format of hh:mm:ss- mm/dd/yyyy or *hh:mm:ss-yyyy/mm/dd*. If this argument is specified, the system will display information about the buffered stop-accounting requests in the time range from *start-time* to *stop-time*.

user-name *user-name*: Displays information about the buffered stop-accounting requests of the specified user name.

slot *slot-number*: Displays information about the stop-accounting requests on the module of the specified slot.

Description Use the **display stop-accounting-buffer** command to display information about the stop-accounting requests buffered in the device by scheme, session ID, time range, user name, or slot.

Related commands: **reset stop-accounting-buffer**, **stop-accounting-buffer enable**, **retry stop-accounting**.

Examples # Display information about the buffered stop-accounting requests for HWTACACS scheme hwt1.

```
<Sysname> display stop-accounting-buffer hwtacacs-scheme hwt1
Total 0 record(s) Matched
```

hwtacacs nas-ip

Syntax **hwtacacs nas-ip** *ip-address*

undo hwtacacs nas-ip

View System view

Parameters *ip-address*: IP address in dotted decimal notation. It must be an address of the device and cannot be all 0s address, all 1s address, a class D address, a class E address or a loopback address.

Description Use the **hwtacacs nas-ip** command to set the IP address for the device to use as the source address of the HWTACACS packets to be sent to the server.

Use the **undo hwtacacs nas-ip** command to remove the configuration.

By default, the source IP address of a packet sent to the server is the IP address of the outbound port.

Note that:

- Specifying a source address for the HWTACACS packets to be sent to the server can avoid the situation where the packets sent back by the HWTACACS server cannot reach the device as the result of a physical interface failure.
- If you configure the command for more than one time, the last configuration takes effect.
- The **nas-ip** command in HWTACACS scheme view is only for the current HWTACACS scheme, while the **hwtacacs nas-ip** command in system view is for all HWTACACS schemes. However, the **nas-ip** command in HWTACACS scheme view overwrites the configuration of the **hwtacacs nas-ip** command.

Related commands: **nas-ip**.

Examples # Set the IP address for the device to use as the source address of the HWTACACS packets to 129.10.10.1.

```
<Sysname> system-view
[Sysname] hwtacacs nas-ip 129.10.10.1
```

hwtacacs scheme

Syntax **hwtacacs scheme** *hwtacacs-scheme-name*

undo hwtacacs scheme *hwtacacs-scheme-name*

View System view

Parameters *hwtacacs-scheme-name*: HWTACACS scheme name, a case-insensitive string of 1 to 32 characters.

Description Use the **hwtacacs scheme** command to create an HWTACACS scheme and enter HWTACACS scheme view.

Use the **undo hwtacacs scheme** command to delete an HWTACACS scheme.

By default, no HWTACACS scheme exists.

Examples # Create an HWTACACS scheme named hwt1 and enter HWTACACS scheme view.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1]
```

key (HWTACACS scheme view)

Syntax **key** { **accounting** | **authentication** | **authorization** } *string*

undo key { **accounting** | **authentication** | **authorization** } *string*

View HWTACACS scheme view

Parameters **accounting**: Sets the shared key for HWTACACS accounting packets.

authentication: Sets the shared key for HWTACACS authentication packets.

authorization: Sets the shared key for HWTACACS authorization packets.

string: Shared key, a string of 1 to 16 characters.

Description Use the **key** command to set the shared key for HWTACACS authentication, authorization, or accounting packets.

Use the **undo key** command to remove the configuration.

By default, no shared key exists.

Related commands: **display hwtacacs**.

Examples # Set the shared key for HWTACACS accounting packets to hello for HWTACACS scheme hwt1.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] key accounting hello
```

nas-ip (HWTACACS scheme view)

Syntax **nas-ip** *ip-address*

undo nas-ip

View HWTACACS scheme view

Parameters *ip-address*: IP address in dotted decimal notation. It must be an address of the device and cannot be all 0s address, all 1s address, a class D address, a class E address or a loopback address.

Description Use the **nas-ip** command to set the IP address for the device to use as the source address of the HWTACACS packets to be sent to the server.

Use the **undo nas-ip** command to remove the configuration.

By default, the source IP address of a packet sent to the server is the IP address of the outbound port.

Note that:

- Specifying a source address for the HWTACACS packets to be sent to the server can avoid the situation where the packets sent back by the HWTACACS server cannot reach the device as the result of a physical interface failure.
- If you configure the command for more than one time, the last configuration takes effect.
- The **nas-ip** command in HWTACACS scheme view is only for the current HWTACACS scheme, while the **hwtacacs nas-ip** command in system view is for all HWTACACS schemes. However, the **nas-ip** command in HWTACACS scheme view overwrites the configuration of the **hwtacacs nas-ip** command.

Related commands: **hwtacacs nas-ip**.

Examples # Set the IP address for the device to use as the source address of the HWTACACS packets to 10.1.1.1.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] nas-ip 10.1.1.1
```

primary accounting (HWTACACS scheme view)

Syntax **primary accounting** *ip-address* [*port-number*]

undo primary accounting

View HWTACACS scheme view

Parameters *ip-address*: IP address of the server, a valid unicast address in dotted decimal notation. The default is 0.0.0.0.

port-number: Port number of the server. It ranges from 1 to 65535 and defaults to 49.

Description Use the **primary accounting** command to specify the primary HWTACACS accounting server.

Use the **undo primary accounting** command to remove the configuration.

Note that:

- The IP addresses of the primary and secondary accounting servers cannot be the same. Otherwise, the configuration fails.
- If you configure the command for more than one time, the last configuration takes effect.
- You can remove an accounting server only when no active TCP connection for sending accounting packets is using it.

Examples # Configure the primary accounting server.

```
<Sysname> system-view
[Sysname] hwtacacs scheme test1
[Sysname-hwtacacs-test1] primary accounting 10.163.155.12 49
```

primary authentication (HWTACACS scheme view)

Syntax **primary authentication** *ip-address* [*port-number*]

undo primary authentication

View HWTACACS scheme view

Parameters *ip-address*: IP address of the server, a valid unicast address in dotted decimal notation. The default is 0.0.0.0.

port-number: Port number of the server. It ranges from 1 to 65535 and defaults to 49.

Description Use the **primary authentication** command to specify the primary HWTACACS authentication server.

Use the **undo primary authentication** command to remove the configuration.

Note that:

- The IP addresses of the primary and secondary authentication servers cannot be the same. Otherwise, the configuration fails.
- If you configure the command for more than one time, the last configuration takes effect.
- You can remove an authentication server only when no active TCP connection for sending authentication packets is using it.

Related commands: **display hwtacacs**.

Examples # Set the primary authentication server.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] primary authentication 10.163.155.13 49
```

primary authorization

Syntax **primary authorization** *ip-address* [*port-number*]

undo primary authorization

View HWTACACS scheme view

Parameters *ip-address*: IP address of the server, a valid unicast address in dotted decimal notation. The default is 0.0.0.0.

port-number: Port number of the server. It ranges from 1 to 65535 and defaults to 49.

Description Use the **primary authorization** command to specify the primary HWTACACS authorization server.

Use the **undo primary authorization** command to remove the configuration.

Note that:

- The IP addresses of the primary and secondary authorization servers cannot be the same. Otherwise, the configuration fails.
- If you configure the command for more than one time, the last configuration takes effect.
- You can remove an authorization server only when no active TCP connection for sending authorization packets is using it.

Related commands: **display hwtacacs**.

Examples # Configure the primary authorization server.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] primary authorization 10.163.155.13 49
```

reset hwtacacs statistics

Syntax **reset hwtacacs statistics** { **accounting** | **all** | **authentication** | **authorization** } [**slot** *slot-number*]

View User view

Parameters **accounting**: Clears HWTACACS accounting statistics.

all: Clears all HWTACACS statistics.

authentication: Clears statistics of HWTACACS authentication.

authorization: Clears statistics of HWTACACS authorization.

slot *slot-number*: Clears HWTACACS statistics on the interface module in the specified slot.

Description Use the **reset hwtacacs statistics** command to clear HWTACACS statistics.

Related commands: **display hwtacacs**.

Examples # Clear all HWTACACS statistics.

```
<Sysname> reset hwtacacs statistics all
```

reset stop-accounting-buffer (User view)

Syntax **reset stop-accounting-buffer** { **hwtacacs-scheme** *hwtacacs-scheme-name* | **session-id** *session-id* | **time-range** *start-time stop-time* | **user-name** *user-name* } [**slot** *slot-number*]

View User view

Parameters **hwtacacs-scheme** *hwtacacs-scheme-name*: Clears the buffered stop-accounting requests of the specified HWTACACS scheme.*hwtacacs-server-name* specifies a HWTACACS scheme name, a string of 1 to 32 characters.

session-id *session-id*: Clears the buffered stop-accounting requests of the specified session. *session-id* specifies a session by its ID, a string of 1 to 50 characters.

time-range *start-time stop-time*: Clears the buffered stop-accounting requests in the specified time range. *start-time* specifies the start time of a time range, and *stop-time* specifies the end time of a time range. They are in the format of hh:mm:ss- mm/dd/yyyy or *hh:mm:ss-yyyy/mm/dd*.

user-name *user-name*: Clears the buffered stop-accounting requests of the specified user name.

slot *slot-number*: Clears the buffered stop-accounting requests of the module on the specified slot.

Description Use the **reset stop-accounting-buffer** command to delete the buffered stop-accounting requests that get no responses.

Related commands: **stop-accounting-buffer enable**, **retry stop-accounting**, **display stop-accounting-buffer**.

Examples # Clear the buffered stop-accounting requests for HWTACACS scheme hwt1.

```
<Sysname> reset stop-accounting-buffer hwtacacs-scheme hwt1
```

retry stop-accounting (HWTACACS scheme view)

Syntax **retry stop-accounting** *retry-times*

undo retry stop-accounting

View HWTACACS scheme view

Parameters *retry-times*: Maximum number of stop-accounting request transmission attempts. It ranges from 1 to 300 and defaults to 100.

Description Use the **retry stop-accounting** command to set the maximum number of stop-accounting request transmission attempts.

Use the **undo retry stop-accounting** command to restore the default.

Related commands: **reset stop-accounting-buffer**, **hwtacacs scheme**, **display stop-accounting-buffer**.

Examples # Set the maximum number of stop-accounting request transmission attempts to 50.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] retry stop-accounting 50
```

secondary accounting (HWTACACS scheme view)

Syntax **secondary accounting** *ip-address* [*port-number*]

undo secondary accounting

View HWTACACS scheme view

Parameters *ip-address*: IP address of the server, a valid unicast address in dotted decimal notation. The default is 0.0.0.0.

port-number: Port number of the server. It ranges from 1 to 65535 and defaults to 49.

Description Use the **secondary accounting** command to specify the secondary HWTACACS accounting server.

Use the **undo secondary accounting** command to remove the configuration.

Note that:

- The IP addresses of the primary and secondary accounting servers cannot be the same. Otherwise, the configuration fails.
- If you configure the command for more than one time, the last configuration takes effect.
- You can remove an accounting server only when no active TCP connection for sending accounting packets is using it.

Examples # Configure the secondary accounting server.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] secondary accounting 10.163.155.12 49
```

secondary authentication (HWTACACS scheme view)

Syntax **secondary authentication** *ip-address* [*port-number*]

undo secondary authentication

View HWTACACS scheme view

Parameters *ip-address*: IP address of the server, a valid unicast address in dotted decimal notation. The default is 0.0.0.0.

port-number: Port number of the server. It ranges from 1 to 65535 and defaults to 49.

Description Use the **secondary authentication** command to specify the secondary HWTACACS authentication server.

Use the **undo secondary authentication** command to remove the configuration.

Note that:

- The IP addresses of the primary and secondary authentication servers cannot be the same. Otherwise, the configuration fails.
- If you configure the command for more than one time, the last configuration takes effect.
- You can remove an authentication server only when no active TCP connection for sending authentication packets is using it.

Related commands: **display hwtacacs**.

Examples # Configure the secondary authentication server.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] secondary authentication 10.163.155.13 49
```

secondary authorization

Syntax **secondary authorization** *ip-address* [*port-number*]

undo secondary authorization

View HWTACACS scheme view

Parameters *ip-address*: IP address of the server, a valid unicast address in dotted decimal notation. The default is 0.0.0.0.

port-number: Port number of the server. It ranges from 1 to 65535 and defaults to 49.

Description Use the **secondary authorization** command to specify the secondary HWTACACS authorization server.

Use the **undo secondary authorization** command to remove the configuration.

Note that:

- The IP addresses of the primary and secondary authorization servers cannot be the same. Otherwise, the configuration fails.
- If you configure the command for more than one time, the last configuration takes effect.
- You can remove an authorization server only when no active TCP connection for sending authorization packets is using it.

Related commands: **display hwtacacs**.

Examples # Configure the secondary authorization server.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] secondary authorization 10.163.155.13 49
```

stop-accounting-buffer enable (HWTACACS scheme view)

Syntax **stop-accounting-buffer enable**

undo stop-accounting-buffer enable

View HWTACACS scheme view

Parameters None

Description Use the **stop-accounting-buffer enable** command to enable the device to buffer stop-accounting requests getting no responses.

Use the **undo stop-accounting-buffer enable** command to disable the device from buffering stop-accounting requests getting no responses.

By default, the device is enabled to buffer stop-accounting requests getting no responses.

Since stop-accounting requests affect the charge to users, a NAS must make its best effort to send every stop-accounting request to the HWTACACS accounting servers. For each stop-accounting request getting no response in the specified period of time, the NAS buffers and resends the packet until it receives a response or the number of transmission retries reaches the configured limit. In the latter case, the NAS discards the packet.

Related commands: **reset stop-accounting-buffer**, **hwtacacs scheme**, **display stop-accounting-buffer**.

Examples # In HWTACACS scheme hwt1, enable the device to buffer the stop-accounting requests getting no responses.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] stop-accounting-buffer enable
```

timer quiet (HWTACACS scheme view)

Syntax **timer quiet** *minutes*

undo timer quiet

View HWTACACS scheme view

Parameters *minutes*: Primary server quiet period, in minutes. It ranges from 1 to 255 and defaults to 5.

Description Use the **timer quiet** command to set the quiet timer for the primary server, that is, the duration that the status of the primary server stays blocked before resuming the active state.

Use the **undo timer quiet** command to restore the default.

Related commands: **display hwtacacs**.

Examples # Set the quiet timer for the primary server to 10 minutes.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] timer quiet  10
```

timer realtime-accounting (HWTACACS scheme view)

Syntax **timer realtime-accounting** *minutes*

undo timer realtime-accounting

View HWTACACS scheme view

Parameters *minutes*: Real-time accounting interval in minutes. It is a multiple of 3 in the range 3 to 60 and defaults to 12.

Description Use the **timer realtime-accounting** command to set the real-time accounting interval.

Use the **undo timer realtime-accounting** command to restore the default.

Note that:

- For real-time accounting, a NAS must transmit the accounting information of online users to the HWTACACS accounting server periodically. This command is for setting the interval.
- The setting of the real-time accounting interval somewhat depends on the performance of the NAS and the HWTACACS server: a shorter interval requires higher performance. You are therefore recommended to adopt a longer interval when there are a large number of users (more than 1000, inclusive). The following table lists the recommended ratios of the interval to the number of users.

Table 321 Recommended ratios of the accounting interval to the number of users

Number of users	Real-time accounting interval (minute)
1 to 99	3
100 to 499	6
500 to 999	12
1000 or more	15 or more

Examples # Set the real-time accounting interval to 51 minutes for HWTACACS scheme hwt1.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] timer realtime-accounting 51
```

timer response-timeout (HWTACACS scheme view)

Syntax **timer response-timeout** *seconds*

undo timer response-timeout

View HWTACACS scheme view

Parameters *seconds*: HWTACACS server response timeout period in seconds. It ranges from 1 to 300 and defaults to 5.

Description Use the **timer response-timeout** command to set the HWTACACS server response timeout timer.

Use the **undo timer** command to restore the default.

As HWTACACS is based on TCP, the timeout of the server response timeout timer and/or the TCP timeout timer will cause the device to be disconnected from the HWTACACS server.

Related commands: **display hwtacacs**.

Examples # Set the HWTACACS server response timeout timer to 30 seconds for HWTACACS scheme hwt1.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] timer response-timeout 30
```

user-name-format (HWTACACS scheme view)

Syntax **user-name-format** { **with-domain** | **without-domain** }

View HWTACACS scheme view

Parameters **with-domain**: Includes the ISP domain name in the username sent to the HWTACACS server.

without-domain: Excludes the ISP domain name from the username sent to the HWTACACS server.

Description Use the **user-name-format** command to specify the format of the username to be sent to a HWTACACS server.

By default, the ISP domain name is included in the username.

Note that:

- A username is generally in the format of userid@isp-name, of which isp-name is used by the device to determine the ISP domain to which a user belongs. Some earlier HWTACACS servers, however, cannot recognize a username including an ISP domain name. Before sending a username including a domain name to such a HWTACACS server, the device must remove the domain name. This command is thus provided for you to decide whether to include a domain name in a username to be sent to a HWTACACS server.
- If a HWTACACS scheme defines that the username is sent without the ISP domain name, do not apply the HWTACACS scheme to more than one ISP domain, thus avoiding the confused situation where the HWTACACS server regards two users in different ISP domains but with the same userid as one.

Related commands: **hwtacacs scheme**.

Examples # Specify the device to include the ISP domain name in the username sent to the HWTACACS servers for the HWTACACS scheme hwt1.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] user-name-format without-domain
```

77 802.1X CONFIGURATION COMMANDS

debugging dot1x

Syntax **debugging dot1x** { **all** | **error** | **event** | **packet** } [**slot** *slot-number*]

undo debugging dot1x { **all** | **error** | **event** | **packet** } [**slot** *slot-number*]

View User view

Parameters **All**: Enables all debugging.

Error: Enables error debugging.

Event: Enables event debugging.

Packet: Enables packet debugging.

slot *slot-number*: Enables debugging for the specified slot.

Description Use the **debugging dot1x** command to enable 802.1x debugging.

Use the **undo debugging dot1x** command to disable 802.1x debugging.

By default, 802.1x debugging is disabled.

Examples # Enable all 802.1x debugging.

```
<Sysname> debugging dot1x all
```

display dot1x

Syntax **display dot1x** [**sessions** | **statistics**] [**interface** *interface-list*]

View Any view

Parameters **sessions**: Displays 802.1x session information.

statistics: Displays 802.1x statistics.

interface *interface-list*: Specifies an Ethernet port list, which can contain multiple Ethernet ports. The *interface-list* argument is in the format of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } & <1-10>,

where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 port indexes/port index lists for this argument. The start port number must be smaller than the end number and the two ports must of the same type.

Description Use the **display dot1x** command to display 802.1x session information, statistics, or configuration information of specified or all ports.

With both the **sessions** keyword and the **statistics** keyword not provided, this command displays 802.1x configuration information.

Examples # Display 802.1x configuration information.

```
<Sysname> display dot1x
Global 802.1X protocol is enabled
CHAP authentication is enabled
Proxy trap checker is disabled
Proxy logoff checker is disabled

Configuration: Transmit Period     30 s,  Handshake Period       15 s
               Quiet Period        60 s,  Quiet Period Timer is disabled
               Supp Timeout        30 s,  Server Timeout         100 s
               The maximal retransmitting times          3

Total maximum 802.1x user resource number is 1024 per slot
Total current used 802.1x resource number is 0

Ethernet3/1/1  is link-up
  802.1X protocol is disabled
  Proxy trap checker is disabled
  Proxy logoff checker is disabled
  Handshake is disabled
  The port is an authenticator
  Authenticate Mode is Auto
  Port Control Type is Mac-based
  Guest VLAN: 0
  Max number of on-line user number users is 2561024
  EAPOL Packet: Tx 0, Rx 0
  Sent EAP Request/Identity Packets : 0
       EAP Request/Challenge Packets: 0
       EAP Success Packets: 0, Fail Packets: 0
  Received EAPOL Start Packets : 0
           EAPOL LogOff Packets: 0
           EAP Response/Identity Packets : 0
           EAP Response/Challenge Packets: 0
           Error Packets: 0

   EAPOL Packet: Tx 0, Rx 0
   Sent EAP Request/Identity Packets : 0
        EAP Request/Challenge Packets: 0
        EAP Success Packets: 0, Fail Packets: 0
   Received EAPOL Start Packets : 0
            EAPOL LogOff Packets: 0
            EAP Response/Identity Packets : 0
            EAP Response/Challenge Packets: 0
            Error Packets: 0

  Controlled User(s) amount to 0
```

Table 322 Descriptions on the fields of the display dot1x command

Field	Description
Global 802.1X protocol is enabled	Indicates whether 802.1x is enabled

Table 322 Descriptions on the fields of the display dot1x command

Field	Description
CHAP authentication is enabled	Indicates whether CHAP authentication is enabled
Proxy trap checker is disabled	Indicates whether the device is configured to send a trap packet when detecting that a user is trying to login through a proxy
Proxy logoff checker is disabled	Indicates whether the device is configured to get offline any user trying to login through a proxy
Transmit Period	Setting of the username request timeout timer
Handshake Period	Setting of the handshake timer
Quiet Period	Setting of the quiet timer
Quiet Period Timer is disable	Indicates whether the quiet timer is enabled
Supp Timeout	Setting of the supplicant timeout timer
Server Timeout	Setting of the server timeout timer
The maximal retransmitting times	Maximum number of attempts for the authenticator to send authentication requests to the supplicant
Total maximum 802.1x user resource number	Maximum number of users supported per module
Total current used 802.1x resource number	Total number of online users
Ethernet3/1/1 is link-up	Status of port Ethernet 3/1/1
802.1X protocol is disabled	Indicates whether 802.1x is enabled on the port
Proxy trap checker is disabled	Indicates whether the port is configured to send a trap packet when detecting that a user is trying to login through a proxy
Proxy logoff checker is disabled	Indicates whether the port is configured to get offline any user trying to login through a proxy
Handshake is disabled	Indicates whether handshake is enabled on the port
The port is an authenticator	Role of the port
Authenticate Mode is Auto	Access control mode for the port
Port Control Type is Mac-based	Access control method for the port
Guest VLAN	Guest VLAN configured for the port. The value of 0 means that no guest VLAN is configured.
Max number of on-line users	Maximum number of users supported on the port
EAPOL Packet	Number of EAPOL packets received (Tx) or sent (Rx)
Sent EAP Request/Identity Packets	Number of EAP Request/Identity packets sent
EAP Request/Challenge Packets	Number of EAP Request/Challenge packets sent
EAP Success Packets	Number of EAP Success packets sent
Received EAPOL Start Packets	Number of EAPOL Start packets received
EAPOL LogOff Packets	Number of EAPOL LogOff packets received
EAP Response/Identity Packets	Number of EAP Response/Identity packets received

Table 322 Descriptions on the fields of the display dot1x command

Field	Description
EAP Response/Challenge Packets	Number of EAP Response/Challenge packets received
Error Packets	Number of erroneous packets received
Controlled User(s) amount to 0	Number of controlled users on the port

dot1x

Syntax **dot1x** [**interface** *interface-list*]

undo dot1x [**interface** *interface-list*]

View System view, Ethernet interface view

Parameters **interface** *interface-list*: Specifies an Ethernet port list, which can contain multiple Ethernet ports. The *interface-list* argument is in the format of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 port indexes/port index lists for this argument. The start port number must be smaller than the end number and the two ports must of the same type.

Description Use the **dot1x** command in system view to enable 802.1x globally.

Use the **undo dot1x** command in system view to disable 802.1x globally.

Use the **dot1x interface** *interface-list* command in system view or the **dot1x** command in Ethernet interface view to enable 802.1x for specified ports.

Use the **undo dot1x interface** *interface-list* command in system view or the **undo dot1x** command in Ethernet interface view to disable 802.1x for specified ports.

By default, 802.1x is neither enabled globally nor enabled for any port.

Note that:

- 802.1x must be enabled both globally in system view and for the intended ports in system view or Ethernet interface view. Otherwise, it does not function.
- You can configure 802.1x parameters either before or after enabling 802.1x.

Related commands: **display dot1x**.

Examples # Enable 802.1x for ports Ethernet 3/1/1, and Ethernet 3/1/5 to Ethernet 3/1/7.

```
<Sysname> system-view
[Sysname] dot1x interface ethernet 3/1/1 ethernet 3/1/5 to ethernet 3/1/7
```

Or

```
<Sysname> system-view
[Sysname] interface ethernet 3/1/1
[Sysname-Ethernet3/1/1] dot1x
[Sysname-Ethernet3/1/1] quit
[Sysname] interface ethernet 3/1/5
[Sysname-Ethernet3/1/5] dot1x
[Sysname-Ethernet3/1/5] quit
[Sysname] interface ethernet 3/1/6
[Sysname-Ethernet3/1/6] dot1x
[Sysname-Ethernet3/1/6] quit
[Sysname] interface ethernet 3/1/7
[Sysname-Ethernet3/1/7] dot1x
```

Enable 802.1x globally.

```
<Sysname> system-view
[Sysname] dot1x
```

dot1x authentication-method

Syntax **dot1x authentication-method** { **chap** | **eap** | **pap** }

undo dot1x authentication-method

View System view

Parameters **chap**: Authenticates supplicants using CHAP.

eap: Authenticates supplicants using EAP.

pap: Authenticates supplicants using PAP.

Description Use the **dot1x authentication-method** command to set the 802.1x authentication method.

Use the **undo dot1x authentication-method** command to restore the default.

By default, CHAP is used.

Note that:

- The password authentication protocol (PAP) transports passwords in clear text.
- The challenge handshake authentication protocol (CHAP) transports only usernames over the network. Compared with PAP, CHAP provides better security.
- With EAP relay authentication, the authenticator encapsulates 802.1x user information in the EAP attributes of RADIUS packets and sends the packets to the RADIUS server for authentication; it does not need to repackage the EAP packets into standard RADIUS packets for authentication. In this case, you can configure the **user-name-format** command but it does not take effect.

- Local authentication supports only PAP and CHAP.

Related commands: **display dot1x**.

Examples # Set the 802.1x authentication method to **PAP**.

```
<Sysname> system-view
[Sysname] dot1x authentication-method pap
```

dot1x guest-vlan

Syntax In system view:

dot1x guest-vlan *vlan-id* [**interface** *interface-list*]

undo dot1x guest-vlan [**interface** *interface-list*]

In Ethernet interface view:

dot1x guest-vlan *vlan-id*

undo dot1x guest-vlan

View System view, Ethernet interface view

Parameters *vlan-id*: ID of the VLAN to be specified as the guest VLAN, in the range 1 to 4094.

interface *interface-list*: Specifies an Ethernet port list, which can contain multiple Ethernet ports. The *interface-list* argument is in the format of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 port indexes/port index lists for this argument. The start port number must be smaller than the end number and the two ports must of the same type.

Description Use the **dot1x guest-vlan** command to configure the guest VLAN for specified or all ports.

Use the **undo dot1x guest-vlan** command to remove the guest VLAN(s) configured for specified or all ports.

By default, a port is configured with no guest VLAN.

In system view, this command configures guest VLAN for all ports with *interface-list* not provided, and configures guest VLAN for specified with *interface-list* provided.

In Ethernet interface view, you cannot specify the *interface-list* argument and can only configure guest VLAN for the current port.

For the guest VLAN feature to take effect on a port, make sure that:

- 802.1x is enabled.
- The port access control method is set to **portbased**.
- The port access control mode is set to **auto**.
- The link type of the port is set to **access**.

Note that:

- You cannot delete a VLAN that has been configured as a guest VLAN.
- A super VLAN cannot be set as the guest VLAN. Similarly, a guest VLAN cannot be set as the super VLAN. For information about super VLAN, refer to "Super VLAN Configuration Commands" on page 227.
- The guest VLAN function does not apply to non-access interfaces.

Examples # Specify port Ethernet 1/1/1 to use VLAN 999 as its guest VLAN.

```
<Sysname> system-view
[Sysname] dot1x guest-vlan 999 interface ethernet 1/1/1
```

Specify ports Ethernet 1/1/2 to Ethernet 1/1/5 to use VLAN 10 as its guest VLAN.

```
<Sysname> system-view
[Sysname] dot1x guest-vlan 10 interface ethernet 1/1/1 to ethernet 1/1/5
```

Specify all ports to use VLAN 7 as their guest VLAN.

```
<Sysname> system-view
[Sysname] dot1x guest-vlan 7
```

Specify port Ethernet 1/1/7 to use VLAN 3 as its guest VLAN.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1/7
[Sysname-Ethernet1/1/7] dot1x guest-vlan 3
```

dot1x handshake

Syntax **dot1x handshake**

undo dot1x handshake

View Ethernet interface view

Parameters None

Description Use the **dot1x handshake** command to enable the online user handshake function so that the device can periodically send handshake messages to the client to check whether a user is online.

Use the **undo dot1x handshake** command to disable the function.

By default, the function is enabled.

Note that the 802.1x proxy detection function depends on the online user handshake function. Be sure to enable handshake before enabling proxy detection and to disable proxy detection before disabling handshake.

Examples # Enable online user handshake.

```
<Sysname> system-view
[Sysname] interface ethernet 0/4/1
[Sysname-Ethernet0/4/1] dot1x handshake
```

Disable online user handshake.

```
<Sysname> system-view
[Sysname] interface ethernet 0/4/1
[Sysname-Ethernet0/4/1] undo dot1x handshake
```

dot1x max-user

Syntax **dot1x max-user** *user-number* [**interface** *interface-list*]

undo dot1x max-user [**interface** *interface-list*]

View System view, Ethernet interface view

Parameters *user-number*: Maximum number of users to be supported simultaneously. It ranges from 1 to 1024 and defaults to 1024.

interface *interface-list*: Specifies an Ethernet port list, which can contain multiple Ethernet ports. The *interface-list* argument is in the format of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 port indexes/port index lists for this argument. The start port number must be smaller than the end number and the two ports must of the same type.

Description Use the **dot1x max-user** command to set the maximum number of users to be supported simultaneously for specified or all ports.

Use the **undo dot1x max-user** command to restore the default.

With no interface specified, the command sets the threshold for all ports.

Related commands: **display dot1x**.

Examples # Set the maximum number of users for port Ethernet 3/1/1 to support simultaneously as 32.

```
<Sysname> system-view
[Sysname] dot1x max-user 32 interface ethernet 3/1/1
```

Or

```
<Sysname> system-view
[Sysname] interface ethernet 3/1/1
[Sysname-Ethernet3/1/1] dot1x max-user 32
```

dot1x port-control

Syntax **dot1x port-control** { **authorized-force** | **auto** | **unauthorized-force** } [**interface** *interface-list*]

undo dot1x port-control [**interface** *interface-list*]

View System view, Ethernet interface view

Parameters **authorized-force**: Places the specified or all ports in the state of authorized, allowing users of the ports to access the network without authentication.

auto: Places the specified or all ports in the state of unauthorized initially to allow only EAPOL frames to pass, and turns the ports into the state of authorized to allow access to the network after the users pass authentication. This is the most common choice.

unauthorized-force: Places the specified or all ports in the state of unauthorized, denying any access requests from users of the ports.

interface *interface-list*: Specifies an Ethernet port list, which can contain multiple Ethernet ports. The *interface-list* argument is in the format of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 port indexes/port index lists for this argument. The start port number must be smaller than the end number and the two ports must of the same type.

Description Use the **dot1x port-control** command to set the access control mode for specified or all ports.

Use the **undo dot1x port-control** command to restore the default.

The default access control mode is **auto**.

Related commands: **display dot1x**.

Examples # Set the access control mode of port Ethernet 3/1/1 to **unauthorized-force**.

```
<Sysname> system-view
[Sysname] dot1x port-control unauthorized-force interface ethernet 3/1/1
```

Or

```
<Sysname> system-view
[Sysname] interface ethernet 3/1/1
[Sysname-Ethernet3/1/1] dot1x port-control unauthorized-force
```

dot1x port-method

Syntax **dot1x port-method** { **macbased** | **portbased** } [**interface** *interface-list*]

undo dot1x port-method [**interface** *interface-list*]

View System view, Ethernet interface view

Parameters **macbased**: Specifies to use the **macbased** authentication method. With this method, each user of a port must be authenticated separately, and when an authenticated user goes offline, no other users are affected.

portbased: Specifies to use the **portbased** authentication method. With this method, after the first user of a port passes authentication, all other users of the port can access the network without authentication, and when the first user goes offline, all other users get offline at the same time.

interface *interface-list*: Specifies an Ethernet port list, which can contain multiple Ethernet ports. The *interface-list* argument is in the format of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 port indexes/port index lists for this argument. The start port number must be smaller than the end number and the two ports must of the same type.

Description Use the **dot1x port-method** command to set the access control method for specified or all ports.

Use the **undo dot1x port-method** command to restore the default.

The default access control method is **macbased**.

Related commands: **display dot1x**.

Examples # Set the access control method to **portbased** for port Ethernet 3/1/1.

```
<Sysname> system-view
[Sysname] dot1x port-method portbased interface ethernet 3/1/1
```

Or

```
<Sysname> system-view
[Sysname] interface ethernet 3/1/1
[Sysname-Ethernet3/1/1] dot1x port-method portbased
```

dot1x quiet-period

Syntax **dot1x quiet-period**

undo dot1x quiet-period

View System view

Parameters None

Description Use the **dot1x quiet-period** command to enable the quiet timer function.

Use the **undo dot1x quiet-period** command to disable the function.

By default, the function is disabled.

After a supplicant fails the authentication, the authenticator refuses further authentication requests from the supplicant in the period dictated by the quiet timer.

Related commands: **display dot1x, dot1x timer**.

Examples # Enable the quiet timer.

```
<Sysname> system-view
[Sysname] dot1x quiet-period
```

dot1x retry

Syntax **dot1x retry** *max-retry-value*

undo dot1x retry

View System view

Parameters *max-retry-value*: Maximum number of attempts to send an authentication request to a supplicant, in the range 1 to 10.

Description Use the **dot1x retry** command to set the maximum number of attempts to send an authentication request to a supplicant.

Use the **undo dot1x retry** command to restore the default.

By default, the authenticator can send an authentication request to a supplicant for up to twice.

Note that:

- The **dot1x retry** command is used to set the maximum number of times that a switch sends request packets to a user. If you set the number to 1, the switch only sends request packets once, and 2 means that the switch sends request packets for second time if no response comes back, and so on.
- After sending an authentication request to a supplicant, the authenticator may retransmit the request if it does not receive any response at an interval specified by the **dot1x timer tx-period** *tx-period-value* command or the **dot1x timer**

supp-timeout *supp-timeout-value* command. The number of retransmission attempts is one less than the value set by this command.

- This command applies to all ports.

Related commands: **display dot1x**.

Examples # Set the maximum number of attempts to send an authentication request to a supplicant as 9.

```
<Sysname> system-view
[Sysname] dot1x retry 9
```

dot1x supp-proxy-check

Syntax **dot1x supp-proxy-check** { **logoff** | **trap** } [**interface** *interface-list*]

undo dot1x supp-proxy-check { **logoff** | **trap** } [**interface** *interface-list*]

View System view, Ethernet interface view

Parameters **logoff**: Gets offline any user trying to login through a proxy.

trap: Sends a trap packet to the network management system when detecting that a user is trying to login through a proxy.

interface *interface-list*: Specifies an Ethernet port list, which can contain multiple Ethernet ports. The *interface-list* argument is in the format of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 port indexes/port index lists for this argument. The start port number must be smaller than the end number and the two ports must of the same type.

Description Use the **dot1x supp-proxy-check** command to enable detection and control of users logging in through proxies for specified or all ports.

Use the **undo dot1x supp-proxy-check** command to disable the function for specified or all ports.

By default, the function is disabled.

Note that:

- This function requires the cooperation of the 802.1x client program (V1.29 or higher) by 3Com.
- In system view, this command enables detection and control of users' login for all ports with *interface-list* not provided, and enables detection and control of users' login for specified with *interface-list* provided.
- In Ethernet interface view, you cannot specify the *interface-list* argument and can only enable detection and control of users' login for the current port.

- This function must be enabled both globally in system view and for the intended ports in system view or Ethernet interface view. Otherwise, it does not work.

Related commands: **display dot1x**.

Examples # Specify ports Ethernet 3/1/1 to 3/1/8 to get offline users trying to login through proxies.

```
<Sysname> system-view
[Sysname] dot1x supp-proxy-check logoff
[Sysname] dot1x supp-proxy-check logoff interface ethernet 3/1/1 to ethernet
 3/1/8
```

Specify port Ethernet 3/1/9 to send a trap packet when detecting that a user is trying to login through a proxy.

```
<Sysname> system-view
[Sysname] dot1x supp-proxy-check trap
[Sysname] dot1x supp-proxy-check trap interface ethernet 3/1/9
```

Or

```
<Sysname> system-view
[Sysname] dot1x supp-proxy-check trap
[Sysname] interface ethernet 3/1/9
[Sysname-Ethernet3/1/9] dot1x supp-proxy-check trap
```

dot1x timer

Syntax **dot1x timer** { **handshake-period** *handshake-period-value* | **quiet-period** *quiet-period-value* | **server-timeout** *server-timeout-value* | **supp-timeout** *supp-timeout-value* | **tx-period** *tx-period-value* }

undo dot1x timer { **handshake-period** | **quiet-period** | **server-timeout** | **supp-timeout** | **tx-period** }

View System view

Parameters

- *handshake-period-value*: Setting for the handshake timer in seconds. It ranges from 5 to 1024 and defaults to 15.
- *quiet-period-value*: Setting for the quiet timer in seconds. It ranges from 10 to 120 and defaults to 60.
- *server-timeout-value*: Setting for the server timeout timer in seconds. It ranges from 100 to 300 and defaults to 100.
- *supp-timeout-value*: Setting for the supplicant timeout timer in seconds. It ranges from 10 to 120 and defaults to 30.
- **tx-period** *tx-period-value*: Setting for the username request timeout timer in seconds. It ranges from 10 to 120 and defaults to 30.

Description Use the **dot1x timer** command to set 802.1x timers.

Use the **undo dot1x timer** command to restore the defaults.

Several timers are used in the 802.1x authentication process to guarantee that the supplicants, the authenticators, and the RADIUS server interact with each other in a reasonable manner. You can use this command to set these timers:

- Handshake timer (handshake-period): After a supplicant passes authentication, the authenticator sends to the supplicant handshake requests at this interval to check whether the supplicant is online. If the authenticator receives no response after sending the allowed maximum number of handshake requests, it considers that the supplicant is offline.
- Quiet timer (quiet-period): When a supplicant fails the authentication, the authenticator refuses further authentication requests from the supplicant in this period of time.
- Server timeout timer (server-timeout): Once an authenticator sends a RADIUS Access-Request packet to the authentication server, it starts this timer. If this timer expires but it receives no response from the server, it retransmits the request.
- Supplicant timeout timer (supp-timeout): Once an authenticator sends an EAP-Request/MD5 Challenge frame to a supplicant, it starts this timer. If this timer expires but it receives no response from the supplicant, it retransmits the request.
- Username request timeout timer (tx-period): Once an authenticator sends an EAP-Request/Identity frame to a supplicant, it starts this timer. If this timer expires but it receives no response from the supplicant, it retransmits the request. In addition, to be compatible with clients that do not send EAPOL-Start requests unsolicitedly, the Switch 8800 multicasts EAP-Request/Identity frame periodically to detect the clients, with the multicast interval defined by tx-period.

Generally, it is unnecessary to change the timers unless in some special or extreme network environments.

Related commands: **display dot1x**.

Examples # Set the server timeout timer to 150 seconds.

```
<Sysname> system-view
[Sysname] dot1x timer server-timeout 150
```

reset dot1x statistics

Syntax **reset dot1x statistics** [**interface** *interface-list*]

View User view

Parameters **interface** *interface-list*: Specifies an Ethernet port list, which can contain multiple Ethernet ports. The *interface-list* argument is in the format of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the

port number, and & <1-10> means that you can provide up to 10 port indexes/port index lists for this argument. The start port number must be smaller than the end number and the two ports must of the same type.

Description Use the **reset dot1x statistics** command to clear 802.1x statistics.

With the **interface** *interface-list* argument specified, the command clears 802.1x statistics on the specified ports. With the argument unspecified, the command clears global 802.1x statistics and 802.1x statistics on all ports.

This command does not apply to the port with MAC authentication enabled.

Related commands: **display dot1x**.

Examples # Clear 802.1x statistics on port Ethernet 3/1/1.

```
<Sysname> reset dot1x statistics interface ethernet 3/1/1
```

78 SSH2.0 CONFIGURATION COMMANDS

debugging ssh client

Syntax **debugging ssh client** { **all** | **error** | **event** | **message** }

undo debugging ssh client { **all** | **error** | **event** | **message** }

View User view

Parameters **all**: Enables all types of debugging.

error: Enables error debugging.

event: Enables event debugging.

message: Enables message debugging.

Description Use the **debugging ssh client** command to enable debugging for SSH clients and to debug a user interface separately.

Use the **undo debugging ssh client** command to disable debugging for SSH clients.

Be default, debugging is disabled for SSH clients.

Table 323 Field descriptions of the debugging ssh client event command

Field	Description
ProcessSession:	Session processing
InEncrypt:*key-algorithm*	Incoming encryption algorithm information
OutEncrypt: *key-algorithm*	Outgoing encryption algorithm information
InMac:*mac-algorithm*	Incoming MAC algorithm information
OutMac: *mac-algorithm*	Outgoing MAC algorithm information
KeyType:*key-type*	Key type
Process Kex Init:	Initialize algorithm negotiation
Connect Socket:	Socket connection
FSM from *fsm1* to *fsm2*	The state of the state machines is changed from Connected to version negotiation.

Table 323 Field descriptions of the debugging ssh client event command

Read Buffer	Read the buffer of the client
Client_SUB1_FSM from *fsm1* to *fsm2*	On the client, the state of the Sub1 state machine is changed.

Table 324 Field descriptions of the debugging ssh client message command

Field	Description
STELC:	Stelnet client
Client Data Flow Control:	Flow control on the client
Send Disconnect:	Send the Disconnect information
Window Adjust:	The channel window on the client is adjusted.
AuthReq:	Send an authentication request
ServiceReq:	Service request
NewKey:	The client is in newkey state.
GEX Init:	Initialize the GEX algorithm
GEX Request:	GEX request
Send GEX Request:	Send a GEX request
Send GRP Init:	Send a GEX initialization message
SendKexInit:	Send a KEX initialization message
Client_SendVersionString:	The client sends a version character string.
SFTPC:	SFTP client
SFTPC CUSTOM CLOSED	Customer Closed message

Table 325 Field descriptions of the debugging ssh client error command

Field	Description
ProcessSession Error:	Session processing error
Error:	Error message
GEX Init Error:	An error occurs to initialization of the GEX algorithm.
GRP Init Error:	An error occurs to initialization of the GRP algorithm.
Process Kex Init Error:	Key exchange error
VersionString Received Error:	An error occurs to the received version string.
DoClose:	An error occurs when the file is closed.
Process RealPath Error:	An error occurs when a relative path is converted to an absolute path.
Connect Socket Error:	Error of Socket connection

Examples # Enable event debugging on the SSH client. The IP address of the SSH client is 10.1.1.1. The user (username: client; password: aabbcc) logs into the SSH server with the IP address of 10.1.1.2 from the SSH client.

```
<Sysname> debugging ssh client event
<Sysname> system-view
```

```
[Sysname] ssh2 10.1.1.2
Username: client
Trying 10.1.1.2 ...
Press CTRL+K to abort
Connected to 10.1.1.2 ...
*Oct 12 09:21:00:252 2006 Sysname SSH/7/Client_EVENT: FSM from SSH_M
ain_Connect to SSH_Main_VersionMatch
```

// The client performs version negotiation with the server.

```
*Oct 12 09:21:00:254 2006 Sysname SSH/7/Client_EVENT: FSM from SSH_M
ain_Connect to SSH2_Main_KEX_Init
*Oct 12 09:21:00:478 2006 Sysname SSH/7/Client_EVENT: Read Buffer:
  Receive Packet(len=284).
```

// Receive a 284-byte packet.

```
*Oct 12 09:21:00:478 2006 Sysname SSH/7/Client_EVENT: Process Kex Init:
  InEncrypt:aes128-cbc, OutEncrypt:aes128-cbc
  InMac:hmac-sha1-96, OutMac:hmac-sha1-96
  KeyType:KEX_DH_GEX_SHA1
```

// Perform algorithm negotiation.

```
*Oct 12 09:21:00:479 2006 Sysname SSH/7/Client_EVENT: FSM from SSH2_
Main_KEX_Init to SSH2_Main_KEX_GEX_Request
*Oct 12 09:21:00:889 2006 Sysname SSH/7/Client_EVENT: Read Buffer:
  Receive Packet(len=276).
*Oct 12 09:21:00:889 2006 Sysname SSH/7/Client_EVENT: FSM from SSH2_
Main_KEX_GEX_Request to SSH2_Main_KEX_GEX_Init
```

// Negotiate about the GEX algorithm.

```
*Oct 12 09:21:01:441 2006 Sysname SSH/7/Client_EVENT: Read Buffer:
  Receive Packet(len=572).
*Oct 12 09:21:01:441 2006 Sysname SSH/7/Client_EVENT: FSM from SSH2_
Main_KEX_GEX_Init to SSH2_Main_KEX_NewKey
```

// Update the key.

```
*Oct 12 09:21:01:539 2006 Sysname SSH/7/Client_EVENT: Read Buffer:
  Receive Packet(len=12).
*Oct 12 09:21:01:540 2006 Sysname SSH/7/Client_EVENT: FSM from SSH2_
Main_KEX_NewKey to SSH2_Main_Authentication
```

// Authenticate the user.

```
*Oct 12 09:21:01:640 2006 Sysname SSH/7/Client_EVENT: Read Buffer:
  Receive Packet(len=28).
*Oct 12 09:21:01:641 2006 Sysname SSH/7/Client_EVENT: Client_SUB1_FS
M from SSH2_Sub1_Service_Req to SSH2_Sub1_Auth_Req
Enter password:
```

// Prompt the user to enter a password.

```
*Oct 12 09:21:01:739 2006 Sysname SSH/7/Client_EVENT: Read Buffer:
  Receive Packet(len=28).
```

```
*Oct 12 09:21:09:841 2006 Sysname SSH/7/Client_EVENT: Read Buffer:
  Receive Packet(len=12).
*Oct 12 09:21:09:842 2006 Sysname SSH/7/Client_EVENT: Client_SUB1_FS
M from SSH2_Sub1_Auth_Req to SSH2_Sub1_Service_Req
```

// Service request.

```
*Oct 12 09:21:09:843 2006 Sysname SSH/7/Client_EVENT: FSM from SSH2_
Main_Authentication to SSH2_Main_Channel
```

// Channel request.

```
*Oct 12 09:21:09:941 2006 Sysname SSH/7/Client_EVENT: Read Buffer:
  Receive Packet(len=28).
*Oct 12 09:21:09:942 2006 Sysname SSH/7/Client_EVENT: FSM from SSH2_
Main_Channel to SSH2_Main_Pty
```

// Send a channel request of PTY type.

```
*Oct 12 09:21:10:42 2006 Sysname SSH/7/Client_EVENT: Read Buffer:
  Receive Packet(len=12).
*Oct 12 09:21:10:42 2006 Sysname SSH/7/Client_EVENT: FSM from SSH2_M
ain_Pty to SSH2_Main_Shell
```

// Send a channel request of Shell type.

```
*Oct 12 09:21:10:141 2006 Sysname SSH/7/Client_EVENT: Read Buffer:
  Receive Packet(len=12).
*Oct 12 09:21:10:142 2006 Sysname SSH/7/Client_EVENT: FSM from SSH2_
Main_Shell to SSH2_Main_Session
```

Establish a session.

debugging ssh server

Syntax **debugging ssh server** { **all** | **vty** *vty-num* { **all** | **error** | **event** | **message** } }

undo debugging ssh server { **all** | **vty** *vty-num* { **all** | **error** | **event** | **message** } }

View User view

Parameters **all**: Enables debugging for all SSH channels.

vty-num: SSH channel to be debugged. Its value depends on the number of VTY user view, and ranges from 0 to 4.

all: Enables all types of debugging.

error: Enables error debugging.

event: Enables event debugging.

message: Enables message debugging.

Description Use the **debugging ssh server** command to enable debugging for SSH servers and to debug a user interface separately.

Use the **undo debugging ssh server** command to disable debugging for SSH servers.

Be default, debugging is disabled for SSH servers.

Table 326 Field descriptions of the debugging ssh server vty error command

Field	Description
VTY[*vty-num*]	Current user interface
STELS Data Error:	Data resolution error
Read Buffer Error:	An error occurs when the buffer is read.
Read Buffer:	Read the buffer
CRC WRONG:	An error occurs during the CRC.
READ LENGTH WRONG:	An error occurs when the length is read.
Accept Error:	Accept error of the Socket
ProcessAuthentication Error:	Error of authentication
ProcessSub1Password Error:	Error of the password
ProcessSessionKey Error:	Error of the session key
Received unexpected packet:	Receive an unexpected packet
Session Key Store Error:	Error of key storage
Unsupported Cookie_type:	Unsupported cookie type
Unsupported Cipher_type:	Unsupported Cipher type
SSH1 VersionMatch Error:	Error of version match
Verify UserName Error:	Error of the username
Process RsaChallenge Error:	Error of RSA processing
Receive error msgtype:	Receive an erroneous message type
Process Auth Sign Error:	An error occurs to the digital signature authentication on the server.
Process AuthPK Error:	An error occurs to authentication of the public key on the server.
Process Password Error:	Error of the authenticated password
User Auth Init Error:	Fail to initialize the authentication on the server
Service Auth Error:	The request for ID authentication fails.
NewKey Error:	An error occurs to the processing of the newkey state machine on the server.
GEX_Reply Error:	An error occurs to the reply of the GEX public key.
GEX_Group Error:	An error occurs to the processing of the key exchange algorithm.
GRP Reply Error:	An error occurs to the reply of the GRP public key.
Server Key Init Error:	An error occurs to the initialization of algorithm negotiation.
Rename Error:	An error occurs when the file is renamed.

Table 326 Field descriptions of the debugging ssh server vty error command

SFTPS Opendir:	An error occurs when the SFTP server opens a directory.
SFTPS Open Error:	An error occurs when the file is opened.
SFTPS Process Error:	An error occurs when the SFTP server processes a message.

Table 327 Field descriptions of the debugging ssh server vty event command

Field	Description
VTY[*vty-num*]	Current user interface
Accept:	Accept event of the Socket
Send Version To CLient:	Send version information to the client
Succeed to send version string: *version-string*	Send the version string successfully
Socket:*soketid*	ID of the current Socket
LineIndex:*lineindex*	Index to the current line resource
IP:*ipaddress*	IP address of the login user
FSM Change: From *fsm1* to *fsm2*	The state of the state machine is changed.
Read:	Read event of the Socket
Read Buffer:	Read the buffer on the server
Receive Packet(len=*length*)	Receive a packet with the length specified by *length*
Server Key Init:	Initialize the server key on the server
InEncrypt:*key-algorithm*	Incoming encryption algorithm information
OutEncrypt: *key-algorithm*	Outgoing encryption algorithm information
InMac:*mac-algorithm*	Incoming MAC algorithm information
OutMac: *mac-algorithm*	Outgoing MAC algorithm information
KeyType:*key-type*	Key type
SUB1_FSM Change: From *sub1_fsm1* to *sub1_fsm2*	The state of the Sub1 state machine is changed.
SUB2_Auth_FSM from *sub2_fsm1* to *sub2_fsm2*	The state of the Sub2 state machine is changed.
UserAuthInit:	Initialize user authentication
Get user name:*user-name*!	Username of the client
Sub2Password:	Password authentication
User: *user-name*	Username
PasswordLen:*length*	Password length
LOGIN Succeed:	Successful login
LOGIN Failed:	Login failure
Channel Request:	Channel request on the client
Received channel request:*request-type*	Type of the received channel request message
STELS Start Shell:	Start the Shell
SFTPS_TaskQuit:	The SFTP task quits.
SFTPS Requeset SubSystem:	SFTP subsystem requests

Table 327 Field descriptions of the debugging ssh server vty event command

Receive message:	Received message from the SFTP client
Successful to create task: Id=*taskid*	Create an SFTP task successfully
SFTP Server Init:	Initialize SFTP version negotiation
SFTPS Open:	Open the file
SFTPS Close:	Close the file
SFTPS Read:	Read the file
SFTPS Write:	Write data into the file
SFTPS Opendir:	Open the directory
Readdir:	Read the directory
SFTPS Remove:	Remove the file
SFTPS Mkdir:	Create a directory
SFTPS Rmdir:	Delete a directory
SFTPS RealPath:	Convert a relative path is into an absolute path
SFTPS Rename:	Rename the file
SFTPS SetStat:	Set file attributes
Window Adjust:	Adjust the sliding window
Verify UserName:	Verify the username
UserNameDazzle:	Dazzle the username
Session Key Store:	Store the session key

Table 328 Field descriptions of the debugging ssh server vty message command

Field	Description
VTY[*vty-num*]	Current user interface
Send Message:	Send a message to the client
SSH_VERSION_SEND from SocketID *socketid*	The server sends version information.
VersionReseived:	Receive the version of the client
Received VersionString[len=*length*]: *version-string*	Received version string and its length
SendKexInit:	Send the key negotiation information on the server
Read Buffer:	Read the buffer on the server
Received Message[Type=*type-number*]:*message-type*	Type of the received message
GEX_Group:	GEX key exchange algorithm
GEX Reply:	The server replies to the GEX key exchange algorithm.
Service Auth:	Authentication service
Authentication Failure:	Authentication failure
Authentication Success:	Authentication is successful.
Process Channel:	Process the channel message
STELS Request PTY:	PTY request from the Stelnet client
SSH Channel:	SSH channel message
STELS Start Shell:	Start the Shell
Process Session:	Process the session message

Table 328 Field descriptions of the debugging ssh server vty message command

STELS Data:	Process the data message
SFTPS Trans:	Send a packet to the client
Data Flow Control:	Flow control on the SFTP server
SFTPS Send Data:	Send data
SFTPS Send Handle:	Send a handle message
SFTPS Send Status:	Send a status message
SFTPS Send Names:	Send a filename
SFTPS Send Attrs:	Send file attributes
Send Disconnect:	Send a Disconnect message

Examples # Enable event debugging for the SSH server on the user interface VTY 1. The IP address of the SSH client is 10.1.1.1. The user (username: client; password: aabbcc) logs into the SSH server with the IP address of 10.1.1.2 from the SSH client.

```
<Sysname> debugging ssh server vty 1 event
*Oct 12 09:32:58:462 2006 Sysname SSH/7/Server_EVENT: VTY[1]:Accept:
Socket:6 LineIndex:83,IP:10.1.1.1
```

// The user logs in from VTY 1, and creates a socket on the server.

```
*Oct 12 09:32:58:463 2006 Sysname SSH/7/Server_EVENT: VTY[1]:Accept:
SSH user comes from 10.1.1.1, and current FSM is SSH_Main_Connect
```

// The user logs in from a client with the IP address of 10.1.1.1. A TCP connection has been established.

```
*Oct 12 09:32:58:463 2006 Sysname SSH/7/Server_EVENT: VTY[1]:Send Ve
rsion To CLient:
Successful to send version string: SSH-1.99-CMW-3.4
```

// Send version information to the client.

```
*Oct 12 09:32:58:464 2006 Sysname SSH/7/Server_EVENT: VTY[1]:FSM Change:
  From SSH_Main_Connect to SSH_Main_VersionMatch.
```

// The client performs version negotiation with the server.

```
*Oct 12 09:32:58:467 2006 Sysname SSH/7/Server_EVENT: VTY[1]:Read:
   Process user [] from 10.1.1.1.
```

// Process user data from the IP address of 10.1.1.1.

```
*Oct 12 09:32:58:467 2006 Sysname SSH/7/Server_EVENT: VTY[1]:FSM Change:
  From SSH_Main_VersionMatch to SSH_Main_SSHProcess.

*Oct 12 09:32:58:564 2006 Sysname SSH/7/Server_EVENT: VTY[1]:Read:
  Process user [] from 10.1.1.1.
*Oct 12 09:32:58:565 2006 Sysname SSH/7/Server_EVENT: VTY[1]:Read Buffer:
  Receive Packet(len=284).
```

// Receive a 284-byte packet.

```
*Oct 12 09:32:58:566 2006 Sysname SSH/7/Server_EVENT: VTY[1]:Server Key Init:
  InEncrypt:aes128-cbc, OutEncrypt:aes128-cbc
  InMac:hmac-sha1-96, OutMac:hmac-sha1-96
  KeyType:KEX_DH_GEX_SHA1
```

// Initialize the key on the server.

```
*Oct 12 09:32:58:566 2006 Sysname SSH/7/Server_EVENT: VTY[1]:SUB1_FSM Change:
  From SSH_Sub1_KEX_Init to SSH_Sub1_KEX_GEX_Group.

*Oct 12 09:32:58:943 2006 Sysname SSH/7/Server_EVENT: VTY[1]:Read:
  Process user [] from 10.1.1.1.
*Oct 12 09:32:58:944 2006 Sysname SSH/7/Server_EVENT: VTY[1]:Read Buffer:
  Receive Packet(len=20).
*Oct 12 09:32:58:944 2006 Sysname SSH/7/Server_EVENT: VTY[1]:SUB1_FSM Change:
  From SSH_Sub1_KEX_GEX_Group to SSH_Sub1_KEX_GEX_Reply.
```

// Negotiate about the GEX algorithm.

```
*Oct 12 09:32:58:955 2006 Sysname SSH/7/Server_EVENT: VTY[1]:Read:
  Process user [] from 10.1.1.1.
*Oct 12 09:32:59:263 2006 Sysname SSH/7/Server_EVENT: VTY[1]:Read Buffer:
  Receive Packet(len=268).
*Oct 12 09:32:59:263 2006 Sysname SSH/7/Server_EVENT: VTY[1]:SUB1_FSM Change:
  From SSH_Sub1_KEX_GEX_Reply to SSH_Sub1_KEX_NewKey.
```

// Update the key.

```
*Oct 12 09:32:59:507 2006 Sysname SSH/7/Server_EVENT: VTY[1]:Read:
  Process user [] from 10.1.1.1.
*Oct 12 09:32:59:508 2006 Sysname SSH/7/Server_EVENT: VTY[1]:Read Buffer:
  Receive Packet(len=12).
*Oct 12 09:32:59:509 2006 Sysname SSH/7/Server_EVENT: VTY[1]:SUB1_FSM Change:
  From SSH_Sub1_KEX_NewKey to SSH_Sub1_Authentication.
```

// Authenticate the user.

```
*Oct 12 09:32:59:605 2006 Sysname SSH/7/Server_EVENT: VTY[1]:Read:
  Process user [] from 10.1.1.1.
*Oct 12 09:32:59:606 2006 Sysname SSH/7/Server_EVENT: VTY[1]:Read Buffer:
  Receive Packet(len=28).
*Oct 12 09:32:59:607 2006 Sysname SSH/7/Server_EVENT: VTY[1]:SUB2_Auth_FSM
  from SSH_Sub2_Service_Acc to SSH_Sub2_Auth_Init
```

// Initialize user authentication.

```
*Oct 12 09:32:59:707 2006 Sysname SSH/7/Server_EVENT: VTY[1]:Read:
  Process user [] from 10.1.1.1.
*Oct 12 09:32:59:707 2006 Sysname SSH/7/Server_EVENT: VTY[1]:Read Buffer:
  Receive Packet(len=44).
*Oct 12 09:32:59:708 2006 Sysname SSH/7/Server_EVENT: VTY[1]:UserAuthInit:
  Get user name: client!
```

// The login user is named "client".

```
*Oct 12 09:32:59:709 2006 Sysname SSH/7/Server_EVENT: VTY[1]:UserAuthInit:
  Current AuthType is SSH_AUTH_PASSWORD
```

// The authentication mode is "password".

```
*Oct 12 09:33:01:585 2006 Sysname SSH/7/Server_EVENT: VTY[1]:Read:
  Process user [client] from 10.1.1.1.
*Oct 12 09:33:01:585 2006 Sysname SSH/7/Server_EVENT: VTY[1]:Read Buffer:
  Receive Packet(len=60).
```

```
*Oct 12 09:33:01:586 2006 Sysname SSH/7/Server_EVENT: VTY[1]:UserAuthInit:
  Get user name: client!
*Oct 12 09:33:01:587 2006 Sysname SSH/7/Server_EVENT: VTY[1]:SUB2_Auth_FSM
  from SSH_Sub2_Auth_Init to SSH_Sub2_Auth_Password
*Oct 12 09:33:01:587 2006 Sysname SSH/7/Server_EVENT: VTY[1]:Sub2Password:
  User:client  PasswordLen: 6
```

// The password of the "client" user is 6 in length.

```
*Oct 12 09:33:01:613 2006 Sysname SSH/7/Server_EVENT: VTY[1]:Sub2Password: S
SH user client succeeded to login from 10.1.1.1 on VTY1.
*Oct 12 09:33:01:614 2006 Sysname SSH/7/Server_EVENT: VTY[1]:LOGIN Succeed:
   SSH user client succeeded to login from 10.1.1.1(000f-e200-0001) on VTY1.
```

// Succeed in authenticating the "client" user.

```
*Oct 12 09:33:01:615 2006 Sysname SSH/7/Server_EVENT: VTY[1]:SUB2_Auth_FSM
  from SSH_Sub2_Auth_Password to SSH_Sub2_Auth_Init
```

// The Sub2 state machine returns to the authentication initialization state.

```
*Oct 12 09:33:01:615 2006 Sysname SSH/7/Server_EVENT: VTY[1]:SUB1_FSM Change
:
  From SSH_Sub1_Authentication to SSH_Sub1_Channel.
```

// Channel request.

```
*Oct 12 09:33:01:696 2006 Sysname SSH/7/Server_EVENT: VTY[1]:Read:
  Process user [client] from 10.1.1.1.
*Oct 12 09:33:01:697 2006 Sysname SSH/7/Server_EVENT: VTY[1]:Read Buffer:
  Receive Packet(len=44).
*Oct 12 09:33:01:697 2006 Sysname SSH/7/Server_EVENT: VTY[1]:SUB1_FSM Change:
  From SSH_Sub1_Channel to SSH_Sub1_Session.
```

// Establish a session.

```
*Oct 12 09:33:01:796 2006 Sysname SSH/7/Server_EVENT: VTY[1]:Read:
  Process user [client] from 10.1.1.1.
*Oct 12 09:33:01:797 2006 Sysname SSH/7/Server_EVENT: VTY[1]:Read Buffer:
  Receive Packet(len=60).
*Oct 12 09:33:01:797 2006 Sysname SSH/7/Server_EVENT: VTY[1]:Channel Request:
  Received channel request: pty-req
```

// Receive a channel request of pty-req type.

```
*Oct 12 09:33:01:798 2006 Sysname SSH/7/Server_EVENT: VTY[1]:STELS Requeset PTY:
  Successful to send SSH2_MSG_CHANNEL_SUCCESS(99) from 10.1.1.2 to 10.1.1.1
```

// Send an SSH2_MSG_CHANNEL_SUCCESS message successfully.

```
*Oct 12 09:33:01:897 2006 Sysname SSH/7/Server_EVENT: VTY[1]:Read:
  Process user [client] from 10.1.1.1.
*Oct 12 09:33:01:898 2006 Sysname SSH/7/Server_EVENT: VTY[1]:Read Buffer:
  Receive Packet(len=28).
*Oct 12 09:33:01:898 2006 Sysname SSH/7/Server_EVENT: VTY[1]:Channel Request:
  Received channel request: shell
```

// Receive a channel request of shell type.

```
*Oct 12 09:33:01:899 2006 Sysname SSH/7/Server_EVENT: VTY[1]:STELS Start Shell:
  Send SSH2_MSG_CHANNEL_SUCCESS(99) from 10.1.1.2 to 10.1.1.1

%Oct 12 09:33:02:01 2006 Sysname SHELL/4/LOGIN: client login from 10.1.1.1
```

// The "client" user logs into the server from a client with the IP address of 10.1.1.1.

display rsa local-key-pair public

Syntax **display rsa local-key-pair public**

View Any view

Parameters None

Description {Use the **display rsa local-key-pair public** command to display the public key information of the host key pair on the server and of server key pair. If no key is generated, the system prompts that no key is found.

Related commands: **rsa local-key-pair create**.

Examples # Display the public key information of the host key pair on the server and of the server key pair.

```
<Sysname> display rsa local-key-pair public
=====================================================
Time of Key pair created: 13:41:21  2004/11/12
Key name: Sysname_Host
Key type: RSA encryption Key
=====================================================
Key code:
3047
  0240
    C30B0C1E 1AC2A028 984B7801 9583105D 78E69F6C
    62561976 95E3B92B 7D9EC59C 150AE9CC 92E7CEF7
    F025D3E0 C15408F5 4C9F4945 308A2DCF 1BA59D60
    53DB5825
  0203
    010001

=====================================================
Time of Key pair created: 13:41:25  2004/11/12
Key name: Sysname_Server
Key type: RSA encryption Key
=====================================================
Key code:
3067
  0260
    E0DC0229 0525E04D AE3B8998 C56A18A1 997A609B
    043B9302 F843715B FC727A3D 4A503B32 333DFD46
    D95F4BD7 5AF63BBF 99100F9E EEAE4B3E DC6FBE42
    1757F88D 1F7A098F 2C3FFFDF 8E2DA17D 991111ED
    C318E857 6D40D224 4114AD15 A42068B9
  0203
    010001
```

Table 329 Field descriptions of the display rsa local-key-pair public command

Field	Description
Time of Key pair created	Time when the key pair is created
Key name	Key name
Key type	Key type, for example, RSA encryption Key
Key code	Key data

display rsa peer-public-key

Syntax **display rsa peer-public-key** [**brief** | **name** *keyname*]

View Any view

Parameters **brief**: Displays brief information about all remote public keys.

name *keyname*: Specifies a key by its name, a string of 1 to 64 characters.

Description Use the **display rsa peer-public-key** command to displays remote RSA public keys.

If no parameters are specified, the system displays detailed information about all public keys.

Related commands: **rsa local-key-pair create**.

Examples # Display detailed information about all public keys.

```
<Sysname> display rsa peer-public-key
=====================================
    Key name: aa
    Key address:
=====================================
Key Code:
308186
  028180
    6B494EC4 EBD23DEE 1375C2B5 AB892F69 F2529D09 5B559E26 26011A1F C58AA5E3
    60258B01 26494D0E 7221BB98 1C844CCD 8F0F8AEA 4AA1CD5B 9C3C5EF5 3093319F
    6F3AEA80 351E5E8D 29F1511C D4AC08B4 3FDF5B7B E30A4E47 6FF75B9A 63BE5E94
    E9C344B7 F0EC9D53 AE54E0A3 0567184A 2E80BEC3 89A2DAFA 83C18591 5B29EAA1
  0201
    25
```

Table 330 Field descriptions of the display rsa peer-public-key command

Field	Description
Key name	Key name
Key address	Key address
Key code	Key data

Display brief information about all remote public keys.

```
<Sysname>display rsa peer-public-key brief
Address         Bits   Name
```

```
-------------------------
                1023    aaa
```

Table 331 Field descriptions of the display rsa peer-public-key brief command

Field	Description
Field	**Description**
Address	Remote address
Bits	Number of bits of the remote public key
Name	Name of the remote public key

display sftp client source

Syntax **display sftp client source**

View Any view

Parameters None

Description Use the **display sftp client source** command to display the source IP address or source interface currently set for the SFTP client.

If neither source IP address nor source interface is specified for the SFTP client, "You didn't specify the source" will be displayed.

Related commands: **sftp client source**.

Examples # Display the source IP address of the SFTP client.

```
<Sysname> display sftp client source
The source IP address you specified is 192.168.0.1
```

display ssh client source

Syntax **display ssh client source**

View Any view

Parameters None

Description Use the **display ssh client source** command to display the source IP address or source interface currently set for the SSH client.

If neither source IP address nor source interface is specified for the SSH client, "You didn't specify the source" will be displayed.

Related commands: **ssh client source**.

Examples # Display the source IP address of the SSH client.

```
<Sysname> display ssh client source
The source IP address you specified is 192.168.0.1
```

display ssh server

Syntax **display ssh server** { **status** | **session** }

View Any view

Parameters **status**: Displays the status information of the SSH server.

session: Displays the session information of the SSH server.

Description Use the **display ssh server** command to display the status information or session information of an SSH server.

Related commands: **ssh server authentication-retries**, **ssh server rekey-interval**, **ssh server authentication-timeout**, and **ssh server enable**.

Examples # Display the status information of the SSH server.

```
<Sysname> display ssh server status
 SSH Server: Disable
 SSH version : 1.99
 SSH authentication-timeout : 60 second(s)
 SSH server key generating interval : 0 hour(s)
 SSH Authentication retries : 3 time(s)
 SFTP Server: Disable
 SFTP Server Idle-Timeout: 10 minute(s)
```

Table 332 Description on fields of the display ssh server status command

Field	Description
SSH Server	Whether the SSH server function is enabled
SSH version	SSH protocol version
SSH authentication-timeout	Authentication timeout period
SSH server key generating interval	SSH server key pair update interval
SSH Authentication retries	Maximum number of SSH authentication attempts
SFTP Server	Whether the SFTP server function is enabled
SFTP Server Idle-Timeout	SFTP connection idle timeout period

Display the session information of the SSH server.

```
<Sysname> display ssh server session
 Conn    Ver    Encry    State         Retry    SerType  Username
 VTY 0   2.0    3DES      Established   0        SFTP     client001
```

Table 333 Description on fields of the display ssh server session command

Field	Description
Conn	Connected VTY channel
Ver	SSH server protocol version
Encry	Encryption algorithm
State	Status of the session, including: Init, Ver-exchange, Keys-exchange, Auth-request, Serv-request, Established, Disconnected
Retry	Number of authentication attempts
SerType	Service type (SFTP, Stelnet)
Username	Name of a user during login

display ssh server-info

Syntax **display ssh server-info**

View Any view

Parameters None

Description Use the **display ssh server-info** command to display the mappings between host public keys and SSH servers saved on a client.

Examples # Display the mappings between host public keys and SSH servers saved on the client.

```
<Sysname> display ssh server-info
Server Name(IP)                 Server public key name
_____________________________________________________
192.168.0.1                      abc_key01
192.168.0.2                      abc_key02
```

Table 334 Descriptions on fields of the display ssh server-info command

Field	Description
Server Name(IP)	Name or IP address of the server
Server public key name	Name of the host public key of the server

display ssh user-information

Syntax **display ssh user-information** [*username*]

View Any view

Parameters *username*: SSH username, a string of 1 to 80 characters.

Description Use the **display ssh user-information** command to display information about a specified or all SSH users.

With the *username* argument not specified, the command displays information about all users.

Related commands: **ssh user assign rsa-key**, **ssh user authentication-type**, **ssh user service-type**.

Examples # Display information about all SSH users.

```
<Sysname> display ssh user-information
 Total ssh users : 2
 Username            Authentication-type  User-public-key-name  Service-type
 yemx                 password               putty                    stelnet|sftp
 test              rsa                  null                   sftp
```

Table 335 Description on fields of the display ssh user-information command

Field	Description
Username	Name of the user
Authentication-type	Authentication type
User-public-key-name	Public key of the user
Service-type	Service type

peer-public-key end

Syntax **peer-public-key end**

View Public key view

Parameters None

Description Use the **peer-public-key end** command to return from public key view to system view.

Related commands: **rsa peer-public-key**.

Examples # Exit public key view.

```
<Sysname> system-view
[Sysname] rsa peer-public-key Sysname003
[Sysname-rsa-public-key] peer-public-key end
[Sysname]
```

protocol inbound (VTY user interface view)

Syntax **protocol inbound** { **all** | **ssh** | **telnet** }

View VTY user interface view

Parameters **all**: Supports all of the three protocols: Telnet and SSH.

ssh: Supports SSH only.

telnet: Supports Telnet only.

Description Use the **protocol inbound** command to enable the current user interface to support Telnet, and SSH.

By default, a user interface supports all of the three protocols: Telnet, PAD, and SSH.

The configuration of this command takes effect at next login.

If you configure the current user interface to support SSH, be sure to configure the **authentication-mode scheme** command.

Related commands: **user-interface vty** in *User Interface Commands* of *System Volume*.

Examples # Enable VTYs 0 to 4 to support SSH only.

```
<Sysname> system-view
[Sysname] user-interface vty 0 4
[Sysname-ui-vty0-4] authentication-mode scheme
[Sysname-ui-vty0-4] protocol inbound ssh
```

public-key-code begin

Syntax **public-key-code begin**

View Public key view

Parameters None

Description Use the **public-key-code begin** command to enter RSA key code view.

After entering public key code view, you can input the key data. It must be a hexadecimal string that is generated randomly by the SSH-supported client software and coded compliant to PKCSIt is generated at random by the client software that supports SSH.

Related commands: **rsa peer-public-key**, **public-key-code end**.

Examples # Enter public key code view to input the key.

```
<Sysname> system-view
[Sysname] rsa peer-public-key Sysname003
[Sysname-rsa-public-key] public-key-code begin
[Sysname-rsa-key-code] 30818602 818078C4 32AD7864 BB0137AA 516284BB 3F55F0E3
[Sysname-rsa-key-code] F6DD9FC2 4A570215 68D2B3F7 5188A1C3 2B2D40BE D47A08FA
[Sysname-rsa-key-code] CF41AF4E 8CCC2ED0 C5F9D1C5 22FC0625 BA54BCB3 D1CBB500
[Sysname-rsa-key-code] A177E917 642BE3B5 C683B0EB 1EC041F0 08EF60B7 8B6ED628
[Sysname-rsa-key-code] 9830ED46 0BA21FDB F55E7C81 5D1A2045 54BFC853 5358E5CF
[Sysname-rsa-key-code] 7D7DDF25 03C44C00 E2F49539 5C4B0201 25
```

public-key-code end

Syntax **public-key-code end**

View RSA key code view

Parameters None

Description Use the **public-key-code end** command to return from public key code view to public key view.

The system verifies the key before saving it. If the key contains illegal characters, the system displays an error message, indicating that an illegal character is entered, and discards the key.

Related commands: **rsa peer-public-key**, **public-key-code begin**.

Examples # Exit RSA key code view.

```
<Sysname> system-view
[Sysname] rsa peer-public-key Sysname003
[Sysname-rsa-public-key] public-key-code begin
[Sysname-rsa-key-code] public-key-code end
[Sysname-rsa-public-key]
```

rsa local-key-pair create

Syntax **rsa local-key-pair create**

View System view

Parameters None

Description Use the **rsa local-key-pair create** command to generate RSA host key pairs and server key pairs.

Note that:

- After you enter this command, the system prompts you to enter the number of bits of the key pair. For a host key pair and server key pair, the minimum length is 512 bits, and the maximum length is 2,048 bits. If a key pair already exists, you need to decide whether to modify it.
- You only need to execute this command once. You do not need to execute it again after the device is restarted.

Related commands: **rsa local-key-pair destroy** and **display rsa local-key-pair public**.

Examples # Generate a host key pair and server key pair.

```
<Sysname> system-view
[Sysname] rsa local-key-pair create
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
       It will take a few minutes.
Input the bits in the modulus[default = 1024]:
Generating keys...
..........++++++++++++
..............++++++++++++
.......++++++++
....++++++++
Done!
```

rsa local-key-pair destroy

Syntax **rsa local-key-pair destroy**

View System view

Parameters None

Description Use the **rsa local-key-pair destroy** command to destroy RSA host key pairs and server key pairs.

After entering this command, you need to decide whether to destroy RSA host key pairs and server key pairs.

Related commands: **rsa local-key-pair create**.

Examples # Destroy an RSA host key pair and server key pair.

```
<Sysname> system-view
[Sysname] rsa local-key-pair destroy
The local-key-pair will be destroyed.
Confirm to destroy these keys? [Y/N]:y
..........Done!
```

rsa local-key-pair export

Syntax **rsa local-key-pair export** { **ssh1** | **ssh2** | **openssh** } [*filename*]

View Any view

Parameters **ssh1**: An RSA host public key is in the format of "SSH1".

ssh2: An RSA host public key is in the format of "SSH2".

openssh: An RSA host public key is in the format of "OpenSSH".

filename: Name of the exported RSA host public key file. If a host public key filename is denoted in the format of "filename", *filename* is a string of 1 to 91 characters. If a host public key filename is denoted in the format of "directory + filename", *filename* is a string of 1 to 136 characters (the filename consists of a maximum of 91 characters).

Description Use the **rsa local-key-pair export** command to display RSA host public keys in the screen in a specified format or to export RSA host public keys to a specified file.

If no filename is specified, the system displays RSA host public keys in the screen. Otherwise, the system exports and saves RSA host public keys to the specified file.

SSH1, SSH2 and OpenSSH indicate three different types of public key file formats.

Related commands: **rsa local-key-pair create** and **rsa local-key-pair destroy**.

Examples # Export RSA host public keys in the format of "OpenSSH".

```
<Sysname> rsa local-key-pair export OpenSSH myOpenSSH
The file of public key is successfully generated.
```

Display RSA host public keys in the format of "SSH2".

```
<Sysname> rsa local-key-pair export SSH2
Host public key for SSH2 format code:
---- BEGIN SSH2 PUBLIC KEY ----
AAAAB3NzaC1yc2EAAAADAQABAAAAgQCusCaLG/BIkVdFQT7pND+ETtHZGnOclMuK
9zxdbzcjcAdWIZY4Hwu/AOGbn7Sj2NJZNeqUzFrYNeOjD1cGqO5NkgLvy+2lAUSW
+L9usdsIk67fiF63Msu3i9HcqyA0mUuToNjQUZoltU1kbqFK7zE1CCZAt7+55rWk
SqcCGqFBsw==
---- END SSH2 PUBLIC KEY ----
[Sysname]
```

Display RSA host public keys in the format of "OpenSSH".

```
<Sysname> rsa local-key-pair export OpenSSH
Public key code for pasting into OpenSSH authorized_keys file :
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAgQCusCaLG/BIkVdFQT7pND+ETtHZGnOc
lMuK9zxdbzcj
cAdWIZY4Hwu/AOGbn7Sj2NJZNeqUzFrYNeOjD1cGqO5NkgLvy+2lAUSW+L9usdsIk67f
iF63Msu3i9HcqyA0mUuToNjQUZoltU1kbqFK7zE1CCZAt7+55rWkSqcCGqFBsw== rsa
-key
```

rsa peer-public-key

Syntax **rsa peer-public-key** *keyname*

undo rsa peer-public-key *keyname*

View System view

Parameters *keyname*: Name of a public key, a string of 1 to 64 characters.

Description Use the **rsa peer-public-key** command to enter public key view.

Use the **undo rsa peer public-key** command to delete the configured remote public keys.

In public key view, you can configure remote public keys using the **public-key-code begin** and **public-key-code end** commands together. You need to first obtain the remotely generated hexadecimal public keys.

Related commands: **public-key-code begin** and **public-key-code end**.

Examples # Enter public key view (the public key is named "abc123").

```
<Sysname> system-view
[Sysname] rsa peer-public-key abc123
[Sysname-pkeyrsa-public-key]
```

rsa peer-public-key import sshkey

Syntax **rsa peer-public-key** *keyname* **import sshkey** *filename*

undo rsa peer-public-key *keyname*

View System view

Parameters *keyname*: Name of a public key, a string of 1 to 64 characters.

filename: Name of a public key file, a string of 1 to 136 characters.

Description Use the **rsa peer-public-key import sshkey** command to import remote public keys from a public key file.

Use the **undo rsa peer public-key** command to delete the configured remote public keys.

After you execute this command, the system automatically converts the generated public key files (support SSH1, SSH2, and OpenSSH formats) into PKCS codes, and configures remote public keys. The remote public key file of the RSA key must be FTPed/TFTPed to the local device in advance.

Examples # Import the remote public key named "abc456" from the public file "pub2".

```
<Sysname> system-view
[Sysname] rsa peer-public-key abc456 import sshkey pub2
```

sftp

Syntax **sftp** { *host-ip* | *host-name* } [*port-number*] [**prefer_ctos_cipher** { **3des** | **aes128** | **des** } | **prefer_ctos_hmac** { **md5** | **md5_96** | **sha1** | **sha1_96** } | **prefer_kex** {

dh_exchange_group | **dh_group1** } | **prefer_stoc_cipher** { **3des** | **aes128** | **des** } | **prefer_stoc_hmac** { **md5** | **md5_96** | **sha1** | **sha1_96** }] *

View System view

Parameters *host-ip*: IPv4 address of the server.

host-name: Server name, a string of 1 to 20 characters.

port-number: Port number of the server, in the range 0 to 65535. The default is 22.

prefer_ctos_cipher: Preferred encryption algorithm from client to server, defaulted to **aes128**.

- **3des**: Encryption algorithm 3des_cbc.
- **aes128**: Encryption algorithm aes128_cbc.
- **des**: Encryption algorithm des_cbc.

prefer_ctos_hmac: Preferred HMAC algorithm from client to server, defaulted to **sha1**.

- **md5**: HMAC algorithm hmac-md5.
- **md5_96**: HMAC algorithm hmac-md5-96.
- **sha1**: HMAC algorithm hmac-sha1.
- **sha1_96**: HMAC algorithm hmac-sha1-96.

prefer_kex: Preferred key exchange algorithm, defaulted to **dh_group1**.

- **dh_exchange_group**: Key exchange algorithm diffie-hellman-group-exchange-sha1.
- **dh_group1**: Key exchange algorithm diffie-hellman-group1-sha1.

prefer_stoc_cipher: Preferred algorithm from server to client, defaulted to **aes128**.

prefer_stoc_hmac: Preferred HMAC algorithm from server to client, defaulted to **sha1**.

Description Use the **sftp** command to establish a connection to a remote IPv4 SFTP server and enter SFTP client view.

Examples

```
<Sysname> system-view
[Sysname] sftp 10.1.1.2
Input Username:
```

sftp client ipv6 source

Syntax **sftp client ipv6 source** { **ipv6** *ipv6-address* | **interface** *interface-type interface-number* }

undo sftp client ipv6 source

View System view

Parameters *ipv6-address*: Source IPv6 address.

interface-type interface-number: Specifies a source interface by its type and number.

Description Use the **sftp client ipv6 source** command to specify the source IPv6 address or source interface for an SFTP client.

Use the **undo sftp client ipv6 source** command to remove the configuration.

By default, the client uses the interface address specified by the route of the device to access the SFTP server.

If the specified interface does not exist, the system prompts failure.

Related commands: **display sftp client source**.

Examples # Specify the source IPv6 address of the SFTP client as 2:2::2:2.

```
<Sysname> system-view
[Sysname] sftp client ipv6 source ipv6 2:2::2:2
```

sftp client source

Syntax **sftp client source** { **ip** *ip-address* | **interface** *interface-type interface-number* }

undo sftp client source

View System view

Parameters *ip-address*: Source IPv4 address.

interface-type interface-number: Specifies a source interface by its type and number.

Description Use the **sftp client source** command to specify the source IPv4 address or interface of an SFTP client.

Use the **undo sftp source-interface** command to remove the configuration.

By default, a client uses the IP address or interface specified by the route to access the SFTP server.

Related commands: **display sftp client source**.

Examples # Specify the source IP address of the SFTP client as 192.168.0.1.

```
<Sysname> system-view
[Sysname] sftp client source ip 192.168.0.1
```

sftp ipv6

Syntax **sftp ipv6** { *ipv6-address* | *host-name* } [*port-number*] [**prefer_ctos_cipher** { **3des** | **aes128** | **des** } | **prefer_ctos_hmac** { **md5** | **md5_96** | **sha1** | **sha1_96** } | **prefer_kex** { **dh_exchange_group** | **dh_group1** } | **prefer_stoc_cipher** { **3des** | **aes128** | **des** } | **prefer_stoc_hmac** { **md5** | **md5_96** | **sha1** | **sha1_96** }] *

View System view

Parameters *ipv6-address*: IPv6 address of the server.

host-name: Server name, a string of 1 to 46 characters.

port-number: Port number of the server, in the range 0 to 65535. The default is 22.

prefer_ctos_cipher: Preferred encryption algorithm from client to server, defaulted to **aes128**.

- **3des**: Encryption algorithm 3des_cbc.
- **aes128**: Encryption algorithm aes128_cbc.
- **des**: Encryption algorithm des_cbc.

prefer_ctos_hmac: Preferred HMAC algorithm from client to server, defaulted to **sha1**.

- **md5**: HMAC algorithm hmac-md5.
- **md5_96**: HMAC algorithm hmac-md5-96.
- **sha1**: HMAC algorithm hmac-sha1.
- **sha1_96**: HMAC algorithm hmac-sha1-96.

prefer_kex: Preferred key exchange algorithm, defaulted to **dh_group1**.

- **dh_exchange_group**: Key exchange algorithm diffie-hellman-group-exchange-sha1.
- **dh_group1**: Key exchange algorithm diffie-hellman-group1-sha1.

prefer_stoc_cipher: Preferred encryption algorithm from server to client, defaulted to **aes128**.

prefer_stoc_hmac: Preferred HMAC algorithm from server to client, defaulted to **sha1**.

Description Use the **sftp ipv6** command to establish a connection to a remote IPv6 SFTP server and enter SFTP client view.

Examples # Connect to server 2:5::8:9.

```
<Sysname> system-view
[Sysname] sftp ipv6 2:5::8:9
Input Username:
```

sftp server enable

Syntax **sftp server enable**

undo sftp server enable

View System view

Parameters None

Description Use the **sftp server enable** command to enable SFTP server.

Use the **undo sftp server enable** command to disable SFTP server.

By default, SFTP server is disabled.

Related commands: **display ssh server**.

Examples # Enable SFTP server.

```
<Sysname> system-view
[Sysname] sftp server enable
```

sftp server idle-timeout

Syntax **sftp server idle-timeout** *time-out-value*

undo sftp server idle-timeout

View System view

Parameters *time-out-value*: Timeout period in minutes. It ranges from 1 to 35,791.

Description Use the **sftp server idle-timeout** command to set the idle timeout period for SFTP user connections.

Use the **undo sftp server idle-timeout** command to restore the default.

By default, the idle timeout period is 10 minutes.

Related commands: **display ssh server**.

Examples # Set the idle timeout period for SFTP user connections to 500 minutes.

```
<Sysname> system-view
[Sysname] sftp server idle-timeout 500
```

ssh client authentication server

Syntax **ssh client authentication server** { *server-ip* | *server-name* } **assign rsa-key** *keyname*

undo ssh client authentication server { *server-ip* | *server-name* } **assign rsa-key**

View System view

Parameters *server-ip*: IP address of the server, a string of 1 to 80 characters.

server-name: Server name, a string of 1 to 64 characters.

keyname: Name of the host public key on the server.

Description Use the **ssh client authentication server** command to configure the host public key of the server so that the client can determine whether the server is trustworthy.

Use the **undo ssh authentication server** command to remove the configuration.

By default, the host public key of the server is not configured, and when logging into the server, the client uses the IP address or host name used for login as the public key name.

Examples # Configure the public key of the server with the IP address of 192.168.0.1 to be abc.

```
<Sysname> system-view
[Sysname] ssh client authentication server 192.168.0.1 assign rsa-key abc
```

ssh client first-time enable

Syntax **ssh client first-time enable**

undo ssh client first-time

View System view

Parameters None

Description Use the **ssh client first-time enable** command to enable the first authentication function.

Use the **undo ssh client first-time** command to disable the function.

By default, the function is enabled.

When an SSH client tries to access a server whose public host key it does not know for the first time, the first authentication function enables it to access the server and obtain and save the public host key of the server. When the client accesses the server later, it can use the locally saved public host key of the server to authenticate the server.

With the first authentication function disabled, an SSH client cannot access any server whose public host key it does not know. In this case, you must configure the public host key of the server to be accessed and specify the public key name on the client at first.

Examples # Enable the first authentication function.

```
<Sysname> system-view
[Sysname] ssh client first-time enable
```

ssh client ipv6 source

Syntax **ssh client ipv6 source** { **ipv6** *ipv6-address* | **interface** *interface-type interface-number* }

undo ssh client ipv6 source

View System view

Parameters *ipv6-address*: Source IPv6 address.

interface-type interface-number: Specifies a source interface by its type and number.

Description Use the **ssh client ipv6 source** command to specify the source IPv6 address or source interface for the SSH client.

Use the **undo ssh client ipv6 source** command to remove the configuration.

By default, the client uses the source address specified by the route of the device to access the SSH server.

Examples # Specify the source IPv6 address as 2:2::2:2 for the SSH client.

```
<Sysname> system-view
[Sysname] ssh client ipv6 source ipv6 2:2::2:2
```

ssh client source

Syntax **ssh client source** { **ip** *ip-address* | **interface** *interface-type interface-number* }

undo ssh client source

View System view

Parameters *ip-address*: Source IPv4 address.

interface-type interface-number: Specifies a source interface by its type and number.

Description Use the **ssh client source** command to specify the source IPv4 address or source interface of the SSH client.

Use the **undo ssh client source** command to remove the configuration.

By default, an SSH client uses the IP address or interface specified by the route to access the SSH server.

If the specified interface does not exist, the system prompts failure.

Related commands: **display ssh client source**.

Examples # Specify the source IPv4 address of the SSH client as 192.168.0.1.

```
<Sysname> system-view
[Sysname] ssh client source ip 192.168.0.1
```

ssh server authentication-retries

Syntax **ssh server authentication-retries** *times*

undo ssh server authentication-retries

View System view

Parameters *times:* Maximum number of authentication attempts, in the range 1 to 5.

Description Use the **ssh server authentication-retries** command to set the maximum number of SSH connection authentication attempts, which takes effect at next login.

Use the **undo ssh server authentication-retries** command to restore the default.

By default, the maximum number of SSH connection authentication attempts is 3.

Note that the threshold specified by using the **ssh server authentication-retries** command takes into account both RSA authentication attempts and password authentication attempts.

Related commands: **display ssh server**.

Examples # Set the maximum number of SSH connection authentication attempts to four.

```
<Sysname> system-view
[Sysname] ssh server authentication-retries 4
```

ssh server authentication-timeout

Syntax **ssh server authentication-timeout** *time-out-value*

undo ssh server authentication-timeout

View System view

Parameters *time-out-value*: Authentication timeout period in seconds, in the range 1 to.

Description Use the **ssh server authentication-timeout** command to set the SSH user authentication timeout period on the SSH server.

Use the **undo ssh server authentication-timeout** command to restore the default.

By default, the authentication timeout period is 60 seconds.

Related commands: **display ssh server**.

Examples # Set the SSH user authentication timeout period to 10 seconds.

```
<Sysname> system-view
[Sysname] ssh server authentication-timeout 10
```

ssh server enable

Syntax **ssh server enable**

undo ssh server enable

View System view

Parameters None

Description Use the **ssh server enable** command to enable SSH server.

Use the **undo ssh server enable** command to disable SSH server.

By default, SSH server is disabled.

Examples # Enable SSH server.

```
<Sysname> system-view
[Sysname] ssh server enable
```

ssh server rekey-interval

Syntax **ssh server rekey-interval** *hours*

undo ssh server rekey-interval

View System view

Parameters *hours:* Server key pair update interval in hours, in the range 1 to 24.

Description Use the **ssh server rekey-interval** command to set the interval for updating the server key pair.

Use the **undo ssh server rekey-interval** command to restore the default.

By default, the update interval of the server key pair is 0, that is, the server key pair is not updated.

Related commands: **display ssh server**.

Examples # Set the server key pair update interval to three hours.

```
<Sysname> system-view
[Sysname] ssh server rekey-interval 3
```

ssh user assign rsa-key

Syntax **ssh user** *username* **assign rsa-key** *keyname*

undo ssh user *username* **assign rsa-key**

undo ssh user *username*

View System view

Parameters *username*: SSH username, a string of 1 to 80 characters.

keyname: Name of an existing client public key, a string of 1 to 64 characters.

Description Use the **ssh user assign rsa-key** command to assign an existing public key to the specified SSH user.

Use the **undo ssh user assign rsa-key** command to remove the mapping between a user and its public key.

Note that:

- The system creates an SSH user while you configure the **ssh user assign rsa-key** command. By default, the authentication mode is RSA, and the service type is stelnet. Use the **undo ssh user** *username* command to delete SSH users.
- If you configure the **ssh user assign rsa-key** command for a user with a public key, the new public key overwrites the old one.
- The new public key takes effect when the user logs in next time.

Related commands: **display ssh user-information**.

Examples # Assign key named "key1" to the user named "aaa".

```
<Sysname> system-view
[Sysname] ssh user aaa assign rsa-key key1
```

ssh user authentication-type

Syntax **ssh user** *username* **authentication-type** { **password** | **rsa** | **password-publickey** | **all** }

undo ssh user *username* **authentication-type**

undo ssh user *username*

View System view

Parameters *username*: Name of the SSH user, a string of 1 to 80 characters.

password: Sets the authentication mode of the user to "password" forcibly.

rsa: Sets the authentication mode of the user to "RSA" forcibly.

password-publickey: Sets the authentication mode of the user to "RSA" plus "password" forcibly.

all: Sets the authentication mode to either "password" or "RSA". Clients will attempt to log in through RSA first.

For the authentication mode specified by password-publickey:

- *SSH1 users can log in successfully if passing one kind of authentication.*
- *SSH2 users cannot log in successfully unless passing both kinds of authentication.*

Description Use the **ssh user authentication-type** command to specify an authentication mode for a specific user. Use the **undo ssh user authentication-type** command to restore the default authentication mode.

By default, the system specifies the authentication mode as "RSA".

Note that:

- This command is used to specify an optional authentication mode for user login on the server. In practice, users can adopt an authentication mode on a client at their discretion.
- The system creates an SSH user while you configure the **ssh user authentication-type** command. The default service type is "stelnet". Use the **undo ssh user** command to delete SSH users.
- A newly configured authentication mode will take effect when users log in next time.
- If a user uses the RSA authentication mode, this user and its public key must be configured on a switch. If a user uses the password authentication mode, its account information can be configured on a switch or remote authentication server (for example, a RADIUS authentication server).

Related commands: **display ssh user-information**.

Examples # Specify the authentication mode of the user named "aaa" as a password.

```
<Sysname> system-view
[Sysname] ssh user aaa authentication-type password
```

ssh user service-type

Syntax **ssh user** *username* **service-type** { **stelnet** | **sftp** | **all** }

undo ssh user *username* **service-type**

undo ssh user *username*

View System view

Parameters *username*: Name of the SSH user, a string of 1 to 80 characters.

stelnet: The service type is secure Telnet.

sftp: The service type is Secure FTP.

all: Two service types including Stelnet and SFTP.

Description Use the **ssh user service-type** command to specify a service type for a specific user. Use the **undo ssh user service-type** command to restore the default service type.

By default, the service type is Stelnet.

The system creates an SSH user while you configure the **ssh user service-type** command. The default service type is "RSA". Use the **undo ssh user** command to delete SSH users.

Related commands: **display ssh user-information**.

Examples # Specify the service type as SFTP for the user named "aaa".

```
<Sysname> system-view
[Sysname] ssh user aaa service-type sftp
```

ssh2

Syntax **ssh2** { *host-ip* | *host-name* } [*port-number*] [**prefer_ctos_cipher** { **3des** | **aes128** | **des** } | **prefer_ctos_hmac** { **md5** | **md5_96** | **sha1** | **sha1_96** } | **prefer_kex** { **dh_exchange_group** | **dh_group1** } | **prefer_stoc_cipher** { **3des** | **aes128** | **des** } | **prefer_stoc_hmac** { **md5** | **md5_96** | **sha1** | **sha1_96** }] *

View System view

Parameters *host-ip*: IPv4 address of the server.

host-name: Server name, a string of 1 to 20 characters.

port-number: Port number of the server, in the range 0 to 65535. The default is 22.

prefer_ctos_cipher: Preferred encryption algorithm from client to server, defaulted to **aes128**.

- **3des**: Encryption algorithm 3des_cbc.
- **aes128**: Encryption algorithm aes128_cbc
- **des**: Encryption algorithm des_cbc.

prefer_ctos_hmac: Preferred HMAC algorithm from client to server, defaulted to **sha1**.

- **md5**: HMAC algorithm hmac-md5.
- **md5_96**: HMAC algorithm hmac-md5-96.
- **sha1**: HMAC algorithm hmac-sha1.
- **sha1_96**: HMAC algorithm hmac-sha1-96.

prefer_kex: Preferred key exchange algorithm, defaulted to **dh_group1**.

- **dh_exchange_group**: Key exchange algorithm diffie-hellman-group-exchange-sha1.
- **dh_group1**: Key exchange algorithm diffie-hellman-group1-sha1.

prefer_stoc_cipher: Preferred encryption algorithm from server to client, defaulted to **aes128**.

prefer_stoc_hmac: Preferred HMAC algorithm from server to client, defaulted to **sha1**.

Description Use the **ssh2** command to establish a connection to an SSH server, and specify the preferred key exchange algorithm, encryption algorithms, and HMAC algorithms of the client and the server.

Examples # Login to remote SSH2 server 10.214.50.51, setting the algorithms as follows:

- Preferred key exchange algorithm: DH_exchange_group
- Preferred encryption algorithm from server to client: AES128
- Preferred HMAC algorithm from client to server: MD5
- Preferred HMAC algorithm from server to client: SHA1-96.

```
<Sysname> system-view
[Sysname] ssh2 10.214.50.51 prefer_kex dh_exchange_group prefer_stoc
_cipher aes128 prefer_ctos_hmac md5 prefer_stoc_hmac sha1_96
```

ssh2 ipv6

Syntax **ssh2 ipv6** { *ipv6-address* | *host-name* } [*port-number*] [**prefer_ctos_cipher** { **3des** | **aes128** | **des** } | **prefer_ctos_hmac** { **md5** | **md5_96** | **sha1** | **sha1_96** } | **prefer_kex** { **dh_exchange_group** | **dh_group1** } | **prefer_stoc_cipher** { **3des** | **aes128** | **des** } | **prefer_stoc_hmac** { **md5** | **md5_96** | **sha1** | **sha1_96** }] *

View System view

Parameters *ipv6-address*: IPv6 address of the server.

host-name: Server name, a string of 1 to 46 characters.

port-number: Port number of the server, in the range 0 to 65535. The default is 22.

prefer_ctos_cipher: Preferred encryption algorithm from client to server, defaulted to **aes128**.

- **3des**: Encryption algorithm 3des_cbc.
- **aes128**: Encryption algorithm aes128_cbc.
- **des**: Encryption algorithm des_cbc.

prefer_ctos_hmac: Preferred HMAC algorithm from client to server, defaulted to **sha1**.

- **md5**: HMAC algorithm hmac-md5.
- **md5_96**: HMAC algorithm hmac-md5-96.
- **sha1**: HMAC algorithm hmac-sha1.

- **sha1_96**: HMAC algorithm hmac-sha1-96.

prefer_kex: Preferred key exchange algorithm, default to **dh_group1**.

- **dh_exchange_group**: Key exchange algorithm diffie-hellman-group-exchange-sha1.
- **dh_group1**: Key exchange algorithm diffie-hellman-group1-sha1.

prefer_stoc_cipher: Preferred encryption algorithm from server to client, defaulted to **aes128**.

prefer_stoc_hmac: Preferred HMAC algorithm from server to client, defaulted to **sha1**.

Description Use the **ssh2 ipv6** command to establish a connection to an IPv6 SSH server and specify the preferred key exchange algorithm, encryption algorithms, and HMAC algorithms of the client and the server.

Examples # Login to remote SSH2 server 2000::1, setting the algorithms as follows:

- Preferred key exchange algorithm: DH_exchange_group
- Preferred encryption algorithm from server to client: AES128
- Preferred HMAC algorithm from client to server: MD5
- Preferred HMAC algorithm from server to client: SHA1-96.

```
<Sysname> system-view
[Sysname] ssh2 ipv6 2000::1 prefer_kex dh_exchange_group prefer_stoc
_cipher aes128 prefer_ctos_hmac md5 prefer_stoc_hmac sha1_96
```

79 SFTP CONFIGURATION COMMANDS

bye (SFTP client view)

Syntax **bye**

View SFTP client view

Parameters None

Description Use the **bye** command to terminate the connection with a remote SFTP server and return to system view.

This command functions as the **exit** and **quit** commands.

Examples # Terminate the connection with the remote SFTP server.

```
sftp-client> bye
Bye
[Sysname]
```

cd (SFTP client view)

Syntax **cd** [*remote-path*]

View SFTP client view

Parameters *remote-path*: Name of a path on the server.

Description Use the **cd** command to change the working path on a remote SFTP server. With the argument not specified, the command displays the current working path.

- *You can use the **cd ..** command to return to the upper-level directory.*
- *You can use the **cd /** command to return to the root directory of the system.*

Examples # Change the working path to new1.

```
sftp-client> cd new1
Current Directory is:
/new1
```

cdup (SFTP client view)

Syntax **cdup**

View SFTP client view

Parameters None

Description Use the **cdup** command to return to the upper-level directory.

Examples # From the current working directory /new1, return to the upper-level directory.

```
sftp-client> cdup
Current Directory is:
/
```

delete (SFTP client view)

Syntax **delete** *remote-file*&<1-10>

View SFTP client view

Parameters *remote-file*&<1-10>: Name of a file on the server. &<1-10> means that you can provide up to 10 filenames, which are separated by space.

Description Use the **delete** command to delete a specified file from a server.

This command functions as the **remove** command.

Examples # Delete file temp.c from the server.

```
sftp-client> delete temp.c
The following files will be deleted:
/temp.c
Are you sure to delete it? [Y/N]:y
This operation may take a long time.Please wait...

File successfully Removed
```

dir (SFTP client view)

Syntax **dir** [**-a** | **-l**] [*remote-path*]

View SFTP client view

Parameters **-a**: Displays the filenames or the folder names of the specified directory.

-l: Displays in list form detailed information of the files and folder of the specified directory

remote-path: Name of the directory to be queried.

Description Use the **dir** command to display file and folder information under a specified directory.

With the **-a** and **-l** keyword not specified, the command displays detailed information of files and folder under the specified directory in a list form.

With the *remote-path* not specified, the command displays the file and folder information of the current working directory.

This command functions as the **ls** command.

Examples # Display in a list form detailed file and folder information under the current working directory.

```
sftp-client> dir
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey1
-rwxrwxrwx   1 noone    nogroup       225 Sep 28 08:28 pub1
drwxrwxrwx   1 noone    nogroup         0 Sep 28 08:24 new1
drwxrwxrwx   1 noone    nogroup         0 Sep 28 08:18 new2
-rwxrwxrwx   1 noone    nogroup       225 Sep 28 08:30 pub2
```

exit (SFTP client view)

Syntax **exit**

View SFTP client view

Parameters None

Description Use the **exit** command to terminate the connection with a remote SFTP server and return to system view.

This command functions as the **bye** and **quit** commands.

Examples # Terminate the connection with the remote SFTP server.

```
sftp-client> exit
Bye
[Sysname]
```

get (SFTP client view)

Syntax **get** *remote-file* [*local-file*]

View SFTP client view

Parameters *remote-file*: Name of a file on the remote SFTP server.

local-file: Name for the local file.

Description Use the **get** command to download a file from a remote SFTP server and save it locally.

If you do not specify the *local-file* argument, the file will be saved locally with the same name as that on the remote SFTP server.

Examples # Download file temp1.c and save it as temp.c locally.

```
sftp-client> get temp1.c temp.c
Remote  file:/temp1.c --->  Local file: temp.c
Downloading file successfully ended
```

help (SFTP client view)

Syntax **help** [**all** | *command-name*]

View SFTP client view

Parameters **all**: Displays a list of all commands.

command-name: Name of a command.

Description Use the **help** command to display a list of all commands or the help information of an SFTP client command.

With neither the argument nor the keyword specified, the command displays a list of all commands.

Examples # Display the help information of the **get** command.

```
sftp-client> help get
get remote-path [local-path]  Download file
Default local-path is the same with remote-path
```

ls (SFTP client view)

Syntax **ls** [**-a** | **-l**] [*remote-path*]

View SFTP client view

Parameters **-a**: Displays the filenames or the folder names of the specified directory.

-l: Displays in list form detailed information of the files and folder of the specified directory

remote-path: Name of the directory to be queried.

Description Use the **ls** command to display file and folder information under a specified directory.

With the **-a** and **-l** keyword not specified, the command displays detailed information of files and folder under the specified directory in a list form.

With the *remote-path* not specified, the command displays the file and folder information of the current working directory.

This command functions as the **dir** command.

Examples # Display in a list form detailed file and folder information under the current working directory.

```
sftp-client> ls
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey1
-rwxrwxrwx   1 noone    nogroup       225 Sep 28 08:28 pub1
drwxrwxrwx   1 noone    nogroup         0 Sep 28 08:24 new1
drwxrwxrwx   1 noone    nogroup         0 Sep 28 08:18 new2
-rwxrwxrwx   1 noone    nogroup       225 Sep 28 08:30 pub2
```

mkdir (SFTP client view)

Syntax **mkdir** *remote-path*

View SFTP client view

Parameters *remote-path*: Name for the directory on a remote SFTP server.

Description Use the **mkdir** command to create a directory on a remote SFTP server.

Examples # Create a directory named test on the remote SFTP server.

```
sftp-client> mkdir test
New directory created
```

put (SFTP client view)

Syntax **put** *local-file* [*remote-file*]

View SFTP client view

Parameters *local-file*: Name of a local file.

remote-file: Name for the file on a remote SFTP server.

Description Use the **put** command to upload a local file to a remote SFTP server.

If you do not specify the *remote-file* argument, the file will be saved remotely with the same name as the local one.

Examples # Upload local file temp.c to the remote SFTP server and save it as temp1.c.

```
sftp-client> put temp.c temp1.c
Local file:temp.c --->  Remote file: /temp1.c
Uploading file successfully ended
```

pwd (SFTP client view)

Syntax **pwd**

View SFTP client view

Parameters None

Description Use the **pwd** command to display the current working directory of a remote SFTP server.

Examples # Display the current working directory of the remote SFTP server.

```
sftp-client> pwd
/
```

quit (SFTP client view)

Syntax **quit**

View SFTP client view

Parameters None

Description Use the **quit** command to terminate the connection with a remote SFTP server and return to system view.

This command functions as the **bye** and **exit** commands.

Examples # Terminate the connection with the remote SFTP server.

```
sftp-client> quit
Bye
[Sysname]
```

remove (SFTP client view)

Syntax **remove** *remote-file*&<1-10>

View SFTP client view

Parameters *remote-file*&<1-10>: Name of a file on an SFTP server. &<1-10> means that you can provide up to 10 filenames, which are separated by space.

Description Use the **remove** command to delete a specified file from a remote server.

This command functions as the **delete** command.

Examples # Delete file temp.c from the server.

```
sftp-client> remove temp.c
The following files will be deleted:
/temp.c
Are you sure to delete it? [Y/N]:y
This operation may take a long time.Please wait...

File successfully Removed
```

rename (SFTP client view)

Syntax **rename** *oldname newname*

View SFTP client view

Parameters *oldname*: Original file name or directory name.

newname: New file name or directory name.

Description Use the **rename** command to change the name of a specified file or directory on an SFTP server.

Examples # Change the name of a file on the SFTP server from temp1.c to temp2.c.

```
sftp-client> rename temp1.c temp2.c
File successfully renamed
```

rmdir (SFTP client view)

Syntax **rmdir** *remote-path*&<1-10>

View SFTP client view

Parameters *remote-path*&<1-10>: Name of the directory on the remote SFTP server. &<1-10> means that you can provide up to 10 filenames that are separated by space.

Description Use the **rmdir** command to delete a specified directory from an SFTP server.

Examples # On the SFTP server, delete directory temp1 in the current directory.

```
sftp-client> rmdir temp1
Directory successfully removed
```

80 PASSWORD CONTROL CONFIGURATION COMMANDS

display password-control

Syntax **display password-control** [**super**]

View Any view

Parameters **super**: Displays the password control information of the super passwords. Without this keyword, the command displays the password control information for all passwords.

Description Use the **display password-control** command to display password control configuration information.

Examples # Display the global password control configuration information.

```
<Sysname> display password-control
 Global password settings for all users:
 Password aging:                 Enable(30 day(s))
 Password length:                Enable(10 character(s))
 Password composition:              Enable(1 type(s),  1 character(s) per type)
 Password history:               Enable(max history record:4)
 Password alert before expire:   7 day(s)
 Password authentication-timeout:60 second(s)
 Password attempt time(s):       2 times
 Password attempt-failed action: Lock for 120 minute(s)
```

Table 336 Field descriptions of the display password-control command

Field	Description
Password aging	Whether password aging is enabled and, if enabled, the aging time
Password length	Whether the minimum password length restriction function is enabled and, if enabled, the setting
Password composition	Whether the password composition restriction function is enabled and, if enabled, the settings
Password history	Whether the password history function is enabled and, if enabled, the setting
Password alert before expire	Number of days during which the user is warned of the pending password expiration
Password authentication-timeout	Password authentication timeout time
Password attempt time(s)	Allowed maximum number of login attempts
Password attempt-failed action	Action to be taken when a user fails to login after the specified number of attempts

display password-control blacklist

Syntax **display password-control blacklist** [**user-name** *name* | **ip** *ip-address*]

View Any view

Parameters *name*: Username of a user, a string of 1 to 80 characters.

ip-address: IP address of a user.

Description Use the **display password-control blacklist** command to display information about users blacklisted due to authentication failure.

With no arguments provided, this command displays information about all users in the blacklist.

Examples # Display information about users blacklisted due to authentication failure.

```
<Sysname> display password-control blacklist
Username: test
   IP: 192.168.44.1        Login failed times: 1      Lock flag: unlock

Total 1 blacklist item(s) matched. 1 listed.
```

Table 337 Field descriptions of display password-control blacklist

Field	Description
Username	Username of the user
IP	IP address of the user
Login failed times	Number of login failures
Lock flag	Flag indicating whether the user is prohibited from logging in currently, unlock if prohibited and lock if not.

password (Local user view)

Syntax **password**

View Local user view

Parameters None

Description Use the **password** command to set a password for a local user in interactive mode.

By default, no password is set for a local user in interactive mode.

Note that:

- Valid characters for a local user password include uppercase letters A to Z, lowercase letters a to z, numbers 0 to 9, blank space, and these 31 symbols: ~'!@#$%^&*()_+-={}|[]:";'<>,./.
- A local user password configured in interactive mode must satisfy the password control requirement.

Examples # Set a password for local user test in interactive mode.

```
<Sysname> system-view
[Sysname] local-user test
[Sysname-luser-test] password
Password:*****
Confirm :*****
Updating user(s) information, please wait....
```

password-control aging

Syntax **password-control aging** *aging-time*

undo password-control aging

View System view/local user view

Parameters *aging-time*: Password aging time in days, in the range 1 to 365.

Description Use the **password-control aging** command to set the password aging time.

Use the **undo password-control aging** command to remove the configured password aging time..

By default, the password aging time is 90 days.

Note that:

- The setting in system view has global significance, while that in local user view is only for the local user.
- If both global and local settings are specified, the local setting takes effect.
- Executing the **undo password-control aging** command in system view removes the global configuration and restores the default setting; executing this command in local user view removes the configuration of the current local user and restores the global configuration.

Examples # Set the global password aging time to 80 days.

```
<Sysname> system-view
[Sysname] password-control aging 80
```

Set the password aging time to 80 days for local user test.

```
<Sysname> system-view
[Sysname] local-user test
[Sysname-luser-test] password-control aging 80
```

password-control alert-before-expire

Syntax **password-control alert-before-expire** *alert-time*

undo password-control alert-before-expire

View System view

Parameters *alert-time*: Number of days during which the user is warned of the pending password expiration, in the range 1 to 30.

Description Use the **password-control alert-before-expire** command to set the number of days during which the user is warned of the pending password expiration.

Use the **undo password-control alert-before-expire** command to restore the default.

The default is 7 days.

Examples # Set the number of days during which the user is warned of the pending password expiration to 10 days.

```
<Sysname> system-view
[Sysname] password-control alert-before-expire 10
```

password-control authentication-timeout

Syntax **password-control authentication-timeout** *authentication-timeout*

undo password-control authentication-timeout

View System view

Parameters *authentication-timeout*: User authentication timeout time in seconds, in the range 30 to 120.

Description Use the **password-control authentication-timeout** command to set the user authentication timeout time.

Use the **undo password-control authentication-timeout** command to restore the default.

By default, the user authentication timeout time is 60 seconds.

Examples # Set the user authentication timeout time to 40 seconds.

```
<Sysname> system-view
[Sysname] password-control authentication-timeout 40
```

password-control composition

Syntax **password-control composition type-number** *policy-type* [**type-length** *type-length*]

undo password-control composition

View System view/local user view

Parameters *policy-type*: Minimum number of password composition types, in the range 1 to 4.

type-length: Minimum number of characters of each password composition type, in the range 1 to 63.

Description Use the **password-control composition** command to configure the password composition policy.

Use the **undo password-control composition** command to remove the configured password composition policy.

By default, the minimum number of password composition types is 1 and the minimum number of characters of a password composition type is 1 too.

Note that:

- The settings in system view have global significance, while those in local user view are only for the local user.
- If both global and local settings are specified, the local settings take effect.
- Executing the **undo password-control aging** command in system view removes the global configuration and restores the default setting; executing this command in local user view removes the configuration of the current local user and restores the global configuration.

Examples # Set the minimum number of password composition types to 3 and the minimum number of characters of each password composition type to 5 for all passwords.

```
<Sysname> system-view
[Sysname] password-control composition type-number 3 type-length 5
```

Set the minimum number of password composition types to 3 and the minimum number of characters of each password composition type to 5 for local user test.

```
<Sysname> system-view
[Sysname] local-user test
[Sysname-luser-test] password-control composition type-number 3 type-length 5
```

password-control enable

Syntax **password-control** { **aging** | **length** | **history** | **composition** } **enable**

undo password-control { **aging** | **length** | **history** | **composition** } **enable**

View System view

Parameters **aging**: Enables the password aging function.

length: Enables the minimum password length restriction function.

history: Enables the password history function.

composition: Enables the password composition restriction function.

Description Use the **password-control enable** command to enable password control functions.

Use the **undo password-control enable** command to disable password control functions.

By default, the password control functions are enabled.

Note that:

- The system stops recording history passwords after you execute the **undo password-control history enable** command, but the prior records still exist.
- You must enable a function for its relevant configurations to take effect.
- A password can be a combination of characters from the following four categories: uppercase letters A to Z, lowercase letters a to z, digits 0 to 9, and 32 special characters including blank space and ~‘!@#$%^&*()_+-={}|[]:";’<>,./. There are four password combination levels: 1, 2, 3, and 4, each representing the number of categories that a password must at least contain. Level 1 means that a password must contain characters of one category, level 2 at least two categories, and so on.

Examples # Enable the password composition restriction function.

```
<Sysname> system-view
[Sysname] password-control composition enable
Password composition is enabled for all users.
```

Enable the password aging function.

```
<Sysname> system-view
[Sysname] password-control aging  enable
Password aging is enabled for all users.
```

Enable the minimum password length restriction function.

```
<Sysname> system-view
[Sysname] password-control length  enable
Password minimum length is enabled for all users.
```

Enable the password history function.

```
<Sysname> system-view
[Sysname] password-control history  enable
Password history is enabled for all users.
```

Disable the password aging function.

```
<Sysname> system-view
[Sysname] undo password-control aging enable
Password aging is disabled for all users.
```

password-control history

Syntax **password-control history** *max-record-num*

undo password-control history

View System view

Parameters *max-record-num*: Maximum number of history password records for each user, in the range 2 to 15.

Description Use the **password-control history** command to set the maximum number of history password records for each user.

Use the **undo password-control history** command to restore the default.

By default, the maximum number of history password records for each user is 4.

Examples # Set the maximum number of history password records for each user to 10.

```
<Sysname> system-view
[Sysname] password-control history 10
```

password-control length

Syntax **password-control length** *length*

undo password-control length

View System view/local user view

Parameters *length*: Minimum password length in characters, in the range 4 to 32.

Description Use the **password-control length** command to set the minimum password length.

Use the **undo password-control length** command to restore the default.

By default, the minimum password length is 10 characters.

Note that:

- The setting in system view has global significance, while that in local user view is only for the local user.

- If both global and local settings are specified, the local setting takes effect.

Examples # Set the global minimum password length to 9 characters.

```
<Sysname> system-view
[Sysname] password-control length 9
```

Set the minimum password length to 9 characters for local user test.

```
<Sysname> system-view
[Sysname] local-user test
[Sysname-luser-test] password-control length 9
```

password-control login-attempt

Syntax **password-control login-attempt** *login-times* [**exceed** { **lock** | **unlock** | **lock-time** *time* }

undo password-control { **login-attempt** | **exceed** }

View System view

Parameters *login-times*: Maximum number of login attempts, in the range 2 to 10.

exceed: Specifies the action to be taken when a user fails to login after the specified number of attempts.

lock: Prohibits a user that fails to login after the specified number of attempts from logging in permanently.

unlock: Allows a user that fails to login after the specified number of attempts to continue logging in.

lock-time *time*: Forces a user that fails to login after the specified number of attempts to wait for a period of time before trying again. The *time* argument is in minutes and in the range 3 to 360.

Description Use the **password-control login-attempt** command to specify the maximum number of login attempts and the action to be taken when a user fails to login after the specified number of attempts.

Use the **undo password-control** command to restore the default.

By default, the maximum number of login attempts is 3 and a user failing to login after the specified number of attempts must wait for 120 minutes before trying again.

Examples # Set the maximum login attempt number to 4 and prohibit a user failing to login in after four attempts from logging in.

```
<Sysname> system-view
[Sysname] password-control login-attempt 4 exceed lock
```

password-control super aging

Syntax **password-control super aging** *aging-time*

undo password-control super aging

View System view

Parameters *aging-time*: Super password aging time in days, in the range 1 to 365.

Description Use the **password-control super aging** command to set the aging time for super passwords.

Use the **undo password-control super aging** command to remove the setting.

By default, the aging time for super passwords is 90 days.

Note that the setting for super passwords, if present, overrides that for all passwords.

Examples # Set the aging time for super passwords to 10 days.

```
<Sysname> system-view
[Sysname] password-control super aging 10
```

password-control super composition

Syntax **password-control super composition type-number** *policy-type* [**type-length** *type-length*]

undo password-control super composition

View System view

Parameters *policy-type*: Minimum number of super password composition types, in the range 1 to 4.

type-length: Minimum number of characters of each super password composition type, in the range 1 to 63.

Description Use the **password-control super composition** command to configure the composition policy for super passwords.

Use the **undo password-control super composition** command to remove the setting.

By default, the minimum number of password composition types is 1 and the minimum number of characters of a password composition type is 1 too.

Note that the settings for super passwords, if present, override those for all passwords.

Examples # Set the minimum number of password composition types to 3 and the minimum number of characters of each password composition type to 5 for super passwords.

```
<Sysname> system-view
[Sysname] password-control super composition type-number 3  type-length 5
```

password-control super length

Syntax **password-control super length** *length*

undo password-control super length

View System view

Parameters *length*: Minimum length for super passwords in characters, in the range 4 to 16.

Description Use the **password-control super length** command to set the minimum length for super passwords.

Use the **undo password-control super length** command to remove the setting.

By default, the minimum super password length is 10 characters.

Note that the setting for super passwords, if present, overrides that for all passwords.

Examples # Set the minimum length for super passwords to 10 characters.

```
<Sysname> system-view
[Sysname] password-control super length 10
```

reset password-control blacklist

Syntax **reset password-control blacklist** [**user-name** *name*]

View User view

Parameters *name*: Username of the user to be deleted from the blacklist, a string of 1 to 80 characters.

Description Use the **reset password-control blacklist** command to delete all or a user from the blacklist.

Examples # Delete the user named test from the blacklist.

```
<Sysname> reset password-control blacklist user-name test
Are you sure to delete the specified user in blacklist?[Y/N]
```

reset password-control history-record

Syntax **reset password-control history-record** [**user-name** *name* | **super** [**level** *level*]]

View User view

Parameters *name*: Username of the user whose password records are to be deleted.

super: Deletes the super password history records specified by the **level** *level* combination.

level: User level, in the range 1 to 3.

Description Use the **reset password-control history-record** command to delete history password records.

Note that:

- With no arguments and keywords specified, this command deletes the history password records of all local users.
- With the **super** keyword specified but the *level* argument not specified, this command deletes the history records of all super passwords.

Examples # Clear the history password records of all local users (enter Y to confirm).

```
<Sysname> reset password-control history-record
   Are you sure to delete all local user’s history records?[Y/N]
```

81 MAC AUTHENTICATION CONFIGURATION COMMANDS

debugging mac-authentication event

Syntax **debugging mac-authentication event** [**slot** *slot-number*]

undo debugging mac-authentication event [**slot** *slot-number*]

View User view

Parameters **slot** *slot-number*: Enables debugging for the service module in the specified slot of the MAC authentication module.

Description Use the **debugging mac-authentication event** command to enable event debugging for centralized MAC authentication.

Use the **undo debugging mac-authentication event** command to disable event debugging for centralized MAC authentication.

By default, event debugging for MAC authentication is disabled.

Examples # Enable event debugging for centralized MAC authentication.

```
<Sysname> debugging mac-authentication event
```

display mac-authentication

Syntax **display mac-authentication** [**interface** *interface-list*]

View Any view

Parameters **interface** *interface-list*: Specifies an Ethernet port list, in the format of { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>, where &<1-10> indicates that you can specify up to 10 port ranges. A port range defined without the **to** *interface-type interface-number* portion comprises only one port. With an interface range, the end interface number and the start interface number must be of the same type and the former must be greater than the latter.

Description Use the **display mac-authentication** command to display global MAC authentication information or MAC authentication information about specified ports.

Examples # Display global MAC authentication information.

```
<Sysname> display mac-authentication
MAC address authentication is enabled.
          Offline detect period is 180s
          Quiet period is 3 minute(s).
          Server response timeout value is 100s
          The max allowed user number is 1024 per slot
          Current user number amounts to 0
          Current domain is aabbcc.net
Silent MAC User info:
          MAC ADDR             From Port               Port Index
GigabitEthernet4/2/1 is link-up
  MAC address authentication is disabled
  Current online user number is 0
    MAC ADDR         Authenticate state           AuthIndex
GigabitEthernet4/2/2 is link-down
  MAC address authentication is enabled
  Authenticate success: 0, failed: 0
  Current online user number is 0
    MAC ADDR         Authenticate state           AuthIndex
```

.....(omitted)

Table 338 Field descriptions of the display mac-authentication command

Field	Description
MAC address authentication is Enabled	Whether MAC authentication is enabled
Offline detect period	Offline detect timer. It sets the interval of checking whether a user is offline and defaults to 300 seconds.
Quiet period	Quiet timer. It is the period of time during which the switch remains quiet before reinitiating authentication on the user after user authentication fails.
Server response timeout value	Server connection timeout timer. It sets the timeout time for the connection between the switch and the RADIUS server.
The max allowed user number	Maximum number of MAC-authenticated users each slot in the switch supports
Current user number amounts to	Total number of online users
Current domain: not configured, use default domain	Currently used ISP domain
Silent Mac User info	Information on users who are kept silent after failing MAC authentication
Ethernet1/1/1 is link-up	Status of the link on port Ethernet 1/1/1
MAC address authentication is Enabled	Whether MAC authentication is enabled on port Ethernet 1/1/1
Authenticate success: 0, failed: 0	MAC authentication statistics, including the number of successful authentication attempts and that of unsuccessful authentication attempts
Current online user number	Number of online users on the port
MAC ADDR	Online user MAC address

Table 338 Field descriptions of the display mac-authentication command

Field	Description
Authenticate state	User status. Possible values are: ■ CONNECTING: The user is logging in. ■ SUCCESS: The user has passed the authentication. ■ FAILURE: The user failed the authentication. ■ LOGOFF: The user has logged off.
AuthIndex	Authenticator Index

mac-authentication

Syntax **mac-authentication** [**interface** *interface-list*]

undo mac-authentication [**interface** *interface-list*]

View System view/Ethernet interface view

Parameters **interface** *interface-list*: Specifies an Ethernet port list, in the format of { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>, where &<1-10> indicates that you can specify up to 10 port ranges. A port range defined without the **to** *interface-type interface-number* portion comprises only one port.

Description Use the **mac-authentication** command to enable MAC authentication globally or for one or more ports.

Use the **undo mac-authentication** command to disable MAC authentication globally or for one or more ports.

By default, MAC authentication is neither enabled globally nor enabled on any port.

Note that:

- In system view, if you provide the *interface-list* argument, the command enables MAC authentication for the specified ports; otherwise, the command enables MAC authentication globally. In Ethernet interface view, the command enables MAC authentication for the port without requiring the *interface-list* argument.
- You can configure MAC authentication parameters globally or for specified ports either before or after enabling MAC authentication. If no MAC authentication parameters are configured before MAC authentication is enabled globally, the default values are used.
- You can enable MAC authentication for ports before enabling it globally. However, MAC authentication begins to function only after you also enable it globally.

Examples # Enable MAC authentication globally.

```
<Sysname> system-view
[Sysname] mac-authentication
Mac-auth is enabled globally.
```

Enable MAC authentication for port Ethernet 1/1/1.

```
<Sysname> system-view
[Sysname] mac-authentication interface Ethernet 1/1/1
 Mac-auth is enabled on port Ethernet1/1/1.
```

Or

```
<Sysname> systemsystme-view
[Sysname] interface ethernet 1/1/1
[Sysname-Ethernet1/1/1] mac-authentication
 Mac-auth is enabled on port Ethernet1/1/1.
```

mac-authentication domain

Syntax **mac-authentication domain** *isp-name*

undo mac-authentication domain

View System view

Parameters *isp-name*: ISP domain name, a case-insensitive string of 1 to 24 characters.

Description Use the **mac-authentication domain** command to specify the ISP domain for MAC authentication.

Use the **undo mac-authentication domain** command to restore the default.

By default, the default ISP domain (system) is used.

Examples # Specify the ISP domain for MAC authentication as domain1.

```
<Sysname> system-view
[Sysname] mac-authentication domain domain1
```

mac-authentication timer

Syntax **mac-authentication timer** { **offline-detect** *offline-detect-value* | **quiet** *quiet-value* | **server-timeout** *server-timeout-value* }

undo mac-authentication timer { **offline-detect** | **quiet** | **server-timeout** }

View System view

Parameters *offline-detect-value*: Offline detect interval, in the range 1 to 65,535 seconds.

quiet-value: Quiet period, in the range 1 to 65,535 minutes.

server-timeout-value: Server timeout period, in the range 1 to 300 seconds.

Description Use the **mac-authentication timer** command to set the MAC authentication timers.

Use the **undo mac-authentication timer** command to restore the defaults.

By default, the offline detect interval is 300 seconds, the quiet period is one minute, and the server timeout period is 100 seconds.

The following timers function in the process of MAC authentication:

- Offline detect timer: At this interval, the device checks to see whether an online user has gone offline. Once detecting that a user becomes offline, the device sends to the RADIUS server a stop accounting notice.
- Quiet timer: Whenever a user fails MAC authentication, the device does not initiate any MAC authentication of the user during such a period.
- Server timeout timer: During authentication of a user, if the device receives no response from the RADIUS server in this period, it assumes that its connection to the RADIUS server has timed out and forbids the user from accessing the network.

Related commands: **display mac-authentication**.

Examples # Set the server timeout timer to 150 seconds.

```
<Sysname> system-view
[Sysname] mac-authentication timer server-timeout 150
```

reset mac-authentication statistics

Syntax **reset mac-authentication statistics** [**interface** *interface-list*]

View User view

Parameters **interface** *interface-list*: Specifies an Ethernet port list, in the format of { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>, where &<1-10> indicates that you can specify up to 10 port ranges. A port range defined without the **to** *interface-type interface-number* portion comprises only one port.

Description Use the **reset mac-authentication statistics** command to clear MAC authentication statistics.

Note that:

- If you do not specify the *interface-list* argument, the command clears the global MAC authentication statistics and the MAC authentication statistics on all ports.
- If you specify the *interface-list* argument, the command clears the MAC authentication statistics on the specified ports.
- This command does not take effect on a port configured with 802.1x authentication.

Related commands: **display mac-authentication**.

Examples # Clear MAC authentication statistics on Ethernet 1/1/1.

```
<Sysname> reset mac-authentication statistics interface ethernet 1/1/1
```

82 NAT CONFIGURATION COMMANDS

connection-limit default action

Syntax **connection-limit default action** [**permit** | **deny**]

undo connection-limit default action

View System view

Parameters **permit**: Enables the connection-limit function globally.

deny: Disables the connection-limit function globally.

Description Use the **connection-limit default action** command to specify the default connection-limit action globally, either permit or deny. The effect of this command applies to all user connections not defined in the connection-limit policy.

Use the **undo connection-limit default action** command to restore the default.

By default, connection-limit is not enabled.

Examples # Configure the default connection-limit action as permit.

```
<Sysname> system-view
[Sysname] connection-limit default action permit
```

connection-limit default amount

Syntax **connection-limit default amount upper-limit** *max-amount*

undo connection-limit default amount

View System view

Parameters **upper-limit** *max-amount*: Specifies the upper limit of connections. The value range is 1 to 65536.

Description Use the **connection-limit default amount** command to set the limit(s) of user connections globally.

Use the **undo connection-limit default amount** command to restore the default.

By default, the upper limit is 200.

Examples # Configure the upper limit as 100.

```
<Sysname> system-view
[Sysname] connection-limit default amount upper-limit 100
```

connection-limit default rate

Syntax **connection-limit default rate max-rate** *max-rate*

undo connection-limit default rate

View System view

Parameters **max-rate** *max-rate*: Specifies the maximum connection rate, that is, the maximum number of connections allowed per second. The value ranges from 1 to 200.

Description Use the **connection-limit default rate** command to specify a global maximum connection rate.

Use the **undo connection-limit default rate** command to restore the default.

By default, the maximum connection rate is 100.

&Examples # Configure the global maximum connection rate.

```
<Sysname> system-view
[Sysname] connection-limit default rate max-rate 50
```

connection-limit enable

Syntax **connection-limit enable**

undo connection-limit enable

View System view

Parameters None

Description Use the **connection-limit enable** command to enable the connection-limit function.

Use the **undo connection-limit enable** command to disable this function.

By default, the connection-limit function is disabled.

Once this function is enabled, both the connection number and the connection rate are limited.

Examples # Enable the connection-limit function.

```
<Sysname> system-view
[Sysname] connection-limit enable
```

Disable the connection-limit function.

```
[Sysname] undo connection-limit enable
```

connection-limit policy

Syntax **connection-limit policy** *policy-number*

undo connection-limit policy { *policy-number* | **all** }

View System view

Parameters *policy-number*: Connection-limit policy number.

all: Deletes all connection-limit policies.

Description Use the **connection-limit policy** command to create or edit a connection-limit policy and enter connection-limit policy view.

Use the **undo connection-limit policy** command to delete a specified or all connection-limit policies.

Note that:

- A connection-limit policy contains a set of rules that define the connection-limit mode, the maximum connection rate and the connection number. By default, the connection-limit mode and the maximum connection rate are subject to the global configuration.
- When creating a connection-limit policy, you need to assign it a number that uniquely identifies that policy. Polices are matched by number in descending order.
- You can modify the rules in a policy only before binding the policy to a NAT module. No matter a connection-limit policy is bound to a NAT module or not, however, you can modify the connection-limit mode and the maximum connection rate. Additionally, you can add or delete rules to/from the policy. The newly modified connection limit policy will take effect after the flow table ages out.

Examples # Create a connection-limit policy numbered 1.

```
<Sysname> system-view
[Sysname] connection-limit policy 1
```

Delete a connection-limit policy numbered 2.

```
<Sysname> system-view
[Sysname] undo connection-limit policy 2
```

Delete all the existing connection-limit policies.

```
<Sysname> system-view
[Sysname] undo connection-limit policy all
```

debugging nat

Syntax **debugging nat** { **alg** | **event** | **packet** } [**interface** *interface-type interface-number*]

undo debugging nat { **alg** | **event** | **packet** } [**interface** *interface-type interface-number*]

View User view

Parameters **alg**: Enables/disables debugging for the ALG (application level gateway).

event: Enables/disables event debugging.

packet: Enables/disables packet debugging.

interface *interface-type interface-num*: Enables debugging for the NAT data packets on the specified interface. Use the *interface-type interface-number* argument to specify an interface by interface type and interface number.

Description Use the **debugging nat** command to enable specific NAT debugging.

Use the **undo debugging nat** command to disable specific NAT debugging.

By default, NAT debugging is disabled.

Examples # Enable NAT ALG debugging on a NAT-capable device.

```
<Sysname> debugging nat alg
```

Enable NAT event debugging on a NAT-capable device.

```
<Sysname> debugging nat event
```

Enable NAT packet debugging on a NAT-capable device.

```
<Sysname> debugging nat packet
```

debugging connection-limit

Syntax **debugging connection-limit**

undo debugging connection-limit

View User view

Parameters None

Description Use the **debugging connection-limit** command to enable connection limit debugging.

Use the **undo debugging connection-limit** command to disable connection limit debugging.

By default, connection limit debugging is disabled.

Examples # Enable connection limit debugging on a NAT-capable device.

```
<Sysname> debugging connection-limit
```

display connection-limit policy

Syntax **display connection-limit policy** { *policy-number* | **all** }

View Any view

Parameters *policy-number*: Number of a connection-limit policy.

all: Displays all connection-limit policies.

Description Use the **display connection-limit policy** command to display a specific or all connection-limit policies.

Examples # Display all connection-limit policies configured.

```
<Sysname> display connection-limit policy all
There is 1 policy:
Connection-limit policy 1, refcount 0 , 1 limit
 limit mode amount
 limit rate 11
 limit 1 source 192.168.0.12 amount 200
```

Table 339 Field descriptions of the display connection-limit policy all command

Field	Description
Connection-limit policy	Number of the connection-limit policy
refcount	Number of times that a policy is referenced
limit	Number of rules in the policy
limit mode	Connection-limit mode (all, amount, rate): ■ all: limits both connection number and connection rate. ■ amount: limits connection number only. ■ rate: limits connection rate only.
limit rate	Connection rate limit
source	Source address

Table 339 Field descriptions of the display connection-limit policy all command

Field	Description
amount	Upper limit of user connections

display nat address-group

Syntax **display nat address-group**

View Any view

Parameters None

Description Use the **display nat address-group** command to display the NAT address pool information.

Examples # Display the NAT address pool information.

```
<Sysname> display nat address-group
NAT address-group information:
  There are currently 1 nat address-group(s) and 1 virtual address-group(s)
      1 : from      92.1.1.200   to      92.1.1.202
    320 : from        92.1.1.1   to        92.1.1.1
```

Table 340 Field descriptions of the display nat address-group command

Field	Description
NAT address-group information	NAT address pool information
There are currently 1 nat address-group(s) and 1 virtual address-group(s)	There is one NAT address group and one virtual address pool configured with Easy IP
1 : from 92.1.1.200 to 92.1.1.202	The range of IP addresses in address pool 1 is from 92.1.1.200 to 92.1.1.202.
320 : from 92.1.1.1 to 92.1.1.1	Easy IP is configured and the corresponding IP address is 92.1.1.1.

display nat all

Syntax **display nat all**

View Any view

Parameters None

Description Use the **display nat all** command to display the configurations of all NAT parameters.

Examples # Display the configurations of all NAT parameters.

```
<Sysname> display nat all
NAT address-group information:
There are currently 2 nat address-group(s)
      1 : from         1.1.1.4   to         1.1.1.6
```

```
      2 : from       100.0.0.4   to       100.0.0.4
NAT outbound information:
There are currently 2 nat outbound rule(s)
               Vlan-interface1001: acl(2001) --- NAT address-group(1)
               Vlan-interface1000: acl(2000) --- NAT address-group(2)
Server in private network information:
  There are currently 1 internal server(s)
  Interface:Vlan-interface1000, Protocol:6(tcp),
     [global]        100.0.0.8:   21(ftp)    [local]    192.168.0.128:   21(ftp)
NAT log information:
  log enable  :  enable acl 2000
  flow-begin  :  enable
  flow-active :  10(minutes)
```

Table 341 Field descriptions of the display nat all command

Field	Description
NAT address-group information	NAT address pool information
1 : from 1.1.1.4 to 1.1.1.6	The IP address range of address pool 1 is from 1.1.1.4 to 1.1.1.6.
There are currently 2 nat address-group(s)	There are currently two NAT address pools.
2 : from 100.0.0.4 to 100.0.0.4	The IP address range of address pool 2 is from 100.0.0.4 to 100.0.0.4.
NAT outbound information:	Configuration information about internal address-to-external address translation
There are currently 2 nat outbound rule(s)	There are currently two NAT outbound rules.
Vlan-interface1001: acl(2001) --- NAT address-group(1)	Address translation. information configured on VLAN-interface 1001
Vlan-interface1000: acl(2000) --- NAT address-group(2)	Address translation. information configured on VLAN-interface 1000
Server in private network information:	Display information of internal servers
There are currently 1 internal server(s)	There is currently one internal server.
Interface:Vlan-interface1000, Protocol:6(tcp), [global] 100.0.0.8: 21(ftp) [local] 192.168.0.128: 21(ftp),	Internal server configured on VLAN-interface 1000: TCP is used. the public network address is 100.0.0.8, with the port number as 21; the internal IP address is 192.168.0.128, with the port number of 21.
NAT log information :	Displays address translation log information
log enable: enable acl 2000	Logging data flows matching acl 2000
flow-begin: enable	Logging newly established sessions
flow-active: 10(minutes)	Interval in logging active flows (10 minutes)

display nat connection-limit

Syntax **display nat connection-limit** { **all | ip** *user-ip* [**vpn-instance** *vpn-instance-name*] }

View Any view

Parameters **all**: Displays the connection-limit statistics of all users.

ip *user-ip*: Displays the connection-limit statistics of the user defined by the specified IP address.

vpn-instance *vpn-instance-name*: Specifies the MPLS VPN instance that a connection belongs to. The *vpn-instance-name* argument ranges from 1 to 31 characters. Absence of this keyword and argument indicates that the user whose connection statistics are to be displayed belongs to a normal private network rather than an MPLS VPN instance.

Description Use the **display nat connection-limit** command to display NAT connection-limit statistics.

Examples # Display NAT connection-limit statistics.

```
<Sysname> display nat connection-limit all
 There are 1 users' connection-limit information:
  IP-address         Vpn-instance                          Amount     Rate
  10.110.10.0        vpn1                                   0          0
```

Table 342 Field descriptions of the display nat connection-limit command

Field	Description
vpn-instance	MPLS VPN instance that a connection belongs to. "---" indicates that the connection does not belong to any MPLS VPN instance.
amount	Number of active connections
rate	Connection rate

display nat limit

Syntax **display nat limit** { **all | public | vpn-instance** *vpn-instance--name* }

View Any view

Parameters **all**: Displays resource distribution and utilization information about both ordinary (non-VPN) and VPN users.

public: Displays resource distribution and utilization information about the ordinary users.

vpn-instance: Displays resource distribution and utilization information for specified VPN user.

vpn-instance-name: Name of VPN instance.

Description

Use the **display nat limit** command to display the current resource allocation and utilization information.

Note that:

- If you have manually configured the resource limits for ordinary users, this command displays the detailed values allocated for them. If not, this command will not display the detailed values, but assume that all the resources belong to the ordinary users.

Examples

Display the current resource allocation and utilization information (with resources manually allocated for ordinary users).

```
<Sysname> display nat limit all
 The max configurable user amount of system is:                          8192
 The available configurable user amount of system is:                    5192
 The max configurable connection amount of system is:                 1257291
 The available configurable connection amount of system is:           1227291

 Global Configuration
 TYPE               Max-User Amount                  Max- Connection Amount
_____________________________________________________________________________
 Public                   1000                              10000
 VPN1                     1000                              10000
 VPN2                     1000                              10000

 Slot 5              User Amount                    Connection Amount
 TYPE          Max       Cur       Avail        Max       Cur       Avail
_____________________________________________________________________________
 Public       1000       100        900        10000      200        9800
 VPN1         1000         0       1000        10000       0        10000
 VPN2         1000         0       1000        10000       0        10000

 Slot 6              User Amount                    Connection Amount
 TYPE          Max       Cur       Avail        Max       Cur       Avail
_____________________________________________________________________________
 Public       1000         0       1000        10000       0        10000
 VPN1         1000         0       1000        10000       0        10000
 VPN2         1000       500        500        10000      500        9500
```

Display the current resource allocation and utilization information (without manually allocating resources for ordinary users).

```
<Sysname> display nat limit all
The max configurable user amount of system is:                          8192
The available configurable user amount of system is:                    5192
The max configurable connection amount of system is:                 1257291
The available configurable connection amount of system is:           1237291

Global Configuration
TYPE               Max-User Amount                  Max- Connection Amount
Public           ------------                        ------------
VPN1                1000                                 10000
VPN2                 2000                                 10000

 Slot 5              User Amount                    Connection Amount

 TYPE          Max       Cur       Avail        Max       Cur       Avail
_____________________________________________________________________________
 Public      ------       0       ------      -------      0      -------
```

```
VPN1         1000         0         1000         10000        0         10000
VPN2         2000         0         2000         10000        0         10000

Slot 6              User Amount                    Connection Amount
_____________________________________________________________________________
 TYPE          Max        Cur        Avail         Max        Cur        Avail
 Public       ------       0        ------       -------      0        -------
VPN1         1000         0         1000         10000        0         10000
VPN2         2000       500         1500         10000      500          9500
```

Table 343 Field descriptions of the display nat limit command

Field	Description
The max configurable user amount of system is:	Maximum number of users supported on L3+NAT modules
The available configurable user amount of system is:	The remaining user number allowed
The max configurable connection amount of system is:	Maximum number of user connections supported on L3+NAT modules
The available configurable connection amount of system is:	The remaining user connections that can be created
Global Configuration	Global resource distribution information
Slot	Slot number of a L3+NAT module
User Amount	Information about user number
Connection Amount	Information about user connection number
Max-User Amount	Maximum user number
Max- Connection Amount	Maximum number of user connections
TYPE	User type, either public (non-VPN) or VPN user
Max	Maximum number of users or connections
Cur	Number of current users or connections
Avail	Number of users or connections available

display nat log

Syntax **display nat log**

View Any view

Parameters None

Description Use the **display nat log** command to view the NAT log configuration.

Examples # View the NAT log configuration.

```
<Sysname> display nat log
NAT log information:
  log enable  :  enable acl 2000
  flow-begin  :  enable
  flow-active :  10(minutes)
```

Table 344 Field descriptions of the display nat log command:

Field	Description
NAT log information :	NAT log configuration
log enable : enable acl 2000	Logging data flows matching acl 2000.
flow-begin : enable	Logging newly established sessions
flow-active : 10(minutes)	Interval in logging active flows (10 minutes)

display nat outbound

Syntax **display nat outbound**

View Any view

Parameters None

Description Use the **display nat outbound** command to display the address translation information.

Examples # Display the NAT address translation information.

```
<Sysname> display nat outbound
NAT outbound information:
  There are currently 1 nat outbound rule(s)
                  Vlan-interface10: acl(2001) --- NAT address-group(2)
```

Table 345 Field descriptions of the display nat outbound command

Field	Description
NAT outbound information:	Display configured NAT address translation information
There are currently 1 nat outbound rule(s)	There is currently one NAT outbound rule.
Vlan-interface10: acl(2001) --- NAT address-group(2)	ACL 2001 is associated with address pool 2 on VLAN-interface 10 to provide many-to-many NAT.

display nat server

Syntax **display nat server**

View Any view

Parameters None

Description Use the **display nat server** command to display information about internal servers.

Examples # Display information about internal servers.

```
<Sysname> display nat server
Server in private network information:
  There are currently 1 internal server(s)
  Interface: Vlan-interface10, Protocol:6(tcp),
     [global]    202.110.10.10:      8080    [local]     10.110.10.10:    80(www)
```

Table 346 Field descriptions of the display nat server command

Field	Description
Server in private network information	Information about internal servers
There are currently 1 internal server(s)	There is currently one internal server.
Interface: Vlan-interface10, Protocol:6(tcp), [global] 202.110.10.10: 8080 [local] 10.110.10.10: 80(www)	On VLAN-interface 10, a WWW server is configured. Its internal address and port number are 10.110.10.10 and 80, respectively. Its external address and port number are 202.110.10.10 and 8080, respectively. The protocol type is TCP.

display nat session

Syntax **display nat session slot** *slot-number* **protocol** { **tcp** | **udp** } [**vpn-instance** *vpn-instance-name*] **source** { **global** *global-address global-port* | **inside** *inside-address inside-port* } **destination** *dst-address destination-port*

View Any view

Parameters **protocol** { **tcp** | **udp** }: Specifies a protocol for NAT session

vpn-instance *vpn-instance-name*: Displays NAT translation table entries in the specified MPLS VPN instance.

slot *slot-number*: Displays the NAT sessions for a module on the specified slot.

source global *global-address*: Displays NAT translation table entries for the specified external source IP address.

source inside *inside-address*: Displays NAT translation table entries for the specified internal source IP address.

destination *dst-address*: Displays NAT translation table entries for the specified destination IP address.

global-port, *inside-port*: Source port number.

destination-port: Destination port number.

Description Use the **display nat session** command to display the active NAT sessions.

Examples # Display the active NAT sessions.

```
<Sysname> dis nat session slot 10 protocol tcp vpn-instance vpn1 source inside 20
0.1.4.1 1024 destination 5.45.0.2 1025
SlotNumber   10
Protocol      GlobalAddr  Port   VPN      InsideAddr  Port        DestAddr  Port
%Aug 21 09:28:20:822 2006 9512-7 SHELL/4/LOGIN: VTY login from 172.16.1.234
```

```
      6      5.45.0.212 16384     1       200.1.4.1  1024        5.45.0.2  1025
                    status: 0,        TTL: 01:00:00,       Left: 00:00:00
```

Table 347 Field descriptions of the display nat session command

Field	Description
Protocol	Protocol number. A value of 6 represents TCP.
GlobalAddr Port	Address and port number after translation
InsideAddr Port	Private IP address and port number
DestAddr Port	Destination IP address and port number
VPN	Index of the MPLS VPN instance to which translation table entries belong. Its value varies from system to system. For systems that support 1,024 VPN instances, this parameter ranges from 0 to 1,023. A value of 0 indicates that translation table entries do not belong to any MPLS VPN instance.
status	Status of translation table entries
TTL	Lifetime of translation table entries, in the format of hh:mm:ss
Left	Remaining lifetime of translation table entries, in the format of hh:mm:ss

display nat statistics

Syntax **display nat statistics slot** *slot-number*

View Any view

Parameters **slot** *slot-number*: Displays NAT statistics for a module in the specified slot.

Description Use the **display nat statistics** command to display NAT statistics.

Examples # Display NAT statistics.

```
<Sysname> display nat statistics slot 6
 Slot number : 6
  total PAT session table count: 0
  total NO-PAT session table count: 0
  total SERVER session table count: 5
  total STATIC session table count: 0
  total FRAGMENT session table count: 0
  total session table count HASH by Internet side IP: 0
  active PAT session table count: 0
  active NO-PAT session table count: 0
  active FRAGMENT session table count: 0
  active session table count HASH by Internet side IP: 0
```

Table 348 Field descriptions of the display nat statistics command

Field	Description
total PAT session table count	Number of PAT session entries
total NO-PAT session table count	Number of No-PAT session entries
total SERVER session table count	Number of SERVER session entries

Table 348 Field descriptions of the display nat statistics command

Field	Description
total STATIC session table count	Number of STATIC session entries
total FRAGMENT session table count	Number of FRAGRANT session entries
total session table count HASH by Internet side IP	Number of HASH entries calculated based upon the external IP address
active PAT session table count	Number of active PAT session entries
active NO-PAT session table count	Number of active No-PAT session entries
active FRAGMENT session table count	Number of active FRAGRANT session entries
active session table count HASH by Internet side IP	Number of active HASH entries calculated based upon the external IP address

display userlog export

Syntax **display userlog export slot** *slot-number*

View Any view

Parameters *slot-number*: Displays the NAT log information for the module in the specified slot.

Description Use the **display userlog export** command to view the configuration and statistics of NAT logs for a module.

Related commands: userlog nat export

Examples # Display the configuration and statistics of the NAT logs for the module in Slot 2 of the switch.

```
<Sysname> display userlog export slot 2
NAT:
   Version 1 export is enabled
   Export logs to 1.2.3.6 (port: 7013)
   Source address of UDP packet of userlog is 1.2.3.7
   137 logs exported in 85 UDP packets
   0 logs in 0 UDP packets failed to be outputted
   0 entries buffered
```

Table 349 Field descriptions of the display userlog export command

Field	Description
NAT	NAT log information to be displayed
Version 1 export is enabled	UDP packet export enabled, in the version 1 format
Export logs to (port:)	IP address and port number of the NAT log server
Source address of UDP packet of userlog is	Source IP address of NAT logs
137 logs exported in 85 UDP packets	137 logs exported in 85 UDP packets
0 logs in 0 UDP packets failed to be outputted	0 logs in 0 UDP packets failed to be outputted
0 entries buffered	Number of entries in the buffer

Table 349 Field descriptions of the display userlog export command

Field	Description
No userlog export is enabled	This message appears in one of the following cases: ■ NAT log function is not enabled, ■ NAT log function is enabled but the logs are not configured to be exported to the information center, ■ NAT log function is enabled and logs are exported to the information center, but the IP address and UDP port number of the corresponding log server are not configured.

limit mode

Syntax **limit mode** { **all** | **amount** | **rate** }

undo limit mode

View Connection-limit policy view

Parameters **all**: Limits both the connection number and the connection rate.

amount: Limits the number of connections only.

rate: Limits the connection rate only.

Description Use the **limit mode** command to specify a connection-limit mode.

Use the **undo limit mode** command to remove the configuration and restore the connection limit mode configured globally.

By default, both the connection number and connection rate are limited.

The support for this command varies by device models.

Examples # Specify a connection-limit mode for connection-limit policy 1.

```
<Sysname> system-view
[Sysname] connection-limit policy 1
[Sysname-connection-limit-policy-1] limit mode amount
```

limit rate

Syntax **limit rate** *max-rate*

undo limit rate

View Connection-limit policy view

Parameters *max-rate*: Specifies the maximum connection rate (number of connections that can be established in a second) for the current connection-limit policy. The value ranges from 1 to 200 and defaults to 100.

Description Use the **limit rate** command to configure the maximum connection rate for a connection-limit policy.

Use the **undo limit rate** command to remove the configuration and restore the default.

Examples # Configure the maximum connection rate for connection-limit policy 1 as 80.

```
<Sysname> system-view
[Sysname] connection-limit policy 1
[Sysname-connection-limit-policy-1]limit rate 80
```

limit source

Syntax **limit** *limit-id* **source** *user-ip* [**vpn-instance** *vpn-instance-name*] { **amount** *max-amount* | **rate** } *

undo limit *limit-id*

View Connection-limit policy view

Parameters *limit-id*: ID of a rule in a connection-limit policy. The value is in the range of 0 to 1023.

source: Limits connections based on the source IP address.

user-ip: Source IP address of a user.

vpn-instance-name: Name of a VPN instance to which an internal server belongs. Absence of this argument indicates that the internal server belongs to a normal private network instead of an MPLS VPN instance.

amount: Specifies the connection-limit limits.

max-amount: Value of upper limit, in the range of 1 to 65535.

rate: Applies rate limit configured in connection-limit policy view. Without this keyword, the globally configured rate limit will be adopted.

Description Use the **limit source** command to configure a connection-limit rule.

Use the **undo limit** command to remove the configuration.

Examples # Configure connection-limit rule 1, gathering statistics on users with the source IP address being 1.1.1.1, setting the upper connection number limit to 200.

```
<Sysname> system-view
[Sysname] connection-limit policy 1
[Sysname-connection-limit-policy-1] limit 1 source 1.1.1.1 amount 200
```

nat address-group

Syntax **nat address-group** *group-number start-address end-address*

undo nat address-group *group-number*

View System view

Parameters *group-number*: Index of an address pool, in the range of 0 to 319.

start-address: The beginning IP address in an address pool.

end-address: The ending IP address in an address pool. The *end-address* must be not smaller than the *start-address*.

Description Use the **nat address-group** command to specify an address pool for NAT.

Use the **undo nat address-group** command to remove the configuration.

An address pool is a set of continuous IP addresses. When an internal packet is forwarded to the external network, the system selects an address from the pool to serve as the source address after address translation. An equal *start-address* and *end-address* means there is only one IP address in the address pool.

- An address pool is not needed in the case of Easy IP where the interface's public IP address is used as the translated IP address.

CAUTION:

- *The volume of an address pool, namely, the number of addresses contained, cannot exceed 255.*
- *You cannot delete an address pool which has been associated with an ACL.*
- *For Ethernet switches, when NAPT translation is used, the number of addresses contained in an address pool cannot exceed 3.*
- *The addresses in common address pools cannot be repeated. The addresses in a common address pool cannot contain any IP address in a virtual address pool. The addresses in a common address pool cannot contain any public network IP address of the internal server.*

Examples # Configure an address pool numbered 1 that contains addresses 202.110.10.10 to 202.110.10.15.

```
<Sysname> system-view
[Sysname] nat address-group 1 202.110.10.10 202.110.10.15
```

nat alg

Syntax **nat alg** { **all** | **dns** | **ftp** | **ils** | **nbt** }

undo nat alg { **all** | **dns** | **ftp** | **ils** | **nbt** }

View System view

Parameters **all**: Supports all special protocols.

dns: Supports DNS.

ftp: Supports FTP.

ils: Supports ILS.

nbt: Supports NBT.

Description Use the **nat alg** command to enable NAT application layer gateway for the specified protocol.

Use the **undo nat alg** command to disable NAT application layer gateway.

By default, NAT application layer gateway is enabled.

Examples # Enable NAT application layer gateway for FTP.

```
<Sysname> system-view
[Sysname] nat alg ftp
```

nat binding

Syntax **nat binding interface** *interface-type interface-number*

undo nat binding interface *interface-type interface-number*

View NAT service interface view

Parameters *interface-type interface-number*: Specifies interface type and interface number. Currently, only VLAN interfaces are supported.

Description Use the **nat binding** command to bind an NAT-enabled VLAN interface to the current NAT service interface.

Use the **undo nat binding** command to remove the binding.

Caution:

- *An NAT service interface can be bound to multiple NAT-enabled interfaces. In contrast, an NAT-enabled interface can be bound to only one service interface.*
- *Once a VLAN interface is bound to a NAT service virtual interface, it can no longer serve as the outbound interface for QoS redirection. This is because the packets exported from this VLAN interface are redirected to the L3+NAT module, causing QoS redirection ineffective.*

Examples # Configure ACL 2000, enabling NAT for the packets from 10.110.10.0/24.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 10.110.10.0 0.0.0.255
[Sysname-acl-basic-2000] quit
```

Configure the address pool.

```
[Sysname] nat address-group 1 202.110.10.10 202.110.10.12
```

Perform NAT with the addresses from the address pool 1 while using port information.

```
[Sysname] interface Vlan-interface 1000
[Sysname-Vlan-interface1000] nat outbound 2000 address-group 1
[Sysname-Vlan-interface1000] quit
```

Configure the binding relationship.

```
[Sysname] interface nat 6/0/1
[Sysname-NAT6/0/1] nat binding interface vlan-interface 1000
```

nat connection-limit-policy

Syntax **nat connection-limit-policy** *policy-number*

undo nat connection-limit-policy *policy-number*

View System view

Parameters *policy-number*: Number of the connection-limit policy to be bound with the NAT module, in the range of 0 to 255.

Description Use the **nat connection-limit-policy** command to bind a connection-limit policy with the NAT module.

Use the **undo nat connection-limit-policy** command to remove the configuration.

Note that:

- A NAT module can be bound with only one policy.
- The globally configured connection limits are not effective unless a connection-limit policy is bound to the NAT module.
- If there are multiple NAT modules, the configuration applies to all the modules.

CAUTION: *The connection limit policy configured does not take effect in NO-PAT translation.*

Examples # Bind connection-limit policy 1 with the NAT module.

```
<Sysname> system-view
[Sysname]nat connection-limit-policy 1
```

Remove the binding between connection-limit policy 1 and the NAT module.

```
<Sysname> system-view
[Sysname]undo nat connection-limit-policy 1
```

nat limit

Syntax **nat limit** { **public** | **vpn-instance** *vpn-instance-name* } **user-amount** *user-limit* **connection-amount** *connection-limit*

undo nat limit { **public** | **vpn-instance** *vpn-instance-name* }

View View

Parameters **public**: Allocates resources for ordinary users (non-VPN users).

vpn-instance: Allocates resources for VPN users.

vpn-instance-name: Name of VPN instance.

user-amount *user-limit*: Maximum number of users that NAT can handle. The value ranges from 0 to 8192 for ordinary users (0 means ordinary user is not supported) and 1 to 8192 for VPN users.

connection-amount *connection-limit*: Maximum unidirectional connections allowed for NAT. This value ranges from 0 to 1257291 (0 means ordinary user connection is not supported) for ordinary users and 1 to 1257291 for VPN users.

Description Use the **nat limit** command to allocate resources for ordinary or VPN users, including maximum user number and maximum connection number.

Use the **undo nat limit** command to release the resources.

By default, all the system resources belong to the ordinary users.

Note that:

- If you do not allocate resources for VPN users, the VPN users cannot create connections.
- You are recommended to allocate resources for VPN users prior to configuring their connection number limits. This is because VPN users are not supported when a system initializes, nor can they create any connections.

Examples # Configure the maximum number of VPN users as 5000, and maximum connections they can create as 5500.

```
<Sysname> system-view
[Sysname] nat limit vpn-instance vpn1 user-amount 5000 connection-amount 5500
```

nat log enable

Syntax **nat log enable** [**acl** *acl-number*]

undo nat log enable

View System view

Parameters **acl** *acl-number*: Enables the NAT log function for the data flows that match the specified ACL. The *acl-number* parameter ranges from 2,000 to 3,999. Absence of this parameter indicates that NAT log function applies to all non-VPN data flows.

Description Use the **nat log enable** command to enable the NAT log function.

Use the **undo nat log enable** command to disable the NAT log function.

By default, the NAT log function is disabled.

Examples # Enable the NAT log function.

```
<Sysname> system-view
[Sysname] nat log enable acl 2001
```

Disable the NAT log function.

```
<Sysname> system-view
[Sysname] undo nat log  enable
```

nat log flow-active

Syntax **nat log flow-active** *minutes*

undo nat log flow-active

View System view

Parameters *minutes*: Interval in logging the active NAT sessions, in the range 10 to 120 minutes.

Description Use the **nat log flow-active** command to enable logging for NAT active sessions and specify the interval in creating and sending the logs.

Use the **undo nat log flow-active** command to disable this function.

By default, this function is disabled.

This command allows you to log active flows regularly. This solves the problem of logging long-last active sessions as logs are normally generated only when a session is established or deleted.

Examples # Configure the interval between sending NAT active-flow logs as 10 minutes.

```
<Sysname> system-view
[Sysname] nat log flow-active 10
```

Delete the configured interval.

```
<Sysname> system-view
[Sysname] undo nat log flow-active
```

nat log flow-begin

Syntax **nat log flow-begin**

undo nat log flow-begin

View System view

Parameters None

Description Use the **nat log flow-begin** command to generate NAT logs while establishing a NAT session.

Use the **undo nat log flow-begin** command to restore the default.

By default, no log is generated when establishing a session.

Examples # Generate NAT log while establishing a session.

```
<Sysname> system-view
[Sysname] nat log flow-begin
```

nat outbound

Syntax **nat outbound** *acl-number* [**address-group** *group-number* [**no-pat**]]

undo nat outbound *acl-number* [**address-group** *group-number* [**no-pat**]]

View VLAN Interface view

Parameters *acl-number*: ACL (including both the basic and the advanced) number, in the range 2,000 to 3,999.

address-group: Specifies an address pool for NAT. If no address pool is specified, the interface IP address will be used, that is, the Easy IP feature.

group-number: Number of a predefined address pool, in the range of 0 to 319.

no-pat: Translates IP addresses only, without dealing with the port information.

Description Use the **nat outbound** command to enable NAT and associate an ACL with an address pool. Packets that match the ACL rules will have their internal IP address replaced by an address from the address pool.

Use the **undo nat outbound** command to remove the association.

- *For the ACL referenced by NAT, only the source IP address, destination IP address, and VPN instance take effect.*
- *For NO-PAT translation, if multiple NAT rules are configured on a VLAN interface, the device will determine the rule priority based on the ACL numbers bound with the NAT rules and always match the NAT rule with a greater ACL number. The priorities of the rules of an ACL are based on rule number. The smaller the rule number, the higher the priority.*
- *In PAT translation, ACLs are matched according to the "depth-first" order.*

Note that:

- *Translation of the source IP address of the packet that conforms to the ACL is accomplished by configuring the association between the ACL and the address pool. The system performs address translation by selecting one address in the address pool or by directly using the IP address of the interface.*
- *You can configure different associations on one interface. The corresponding **undo** form of the command can be used to delete the related address translation association. Normally, the associations are configured on the egress interface of an internal network that connects to the external network(s).*
- *Executing this command without the **address-group** keyword implements the Easy IP feature. When address translation is performed, the IP address of the interface is used as the translated address and the ACL can be used to control which addresses can be translated.*
- *If the interface address is directly used as the public network address after the NAT translation, after the NAT mapping entry between the private network and the public network is established, modifying the interface address will cause the user to be unable to access the external network through the interface normally because the original entry is not deleted automatically. Therefore, before modifying the interface address, make sure you use the **reset nat session** command to clear the original entry. This ensures that the user can access the external network normally by using this interface address as the public network address. Executing this command interrupts all the NAT services. Therefore, all the users must reinitiate connections. Be cautious about this operation.*
- *After the **undo nat outbound** command is executed, if the address translation association translates only the addresses of the packets in the address pool but not port configuration, the NAT address mapping entries generated with the **nat outbound** command will be deleted automatically. Otherwise, these entries will automatically age out in five to 10 minutes. During this period, users who use these table entries cannot access external networks whereas other users are not affected. You can also use the **reset nat session** command to clear all the NAT address translation table entries. However, use of this command will result in termination of address translation and all users will have to reestablish connections. Users can make a proper choice as required.*

Examples # Enable NAT for hosts in the 10.110.10.0/24 segment, using addresses 202.110.10.10 to 202.110.10.12 as the external IP addresses. Assume that VLAN-interface 1000 is connected to the external network.

```
<Sysname> system-view
[Sysname] acl number 2001
[Sysname-acl-basic-2001] rule permit source 10.110.10.0 0.0.0.255
[Sysname-acl-basic-2001] quit
```

Configure VLAN-interface 1000.

```
[Sysname] vlan 1000
[Sysname-vlan1000] port GigabitEthernet 4/2/1
[Sysname-vlan1000] quit
[Sysname] interface Vlan-interface 1000
[Sysname-Vlan-interface1000] ip address 202.110.10.1 24
```

Configure the address pool.

```
[Sysname] nat address-group 1 202.110.10.10 202.110.10.12
```

Enable NAT. Use the IP addresses from the address pool address-group 1. Use TCP/UDP port information.

```
[Sysname] interface Vlan-interface 1000
[Sysname-interface-vlan1000] nat outbound 2001 address-group 1
```

Remove the associated configuration.

```
[Sysname-interface-vlan1000] undo outbound 2001 address-group 1
```

If you do not use the TCP/UDP port information, do the following:

```
[Sysname-interface-vlan1000] nat outbound 2001 address-group 1 no-pat
```

Remove the associated configuration:

```
[Sysname-interface-vlan1000] undo nat outbound 2001 address-group 1 no-pat
```

To use the IP address of VLAN-interface 1000, do the following:

```
[Sysname-interface-vlan1000] nat outbound 2001
```

Remove the associated configuration.

```
[Sysname-interface-vlan1000] undo nat outbound 2001
```

nat server

Syntax **nat server** [**vpn-instance** *vpn-instance-name*] **protocol** *pro-type* **global** *global-address global-port1 global-port2* **inside** *host-address1 host-address2 host-port*

nat server [**vpn-instance** *vpn-instance-name*] **protocol** *pro-type* **global** *global-address* [*global-port*] **inside** *host-address* [*host-port*]

undo nat server [**vpn-instance** *vpn-instance-name*] **protocol** *pro-type* **global** *global-address global-port1 global-port2* **inside** *host-address1 host-address2 host-port*

undo nat server [**vpn-instance** *vpn-instance-name*] **protocol** *pro-type* **global** *global-address* [*global-port*] **inside** *host-address* [*host-port*]

View VLAN interface view

Parameters *vpn-instance-name*: Instance name of a VPN to which an internal server belongs, in the range 1 to 31 characters. Absence of this parameter indicates that the internal server belongs to a normal private network instead of an MPLS VPN instance.

pro-type: Type of protocols over IP. It can be provided only as a key word, namely, **icmp**, **tcp**, or **udp**.

global-address: A valid IP address designated for external access.

global-port: Port number designated for external access, in the range of 0 to 12287. You can use keywords to represent those well-known port numbers. For example, you can use **www** to represent port number 80 for WWW service and **ftp** to represent port number 21 for FTP service. This argument must be provided is the protocol type is UDP/TCP. If it is not provided, its value will be the same as that of *host-port*.

host-address: IP address of the server in internal LAN.

host-port: Service port number provided by the internal NAT server, in the range of 0 to 12287. You can use keywords to represent those well-known port numbers. For example, you can use **www** to represent port number 80 for WWW service and **ftp** to represent port number 21 for FTP service.

global-port1, global-port2: Jointly specifies a port range that corresponds to the IP address range of internal hosts. Note that *global-port2* must be greater than *global-port1* and the difference between them must be less than or equal to 127.

host-address1, host-address2: Jointly defines a sequence of addresses that corresponds to the port range. Note that *host-address2* must be greater than *host-address1* and that the range and number of the addresses must match those of the ports.

Description Use the **nat server** command to define a translation table for an internal server.

Using the address and port combination defined by the *global-address* and *global-port* parameters, external users can access internal servers with an IP address of *host-address* and a port of *host-port*.

Use the **undo nat server** command to remove the configuration.

Note that:

- Using this command, you can configure internal servers (such as WWW, FTP, Telnet, POP3, or DNS server) that provide services to external users. An internal server can reside in a private network or in an MPLS VPN instance.
- An interface can be configured with at most 256 internal server configuration commands. Each command can create a number of internal servers equal to the difference between *global-port2* and *global-port1*. An interface can be configured with at most 4096 internal servers and a system allows at most 1024 internal server configuration commands.
- In general, this command is configured on the interface that serves as the egress of an internal network and connects to an ISP on the external networks.

CAUTION: *When the protocol type is not* ***udp*** *(with a protocol number of 17) or* ***tcp*** *(with a protocol number of 6), you can only use the (****undo) nat server*** *[* ***vpn-instance*** *vpn-instance-name]* ***protocol*** *pro-type* ***global*** *global-address* ***inside*** *host-address command, that is, one-to-one NAT between an internal IP address and an external IP address.*

Examples # Specify the IP address of the WWW Server in a LAN to be 10.110.10.10, the IP address of the FTP Server in MPLS VPN vrf10 to be 10.110.10.11. It is desired to allow external users to access the WWW Server through http://202.110.10.10:8080, and the FTP Server through ftp://202.110.10.10. Assume that the VLAN-interface 1000 is connected to external networks.

```
<Sysname> system-view
[Sysname] vlan 1000
[Sysname-vlan1000] port GigabitEthernet 4/2/1
[Sysname-vlan1000] quit
[Sysname] interface Vlan-interface 1000
[Sysname-Vlan-interface1000] ip address 10.110.10.1 24
[Sysname-Vlan-interface1000] nat server protocol tcp global 202.110.
10.10 8080 inside 10.110.10.10 www
[Sysname-Vlan-interface1000] quit
[Sysname] ip vpn-instance vrf10
[Sysname-vpn-instance-vrf10] route-distinguisher 100:001
[Sysname-vpn-instance-vrf10] vpn-target 100:001
[Sysname-vpn-instance-vrf10] quit
[Sysname] interface Vlan-interface 1000
[Sysname-Vlan-interface1000] nat server vpn-instance vrf10 protocol
tcp global 202.110.10.10 8070 inside 10.110.10.11 ftp
```

Specify a host with an IP address of 10.110.10.12 in VPN vrf10. An external host pings 202.110.10.11 to examine the connectivity to the host.

```
[Sysname-Vlan-interface1000] nat server vpn-instance vrf10 protocol
icmp global 202.110.10.11 inside 10.110.10.12
```

Specify the external IP address as 202.110.10.10. Telnet the hosts which IP addresses range from 10.110.10.1 to 10.110.10.100 in MPLS VPN vrf10 through the ports ranging from 1001 to 1100, for example, telnet 10.110.10.1 from 202.110.10.10:1001, telnet 10.110.10.2 from 202.110.10.10:1002 and so on.

```
[Sysname-Vlan-interface1000] nat server vpn-instance vrf10 protocol
tcp global 202.110.10.10 1001 1100 inside 10.110.10.1 10.110.10.100
telnet
```

Remove the WWW server using the following commands.

```
[Sysname-Vlan-interface1000] undo nat server protocol tcp global 202
.110.10.10 8080 inside 10.110.10.10 www
```

Remove the FTP server in VPN vrf10 using the following commands.

```
[Sysname-Vlan-interface1000] undo nat server vpn-instance vrf10 prot
ocol tcp global 202.110.10.11 8070 inside 10.110.10.11 ftp
```

reset nat session

Syntax **reset nat session slot** *slot-number*

View User view

Parameters **slot** *slot-number*: Clears the address translation table for the module on the specified slot.

Description Use the **reset nat session** command to clear the address translation table and release the memory dynamically assigned for storing the table.

Examples # Clear the address translation table.

```
<Sysname> reset nat session slot 1
  Clearing NAT session table, please wait...Done!
```

reset userlog export

Syntax **reset userlog export slot** *slot-number*

View Use view

Parameters *slot-number:* Clears NAT log statistics for the module on the specified slot.

Description Use the **reset userlog export** command to clear the NAT log statistics.

Once the NAT log function is enabled, the system will take statistics for NAT logs periodically.

Related commands: display userlog export

Examples # Clear the NAT log information of slot 2

```
<Sysname> reset userlog export slot 2
```

reset userlog nat logbuffer

Syntax **reset userlog nat logbuffer slot** *slot-number*

View User view

Parameters *slot-number*: Clears the NAT log buffer for the module on the specified slot.

Description Use the **reset userlog nat logbuffer** command to clear the NAT log buffer.

CAUTION: *Clearing the NAT log buffer will cause NAT logs loss. You are not recommended to use this command in normal situations.*

Examples # Clear the NAT log buffer for the module on slot 2

```
<Sysname> reset userlog nat logbuffer slot 2
```

userlog nat export host

Syntax **userlog nat export** [**slot** *slot-number*] **host** *ip-address udp-port*

undo userlog nat export [**slot** *slot-number*] **host**

View System view

Parameters **slot** *slot-number*: Specifies a slot.

ip-address: IP address of the NAT log server. The address must be a valid unicast IP address, not a loopback address.

udp-port: UDP port number of the NAT log server, ranging from 0 to 65535.

Description Use the **userlog nat export host** command to configure the IP address and UDP port number of the NAT log server that receives NAT logs.

Use the **undo userlog nat export host** command to restore the default setting.

By default, no IP address or UDP port number of the NAT log server is configured.

Note that:

- You must configure the NAT log server to successfully export NAT logs in UDP packets.

- You are recommended to use a UDP port number greater than 1024 to avoid conflicting with common UDP port numbers.
- On the Switch 8800, each interface module can be configured with a separate NAT log server to share the overall server load. The packets exported from these interface modules are numbered independently (sequence numbers of packet headers). If you do not specify the *slot number,* this command applies to all interface modules without the IP address or UDP port number of the NAT log server configured.

Related commands: userlog nat export source-ip

Examples # Export the NAT logs of interface module 2 to the NAT log server whose IP address is 169.254.1.1:2000.

```
<Sysname> system-view
[Sysname] userlog nat export slot 2 host 169.254.1.1 2000
```

userlog nat export source-ip

Syntax **userlog nat export source-ip** *ip-address*

undo userlog nat export source-ip

View System view

Parameters *ip-address*: Source IP address of the exported UDP packets.

Description Use the **userlog nat export source-ip** command to set the source IP address of the UDP packets that carry NAT logs.

Use the **undo userlog nat export source-ip** command to restore the default.

By default, the source IP address of the UDP packets that carry NAT logs is the IP address of the interface that sends the UDP packets.

Related commands: userlog nat export host.

Examples # Set 169.254.1.2 as the source IP address of the UDP packets that carry NAT logs.

```
<Sysname> system-view
[Sysname] userlog nat export source-ip 169.254.1.2
```

userlog nat export version

Syntax **userlog nat export version** *version-number*

undo userlog nat export version

View System view

Parameters *version-number*: Version number of NAT logs. Currently, the system supports version 1 only.

Description Use the **userlog nat export version** command to set the version number of NAT logs.

Use the **undo userlog nat export version** command to restore the default.

By default, the version number of NAT logs is 1.

Examples # Set the version number of NAT logs to 1.

```
<Sysname> system-view
[Sysname] userlog nat export version 1
```

userlog nat syslog

Syntax **userlog nat syslog**

undo userlog nat syslog

View System view

Parameters None

Description Use the **userlog nat syslog** command to export NAT logs to the information center.

Use the **undo userlog nat syslog** command to restore the default.

By default, NAT logs are exported to the NAT log server.

Note that as NAT logs may occupy large memory, it is not advisable to export large amount of NAT logs to the information center.

Examples # Export NAT logs to the information center.

```
<Sysname> system-view
[Sysname] userlog nat syslog
```

83 DEVICE MANAGEMENT COMMANDS

File names in this document comply with the following rules:

- Path + file name (namely, a full file name): File on a specified path. A full file name consists of 1 to 135 characters.
- File name" (namely, only a file name without a path): File on the current working path. The file name without a path consists of 1 to 91 characters.

boot-loader

Syntax **boot-loader file** *file-url* **slot** *slot-number* { **main** | **backup** }

View User view

Parameter **file** *file-url*: Specifies a file name.

slot *slot-number*: Specifies the slot number of a module.

main: Specifies a file as a primary boot file.

backup: Specifies a file as a secondary boot file.

Description Use the **boot-loader** command to specify a boot file on a module.

By default, the boot file is specified as a primary boot file.

A primary boot file is used to boot a device and a secondary boot file is used to boot a device only when a primary boot file is unavailable.

Related command: **display boot-loader**.

Example # Specify the primary boot file of the module in slot 1 on a device as SW8800.app.

```
<Sysname> boot-loader file cf:/SW8800.app slot 1 main
  This command will set boot file of the specified board, Continue? [Y/N]:y
  The specified file will be used as a main boot file at the next time!
```

bootrom update

Syntax **bootrom update file** *file-url* **slot** *slot-number-list*

View User view

Parameter **file** *file-url*: Specifies a Boot ROM name and path.

slot *slot-number-list*: Specifies a list of slot numbers of cards, in the format of *slot-number-list* = { *slot-number* [**to** *slot-number*] }&<1-7>. The *slot-number* argument represents the slot number of a module and the value ranges from 1 to the biggest slot number. &<1-7> indicates that you can specify up to seven lists of slot numbers.

Description Use the **bootrom update** command to upgrade the Boot ROM program on a module(s).

Example # Use the LSBSRP1N41203.app file to upgrade the Boot ROM file on slot 0 of a device.

```
<Sysname> bootrom update file cf:/LSBSRP1N41203.app slot 0
  This command will update BootRom file on the specified board(s), Continue?
[Y/N]:y
  Now Updating BootRom, please wait...

 Upgrade board 0 BOOTROM succeeded
```

display boot-loader

Syntax **display boot-loader** [**slot** *slot-number*]

View User view

Parameter *slot-number*: Slot number of a module.

Description Use the **display boot-loader** command to display the path, name, and primary/secondary attribute of a Boot ROM file on a module.

Related command: boot-loader.

Example # Display the file adopted for the current and next boot of a device.

```
<Sysname> display boot-loader
The primary app to boot of board 1 at the next time is: cf:/S9500.APP
The backup  app to boot of board 1 at the next time is: cf:/S9500.APP
The app to boot of board 1 at this time is: cf:/S9500.APP
```

display cpu-usage

Syntax **display cpu-usage** [*number* [*offset*] [**verbose**] [**slave** | **slot** *slot-number*] [**from-device**]] | **slave** | **slot** *slot-number*]

View Any view

Parameter *number*: Number of CPU usage statistics records to be displayed.

offset: Offset between the serial number of the first CPU usage statistics record to be displayed and that of the last CPU usage record to be displayed.

verbose: Specifies to display detailed information of CPU usage statistics.

slave: Specifies to display the statistics of the CPU usage of a standby module.

slot *slot-number*: Specifies to display the statistics of the CPU usage of a module.
from-device: Displays external storage devices such as Flash and hard disk. The Switch 8800s currently do not support the **from-device** keyword.

Description Use the **display cpu-usage** command to display the CPU usage statistics.

The system takes statistics of CPU usage at intervals (usually every 60 seconds) and saves the statistical results in the history record area. **display cpu-usage** *number* indicates the system displays *number* records from the newest (last) record. **display cpu-usage** *number offset* indicates the system displays *number* records from the last but *offset*+1 record.

Equivalent to the **display cpu-usage 1 0 verbose** command, the **display cpu-usage** command displays detailed information of the last CPU usage statistics record.

Example # Display detailed information of the CPU usage statistics record of a module on a device.

```
<Sysname> display cpu-usage slot 3
===== Current CPU usage info =====
CPU Usage Stat. Cycle: 15 (Second)
CPU Usage            : 11%
CPU Usage Stat. Time : 2006-12-29  16:46:31
CPU Usage Stat. Tick : 0x1b(CPU Tick High) 0x6870ce22(CPU Tick Low)
Actual Stat. Cycle   : 0x0(CPU Tick High) 0x17a7bf75(CPU Tick Low)
TaskName        CPU        Runtime(CPU Tick High/CPU Tick Low)
VIDL            89%               0/15330d96
TICK             1%               0/  43b345
STMR             0%               0/   9a7a2
RXTX             0%               0/   28145
IPCQ             0%               0/   c5c6e
RPCQ             0%               0/  3002e0
DEVD             0%               0/   1a9e7
DIAG             0%               0/   12e77
ADJ6             0%               0/   47c53
INFA             0%               0/    1513
BOTT             0%               0/    357e
PPSP             0%               0/   12623
L2ST             0%               0/  2889f6
L2Ma             0%               0/   2a285
L2Ch             0%               0/     77a
L2PS             0%               0/  27161f
DMPL             0%               0/  2924c8
RtCh             0%               0/  278923
L3MC             0%               0/  289a45
 DEV             0%               0/   5bde5
ADJ4             0%               0/   43a96
 mac             0%               0/   347b5
```

```
LAGG              0%                0/   25de6
MSTP              0%                0/    999b
GARP              0%                0/   67335
 ARP              0%                0/   6474f
  IP              0%                0/  365f37
FIB6              0%                0/    86a8
  ND              0%                0/   f236a
DT1X              0%                0/  2ab26c
 ACM              0%                0/  2c4795
RDSO              0%                0/   10019
 RDS              0%                0/  28d644
  SC              0%                0/  2770f6
 TAC              0%                0/   4f754
MFIB              0%                0/   358a1
IFNT              0%                0/    91f5
```

Table 350 Description on fields of the display cpu-usage command

Field	Description
CPU usage info	Information of CPU usage records
CPU Usage Stat. Cycle	CPU usage measurement period in seconds
CPU Usage	CPU usage in percentage
CPU Usage Stat. Time	CPU usage statistics time in seconds
CPU Usage Stat. Tick	System runtime in ticks, represented by a 64-bit hexadecimal. CPU Tick High represents the most significant 32 bits and the CPU Tick Low the least significant 32 bits.
Actual Stat. Cycle	Actual CPU usage measurement period in ticks, represented by a 64-bit hexadecimal. CPU Tick High represents the most significant 32 bits and the CPU Tick Low the least significant 32 bits. Owing to the precision of less than one second, the actual measurement periods of different CPU usage records may differ slightly.
TaskName	Task name
CPU	CPU usage of the current task
Runtime(CPU Tick High/CPU Tick Low)	Running time of the current task

display device

Syntax **display device** [**cf-card**] [[**shelf** *shelf-number*] [**frame** *frame-number*] [**slot** *slot-number* [**subslot** *subslot-number*]] | **verbose**]

View Any view

Parameter **cf-card**: Displays information of a compact Flash (CF).

shelf *shelf-number*: Displays detailed information of the specified shelf or unit. The *shelf-number* argument represents a shelf number or unit number.

frame *frame-number*: Displays detailed information of the specified frame. The *frame-number* argument represents a frame number.

slot *slot-number*: Displays detailed information of the specified module. The *slot-number* argument represents the slot number of a module.

subslot *subslot-number*: Displays detailed information of the specified subcard. The *subslot-number* represents the subslot of a subcard.

verbose: Displays detailed information.

Description Use the **display device** command to display information about specified devices on a switch.

CAUTION: *The Switch 8800s do not support the* ***cf-card****,* ***shelf****,* ***frame*** *and* ***subslot*** *keyword.*

Example # Display brief information of cards on a device.

```
<Sysname> display device
Slot No.   Brd Type   Brd Status   Subslot Num    Sft Ver
 0         LSB1SRP1N6 Master       0              V200R001B02BBITSP12
 1         LSB1SRP1N6 Slave        0              V200R001B02BBITSP12
 2         LSB1GT12B  Normal       3              V200R001B02BBITSP12
 3         NONE       Absent       Absent         None
 4         LSB2FT48C  Normal       1              V200R001B02BBITSP12
 5         LSB1GP12C  Normal       3              V200R001B02BBITSP12
 6         NONE       Absent       Absent         None
```

Table 351 Field descriptions of the display device command

Field	Description
Slot No.	Slot number of a module
Brd Type	Hardware type of a module
Brd Status	Module status
Subslot Num	Number of subslots
Sft Ver	Software version

display device manuinfo

Syntax **display device manuinfo** [**slot** *slot-number*]

View Any view

Parameter **slot** *slot-number*: Displays detailed information of the specified module. The *slot-number* argument represents the slot number of a module.

Description Use the **display device manuinfo** command to display manufacture information about the device.

Example # Display manufacturing information of slot 1 on the device.

```
<Sysname> display device manuinfo slot 1
DEVICE_NAME          : SW8800
DEVICE_SERIAL_NUMBER : DPPMWWB000111
MAC_ADDRESS          : 005e-2542-0210
```

```
MANUFACTURING_DATE    : 2004-11-12
VENDOR_NAME           : HUAWEI-3COM
```

Table 352 Field descriptions of the display device manuinfo command

Field	Description
DEVICE_NAME	Device name
DEVICE_SERIAL_NUMBER	Device serial number
MAC_ADDRESS	MAC address of the device
MANUFACTURING_DATE	Manufacturing date of the device
VENDOR_NAME	Manufacturer name

display environment

Syntax **display environment**

View Any view

Parameter None

Description Use the **display environment** command to display the temperature information, including the current temperature and temperature thresholds of cards.

Example # Display the temperature information of cards.

```
<Sysname> display environment
System Temperature information (degree centigrade):
---------------------------------------------------
 SlotNo     Temperature       Lower limit      Upper limit
 0          53                10               70
 1          42                10               70
 2          38                10               70
 3          40                10               70
```

Table 353 Field descriptions of the display environment command

Field	Description
System Temperature information (degree centigrade)	Temperature information of system cards (degree centigrade)
Board	Module number
Temperature	Current temperature
Lower limit	Lower limit of temperature
Upper limit	Upper limit of temperature

display fan

Syntax **display fan** [*fan-id*]

View Any view

Parameter *fan-id*: Built-in fan number.

Description Use the **display fan** command to display the operating state of built-in fans.

Example # Display the operating state of all fans in a device.

```
<Sysname> display fan
 Fan  1 State: Normal
 Fan  2 State: Normal
```

The above information displays that fan 1 and fan 2 work normally.

display memory (Any view)

Syntax **display memory** [**slave** | **slot** *slot-number*]

View Any view

Parameter **slave**: Displays the memory usage of the standby module.

slot *slot-number*: Specifies the slot number of a module, in the range 0 to the biggest slot number.

Description Use the **display memory** command to display the usage of the memory of all or specified cards of a device.

Example # Display the usage of the memory of a device.

```
<Sysname> display memory
System Total Memory(bytes): 431869088
Total Used Memory(bytes): 71963156
Used Rate: 16%
```

Table 354 Description on the fields on the display memory command

Field	Description
System Total Memory(bytes)	Total size of the system memory (in bytes)
Total Used Memory(bytes)	Size of the memory used (in bytes)
Used Rate	Percentage of the memory used to the total memory

display power

Syntax **display power** [*power-id*]

View Any view

Parameter *power-id*: Power supply number.

Description Use the **display power** to display the status of the power supply of a device.

Example # Display the status of the power supply of a device.

```
<Sysname> display power
 Power   1 State: Absent
 Power   2 State: Normal
```

The above information indicates that power supply 2 works normally, and power supply 1 is absent.

display schedule reboot

Syntax **display schedule reboot**

View Any view

Parameter None

Description Use the **display schedule reboot** command to display the device reboot time set by the user.

Related command: **schedule reboot at**,**schedule reboot delay**.

Example # Display the reboot time of a device.

```
<Sysname> display schedule reboot
System will reboot at 16:00:00 2006/03/10 (in 2 hours and 5 minutes).
```

The above information indicates the system will reboot at 16:00:00 on March 10, 2006 (in two hours and five minutes).

display xbar

Syntax **display xbar**

View Any view

Parameter None

Description Use the **display xbar** command to display the load mode of the active and standby cards of the system, including configured load mode and currently running load mode.

Related command: **xbar**.

The configured load mode may be different from the currently running load mode. Only when both the active module and the standby module are in the slot can the load sharing mode become valid; otherwise, even if the load sharing mode is configured the active module will automatically switch to the active-standby mode.

Example # Display the load mode of the active and standby cards of a device.

```
[Sysname] display xbar
The configured system HA xbar load mode is BALANCE
The activated system HA xbar load mode is SINGLE
The above information indicates that the configured mode is load mod
e and the currently running load mode is standby.
```

reboot

Syntax **reboot** [**slot** *slot-number*]

View User view

Parameter **slot** *slot-number*: Specifies the slot number of a module.

Description Use the **reboot** command to reboot a module, a subcard, or the whole system.

CAUTION:

- *This command reboots the device, thus resulting in service interruption. Please use it with caution.*
- *If a primary boot file fails or does not exist, the device cannot be rebooted with this command. In this case, you can re-specify a primary boot file to reboot the device, or you can power off the device then power it on and the system automatically uses the secondary boot file to restart the device.*
- *If you are performing file operations when the device is to be rebooted, the system removes the reboot operation for the sake of security.*

Example # Reboot the device.

```
<Sysname> reboot
```

reset unused porttag

Syntax **reset unused porttag**

View User view

Parameter None

Description Use the **reset unused porttag** command to clear the 16bit index saved but not used in the current system.

A confirmation is required when you carry out this command. If you fail to make a confirmation within 30 seconds or enter "N" to cancel the operation, the command will not be carried out.

Example # Clear the 16bit index saved but not used in the current system.

```
<Sysname> reset unused porttag
Current operation will delete all unused port tag(s). Continue? [Y/N]:y
<Sysname>
```

schedule reboot at

Syntax **schedule reboot at** *hh:mm* [*date*]

undo schedule reboot

View User view

Parameter *hh:mm*: Reboot time of a device, in the format of hh:mm (hours:minutes). The value of the *hh* argument ranges of is 0 to 23, and the value of the *mm* argument ranges from 0 to 59.

date: Reboot date of a device, in the format mm/dd/yyyy (Month/day/year) or in the format yyyy/mm/dd (year/month/day) The yyyy value ranges from 2000 to 2035, the mm value ranges from 1 to 12, and the dd value depends on a specific month.

Description Use the **schedule reboot at** command to enable the scheduled reboot function and specify a specific reboot time and date.

Use the **undo schedule reboot** command to disable the scheduled reboot function.

By default, the scheduled reboot function is disabled.

There are two cases if no specific reboot date is specified:

- When the specified reboot time is later than the current time, the device will be rebooted at the reboot time of the current day.
- When the specified reboot time is earlier than the current time, the device will be rebooted at the reboot time the next day.
- If you are performing file operations when the device is to be rebooted, the system does not execute the command for the sake of security.

Note that:

- The precision of the device timer is 1 minute. One minute before the reboot time, the device will prompt "REBOOT IN ONE MINUTE" and will be rebooted in one minute.
- The difference between the reboot date and the current date cannot exceed 30 x 24 hours (namely, 30 days).
- After you execute the above command, the device will prompt you to confirm the configuration. You must enter <Y> or <y> to make the configuration take effect. The original configuration will be overwritten at the same time.

- If a date (month/day/year or year/month/day) later than the current date is specified for the **schedule reboot at** command, the device will be rebooted at the reboot time.
- If you use the **clock** command after the **schedule reboot at** command to adjust the system time, the reboot time set by the **schedule reboot at** command will become invalid.

CAUTION:

- *This command reboots the device in a future time, thus resulting in service interruption. Please use it with caution.*
- *If you are performing file operations when the device is to be rebooted, the system removes the reboot operation for the sake of security.*

Example # Configure the device to reboot at 22:00 PM (supposing that the current time is 16:36).

```
<Sysname> schedule reboot at 22:00
Reboot system at 22:00 2006/03/21(in 5 hour(s) and 23 minute(s))
confirm?[Y/N]:
```

If you have used the **terminal logging** command to enable the log display function on the terminal before setting a reboot time, the system will automatically display related log information after you enter <y>. By default, the log display function is enabled.

```
<Sysname>
%Mar 21 16:36:51:601 2006 Sysname CMD/5/REBOOT:
con0: Set schedule reboot parameters at 16:36:51 2006/03/21, and sys
tem will reboot at 22:00 2006/03/21.
```

schedule reboot delay

Syntax **schedule reboot delay** { *hh:mm* | *mm* }

undo schedule reboot

View User view

Parameter *hh:mm*: Device reboot wait time, in the format of hh:mm (hours:minutes). The value of the *hh* argument ranges of is 0 to 720, and the value of the *mm* argument ranges from 0 to 59, and the value of the *hh:mm* argument cannot exceed 720:00.

mm: Device reboot wait time in minutes, in the range of 0 to 43,200.

Description Use the **schedule reboot delay** command to enable the scheduled reboot function and set a reboot wait time.

Use the **undo schedule reboot** command to disable the scheduled reboot function.

By default, the scheduled reboot function is disabled.

Note that:

- The reboot wait time can be in the format of hh:mm (hours:minutes) or mm (absolute minutes). The absolute minutes cannot exceed 30 x 24 x 60 minutes, namely, 30 days.
- The precision of the device timer is 1 minute. One minute before the reboot time, the device will prompt "REBOOT IN ONE MINUTE" and will be rebooted in one minute.
- After you execute the above command, the device will prompt you to confirm the configuration. You must enter <Y> or <y> to make the configuration take effect. The original configuration will be overwritten at the same time.
- If you use the **clock** command after the **schedule reboot delay** command to adjust the system time, the reboot wait time set by the **schedule reboot delay** command will become invalid.
- If you are performing file operations when the device is to be rebooted, the system does not execute the command for the sake of security.

CAUTION:

- *This command reboots the device after the specified delay time, thus resulting in service interruption. Please use it with caution.*
- *If you are performing file operations when the device is to be rebooted, the system removes the reboot operation for the sake of security.*

Example # Configure the device to reboot in 88 minutes (supposing the current time is 16:50).

```
<Sysname> schedule reboot delay 88
Reboot system at 18:18 2006/03/21(in 1 hour(s) and 28 minute(s))
confirm?[Y/N]:
```

If you have used the **terminal logging** command to enable the log display function on the terminal before setting a reboot time, the system will automatically display related log information after you enter <y>. By default, the log display function is enabled on the terminal.

```
<Sysname>
%Mar 21 16:50:13:369 2006 Sysname CMD/5/REBOOT:
con0: Set schedule reboot parameters at 16:50:13 2006/03/21, and sys
tem will reboot at 18:18 2006/03/21.
```

shutdown-interval

Syntax **shutdown-interval** *time*

View System view

Parameter *time*: Detection interval in seconds, in the range 1 to 300.

Description Use the **shutdown-interval** command to set a detection interval.

By default, the detection interval is 30 seconds.

Note that:

- The operation, administration and maintenance (OAM) module detects an exception on a port (for example, abrupt traffic increase resulting from an attack), the port will be closed automatically, without execution of the **shutdown** command. You can set the recovery time of the port by using the **shutdown-interval** command.
- The OAM module protects the system against attacks. The **shutdown-interval** command helps you to dynamically set a detection interval to cooperate with the OAM module.
- The detection is triggered on an interface at the time of t0 and the detection interval of the system is t1. If t1-t0<t2 after the detection interval t1 is changed to t2, the interface will continue the detection and the total detection time will be t2.
- If t1-t0≥t2, the interface will stop the detection and the total detection time will be t1-t0.

Example # Set the detection interval to 100 seconds.

```
<Sysname> system-view
[Sysname] shutdown-interval 100
```

temperature-limit

Syntax **temperature-limit** *slot-number lower-value upper-value*

undo temperature-limit *slot-number*

View System view

Parameter *slot-number*: Slot number.

lower-value: Lower temperature limit in degree centigrade, in the range 0 to 70.

upper-value: Upper temperature limit in degree centigrade, in the range 20 to 90.

Description Use the **temperature-limit** command to set the temperature alarm threshold on a module.

Use the **undo temperature-limit** command to restore the default.

By default, the lower value of the temperature alarm threshold is 10 and the upper value is 70.

The upper-value argument must be bigger than the lower-level argument.

Example # Set the lower temperature limit on module 0 to 10 degree centigrade and the upper temperature limit to 75 degree centigrade.

```
<Sysname> system-view
[Sysname] temperature-limit 0 10 75
Setting temperature limit succeeded.
```

xbar

Syntax **xbar** { **load-balance** | **load-single** }

View System view

Parameter **load-balance**: Specifies the active and standby cards to work in the load sharing mode.

load-single: Specifies the active and standby cards to work in the active-standby mode.

Description Use the **xbar** command to set the load mode for the active and standby cards of the device.

By default, the active and standby cards work in the active-standby mode.

Related command: **display xbar**.

Only when both the active module and the standby module are in the slot can the load sharing mode be valid; otherwise, even if the load sharing mode is configured the active module will automatically switch to the active-standby mode.

Example # Configure a device to work in the load sharing mode.

```
<Sysname> system-view
[Sysname] xbar load-balance
```

84 POE CONFIGURATION COMMANDS

When the PoE power is shut down or unavailable, all PoE related configuration commands will fail.

apply poe-profile

Syntax **apply poe-profile** { **index** *index* | **name** *profile-name* }

undo apply poe-profile { **index** *index* | **name** *profile-name* }

View PoE interface view

Parameter **index** *index*: Specifies the index number of the PoE configuration file. The index number ranges from 1 to 100.

name *profile-name*: Specifies the name of the PoE configuration file. The file name consists of 1 to 15 characters.

Description Use the **apply poe-profile** command to apply the PoE configuration file to the current PoE interface.

Use the **undo apply poe-profile** command to remove the application of the PoE configuration file from the current PoE interface.

Note that the index number, instead of the name, of the PoE configuration file will be displayed when you execute the **display this** command.

Related command: **display poe-profile** and **apply poe-profile interface**.

Example # Apply the PoE configuration file named A20 to PoE interface GigabitEthernet1/1/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/1/1
[Sysname-GigabitEthernet1/1/1] apply poe-profile name A20
[Sysname-GigabitEthernet1/1/1] display this
#
interface GigabitEthernet1/1/1
 port link-mode bridge
 apply poe-profile index 1
#
```

apply poe-profile interface

Syntax **apply poe-profile** { **index** *index* | **name** *profile-name* } **interface** *interface-range*

undo apply poe-profile { **index** *index* | **name** *profile-name* } **interface** *interface-range*

View System view

Parameter **index** *index*: Specifies the index number of the PoE configuration file. The index number ranges from 1 to 100.

name *profile-name*: Specifies the name of the PoE configuration file. The file name consists of 1 to 15 characters.

interface-range: Range of Ethernet interface numbers, indicating multiple Ethernet interfaces. The expression is *interface-range* = *interface-type interface-number* [**to** *interface-type interface-number*], where *interface-type interface-number* represents the interface type and interface number. The start interface number should be less than the end interface number. Ethernet interface numbers can be in any range. If any interface in the specified range does not support PoE, it will be ignored when the PoE configuration file is applied.

Description Use the **apply poe-profile interface** command to apply the PoE configuration file to one or more PoE interfaces.

Use the **undo apply poe-profile interface** command to remove the application of the PoE configuration file from specified PoE interface(s).

Related command: **display poe-profile interface** and **apply poe-profile**.

Example # Apply the PoE configuration file named ABC to PoE interface GigabitEthernet1/1/1.

```
<Sysname> system-view
[Sysname] apply poe-profile name ABC interface GigabitEthernet 1/1/1
```

Apply the PoE configuration file with index 5 to PoE interfaces GigabitEthernet1/1/2 to GigabitEthernet1/1/8.

```
<Sysname> system-view
[Sysname] apply poe-profile index 5 interface GigabitEthernet 1/1/2
to GigabitEthernet 1/1/8
```

display poe device

Syntax **display poe device**

View Any view

Parameter None

Description Use the **display poe device** command to display the mapping between ID, module, and slot of the power sourcing equipment (PSE).

Example # Display the mapping between ID, module, and slot of each PSE.

```
<Sysname> display poe device
 PSE ID  SlotNo PortNum  MaxPower(W)  State   Model
 13       4      48       200          on     LSB1GV48DB
 16       5      48       200          on     LSB1GV48DB
```

Table 355 Description on fields of the display poe device command

Field	Description
PSE ID	ID of the PSE
SlotNo	Slot number of the PSE
PortNum	Number of PoE interfaces on the PSE
MaxPower(W)	Maximum power of the PSE (W)
State	PSE state: on: The PSE is supplying power. off: The PSE stops supplying power. faulty: The PSE is faulty
Model	PSE model

The relation between the ID and the slot number of a PSE is: PSE ID = SlotNo x 3 + 1.

display poe interface

Syntax **display poe interface** [*interface-type interface-number*]

View Any view

Parameter *interface-type interface-number*: Interface type and interface number.

Description Use the **display poe interface** command to display the power information of the specified interface.

If no interface is specified, the power information of all PoE interfaces will be displayed.

Example # Display the power status of GigabitEthernet1/1/1.

```
<Sysname> display poe interface GigabitEthernet 1/1/1
Port Power Enabled                : enable
 Port Power Priority               : critical
 Port Operating Status             : on
 Port IEEE Class                   : 0
 Port Detection Status             : delivering-power
 Port Current Power                : 11592    mW
```

```
Port Average Power                : 11610    mW
Port Peak Power                   : 11684    mW
Port Max Power                    : 15400    mW
Port Current                      : 244      mA
Port Voltage                      : 51.7     V
Port PD Description               : IP Phone For Room 101
```

Table 356 Description on fields of the display poe interface command

Field	Description
Port Power Enabled	PoE enabled/disabled status on the interface: ■ enable: PoE is enabled. ■ disable: PoE is disabled.
Port Power Priority	Power priority of the PoE interface: ■ critical (highest) ■ high ■ low
Port Operating Status	Operating state of the PoE interface: ■ off: PoE is disabled. ■ on: Power is supplied for a PoE interface normally. ■ power lack: The guaranteed remaining power of the PSE is not enough to supply power to a critical PoE interface. ■ power-deny: The PSE refuses to supply power. The power required by the powered device (PD) is higher than the configured power. ■ power-itself: The external equipment is supplying power to itself. ■ power-limit: The PSE is supplying a limited power. The power required by the PD is higher than the configured power and the PSE still supplies the configured power.
Port IEEE class	PD power class
Port Detection Status	Power detection state of the PoE interface: ■ disabled: The PoE function is disabled. ■ searching: The PoE interface is searching for the PD. ■ delivering-power: The PoE interface is supplying power to the PD. ■ fault: There is a fault defined in 802.3af. ■ test: The PoE interface is under test. ■ other-fault: There is a fault other than defined in 802.3af. ■ pd-disconnect: No PD is connected.
Port Current Power	Current power of the PoE interface
Port Average Power	Average power of the PoE interface
Port Peak Power	Peak power of the PoE interface
Port Max Power	Maximum power of the PoE interface
Port Current	Current of the PoE interface
Port Voltage	Voltage of the PoE interface
Port PD Description	Description of the PD connected to the PoE interface, which is used to identify the type and location of the PD.

Display the state of all PoE interfaces.

```
<Sysname> display poe interface
 Interface  Enable   Priority  CurPower  Operating    IEEE   Detection
                              (W)        Status      class  Status
 GE1/1/1     enable    low        4.4       on         0  delivering-power
 GE1/1/2     enable    critical   0         on         0      disabled
 GE1/1/3     enable    low        0         on         0      disabled
 GE1/1/4     enable    critical   0         on         0      searching
 GE1/1/5     enable    low        4.0       on         0  delivering-power
 GE1/1/6     enable    low        0         on         0      disabled
 GE1/1/7     disable   low        0         off        0      fault
 GE1/1/8     disable   low        0         off        0      disabled
 GE1/1/9     disable   low        0         off        0      disabled
 GE1/1/10    disable   low        0         off        0      disabled
 GE1/1/11    disable   low        0         off        0      disabled
 GE1/1/12    disable   low        0         off        0      disabled

---  2 port(s) on,    8.4(W) consumed,   171.6(W) Remaining ---
```

Table 357 Description on fields of the display poe interface command

Field	Description
Interface	Shortened form of a PoE interface
Enable	PoE enabled/disabled status: ■ enable: PoE is enabled. ■ disable: PoE is disabled.
Priority	Power priority of a PoE interface: ■ critical (highest) ■ high ■ low
CurPower	Current power of a PoE interface
Operating Status	Operating state of a PoE interface ■ off: PoE is disabled. ■ on: Power is supplied for a PoE interface normally. ■ power lack: The guaranteed remaining power of the PSE is not high enough to supply power to a critical PoE interface. ■ power-deny: The PSE refuses to supply power. The power required by the powered device (PD) is higher than the configured power. ■ power-itself: The external equipment is supplying power to itself. ■ power-limit: The PSE is supplying a limited power. The power required by the PD is higher than the configured power and the PSE still supplies the configured power.
IEEE class	PD power class stipulated by IEEE
Detection Status	Power detection state of a PoE interface: ■ disabled: The PoE function is disabled. ■ searching: The PoE interface is searching for the PD. ■ delivering-power: The PoE interface is supplying power to the PD. ■ fault: There is a fault defined in 802.3af. ■ test: The PoE interface is under test. ■ There is a fault other than defined in 802.3af. ■ pd-disconnect: The PD is disconnected.
Port(s) on	Number of PoE interfaces that are supplying power
consumed	Power consumed by the current PoE interface

Table 357 Description on fields of the display poe interface command

Field	Description
Remaining	Total remaining power of the system

display poe interface power

Syntax **display poe interface power** [*interface-type interface-number*]

View Any view

Parameter *interface-type interface-number*: Interface type and interface number.

Description Use the **display poe interface power** command to display the power information of a PoE interface(s).

If no interface is specified, the power information of all PoE interfaces will be displayed.

Example # Display the power information of GigabitEthernet1/1/1.

```
<Sysname> display poe interface power GigabitEthernet 1/1/1
Interface  CurPower PeakPower MaxPower PD Description
             (W)        (W)        (W)
 GE1/1/1    15.0       15.3       15.4      Acess Point on Room 509 for Peter
```

Display the power information of all PoE interfaces.

```
<Sysname> display poe interface power
Interface  CurPower PeakPower MaxPower PD Description
             (W)        (W)       (W)
 GE2/1/25    4.4        4.5       4.6          IP Phone on Room 309 for Peter Smit
h....
 GE2/1/26    4.4        4.5       15.4         IP Phone on Room 409 for Peter Pan
 GE2/1/27    15.0      15.3       15.4        Acess Point on Room 509 for Peter
 GE2/1/28    0           0          0           IP Phone on Room 609 for Peter Joh
n....
 GE2/1/29    0           0          0           IP Phone on Room 709 for Jack
 GE2/1/30    0           0          0           IP Phone on Room 809 for Alien

---  3 port(s) on,   23.8(W) consumed,   776.2(W) Remaining ---
```

Table 358 Description on fields of the display poe interface power command

Field	Description
Interface	Shortened form of a PoE interface
CurPower	Current power of a PoE interface
PeakPower	Peak power of a PoE interface
MaxPower	Maximum power of a PoE interface
PD Description	Description of the PD connected with a PoE interface When the description contains more than 34 characters, the first 30 characters followed by four dots will be displayed.
Port(s) on	Number of PoE interfaces that are supplying power
consumed	Power currently consumed by all PoE interfaces
Remaining	Total remaining power of the system

display poe power-usage

Syntax **display poe power-usage**

View Any view

Parameter None

Description Use the **display poe power-usage** command to display the power information of the PoE power and all PSEs

Example # Display the power information of the PoE power and all PSEs.

```
<Sysname> display poe power-usage
 PoE Current Power                : 49    W
 PoE Max Power                    : 1125  W
 PoE Max Guaranteed Power         : 1125  W
 PoE Remaining Allocated Power    : 319   W
 PoE Remaining Guaranteed Power   : 1125  W
 PoE Total Powered Port Number    : 4
 Detailed power usage of PSE(s):
 PSE ID  Max     Current  Peak     Average  Remaining     Powered
         (W)     (W)      (W)      (W)      Guaranteed(W) PortNum
 1       806     49       49       49       806           4
 28      806     0        0        0        0             0
```

Table 359 Description on fields of the display poe power-usage command

Field	Description
PoE Current Power	Total consumption power of the PSE
PoE Max Power	Maximum PoE power
PoE Max Guaranteed Power	Guaranteed maximum PoE power, namely, the maximum power supplied to critical PSEs.
PoE Remaining Allocate Power	Remaining allocable PoE power = Maximum PoE power - the sum of the maximum power of all PoE-enabled PSEs
PoE Remaining Guaranteed Power	Guaranteed remaining PoE power = Guaranteed maximum PoE power - the sum of the maximum power of critical PSEs
PoE Total Powered Port Number	Number of PoE interfaces that are currently supplying power
PSE ID	ID of the PSE
Max	Maximum power of the PSE
Current	Current power of the PSE
Peak	Peak power of the PSE
Average	Average power of the PSE
Remaining Guaranteed	Guaranteed remaining power of the PSE = Guaranteed maximum power of the PSE - the sum of the maximum power of critical PoE interfaces of the PSE
Powered PortNum	Number of PoE interfaces to which the PSE is supplying power

display poe pse

Syntax **display poe pse** [*pse-id*]

View Any view

Parameter *pse-id*: PSE ID. The relation between the ID and the slot number of a PSE is: PSE ID = SlotNo x 3 + 1. If you enter a PSE ID, the information of the PSE will be displayed. Otherwise, the information of all PSEs on the device will be displayed.

Description Use the **display poe pse** command to display the information of the specified PSE.

Example # Display the information of PSE 1.

```
<Sysname> display poe pse 1
 PSE ID                          : 1
 PSE Slot No                     : 0
 PSE SubSlot No                  : 1
 PSE Model                       : LSB1GV48DB
 PSE Power Enabled               : enable
 PSE Power Preempted             : no
 PSE Power Priority              : low
 PSE Current Power               : 49       W
 PSE Average Power               : 49       W
 PSE Peak Power                  : 49       W
 PSE Max Power                   : 806      W
 PSE Remaining Guaranteed        : 806      W
 PSE CPLD Version                : 21
 PSE Software Version            : 290
 PSE Hardware Version            : 0
 PSE Legacy Detection            : disable
 PSE Utilization-threshold       : 80
 PSE Pse-policy Mode             : priority
 PSE Pd-policy Mode              : priority
```

Table 360 Description on fields of the display poe pse command

Field	Description
PSE ID	ID of the PSE
PSE Slot No	Slot number of the PSE
PSE SubSlot No	Sub-slot number of the PSE
PSE Model	Model of the PSE module
PSE Power Enabled	PoE is enabled for the PSE
PSE Power Preempted	PSE power preempted state ■ no: The power of the PSE is not preempted. ■ yes: The power of the PSE is preempted so that it can supply power, although PoE is enabled for the PSE
PSE Power Priority	Power priority of the PSE
PSE Current Power	Current power of the PSE
PSE Average Power	Average power of the PSE

Table 360 Description on fields of the display poe pse command

Field	Description
PSE Peak Power	Peak power of the PSE
PSE Max Power	Maximum power of the PSE
PSE Remaining Guaranteed	Guaranteed remaining power of the PSE = Maximum power of the PSE- the sum of the maximum power of the critical PoE interfaces of the PSE
PSE CPLD Version	PSE CPLD version
PSE Software Version	PSE software version number
PSE Hardware Version	PSE hardware version number
PSE Legacy Detection	Nonstandard PD detection by the PSE: ■ enable: Enabled ■ disable: Disabled
PSE Utilization-threshold	PSE power alarm threshold
PSE Pse-policy Mode	PSE power management policy mode
PSE Pd-policy Mode	PD power management policy mode

display poe pse interface

Syntax **display poe pse** *pse-id* **interface**

View Any view

Parameter **pse** *pse-id*: Specifies a PSE ID. The relation between the ID and the slot number of a PSE is: PSE ID = SlotNo x 3 + 1.

Description Use the **display poe pse interface** command to display the state of all PoE interfaces connected to the specified PSE.

Example # Display the state of all PoE interfaces connected to PSE 1.

```
<Sysname> display poe pse 1 interface
Interface  Enable   Priority  CurPower  Operating   IEEE   Detection
                              (W)       Status      Class  Status
 GE0/1/1    enable   low       12.3      on          0    delivering-power
 GE0/1/2    disable  low       0.0       off         0      disabled
 GE0/1/3    disable  low       0.0       off         0      disabled
 GE0/1/4    disable  low       0.0       off         0      disabled
 GE0/1/5    disable  low       0.0       off         0      disabled
 GE0/1/6    disable  low       0.0       off         0      disabled
 GE0/1/7    disable  low       0.0       off         0      disabled
 GE0/1/8    disable  low       0.0       off         0      disabled
 GE0/1/9    disable  low       0.0       off         0      disabled
 GE0/1/10   disable  low       0.0       off         0      disabled
 GE0/1/11   disable  low       0.0       off         0      disabled
 GE0/1/12   disable  low       0.0       off         0      disabled
 GE0/1/13   disable  low       0.0       off         0      disabled
 GE0/1/14   disable  low       0.0       off         0      disabled
 GE0/1/15   disable  low       0.0       off         0      disabled
 GE0/1/16   disable  low       0.0       off         0      disabled
 GE0/1/17   enable   low       12.3      on          0    delivering-power
 GE0/1/18   disable  low       0.0       off         0      disabled
 GE0/1/19   disable  low       0.0       off         0      disabled
```

```
GE0/1/20   disable  low       0.0       off         0      disabled
GE0/1/21   disable  low       0.0       off         0      disabled
GE0/1/22   disable  low       0.0       off         0      disabled
GE0/1/23   disable  low       0.0       off         0      disabled
GE0/1/24   disable  low       0.0       off         0      disabled
GE0/1/25   disable  low       0.0       off         0      disabled
GE0/1/26   disable  low       0.0       off         0      disabled
GE0/1/27   disable  low       0.0       off         0      disabled
GE0/1/28   disable  low       0.0       off         0      disabled
GE0/1/29   disable  low       0.0       off         0      disabled
GE0/1/30   disable  low       0.0       off         0      disabled
GE0/1/31   disable  low       0.0       off         0      disabled
GE0/1/32   disable  low       0.0       off         0      disabled
GE0/1/33   disable  low       0.0       off         0      disabled
GE0/1/34   disable  low       0.0       off         0      disabled
GE0/1/35   enable   low       12.3      on          0    delivering-power
GE0/1/36   disable  low       0.0       off         0      disabled
GE0/1/37   disable  low       0.0       off         0      disabled
GE0/1/38   disable  low       0.0       off         0      disabled
GE0/1/39   disable  low       0.0       off         0      disabled
GE0/1/40   disable  low       0.0       off         0      disabled
GE0/1/41   disable  low       0.0       off         0      disabled
GE0/1/42   disable  low       0.0       off         0      disabled
GE0/1/43   disable  low       0.0       off         0      disabled
GE0/1/44   disable  low       0.0       off         0      disabled
GE0/1/45   disable  low       0.0       off         0      disabled
GE0/1/46   disable  low       0.0       off         0      disabled
GE0/1/47   enable   low       12.3      on          0    delivering-power
GE0/1/48   disable  low       0.0       off         0      disabled

  ---  4 port(s) on,    49.2 (W) consumed,   756.9 (W) remaining ---
```

Table 361 Description on fields of the display poe pse interface command

Field	Description
Interface	Shortened form of a PoE interface
Enable	PoE enabled/disabled state on a PoE interface. For the value, see Table 356.
Priority	Priority of a PoE interface. For the value, see Table 356.
CurPower	Current power of a PoE interface
Operating	Operating state of a PoE interface. For the value, see Table 356.
IEEE	PD power class
Detection	Power detection state of a PoE interface. For the value, see Table 356.
port(s) on	Number of PoE interfaces that are supplying power
consumed	Power consumed by PoE interfaces on the PSE
Remaining	Remaining power on the PSE

display poe pse interface power

Syntax **display poe** [**pse** *pse-id*] **interface power**

View Any view

Parameter **pse** *pse-id*: Specifies a PSE ID. The relation between the ID and the slot number of a PSE is: PSE ID = SlotNo x 3 + 1.

Description Use the **display poe pse interface power** command to display the power information of PoE interfaces connected with the PSE.

Example # Display the power information of PoE interfaces connected with PSE 1.

```
<Sysname> display poe pse 1 interface power
Interface   CurPower  PeakPower   MaxPower  PD Description
             (W)       (W)         (W)
 GE0/1/1     12.3      12.3        15.4
 GE0/1/2     0.0       0.0         15.4
 GE0/1/3     0.0       0.0         15.4
 GE0/1/4     0.0       0.0         15.4
 GE0/1/5     0.0       0.0         15.4
 GE0/1/6     0.0       0.0         15.4
 GE0/1/7     0.0       0.0         15.4
 GE0/1/8     0.0       0.0         15.4
 GE0/1/9     0.0       0.0         15.4
 GE0/1/10    0.0       0.0         15.4
 GE0/1/11    0.0       0.0         15.4
 GE0/1/12    0.0       0.0         15.4
 GE0/1/13    0.0       0.0         15.4
 GE0/1/14    0.0       0.0         15.4
 GE0/1/15    0.0       0.0         15.4
 GE0/1/16    0.0       0.0         15.4
 GE0/1/17    12.3      12.3        15.4
 GE0/1/18    0.0       0.0         15.4
 GE0/1/19    0.0       0.0         15.4
 GE0/1/20    0.0       0.0         15.4
 GE0/1/21    0.0       0.0         15.4
 GE0/1/22    0.0       0.0         15.4
 GE0/1/23    0.0       0.0         15.4
 GE0/1/24    0.0       0.0         15.4
 GE0/1/25    0.0       0.0         15.4
 GE0/1/26    0.0       0.0         15.4
 GE0/1/27    0.0       0.0         15.4
 GE0/1/28    0.0       0.0         15.4
 GE0/1/29    0.0       0.0         15.4
 GE0/1/30    0.0       0.0         15.4
 GE0/1/31    0.0       0.0         15.4
 GE0/1/32    0.0       0.0         15.4
 GE0/1/33    0.0       0.0         15.4
 GE0/1/34    0.0       0.0         15.4
 GE0/1/35    12.1      12.3        15.4
 GE0/1/36    0.0       0.0         15.4
 GE0/1/37    0.0       0.0         15.4
 GE0/1/38    0.0       0.0         15.4
 GE0/1/39    0.0       0.0         15.4
 GE0/1/40    0.0       0.0         15.4
 GE0/1/41    0.0       0.0         15.4
 GE0/1/42    0.0       0.0         15.4
 GE0/1/43    0.0       0.0         15.4
 GE0/1/44    0.0       0.0         15.4
 GE0/1/45    0.0       0.0         15.4
 GE0/1/46    0.0       0.0         15.4
 GE0/1/47    12.3      12.3        15.4
 GE0/1/48    0.0       0.0         15.4

  ---  4 port(s) on,    49.2 (W) consumed,   756.9 (W) remaining ---
```

Table 362 Description on fields of the display poe pse interface power command

Field	Description
Interface	Shortened form of a PoE interface
CurPower	Current power of a PoE interface

Table 362 Description on fields of the display poe pse interface power command

Field	Description
PeakPower	Peak power of a PoE interface
MaxPower	Maximum power of a PoE interface
PD Description	Description of the PD connected with a PoE interface. When the description contains more than 34 characters, the first 30 characters followed by four dots will be displayed.
Port(s) on	Number of PoE interfaces that are supplying power
consumed	Power currently consumed by all PoE interfaces
Remaining	Remaining power on the PSE

display poe-power

Syntax **display poe-power**

View Any view

Parameter None

Description Use the **display poe-power** command to display the information of the PoE power.

Example # Display the information of the PoE power.

```
<Sysname> display poe-power
 PoE Current Power           : 67       W
 PoE Average Power           : 48       W
 PoE Peak Power              : 62       W
 PoE Max Power               : 1125     W
 PoE Nominal Power           : 2250     W
 PoE Current Current         : 1.15     A
 PoE Current Voltage         : 53.96    V
 PoE Input-threshold Lower   : 90.00    V
 PoE Input-threshold Upper   : 264.00   V
 PoE Output-threshold Lower  : 47.00    V
 PoE Output-threshold Upper  : 55.00    V
 PoE Power Number            : 1
 PoE Power 1:
     Manufacturer            : Tyco electronics Com
     Type                    : PSE4500-A
     Status                  : Normal
```

Table 363 Description on fields of the display poe-power command

Field	Description
PoE Current Power	Current PoE power
PoE Average Power	Average PoE power
PoE Peak Power	Peak PoE power
PoE Max Power	Maximum PoE power
PoE Nominal Power	Nominal PoE power

Table 363 Description on fields of the display poe-power command

Field	Description
PoE Current Current	Current PoE current, with measurement precision of 1 ampere
PoE Current Voltage	Current PoE voltage
PoE Input-threshold Lower	AC input under-voltage threshold
PoE Input-threshold Upper	AC input over-voltage threshold
PoE Output-threshold Lower	DC output under-voltage threshold
PoE Output-threshold Upper	DC output over-voltage threshold
PoE Power Number	Number of PoE power supply units
PoE Power Manufacturer	Manufacturer of the PoE power
PoE Power Type	Type of the PoE power
PoE Power Status	PoE power state: ■ Normal ■ Absent ■ Off ■ Master ■ Slave ■ Balance ■ Redundant ■ Alarm ■ Faulty

display poe-power ac-input state

Syntax **display poe-power ac-input state**

View Any view

Parameter None

Description Use the **display poe-power ac-input state** command to display the state information of the AC input power

Example # Display the state information of the AC input power.

```
<Sysname> display poe-power ac-input state
 Module Number               : 1
 Output AC Current A Alarm   : Normal
 Output AC Current B Alarm   : Normal
 Output AC Current C Alarm   : Normal
 Module 1:
     Volt Phase AB Alarm     : Normal
     Volt Phase BC Alarm     : Lack Phase
     Volt Phase CA Alarm     : Normal
```

Table 364 Description on fields of the display poe-power ac-input state command

Field	Description
Module Number	Number of modules that a power supply unit contains
Output AC Current A/B/C Alarm	Output three-phase AC current state: ■ Normal: The current is normal. ■ Under Limit: The current is below the lower limit. ■ Above Limit: The current is above the upper limit. ■ Lack Phase: A phase is lost. ■ Fuse Broken: The fuse is broken. ■ Switch Off: The switch is turned off. ■ Other Error: Other faults
Volt Phase AB/BC/CA Alarm	AC voltage input state: ■ Normal: The voltage is normal. ■ Under Limit: The voltage is below the lower limit. ■ Above Limit: The voltage is above the upper limit. ■ Lack Phase: A phase is lost. ■ Fuse Broken: The fuse is broken. ■ Switch Off: The switch is turned off. ■ Other Error: Other faults

display poe-power alarm

Syntax **display poe-power alarm**

View Any view

Parameter None

Description Use the **display poe-power alarm** command to display the alarm information of the PoE power.

Example # Display the alarm information of the PoE power.

```
<Sysname> display poe-power alarm
 PSU Number                  : 3
 PSU 1 State                 : Normal
 PSU 2 State                 : Disconnect
 PSU 3 State                 : Over Voltage
                               Over Temperature
```

Table 365 Description on fields of the display poe-power alarm command

Field	Description
PSU Number	Number of power supply units

Table 365 Description on fields of the display poe-power alarm command

Field	Description
PSU x State	PSU state: ■ Normal: The PSU is normal. ■ Disconnect: The PSU is disconnected. ■ Input Error: An input error occurs to the PSU. ■ Output Error: An output error occurs to the PSU. ■ Over Voltage: An over-voltage occurs to the PSU. ■ Over Temperature: An over-temperature occurs to the PSU. ■ Fan Error: A fault occurs to the fan of the PSU. ■ Shut Down: The PSU is shut down. ■ Current Restricted: The current of the PSU is restricted.

display poe-power dc-output state

Syntax **display poe-power dc-output state**

View Any view

Parameter None

Description Use the **display poe-power dc-output state** command to display the state information of the DC output power

Example # Display the state information of the DC output power.

```
<Sysname> display poe-power dc-output state
DC Output State              : Normal
```

Table 366 Description on fields of the display poe-power dc-output state command

Field	Description
DC Output State	DC output state: ■ Normal: The output voltage is normal. ■ Under Limit: The output voltage is below the lower limit. ■ Above Limit: The output voltage is above the upper limit. ■ Fuse Broken: The output fuse is broken. ■ Switch Off: The output switch is turned off. ■ Other Error: Other faults

display poe-power dc-output value

Syntax **display poe-power dc-output value**

View Any view

Parameter None

Description Use the **display poe-power dc-output value** command to display the parameter values of the DC output power.

Example # Display the parameter values of the DC output power.

```
<Sysname> display poe-power dc-output value
 DC Output Voltage           : 54.05 V
 DC Output Current           : 0.35  A
```

Table 367 Description on fields of the display poe-power dc-output value command

Field	Description
DC Output Voltage	DC output voltage
DC Output Current	DC output current, with measurement precision of 1 ampere

display poe-power status

Syntax **display poe-power status**

View Any view

Parameter None

Description Use the **display poe-power status** command to display the status information of the PoE power.

Example # Display the status information of the PoE power.

```
<Sysname> display poe-power status
 Switch Number               : 1
 Switch 1 State               : AC Switch High Voltage
 DC Output State             : Normal
 DC Output Voltage           : 53.97    V
 DC Output Current           : 1.25     A
 Module Number               : 1
 Output AC Current A Alarm   : Normal
 Output AC Current B Alarm   : Normal
 Output AC Current C Alarm   : Normal
 Module 1:
     Volt Phase AB Alarm     : Normal
     Volt Phase BC Alarm     : Lack Phase
     Volt Phase CA Alarm     : Normal
```

Table 368 Description on fields of the display poe-power status command

Field	Description
Switch Number	Number of power switches
Switch State	State of a power switch
DC Output State	DC output state
DC Output Voltage	DC output voltage
DC Output Current	DC output current, with measurement precision of 1 ampere

Table 368 Description on fields of the display poe-power status command

Field	Description
Module Number	Number of modules that a power supply unit contains
Output AC Current A/B/C Alarm	Output three-phase AC current state: ■ Normal: The current is normal. ■ Under Limit: The current is below the lower limit. ■ Above Limit: The current is above the upper limit. ■ Lack Phase: A phase is lost. ■ Fuse Broken: The fuse is broken. ■ Switch Off: The switch is turned off. ■ Other Error: Other faults
Volt Phrase AB/BC/CA Alarm	AC voltage input state: ■ Normal: The voltage is normal. ■ Under Limit: The voltage is below the lower limit. ■ Above Limit: The voltage is above the upper limit. ■ Lack Phase: A phase is lost. ■ Fuse Broken: The fuse is broken. ■ Switch Off: The switch is turned off. ■ Other Error: Other faults

display poe-power supervision-module

Syntax **display poe-power supervision-module**

View Any view

Parameter None

Description Use the **display poe-power supervision-module** command to display the information of the monitoring module of the PoE power.

Example # Display the information of the monitoring module of the PoE power.

```
<Sysname> display poe-power supervision-module
 Supervision Version         : 2.0
 Supervision Name            : Spring Pms
 PoE Power Type              : PSE4500-A
 PoE Current Power           : 67       W
 PoE Average Power           : 48       W
 PoE Peak Power              : 62       W
 PoE Nominal Power           : 2250     W
 PSU Available Number        : 2
 PSU 1:
     Nominal Output Power    : 2500(W)(220V)/1250(W)(110V)
     Hardware Version Info   : NP 2500
 PSU 2:
     Nominal Output Power    : 2500(W)(220V)/1250(W)(110V)
     Hardware Version Info   : NP 2500
```

Table 369 Description on fields of the display poe-power supervision-module command

Field	Description
Supervision Version	Software version number of the monitoring module of the PoE power
Supervision Name	Name of the monitoring module of the PoE power
PoE Power Type	Type of the PoE power
PoE Current Power	Current consumption power
PoE Average Power	Average power
PoE Peak Power	Peak power
PoE Nominal Power	Nominal power
PSU Available Number	Number of available PSUs
Nominal Output Power	Nominal output power of a PSU
Hardware Version Info	Hardware version information of the PSU

display poe-power switch state

Syntax **display poe-power switch state**

View Any view

Parameter None

Description Use the **display poe-power switch state** command to display the switch information of the PoE power.

Example # Display the switch information of the PoE power.

```
<Sysname> display poe-power switch state
 Switch Number               : 3
 Switch 1 State              : AC Switch Off
 Switch 2 State              : AC Switch High Voltage
 Switch 3 State              : AC Switch Off
```

Table 370 Description on fields of the display poe-power switch state command

Field	Description
Switch Number	Number of power switches
State	Switch state: ■ AC Switch On: The AC switch is turned on. ■ Switch Off: The switch is turned off. ■ AC Switch High Voltage: The voltage of the AC switch is high. ■ AC Switch High Voltage: The voltage of the AC switch is low.

display poe-profile

Syntax **display poe-profile** [**index** *index* | **name** *profile-name*]

View Any view

Parameter **index** *index*: Specifies the index number of the PoE configuration file. The index number ranges from 1 to 100.

name *profile-name*: Specifies the name of the PoE configuration file. The file name consists of 1 to 15 characters.

Description Use the **display poe-profile** command to display all information of the configurations and applications of the PoE configuration file.

If no argument is specified, all information of the configurations and applications of existing PoE configuration files will be displayed.

Example # Display all information of the configurations and applications of the current PoE configuration file.

```
<Sysname> display poe-profile
 Poe-profile     Index   ApplyNum  Interface   Configuration
 x               1       1         GE0/1/2     poe enable
                                               poe max-power 12000

 ---  1 poe-profile(s) created, 1 port(s) applied  ---
```

Table 371 Description on fields of the display poe-profile command

Field	Description
Poe-profile	Name of the PoE configuration file
Index	Index number of the PoE configuration file
ApplyNum	Number of PoE interfaces to which a PoE configuration file is applied
Interface	Shortened form of the PoE interface to which the PoE configuration is applied
Configuration	Configurations of the PoE configuration file
poe-profile(s) created	Number of PoE configuration files
port(s) applied	Sum of the number of PoE interfaces to which all PoE configuration files are respectively applied

Display all information of the configurations and applications of the PoE configuration file whose index number is 1.

```
<Sysname> display poe-profile index 1
 Poe-profile      Index  ApplyNum    Interface   Configuration
 AA3456789012345  1      2           GE1/1/2     poe enable
                                     GE1/1/4     poe priority critical
                                                 poe max-power 12300
---  2 port(s) applied  ---
```

Table 372 Description on fields of the display poe-profile index command

Field	Description
Poe-profile	Name of the PoE configuration file
Index	Index number of the PoE configuration file
ApplyNum	Number of PoE interfaces to which a PoE configuration file is applied
Interface	Shortened form of the PoE interface to which the PoE configuration is applied
Configuration	Configurations of the PoE configuration file
port(s) applied	Sum of the number of PoE interfaces to which all PoE configuration files are respectively applied

Display all information of the configurations and applications of the PoE configuration file named AA.

```
<Sysname> display poe-profile name AA
 Poe-profile      Index  ApplyNum  Interface  Configuration
 AA               1      2         GE1/1/1    poe enable
                                   GE1/1/2    poe priority critical
                                              poe max-power 12300
---  2 port(s) applied  ---
```

Table 373 Description on fields of the display poe-profile name command

Field	Description
Poe-profile	Name of the PoE configuration file
Index	Index number of the PoE configuration file
ApplyNum	Number of PoE interfaces to which a PoE configuration file is applied
Interface	Shortened form of the PoE interface to which the PoE configuration is applied
Configuration	Configurations of the PoE configuration file
port(s) applied	Sum of the number of PoE interfaces to which all PoE configuration files are respectively applied

display poe-profile interface

Syntax **display poe-profile interface** *interface-type interface-number*

View Any view

Parameter *interface-type interface-number*: Interface type and interface number.

Description Use the **display poe-profile interface** command to display all information of the configurations and applications of the PoE configuration file that currently take effect on the specified PoE interface.

Example # Display all information of the configurations and applications of the current PoE configuration file applied to GigabitEthernet1/1/1.

```
<Sysname> display poe-profile interface GigabitEthernet 1/1/1
Poe-profile      Index  ApplyNum   Interface     Current Configuration
AA3456789012345  1      2          GE1/1/1       poe enable
                                                 poe priority critical
```

Table 374 Description on fields of the display poe-profile interface command

Field	Description
Poe-profile	Name of the PoE configuration file
Index	Index number of the PoE configuration file
ApplyNum	Number of PoE interfaces to which the PoE configuration file is applied
Interface	Shortened form of the PoE interface to which the PoE configuration is applied
Current Configuration	Configurations of the PoE configuration file that currently take effect on a PoE interface

Because not all the configurations of a PoE configuration file are applied successfully, only the configurations that currently take effect on the interface are displayed.

poe enable

Syntax **poe enable**

undo poe enable

View PoE interface view/PoE-profile file view

Parameter None

Description Use the **poe enable** command to enable PoE on a PoE interface.

Use the **undo poe enable** command to disable PoE on a PoE interface.

By default, PoE is disabled on a PoE interface.

Example # Enable PoE on a PoE interface.

```
<Sysname> system-view
[Sysname] interface gigabitEthernet 1/1/1
[Sysname-GigabitEthernet1/1/1] poe enable
```

Enable PoE through a PoE configuration file on a PoE interface.

```
<Sysname> system-view
[Sysname] poe-profile abc
[Sysname-poe-profile-abc-1] poe enable
[Sysname-poe-profile-abc-1] quit
[Sysname] interface gigabitEthernet 1/1/1
[Sysname-GigabitEthernet1/1/1] apply poe-profile name abc
```

poe enable pse

Syntax **poe enable pse** *pse-id*

undo poe enable pse *pse-id*

View System view

Parameter *pse-id*: PSE ID. The relation between the ID and the slot number of a PSE is: PSE ID = SlotNo x 3 + 1.

Description Use the **poe enable pse** command to enable PoE for the PSE.

Use the **undo poe enable pse** command to disable PoE for the PSE.

By default, PoE is disabled for the PSE.

Example # Enable PoE for PSE 10.

```
<Sysname> system-view
[Sysname] poe enable pse 10
```

poe legacy enable pse

Syntax **poe legacy enable pse** *pse-id*

undo poe legacy enable pse *pse-id*

View System view

Parameter *pse-id*: PSE ID. The relation between the ID and the slot number of a PSE is: PSE ID = SlotNo x 3 + 1.

Description Use the **poe legacy enable** command to enable the PSE to detect nonstandard PDs.

Use the **undo poe legacy enable** command to disable the PSE from detecting nonstandard PDs.

By default, the PSE is disabled from detecting nonstandard PDs.

Example # Enable PSE 10 to detect nonstandard PDs.

```
<Sysname> system-view
[Sysname] poe legacy enable pse 10
```

poe max-power (PoE interface view/PoE-profile file view)

Syntax **poe max-power** *max-power*

undo poe max-power

View PoE interface view/PoE-profile file view

Parameter *max-power*: Maximum power in milliwatts allocated to a PoE interface, ranging from 3000 to 15400.

Description Use the **poe max-power** command to configure the maximum power for a PoE interface.

Use the **undo poe max-power** command to restore the default maximum power of a PoE interface.

By default, the maximum power of the PoE interface is 15,400 milliwatts.

Example # Set the maximum power of Ethernet1/0 to 12,000 milliwatts.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 3/1/1
[Sysname-GigabitEthernet3/1/1] poe max-power 12000
```

Set the maximum power of Ethernet1/0 to 12,000 milliwatts through a PoE configuration file.

```
<Sysname> system-view
[Sysname] poe-profile abc
[Sysname-poe-profile-abc-1] poe max-power 12000
[Sysname-poe-profile-abc-1] quit
[Sysname] interface GigabitEthernet 3/1/1
[Sysname-GigabitEthernet3/1/1] apply poe-profile name abc
```

poe max-power (system view)

Syntax **poe max-power** *max-power* **pse** *pse-id*

undo poe max-power pse *pse-id*

View System view

Parameter *max-power*: Maximum power in watts of the PSE, ranging from 37 to 806.

pse-id: PSE ID. The relation between the ID and the slot number of a PSE is: PSE ID = SlotNo x 3 + 1.

Description Use the **poe max-power** command to configure the maximum power for the PSE.

Use the **undo poe max-power** command to restore the default maximum power of the PSE.

The default maximum power of a PSE is 806 watts.

Note that:

- The maximum power of the PSE must be greater than or equal to the sum of the maximum power of all critical PoE interfaces on the PSE so as to guarantee the power supply to these PoE interfaces. When the consumption power of all PDs connected to the PSE is greater than the maximum power of the PSE, some PDs will be powered off.
- The sum of the maximum power of all PSEs must be less than the maximum PoE power.

Related command: **poe priority (system view)**.

Example # Set the maximum power of PSE 10 to 150 watts.

```
<Sysname> system-view
[Sysname] poe max-power 150 pse 10
```

poe mode

Syntax **poe mode signal**

undo poe mode

View PoE interface view/PoE-profile file view

Parameter **signal**: Specifies the PoE mode as **signal** (powering over signal cables).

Description Use the **poe mode** command to configure a PoE mode.

Use the **undo poe mode** command to restore the default PoE mode.

By default, the PoE mode is **signal** (powering over signal cables).

Example # Set the PoE mode to **signal** (powering over signal cables).

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/1/1
[Sysname-GigabitEthernet1/1/1] poe mode signal
```

Set the PoE mode to **signal** (powering over signal cables) through a PoE configuration file.

```
<Sysname> system-view
[Sysname] poe-profile abc
[Sysname-poe-profile-abc-1] poe mode signal
[Sysname-poe-profile-abc-1] quit
```

```
[Sysname] interface GigabitEthernet 1/1/1
[Sysname-GigabitEthernet1/1/1] apply poe-profile name abc
```

poe pd-description

Syntax **poe pd-description** *string*

undo poe pd-description

View PoE interface view

Parameter *string*: Description of the PD connected to a PoE interface, up to 80 characters.

Description Use the **poe pd-description** command to configure a description for the PD connected to a PoE interface.

Use the **undo poe pd-description** command to remove the description of the PD connected to a PoE interface.

By default, no description is configured.

Example # Describe the PD connected to Ethernet1/0 as IP Phone For Room 101.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet3/1/1
[Sysname-GigabitEthernet3/1/1] poe pd-description IP Phone For Room 101
```

poe pd-policy priority

Syntax **poe pd-policy priority**

undo poe pd-policy priority

View System view

Parameter None

Description Use the **poe pd-policy priority** command to configure a PD power management priority policy.

Use the **undo poe pd-policy priority** command to remove the PD power management priority policy.

By default, no PD power management priority policy is configured.

Example # Configure a PD power management priority policy

```
<Sysname> system-view
[Sysname] poe pd-policy priority
```

poe power max-value

Syntax **poe power max-value** *max-power*

undo poe power max-value

View System view

Parameter *max-power*: Maximum PoE power, namely, maximum power that the device can provide for all PSEs. In consideration of the transient peak power effect, the actual maximum power is 5% higher than the configured one. In the case of 220 VAC input, when the switch uses single or dual power supply modules, you can set at most 2250 W as the maximum PoE power; when the switch uses triple power modules, you can set at most 4500 W as the maximum PoE power. In the case of 110 VAC input, when the switch uses single or dual power supply modules, you can set at most 1125 W as the maximum PoE power; when the switch uses triple power modules, you can set at most 2250 W as the maximum PoE power.

Description Use the **poe power max-value** command to configure the maximum PoE power.

Use the **undo poe power max-value** command to restore the default maximum PoE power.

The default maximum PoE power is 1125 for 220 VAC input and 562 for 110 VAC input.

Note that the configured maximum PoE power cannot exceed the rated PoE power.

Example # Set the maximum PoE power to 2,000 watts for the device.

```
<Sysname> system-view
[Sysname] poe power max-value 2000
```

poe priority (PoE interface view/PoE-profile file view)

Syntax **poe priority** { **critical** | **high** | **low** }

undo poe priority

View PoE interface view/PoE-profile file view

Parameter **critical**: Sets the power priority of a PoE interface to **critical**. The PoE interface whose power priority level is **critical** works in guaranteed mode, that is, power is first supplied to the PD connected to this critical PoE interface.

high: Sets the power priority of a PoE interface to **high**.

low: Sets the power priority of a PoE interface to **low**.

Description Use the **poe priority** command to configure a power priority level for a PoE interface.

Use the **undo poe priority** command to restore the default power priority level.

By default, the power priority of a PoE interface is **low**.

CAUTION:

- *When the PoE power is insufficient, power is first supplied to PoE interfaces with a higher priority level.*
- *If a PoE configuration file is already applied to a PoE interface, you need to remove the application of the file to the PoE interface before configuring the interface in PoE-profile view.*
- *If a PoE configuration file is applied to a PoE interface, you need to remove the application of the file to the PoE interface before configuring the interface in PoE interface view.*
- *If two PoE interfaces have the same priority level, the PoE interface with a smaller ID takes precedence over the other one. The priority levels of any two PoE interfaces are comparable only when the two interfaces are on the same PSE.*

Example # Set the power priority of Ethernet1/0 to **critical**.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/1/1
[Sysname-GigabitEthernet1/1/1] poe priority critical
```

Set the power priority of Ethernet1/0 to **critical** through a PoE configuration file.

```
<Sysname> system-view
[Sysname] poe-profile abc
[Sysname-poe-profile-abc-1] poe priority critical
[Sysname-poe-profile-abc-1] quit
[Sysname] interface GigabitEthernet 1/1/1
[Sysname-GigabitEthernet1/1/1] apply poe-profile name abc
```

poe priority (system view)

Syntax **poe priority** { **critical** | **high** | **low** } **pse** *pse-id*

undo poe priority pse *pse-id*

View System view

Parameter **critical**: Sets the power priority level of the PSE to **critical**. The PSE whose power priority level is **critical** works in guaranteed mode, that is, power is first supplied to the PSE.

high: Sets the power priority of the PSE to **high**.

low: Sets the power priority of the PSE to **low**.

pse-id: PSE ID. The relation between the ID and the slot number of a PSE is: PSE ID = SlotNo x 3 + 1.

Description Use the **poe priority** command to configure a power priority level for the PSE.

Use the **undo poe priority** command to restore the default power priority level of the PSE.

By default, the power priority level of the PSE is **low**.

When the PoE power is insufficient, power is first supplied to PSE with a higher power priority level.

Example # Set the power priority of PSE 10 to critical.

```
<Sysname> system-view
[Sysname] poe priority critical pse 10
```

poe pse-policy priority

Syntax **poe pse-policy priority**

undo poe pse-policy priority

View System view

Parameter None

Description Use the **poe pse-policy priority** command to configure a PSE power management priority policy.

Use the **undo poe pse-policy priority** command to remove the PSE power management priority policy.

By default, no PSE power management priority policy is configured.

Example # Configure a PSE power management priority policy.

```
<Sysname> system-view
[Sysname] poe pse-policy priority
```

poe utilization-threshold

Syntax **poe utilization-threshold** *utilization-threshold-value* **pse** *pse-id*

undo poe utilization-threshold pse *pse-id*

View System view

Parameter *utilization-threshold-value*: Power alarm threshold in percentage, in the range of 1 to 99.

pse-id: PSE ID. The relation between the ID and the slot number of a PSE is: PSE ID = SlotNo x 3 + 1.

Description Use the **poe utilization-threshold** command to configure a power alarm threshold for the PSE.

Use the **undo poe utilization-threshold** command to restore the default power alarm threshold of the PSE.

By default, the power alarm threshold for the PSE is 80%.

CAUTION: *The system will send a Trap message when the percentage of power utilization exceeds the alarm threshold. If the percentage of the power utilization always keeps above the alarm threshold, the system will not send any Trap message. Instead, when the percentage of the power utilization drops below the alarm threshold, the system will send a Trap message again.*

Example # Set the power alarm threshold of PSE 10 to 90%.

```
<Sysname> system-view
[Sysname] poe utilization-threshold 90 pse 10
```

poe-power input-threshold

Syntax **poe-power input-threshold** { **lower** | **upper** } *value*

undo poe-power input-threshold { **lower** | **upper** }

View System view

Parameter **lower** *value*: Specifies an under-voltage threshold in volts. The recommended under-voltage threshold is 181 for 220 VAC input and 90 for 110 VAC input. For the Switch 8800 Family, the default value equals the recommended value.

upper *value*: Specifies an over-voltage threshold in volts. The recommended over-voltage threshold is 264 for 220 VAC input and 132 for 110 VAC input. For the Switch 8800 Family, the default value equals the recommended value.

Description Use the **poe-power input-threshold** command to configure an AC input under-voltage/over-voltage threshold.

Use the **undo poe-power input-threshold** command to restore the default AC input under-voltage/over-voltage threshold.

Example # Set the AC input under-voltage threshold to 181.00 V.

```
<Sysname> system-view
[Sysname] poe-power input-threshold lower 181.00
```

Set the AC input over-voltage threshold to 264.0 V.

```
<Sysname> system-view
[Sysname] poe-power input-threshold upper 264.0
```

poe-power output-threshold

Syntax **poe-power output-threshold** { **lower** *value* | **upper** *value* }

undo poe-power output-threshold { **lower** | **upper** }

View System view

Parameter **lower** *value*: Specifies an under-voltage threshold in volts. The recommended under-voltage threshold is 45 for both 220 VAC input and 110 VAC input. For the Switch 8800 Family, the default value equals the recommended value.

upper *value*: Specifies an over-voltage threshold in volts. The recommended over-voltage threshold is 57 for both 220 VAC input and 110 VAC input. For the Switch 8800 Family, the default value equals the recommended value.

Description Use the **poe-power output-threshold** command to configure a DC output under-voltage/over-voltage threshold.

Use the **undo poe-power output-threshold** command to restore the default DC output under-voltage/over-voltage threshold.

Example # Set a DC output under-voltage threshold to 45 V.

```
<Sysname> system-view
[Sysname] poe-power output-threshold lower 45
```

Set a DC output over-voltage threshold to 57 V.

```
<Sysname> system-view
[Sysname] poe-power output-threshold upper 57
```

poe-profile

Syntax **poe-profile** *profile-name* [*index*]

undo poe-profile { **index** *index* | **name** *profile-name* }

View System view

Parameter *profile-name*: Name of a PoE configuration file, a string of 1 to 15 characters. A PoE configuration file name begins with a letter (a through z or A through Z) and must not contain reserved keywords such as **undo**, **all**, **name**, **interface**, **user**, **poe**, **disable**, **max-power**, **mode**, **priority** and **enable**.

index: Index number of a PoE configuration file, in the range of 1 to 100.

Description Use the **poe-profile** *profile-name* command to create a PoE configuration file and enter PoE-profile view.

Use the **undo poe-profile** command to delete the specified PoE configuration file.

If no index is specified, the system will automatically assign an index to the PoE configuration file, starting from 1.

CAUTION: *If a PoE configuration file is already applied to a PoE interface, you cannot delete it. To delete the file, you must first execute the* ***undo apply poe-profile*** *command to remove the application of the PoE configuration file to the PoE interface.*

Example # Create a PoE configuration file named ABC without specifying an index.

```
<Sysname> system-view
[Sysname] poe-profile ABC
```

Create a PoE configuration file named abc with index 3.

```
<Sysname> system-view
[Sysname] poe-profile abc 3
```

85 SYSTEM MAINTENANCE COMMANDS

ping

Syntax **ping** [**ip**] [**-a** *source-ip* | **-c** *count* | **-f** | **-h** *ttl* | **-i** *interface-type interface-number* | **-m** *interval* | **-n** | **-p** *pad* | **-q** | **-r** | **-s** *packet-size* | **-t** *timeout* | **-tos** *tos* | **-v** | **-vpn-instance** *vpn-instance-name*] * *remote-system*

View Any view

Parameter **ip**: Supports IPv4 protocol.

-a *source-ip*: Specifies the source IP address of an ICMP echo request. It must be a legal IP address configured on the device.

-c *count*: Specifies the number of times that an ICMP echo request is sent, in the range 1 to 4294967295. The default value is 5.

-f: Discards packets larger than the MTU of a given interface, that is, the ICMP echo request is not allowed to be fragmented.

-h *ttl*: Specifies the TTL value for an ICMP echo request, in the range 1 to 255. The default value is 255.

-i *interface-type interface-number*: Specifies the ICMP echo request sending interface by its type and number.

-m *interval*: Specifies the interval (in milliseconds) to send an ICMP echo response, in the range 1 to 65535. The default value is 200 ms.

- If a response from the destination is received within the timeout time, the interval to send the next echo request equals the actual response period plus the value of *interval*.
- If no response from the destination is received within the timeout time, the interval to send the next echo request equals the *timeout* value plus the value of *interval.*

-n: Specifies that the Domain Name System (DNS) is disabled. DNS is enabled by default, that is, the *hostname* is translated into an address.

-p *pad*: Specifies the padded bytes in an ICMP echo request, in hexadecimal format. For example, if *pad* is configured as ff, then the packets will be padded with ff. By default, the padded bytes start from 0x01 up to 0x09, where another round starts again if necessary.

-q: Presence of this parameter indicates that only statistics are displayed. By default, all information is displayed.

-r: Records routes. By default, routes are not recorded.

-s *packet-size*: Specifies length (in bytes) of an ICMP echo request, in the range 20 to 8100. The default value is 56.

-t *timeout*: Specifies the timeout value (in milliseconds) of an ICMP echo request, in the range 1 to 65535. It defaults to 2000.

-tos *tos*: Specifies type of service (ToS) of an echo request, in the range 0 to 255. The default value is 0.

-v: Displays non ICMP echo reply received. By default, the system does not display non ICMP echo reply.

-vpn-instance *vpn-instance-name*: Specifies the name of an MPLS VPN instance, which is a string of 1 to 31 characters. It is case insensitive.

remote-system: IP address or host name (a string of 1 to 20 characters) of the destination device.

Description Use the **ping** command to verify whether the destination device in an IP network is reachable, and to display the related statistics.

Note that:

- You must use the command in the form of **ping ip** *ip* instead of **ping** *ip* if the destination name is a key word, such as **ip**.
- Only the directly connected segment address can be pinged if the outgoing interface is specified with the **-i** argument.

Example # Check whether the device with an IP address of 10.1.1.5 is reachable.

```
<Sysname> ping 10.1.1.5
PING 10.1.1.5 : 56 data bytes, press CTRL_C to break
Reply from 10.1.1.5 : bytes=56 Sequence=1 ttl=255 time = 1 ms
Reply from 10.1.1.5 : bytes=56 Sequence=2 ttl=255 time = 2 ms
Reply from 10.1.1.5 : bytes=56 Sequence=3 ttl=255 time = 1 ms
Reply from 10.1.1.5 : bytes=56 Sequence=4 ttl=255 time = 3 ms
Reply from 10.1.1.5 : bytes=56 Sequence=5 ttl=255 time = 2 ms

--- 10.1.1.5 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 1/2/3 ms
```

ping ipv6

Syntax **ping ipv6** [**-a** *source-ipv6* | **-c** *count* | **-m** *interval* | **-s** *packet-size* | **-t** *timeout*] * *remote-system* [**-i** *interface-type interface-number*]

View Any view

Parameter **-a** *source-ipv6*: Specifies the source IPv6 address of an ICMP echo request. It must be a legal IPv6 address configured on the device.

-c *count*: Specifies the number of times that an ICMPv6 echo request is sent, in the range 1 to 4294967295. The default value is 5.

-m *interval*: Specifies the interval (in milliseconds) to send an ICMPv6 echo request, in the range 1 to 65535. The default value is 200 ms.

- If a response from the destination is received within the timeout time, the interval to send the next echo request equals the actual response period plus the value of *interval.*
- If no response from the destination is received within the timeout time, the interval to send the next echo request equals the *timeout* value plus the value of *interval.*

-s *packet-size*: Specifies length (in bytes) of an ICMPv6 echo request, in the range 20 to 8100. It defaults to 56.

-t *timeout*: Specifies the timeout value (in milliseconds) of an ICMPv6 echo request, in the range 1 to 65535. It defaults to 2000.

remote-system: IPv6 address or host name (a string of 1 to 46 characters) of the destination device.

-i *interface-type interface-number*: Specifies an outgoing interface by its type and number. This parameter can be used only in case that the destination address is the link local address and the specified outgoing interface must have a link local address (For the configuration of link local address, see "IPv6 Basics Configuration Commands" on page 283.

Description Use the **ping ipv6** command to verify whether an IPv6 address is reachable, and display the corresponding statistics.

You must use the command in the form of **ping ipv6** *ipv6* instead of **ping** *ipv6* if the destination name is an ipv6 name.

Example # Verify whether the IPv6 address 2001::1 is reachable.

```
<Sysname> ping ipv6 2001::1
  PING 2001::1 : 56  data bytes, press CTRL_C to break
  Reply from 2001::1  bytes=56 Sequence=1 hop limit=64  time = 20 ms
  Reply from 2001::1  bytes=56 Sequence=2 hop limit=64  time = 0 ms
  Reply from 2001::1  bytes=56 Sequence=3 hop limit=64  time = 0 ms
  Reply from 2001::1  bytes=56 Sequence=4 hop limit=64  time = 0 ms
  Reply from 2001::1  bytes=56 Sequence=5 hop limit=64  time = 0 ms

  --- 2001::1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
round-trip min/avg/max = 0/4/20 ms
```

The "hop limit" field in this prompt information has the same meaning as the "ttl" field in the prompt information displayed by the IPv4 **ping** command, indicating the TTL value in the ICMPv6 echo request.

tracert

Syntax **tracert** [**-a** *source-ip* | **-f** *first-ttl* | **-m** *max-ttl* | **-p** *port* | **-q** *packet-number* | **-vpn-instance** *vpn-instance-name* | **-w** *timeout*] * *remote-system*

View Any view

Parameter **-a** *source-ip*: Specifies the source IP address of a tracert packet. It must be a legal IP address configured on the device.

-f *first-ttl*: Specifies the first TTL, that is, the allowed number of hops for the first packet, in the range 1 to 255. It defaults to 1 and must be less than the maximum TTL.

-m *max-ttl*: Specifies the maximum TTL, that is, the maximum allowed number of hops for a packet, in the range 1 to 255. It defaults to 30, and must be greater than the first TTL.

-p *port*: Specifies the UDP port number of the destination device, in the range 1 to 65535. The default value is 33434. You do not need to modify this parameter.

-q *packet-number*: Specifies the number of probe packets sent each time, in the range 1 to 65535. The default value is 3.

-vpn-instance *vpn-instance-name*: Specifies the name of an MPLS VPN instance, which is a string of 1 to 31 characters.

-w *timeout*: Specifies the packet timeout time, in the range 1 to 65535, in milliseconds. The default value is 5000 ms.

remote-system: IP address or host name (a string of 1 to 20 characters) of the destination device.

Description Use the **tracert** command to trace the routers the packets traverse from the source to the destination device.

After having identified network failure with the **ping** command, you can use the **tracert** command to determine the failed node(s).

Output information of the **tracert** command includes IP addresses of all the switches the packets traverse from the source to the destination device. If a switch times out, * * * will be displayed.

Example # Display the routers the packets traverse from the current device, with an IP address of 8.26.0.115, to the destination device.

```
<Sysname> tracert 18.26.0.115
traceroute to 18.26.0.115(18.26.0.115) 30 hops max,40 bytes packet,
```

```
press CTRL_C to break
1  128.3.112.1  10 ms 10 ms 10 ms
2  128.32.210.1  19 ms 19 ms 19 ms
3  128.32.216.1  39 ms 19 ms 19 ms
4  128.32.136.23  19 ms 39 ms 39 ms
5  128.32.168.22  20 ms 39 ms 39 ms
6  128.32.197.4  59 ms 119 ms 39 ms
7  131.119.2.5  59 ms 59 ms 39 ms
8  129.140.70.13  80 ms 79 ms 99 ms
9  129.140.71.6  139 ms 139 ms 159 ms
10  129.140.81.7  199 ms 180 ms 300 ms
11  129.140.72.17  300 ms 239 ms 239 ms
12  * * *
13  128.121.54.72  259 ms 499 ms 279 ms
14  * * *
15  * * *
16  * * *
17  * * *
18  18.26.0.115  339 ms 279 ms 279 ms
```

tracert ipv6

Syntax **tracert ipv6** [**-f** *first-ttl* | **-m** *max-ttl* | **-p** *port* | **-q** *packet-number* | **-w** *timeout*] * *remote-system*

View Any view

Parameter **-f** *first-ttl*: Specifies the first TTL, that is, the allowed number of hops for the first packet, in the range 1 to 255. It defaults to 1 and must be less than the maximum TTL.

-m *max-ttl*: Specifies the maximum TTL, that is, the maximum allowed number of hops for a packet, in the range 1 to 255. It defaults to 30 and must be greater than the first TTL.

-p *port*: Specifies the UDP port number of the destination device, in the range 1 to 65535. The default value is 33434. It is unnecessary to modify this parameter.

-q *packet-number*: Specifies the number of probe packets sent each time, in the range 1 to 65535, defaulting to 3.

-w *timeout*: Specifies the timeout time of the probe packets, in the range 1 to 65535, in milliseconds. The default value is 5000 ms.

remote-system: IPv6 address or host name (a string of 1 to 46 characters) of the destination device.

Description Use the **tracert ipv6** command to view the routers the IPv6 packets traverse from the source to the destination device.

Example # View the routes involved for packets to travel from the source to the destination with IPv6 address 3002::1.

```
<Sysname> tracert ipv6 3002::1
 traceroute to 3002::1  30 hops max,60 bytes packet
 1 3003::1 30 ms 10 ms 10 ms
 2 3002::1 10 ms 11 ms 9 ms
```

86 SYSTEM DEBUGGING COMMANDS

debugging

Syntax **debugging** { **all** [**timeout** *time*] | *module-name* [*option*] }

undo debugging { **all** | *module-name* [*option*] }

View User view

Parameter all: All debugging functions.

timeout *time*: Specifies the timeout time for the **debugging all** command. When all debugging is enabled, the system automatically executes the **undo debugging all** command after the *time.* The value ranges from 1 to 1440, in minutes.

module-name: Module name, such as ARP or ATM. You can use the **debugging ?** command to display the current module name.

option: Specifies the debugging option for a specific module. Different modules have different debugging options in terms of their number and content. You can use the **debugging** *module-name* **?** command to display the currently supported options.

Description Use the **debugging** command to enable the debugging of a specific module.

Use the **undo debugging** command to disable the debugging of a specific module.

By default, debugging functions of all modules are disabled.

Note the following:

- This command is intended for network administrators to diagnose network failure.
- Output of the debugging information may degrade system efficiency, especially during the execution of the **debugging all** command. Therefore, use the command with caution.
- After finishing debugging, you can use the **undo debugging all** command to disable all the debugging functions.
- You must configure the **debugging**, **terminal debugging** and **terminal monitor** commands first to display detailed debugging information on the terminal. For the detailed description on the **terminal debugging** and

terminal monitor commands, refer to "Information Center Configuration Commands" on page 1445.

Related command: **display debugging**.

Example # Enable IP packet debugging.

```
<Sysname> debugging ip packet
```

display debugging

Syntax **display debugging** [**interface** *interface-type interface-number*] [*module-name*]

View Any view

Parameter *interface-type interface-number*: Specifies an interface by its type and number.

module-name: Module name.

Description Use the **display debugging** command to display enabled debugging functions.

Related command: **debugging**.

Example # Display all enabled debugging functions.

```
<Sysname> display debugging
IP packet debugging is on
```

display lpu fiber-module

Syntax **display lpu fiber-module** [*interface-type interface-number*]

View Any view

Parameter *interface-type*: Interface type.

interface-number: Interface number.

Description Use the **display lpu fiber-module** command to display information about all the optical modules connected to the optical interfaces of the current switch. The information includes: module information, optical module type, connector type, vendor name, part number, single/multiple mode, wave length, and transmission distance, and so on.

Use the **display fiber-module** [*interface-type interface-number*] command to display information about the optical module on the specified interface.

*This command is not available if the command level of the current login user is **access**. For related content, refer to the **user privilege level** command on page 84.*

Example # Display information about all the optical modules connected to the optical interfaces of the current switch.

```
<SW8800> display fiber-module
GigabitEthernet4/2/2:
Card info: 1000BASE-SFP
Fiber connect: LC
VendorName: DELTA
PartNumber: LCP-1250B4QS
SerialNumber: 0000051504100049
Mode: SingleMode
WaveLength: 1310nm
Length for 9um: 10km
```

Table 375 Field descriptions of the display fiber-module command.

Field	Description
GigabitEthernet4/2/2	The optical interface where the optical module resides
Card info	Optical interface information
Fiber connect	Fiber connector type
PartNumber	Part number of the optical module
SerialNumber	Serial number of the optical module
Mode	Single or multiple mode of the fiber connected
Length for X um: Y km/m	The transmission distance is Y km/m over the X um fiber.

87 FILE SYSTEM MANAGEMENT COMMANDS

Throughout this document, a filename can be entered as either of the following:

- *A fully qualified filename with the path included to indicate a file under a specific path. The filename can be 1 to 135 characters in length.*
- *A short filename with the path excluded to indicate a file in the current working path. The filename can be 1 to 91 characters in length.*

cd (User view)

Syntax **cd** *directory*

View User view

Parameter *directory*: Name of the target directory.

Description Use the **cd** command to change the current directory.

Example # Change the current directory to flash:.

```
<Sysname> cd flash:
```

copy (User view)

Syntax **copy** *fileurl-source fileurl-dest*

View User view

Parameter *fileurl-source*: Name of the source file.

fileurl-dest: Name of the target file.

Description Use the **copy** command to copy a file.

If the name of the target file is the same with the name of an existing file, the system asks whether to overwrite the existing one.

Example # Copy file config.cfg and save it as tt.cfg.

```
<Sysname> copy config.cfg tt.cfg
Copy flash:/config.cfg to flash:/tt.cfg?[Y/N]:y
```

```
%Copy file flash:/config.cfg to flash:/tt.cfg...Done.
```

delete (User view)

Syntax **delete** [**/unreserved**] *file-url*

View User view

Parameter **/unreserved**: Permanently deletes the specified file, and the deleted file can never be restored.

file-url: Name of the file to be deleted. Asterisks (*) are acceptable as wildcards. For example, to remove files with the expansion of txt, you may use the **delete *.**txt command.

Description Use the **delete** command to remove a specified file from the storage device permanently (with the **/unreserved** keyword specified) or to the recycle bin (without the **/unreserved** keyword specified), where you can restore the file with the **undelete** command or permanently delete it with the **reset recycle-bin** command.

The **dir /all** command displays the files removed to the recycle bin. These files are enclosed in pairs of brackets.

This command supports the wildcard *.

CAUTION: *If you delete two files in different directories but with the same filename, only the last one is retained in the recycle bin.*

Example # Remove the file tt.cfg from the root directory.

```
<Sysname> delete tt.cfg
Delete flash:/tt.cfg?[Y/N]:y

%Delete file flash:/tt.cfg...Done.
```

dir (User view)

Syntax **dir** [**/all** | *file-url*]

View User view

Parameter **/all**: Displays all files (including those in the recycle bin).

file-url: Name of the file or directory to be displayed. Asterisks (*) are acceptable as wildcards. For example, to display files with the .txt extension under the current directory, you may use the **dir ***.txt command.

Description Use the **dir** command to display information about all visible files and folders in the current directory.

Use the **dir /all** command to display information about all files and folders on your device, including hidden files, hidden subfiles and those in the recycle bin. The names of these deleted files are enclosed in pairs of brackets ([ ]).

The **dir** *file-url* command displays information about a file or folder.

This command supports the wildcard *.

Example # Display information about all files and folders.

```
<Sysname> dir /all
Directory of flash:/

   0   drw-          -  May 08 2006 21:27:24   hafile
   1   -rw-        248  May 08 2006 21:40:44   manuinfo.txt
   2   -rw-        118  Jun 16 2006 10:16:05   ls.pwd
   3   -rw-       3530  Oct 16 2006 16:39:53   config.cfg
   4   -rw-     326944  Jul 24 2006 14:03:04   lsbSRP1N43202.app
   5   -rw-     207624  Jul 07 2006 14:27:30   lsblmcua0110y.app
   6   -rw-     326944  Jul 07 2006 11:05:39   srpbt.app
   7   -rw-     326944  Jul 10 2006 10:40:42   switch.app
15621 KB total (14363 KB free)
```

[ ] indicates this file is in the recycle bin.

execute (User view)

Syntax **execute** *filename*

View System view

Parameter *filename*: Name of a batch file with a .bat extension.

Description Use the **execute** command to execute the specified batch file.

Batch files are command line files. Executing a batch file is to execute a set of command lines in the file.

You should not include invisible characters in a batch file. If an invisible character is found during the execution, the batch process will abort and the commands that have been executed cannot be cancelled.

Not every command in a batch file is sure to be executed. For example, if a certain command is not correctly configured, the system omits this command and goes to the next one.

A batch file does not support hot backup.

Each configuration command in a batch file must be a standard configuration command, meaning the valid configuration information which can be displayed

with the **display current-configuration** command after this command is configured successfully; otherwise, this command may not be executed correctly.

Example # Execute the batch file test.bat in the root directory.

```
<Sysname> system-view
[Sysname] execute test.bat
```

file prompt

Syntax **file prompt** { **alert** | **quiet** }

View System view

Parameter **alert**: Enables the system to warn you about operations that may bring undesirable results such as file corruption or data loss.

quiet: Disables the system to warn you about any operation.

Description Use the **file prompt** command to set a prompt mode for file operations.

By default, the prompt mode is **alert**.

Note that when the prompt mode is set to **quiet**, the system does not warn for any file operation. To prevent undesirable consequents resulted from misoperations, the **alert** mode is preferred.

Example # Set the file operation prompt mode to **alert**.

```
<Sysname> system-view
[Sysname] file prompt alert
```

fixdisk (User view)

Syntax **fixdisk** *device*

View User view

Parameter *device*: Storage device name.

Description Use the **fixdisk** command to restore the space of a storage device when it becomes unavailable because of some abnormal operation.

Example # Restore the space of the Flash.

```
<Sysname> fixdisk flash:
```

format (User view)

Syntax **format** *device*

View User view

Parameter *device*: Storage device name.

Description Use the **format** command to format a storage device.

CAUTION: *Formatting a device results in loss of all the files and these files cannot be restored. In particular, if there is startup configuration file on a storage device, formatting the storage device results in loss of the startup configuration file. Execute this command on the directions of the technical support switch fabricers.*

Example # Format the Flash.

```
<Sysname> format flash:
All data on flash: will be lost, proceed with format ? [Y/N]:y
./
%Format flash: completed.
```

mkdir (User view)

Syntax **mkdir** *directory*

View User view

Parameter *directory*: Name of a directory.

Description Use the **mkdir** command to create a subdirectory under the specified directory on the storage device.

The name of the subdirectory to be created must be unique under the specified directory.

This command does not allow you to create multiple directory levels at one time. For instance, to create a subdirectory "flash:/test/mytest", the test directory must have been created.

Example # Create a directory named dd.

```
<Sysname> mkdir dd
% Created dir flash:/dd
```

Create a subdirectory named **mytest** under test.

```
<Sysname>mkdir test/mytest
%Created dir flash:/test/mytest
```

more (User view)

Syntax **more** *file-url*

View User view

Parameter *file-url*: File name.

Description Use the **more** command to display the contents of the specified file.

So far, this command is valid only for .txt files.

Example # Display the contents of the file test.txt.

```
<Sysname> more test.txt
AppWizard has created this test application for you.
This file contains a summary of what you will find in each of the fi
les that make up your test application.
Test.dsp
This file (the project file) contains information at the project lev
el and is used to build a single project or subproject. Other users
can share the project (.dsp) file, but they should export the makefi
les locally.
```

mount (User view)

Syntax **mount** *device*

View User view

Parameter *device*: Storage device name.

Description Use the **mount** command to mount a hot swappable storage device, such as a CF module, etc (excluding Flash). This command is effective only when the device is in unmounted state.

By default, a storage device is in the mounted state, that is, you can use it without mounting it.

Note that:

- Do not remove the storage device or swap the module when mounting or unmounting the device, or when you are processing files on the storage device. Otherwise, the file system could be damaged.
- When a storage device is connected to a low version system, the system may not be able to recognize the device automatically, you need to use the **mount** command for the storage device to function normally.
- Before removing a mounted storage device from the system, you should first unmount it to avoid damaging the device.

Related command: **umount**.

Example # Mount a CF module of the active main module (AMB).

```
<Sysname> mount cf:
% Mount cf: successfully.
%Apr 23 01:50:00:628 2003 System VFS/4/LOG:
cf: mounted into slot 4.
```

Mount a CF module of the standby main module (SMB) (assume the SMB is in slot 5).

```
<Sysname> mount slot5#cf:
% Mount slot5#cf: successfully.
%Apr 23 01:50:00:628 2003 System VFS/5/LOG:
cf: mounted into slot 5.
```

move (User view)

Syntax **move** *fileurl-source fileurl-dest*

View User view

Parameter *fileurl-source*: Name of the source file.

fileurl-dest: Name of the target file.

Description Use the **move** command to move a file.

If the name of the target file is the same as an existing one in the target directory, the system will ask you whether to overwrite the existing one.

CAUTION: *The original and target directory of the file to be moved must be on the same device. The* ***move*** *command does not support cross-device file moving.*

Example # Move the file flash:/test/sample.txt to flash:/sample.txt.

```
<Sysname> move flash:/test/sample.txt flash:/sample.txt
Move flash:/test/sample.txt to flash:/sample.txt ?[Y/N]:y
% Moved file flash:/test/sample.txt to flash:/sample.txt
```

pwd (User view)

Syntax **pwd**

View User view

Parameter None

Description Use the **pwd** command to display the current path.

If the current path is not set, the operation will fail.

Example # Display the current path.

```
<Sysname> pwd
flash:
```

rename (User view)

Syntax **rename** *fileurl-source fileurl-dest*

View User view

Parameter *fileurl-source*: Name of the source file or directory.

fileurl-dest: Name of the target file or directory.

Description Use the **rename** command to rename a file or directory.

The target file name must be unique under the current path.

Example # Rename the file sample.txt as sample.bak.

```
<Sysname> rename sample.txt sample.bak
Rename flash:/sample.txt to flash:/sample.bak?[Y/N]:y

% Renamed file flash:/sample.txt to flash:/sample.bak
```

reset recycle-bin (User view)

Syntax **reset recycle-bin** [**/force**]

View User view

Parameter **/force**: Empties the recycle bin.

Description Use the **reset recycle-bin** command to permanently remove deleted file or files from the recycle bin.

Unlike this command, the **delete** *file-url* command only moves files to the recycle bin.

Example # Empty the recycle bin.

```
<Sysname> reset recycle-bin
Clear flash:/tt.cfg ?[Y/N]:y
Clearing files from flash may take a long time. Please wait...
.
%Cleared file flash:/~/tt.cfg.
```

rmdir (User view)

Syntax **rmdir** *directory*

View User view

Parameter *directory*: Name of the directory.

Description Use the **rmdir** command to remove a directory.

The directory must be an empty one. If it is not, first delete all files and subdirectory under it with the **delete** command.

Example # Remove directory mydir.

```
<Sysname> rmdir mydir
Rmdir flash:/mydir?[Y/N]:y
.
%Removed directory flash:/mydir.
```

umount (User view)

Syntax **umount** *device*

View User view

Parameter *device*: Storage device name.

Description Use the **umount** command to unmount a hot swappable storage device, such as a CF module, (excluding Flash). This command is effective only when the device is in mounted state.

By default, a storage device is in the mounted state. To remove a storage device, you should unmount it first.

Note that:

- Do not remove the storage device or swap the module when mounting or unmounting the device, or when you are processing files on the storage device. Otherwise, the file system could be damaged.
- When a storage device is connected to a low version system, the system may not be able to recognize the device automatically, you need to use the mount command for the storage device to function normally.
- Before removing a mounted storage device from the system, you should first unmount it to avoid damaging the device. By default, a storage device is in the mounted state. You can use it without mounting it.

Related command: **mount**.

Example # Unmount a CF module of the AMB

```
<Sysname> umount cf:
% Umount cf: successfully.
%Apr 23 01:49:20:929 2003 System VFS/5/LOG:
cf: umounted from slot 4.
```

Unmount a CF module of the SMB (assume the SMB is in slot 5).

```
<Sysname> umount slot5#cf:
% Umount slot5#cf: successfully.
%Apr 23 01:49:20:929 2003 System VFS/5/LOG:
cf: umounted from slot 5.
```

undelete (User view)

Syntax **undelete** *file-url*

View User view

Parameter *filename*: Name of the file to be restored.

Description Use the **undelete** command to restore a file from the recycle bin.

If another file with the same name exists under the same path, the undelete operation will cause it to be overwritten and the system will ask you whether to continue.

Example # Restore file sample.bak from the recycle bin.

```
<Sysname> undelete sample.bak
Undelete flash:/sample.bak ?[Y/N]:y
% Undeleted file flash:/sample.bak
```

88 CONFIGURATION FILE MANAGEMENT COMMANDS

backup startup-configuration

Syntax **backup startup-configuration to** *dest-addr* [*dest-filename*]

View User view

Parameter *dest-addr*: IP address or name of a TFTP server. The address cannot be an IPv6 address.

dest-filename: Target filename used to save the next startup configuration file on the server.

Description Use the **backup startup-configuration** command to backup the startup configuration file (for next startup) using a filename you specify. If you do not specify this filename, the original filename is used.

Presently, the device uses TFTP to backup configuration files.

Example # Backup the configuration file for next startup on the TFTP server with IP address 2.2..2.2, using the filename config.cfg.

```
<Sysname> backup startup-configuration to 2.2.2.2 config.cfg
Backup next startup-configuration file to 2.2.2.2, please wait...
finished!
<Sysname>
```

display saved-configuration

Syntax **display saved-configuration** [**by-linenum**]

View Any view

Parameter **by-linenum**: Identifies each line of displayed information with a line number.

Description Use the **display saved-configuration** command to display the configuration file saved in the storage device.

In case the device malfunctions after being powered on, if you find some configurations are not validated or incorrect, you may use this command to identify the problem.

If you do not use the configuration file when the device starts up, meaning the displayed startup configuration file is NULL after you execute the **display startup** command, no information is displayed when you execute the **display saved-configuration** command; if you have saved the configuration file after the device starts up, the information last saved in the configuration file is displayed.

Related command: **save**, **reset saved-configuration**, and the **display current-configuration** command in *Basic Configuration Commands* in *System Volume*.

Example # Display the configuration file saved in the storage device.

```
<Sysname> display saved-configuration
#
 sysname sysname
#
 local-user abc password simple abc
#
 tcp window 8
#
interface Aux7/0/1
 link-protocol ppp
#
interface Ethernet2/1/1
#
interface Ethernet2/1/2
#
interface Ethernet2/1/3
 ip address 10.110.101.17 255.255.255.0
#
interface NULL0
#
ospf 1
#
 ip route-static 10.12.0.0 255.255.0.0 Ethernet 12/1/1
#
user-interface con 0
user-interface aux 0
user-interface vty 0 4
 authentication-mode none
#
return
```

The configurations are displayed in the order of global, port, and user interface.

display startup

Syntax **display startup**

View Any view

Parameter None

Description Use the **display startup** command to display the configuration file used at this startup and the one used for next startup.

Related command: **startup saved-configuration**.

Example # Display the configuration file used at this startup and the one used for next startup.

```
<Sysname> display startup
MainBoard
  Current startup saved-configuration file:          flash:/config.cfg
  Next startup saved-configuration file:             flash:/config.cfg
```

reset saved-configuration

Syntax **reset saved-configuration**

View User view

Parameter None

Description Use the **reset saved-configuration** command to erase the configuration file saved in the storage device.

CAUTION: *This command will permanently delete the configuration file on the device. Use it with caution.*

Related command: **save**, **display saved-configuration**.

Example # Erase the configuration file saved in the storage device.

```
<Sysname> reset saved-configuration
The saved configuration will be erased.
Are you sure? [Y/N]:y
Configuration in the device is being cleared.
Please wait ...
....
Configuration in the device is cleared.
```

restore startup-configuration

Syntax **restore startup-configuration from** *src-addr src-filename*

View User view

Parameter *src-addr*: IP address or name of a TFTP server. The address cannot be an IPv6 address.

src-filename: Filename of the configuration file to be downloaded from the specified server.

Description Use the **restore startup-configuration** command to download the configuration file from the specified TFTP server for the next startup of the device.

- The command downloads the configuration file to the AMB for next startup and meanwhile copies the file to the SMB for next startup.
- The command downloads the configuration file for the next startup only.

If the file to be downloaded has the same filename as an existing file on the AMB or SMB, you will be prompted whether you want to overwrite the existing file or not. In addition, both the AMB and the SMB are assumed to use the storage device of the same type when checking filename or downloading the configuration file (both to the root directory of the AMB or SMB); otherwise, the restoration fails.

Example # Download the configuration file config.cfg for the next startup from the TFTP server whose IP address is .2.2.2.2.

```
<Sysname>restore startup-configuration from 2.2.2.2 config.cfg
Restore next startup-configuration file from 2.2.2.2. Please wait...
finished!
Now restore next startup-configuration file from main to slave board
, Please wait...finished!
```

save

Syntax **save** [*file-name* | [**safely**]

View Any view

Parameter *file-name*: File name, whose suffix must be .cfg.

safely: Sets the configuration saving mode to safe. If this argument is not specified, the configuration file is saved in fast mode.

Description

- Use the **save** command to save the current configuration file. If no filename is specified, the system saves the configuration file under the default the directory, that is, the root directory.

Note that:

- When you use the **save** *file-name* command, if you specify the saving directory in the *file-name*, the configuration will be saved in the specified directory; if you do not specify a saving directory in the *file-name*, the configuration will be saved in the current directory.
- In interactive mode, if you specify a saving directory in the file name, the directory to be specified must be the directory of the saving device on the AMB.

Related command: **reset saved-configuration**, **display saved-configuration**, and **display current-configuration** in *Basic System Configuration Commands* in the *System Volume*.

Example # Save the current configuration file to the default directory.

```
<Sysname> save
The current configuration will be written to the device. Are you sure? [Y/N]
:y
Please input the file name(*.cfg)[flash:/config.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/config.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait...
Now saving current configuration to the device.
Saving configuration flash:/config.cfg. Please wait...
.................
 Saved the current configuration to mainboard device successfully.
```

slave auto-update config

Syntax **slave auto-update config**

undo slave auto-update config

View System view

Parameter None

Description Use the **slave auto-update config** command to enable auto-update between the AMB and SMB.

Use the **undo slave auto-update config** command to disable auto-update between the AMB and SMB.

By default, auto-update between the AMB and SMB is enabled.

Example # Enable the auto-update between the AMB and SMB.

```
<Sysname> system-view
[Sysname] slave auto-update config
```

startup saved-configuration

Syntax **startup saved-configuration** *cfgfile*

undo startup saved-configuration

View User view

Parameter *cfgfile*: Configuration file name.

Description Use the **startup saved-configuration** command to specify a configuration file for next startup.

Use the **undo startup saved-configuration** command to start up with null configuration, which means startup with the initial configuration of the system.

The specified file must be ended with a .cfg extension and saved in the root directory of the storage device.

Related command: **display startup**.

Example # Specify a configuration file for next startup.

```
<Sysname> startup saved-configuration config.cfg
Please wait ....... Done!
```

89 FTP SERVER CONFIGURATION COMMANDS

display ftp-server

Syntax **display ftp-server**

View Any view

Parameter None

Description Use the **display ftp-server** command to display the FTP server configuration of the device.

After configuring FTP parameters, you may verify them with this command.

Example # Display the FTP server configuration.

```
<Sysname> display ftp-server
   FTP server is running
   Max user number:       1
   User count:            1
   Timeout value(in minute):       30
   Put Method:                     fast
```

The output indicates that the FTP server is running with support to only one concurrent login user; now one logged-in user is present; timeout of the user is 30 minutes, and FTP update mode is **fast**.

display ftp-user

Syntax **display ftp-user**

View Any view

Parameter None

Description Use the **display ftp-user** command to display the detailed information of current FTP users.

Example # Display the detailed information of FTP users.

```
<Sysname> display ftp-user
  UserName              HostIP     Port     Idle              HomeDir
       ftp        192.168.1.54     1190        0               flash:
```

Table 376 Field descriptions of the display ftp-user command

Field	Description
UserName	Name of the present logged-in user
HostIP	IP address of the present logged-in user
Port	Port which the present logged-in user is using
Idle	Duration time of the current FTP connection
HomeDir	Specified path of the present logged-in user

ftp server enable

Syntax **ftp server enable**

undo ftp server

View System view

Parameter None

Description Use the **ftp server enable** command to enable the FTP server.

Use the **undo ftp server** command to disable the FTP server.

By default, the FTP server is disabled to prevent attacks.

Example # Disable the FTP server.

```
<Sysname> system-view
[Sysname] undo ftp server
% Close FTP server
```

ftp timeout

Syntax **ftp timeout** *minute*

undo ftp timeout

View System view

Parameter *minute*: Idle-timeout timer in minutes, in the range 1 to 35791. The default is 30 minutes.

Description Use the **ftp timeout** command to set the idle-timeout timer.

Use the **undo ftp timeout** command to restore the default.

After you log onto the FTP server, you set up an FTP connection. When the connection is disrupted, the FTP server, if not notified, cannot realize that and maintains the connection all the same. To address this problem, you can set an idle-timeout timer to have the FTP server disconnected if no information is received or/and transmitted before the timer expires.

Example # Set the idle-timeout timer to 36 minutes.

```
<Sysname> system-view
[Sysname] ftp timeout 36
```

ftp update

Syntax **ftp update** { **fast** | **normal** }

undo ftp update

View System view

Parameter **fast**: Fast update.

normal: Normal update.

Description Use the **ftp update** command to set the file update mode that the FTP server uses while receiving data.

Use the **undo ftp update** command to restore the default, namely, the normal mode.

Example # Set the FTP update mode to normal.

```
<Sysname> system-view
[Sysname] ftp update normal
```

90 FTP CLIENT CONFIGURATION COMMANDS

*You must use the **ftp** command to enter FTP client view for configurations under this view. For details, refer to "ftp (FTP client view)" on page 1331*

ascii

Syntax **ascii**

View FTP client view

Parameter None

Description Use the **ascii** command to set the file transfer mode to ASCII for the FTP connection.

FTP provides two file transfer modes: ASCII and binary. To transfer text files, use the ASCII mode; to transfer program files, use the binary mode.

By default, the file transfer mode is ASCII.

Example # Set the file transfer mode to ASCII.

```
[ftp] ascii
200 Type set to A
```

binary

Syntax **binary**

View FTP client view

Parameter None

Description Use the **binary** command to set the file transfer mode to binary (also called flow mode).

FTP provides two file transfer modes: ASCII and binary. To transfer text files, use the ASCII mode; to transfer program files, use the binary mode.

By default, the transfer mode is ASCII mode.

Example # Set the file transfer mode to binary.

```
[ftp] binary
200 Type set to I.
```

bye (FTP client view)

Syntax **bye**

View FTP client view

Parameter None

Description Use the **bye** command to disconnect from the remote FTP server and exit to user view.

Example # Terminate the connection with the remote FTP server and exit to user view.

```
[ftp] bye
221 Server closing.
```

cd (FTP client view)

Syntax **cd** *pathname*

View FTP client view

Parameter *pathname*: Path name.

Description Use the **cd** command to change the current working directory on the remote FTP server.

You can use this command to access another authorized directory on the FTP server.

Example # Change the current working directory to flash:/temp.

```
[ftp] cd flash:/temp
250 CWD command successful.
```

cdup (FTP client view)

Syntax **cdup**

View FTP client view

Parameter None

Description Use the **cdup** command to exit the current directory and enter the upper directory of the FTP server.

Example # Change the current working directory path to the upper directory.

```
[ftp] cdup
200 CDUP command successful.
```

close (FTP client view)

Syntax **close**

View FTP client view

Parameter None

Description Use the **close** command to terminate the connection to the FTP server, but remain in FTP client view.

This command is equal to the **disconnect** command.

Example # Terminate the connection to the FTP server and remain in FTP client view.

```
[ftp] close
221 Server closing.
[ftp]
```

delete (FTP client view)

Syntax **delete** *remotefile*

View FTP client view

Parameter *remotefile*: File name.

Description Use the **delete** command to delete a specified file on the remote FTP server.

To do this, you must be a user with the delete permission on the FTP server.

Example # Delete file temp.c.

```
[ftp] delete temp.c
250 DELE command successful.
```

dir (FTP client view)

Syntax **dir** [*remotefile* [*localfile*]]

View FTP client view

Parameter *remotefile*: Name of the file or directory on the remote FTP server.

localfile: Name of the local file to save the displayed information.

Description Use the **dir** command to view detailed information of the files and subdirectories under the current directory on the remote FTP server.

Use the **dir** *remotefile* command to display the detailed information of the specified file or directory on the remote FTP server.

Use the **dir** *remotefile localfile* command to display the detailed information of the specified file or directory on the remote FTP server, and save the displayed information into a local file specified by the *localfile* argument.

*The **ls** command can only display the names of files and directories, whereas the **dir** command can display other related information of the files and directories, such as the size, the date they were created.*

Example # View the information of the file ar-router.cfg, and save the result to aa.txt.

```
[ftp] dir ar-router.cfg aa.txt
227 Entering Passive Mode (192,168,1,50,17,158).
125 ASCII mode data connection already open, transfer starting for config.cfg.
....226 Transfer complete.
FTP: 67 byte(s) received in 4.600 second(s), 14.00 byte(s)/sec.
```

View the content of aa.txt

```
[ftp] quit
<Sysname> more aa.txt
-rwxrwxrwx   1 noone    nogroup      3077 Jun 20 15:34 ar-router.cfg
```

disconnect (FTP client view)

Syntax **disconnect**

View FTP client view

Parameter None

Description Use the **disconnect** command to disconnect from the remote FTP server but remain in FTP client view.

This command is equal to the **close** command.

Example # Disconnect from the remote FTP server but remain in FTP client view.

```
[ftp] disconnect
221 Server closing.
```

display ftp client configuration

Syntax **display ftp client configuration**

View Any view

Parameter None

Description Use the **display ftp client configuration** command to display the configuration information of the FTP client.

Currently this command displays the configuration information of the source address. If the currently valid source address is the source IP address, this command displays the configured source IP address; if it is the source interface, this command displays the configured source interface.

Related command: **ftp client source**.

Example # Display the current configuration information of the FTP client.

```
<Sysname> display ftp client configuration
The source IP address is 192.168.0.123
```

ftp (FTP client view)

Syntax **ftp** [*server-address* [*service-port*] [**source** { **ip** *source-ip-address* | **interface** *interface-type interface-number* }]]

View User view

Parameter *server-address*: IP address or host name of a remote FTP server.

service-port: Port number of the remote FTP server, in the range 0 to 65535. The default value is 21.

ip *source-ip-address:* The source IP address of the current FTP client. This source address must be the one that has been configured on the device.

interface *interface-type interface-number*: Specifies the source interface by its type and number. The primary IP address configured on this interface is the source address of the transmitted packets. If no primary IP address is configured on the source interface, the connection fails.

Description Use the **ftp** command to log onto the remote FTP server and enter FTP client view.

Note that:

- This command applies to IPv4 network.

- If you use this command without specifying any parameters, you will simply enter the FTP client view without logging onto the FTP server.
- If you specify the parameter, you will be asked to enter the username and password for accessing the FTP server.
- The priority of the source address specified with this command is higher than that with the **ftp client source** command. If you specify the source address with the **ftp client source** command first and then with the **ftp** command, the source address specified with the **ftp** command is used to communicate with the FTP server.

Related command: **ftp client source**.

Example # Log from the current device Sysname1 onto the device Sysname2 with the IP address of 192.168.0.211. The source IP address of the packets sent is 192.168.0.212.

```
<Sysname1> ftp 192.168.0.211 source ip 192.168.0.212
Trying 192.168.0.211 ...
Press CTRL+K to abort
Connected to 192.168.0.211.
220 Xlight FTP Server 2.1 ready...
User(192.168.0.211:(none)):abc
331 Password required for abc
Password:
230 Login OK
[ftp]
```

ftp client source

Syntax **ftp client source** { **ip** *source-ip-address* | **interface** *interface-type interface-number* }

undo ftp client source

View System view

Parameter **ip** *source-ip-address:* Source IP address of the FTP connection. It must be an IP address configured on the device.

interface *interface-type interface-number*: Source interface for the FTP connection, including interface type and interface number. The primary IP address configured on the source interface is the source IP address of the packets sent by FTP. If no primary IP address is configured on the source interface, the connection fails.

Description Use the **ftp client source** command to configure the source address of the transmitted FTP packets from the FTP client.

Use the **undo telnet client source** command to restore the default.

By default, a device uses the IP address of the interface determined by the routing protocol as the source IP address to communicate with an FTP server.

Note that:

- The source address includes the source interface and the source IP address. If you use the **ftp client source** command to specify the source interface and the source IP address, the newly specified source IP address overwrites the original one and vice versa.
- If the source address is specified with the **ftp client source** command and then with the **ftp** command, the source address specified with the latter one is used to communicate with the FTP server.
- The source address specified with the **ftp client source** command is valid for all **ftp** connections and the source address specified with the **ftp** command is valid only for the current **ftp** connection.

Related command: **display ftp client configuration**.

Example # Specify the source IP address of the FTP client as 2.2.2.2.

```
<Sysname> system-view
[Sysname] ftp client source ip 2.2.2.2
```

ftp ipv6

Syntax **ftp ipv6** [*server-address* [*service-port*] [**source ipv6** *source-ipv6-address*] [**-i** *interface-type interface-number*]]

View User view

Parameter *server-address*: IP address or host name of the remote FTP server.

service-port: Port number of the FTP server, in the range 0 to 65535. The default value is 21.

source ipv6 *source-ipv6-address*: Specifies a source IPv6 address for transmitted FTP packets. This address must be an IPv6 address that has been configured on the device.

-i *interface-type interface-number*: Specifies the type and number of the egress interface. This parameter can be used only in case that the FTP server address is the link local address and the specified egress interface must have a link local address (For the configuration of link local address, see "IPv6 Basics Configuration Commands" on page 283.

Description Use the **ftp ipv6** command to log onto the FTP server and enter FTP client view.

Note that:

- This command applies to IPv6 network.

- If you use this command without specifying any parameters, you will simply enter the FTP client view without logging onto the FTP server.
- If you specify the parameter, you will be asked to enter the username and password for accessing the FTP server.

Example # Log onto the FTP server with IPv6 address 3000::200.

```
<Sysname> ftp ipv6 3000::200
Trying 3000::200 ...
Press CTRL+K to abort
Connected to 3000::200.
220 Welcome!
User(3000::200:(none)): MY_NAME
331 Please specify the password.
Password:
230 Login successful.
[ftp]
```

get (FTP client view)

Syntax **get** *remotefile* [*localfile*]

View FTP client view

Parameter *remotefile*: File name on the remote FTP server.

localfile: Local file name.

Description Use the **get** command to download a file from a remote FTP server and save it.

If no name is specified, the local file uses the name of the source file on the FTP server by default.

Example # Download file config.cfg and save it as aa.cfg.

```
[ftp]get config.cfg aa.cfg

227 Entering Passive Mode (192,168,1,50,17,163).
125 ASCII mode data connection already open, transfer starting for config.cfg.
.....226 Transfer complete.
FTP: 5190 byte(s) received in 7.754 second(s), 669.00 byte(s)/sec.
```

lcd (FTP client view)

Syntax **lcd**

View FTP client view

Parameter None

Description Use the **lcd** command to display the local directory of the FTP client.

Example # Display the local directory.

```
[ftp] lcd
FTP: Local directory now flash:/temp
```

ls (FTP client view)

Syntax **ls** [*remotefile*] [*localfile*]]

View FTP client view

Parameter *remotefile*: Filename or directory on the remote FTP server.

localfile: Name of a local file used to save the displayed information.

Description Use the **ls** command to view the information of all the files and subdirectories under the current directory of the remote FTP server. The file names and subdirectory names are displayed.

Use the **ls** *remotefile* command to view the information of a specified file or subdirectory.

Use the **ls** *remotefile localfile* command view the information of a specified file or subdirectory, and save the result to a local file specified by the *localfile* argument.

*The **ls** command can only display the names of files and directories, whereas the **dir** command can display other related information of the files and directories, such as the size, the date they are created.*

Example # View the information of all files and subdirectories under the current directory of the FTP server.

```
[ftp] ls
227 Entering Passive Mode (192,168,1,50,17,165).
125 ASCII mode data connection already open, transfer starting for *.
ar-router.cfg
logfile
mainar.bin
arbasicbtm.bin
ftp
test
bb.cfg
config.cfg
226 Transfer complete.
FTP: 87 byte(s) received in 0.132 second(s) 659.00 byte(s)/sec.
```

View the information of directory logfile, and save the result to file aa.txt.

```
[ftp] ls logfile aa.txt
227 Entering Passive Mode (192,168,1,50,17,166).
125 ASCII mode data connection already open, transfer starting for logfile.
.....226 Transfer complete.
FTP: 9 byte(s) received in 0.094 second(s) 95.00 byte(s)/sec.
```

View the content of file aa.txt.

```
[ftp] quit
<Sysname> more aa.txt
logfile
```

mkdir (FTP client view)

Syntax **mkdir** *directory*

View FTP client view

Parameter *directory*: Directory name.

Description Use the **mkdir** command to create a subdirectory under the specified directory on the remote FTP server.

To do this, you must be a user with the permission on the FTP server.

Example # Create subdirectory mytest on the current directory of the remote FTP server.

```
[ftp] mkdir mytest
257 " flash:/mytest" new directory created.
```

open (FTP client view)

Syntax **open** *server-address* [*service-port*]

View FTP client view

Parameter *server-address*: IP address or host name of a remote FTP server.

service-port: Port number of the remote FTP server, in the range 0 to 65535, with the default value of 21.

Description Use the **open** command to log onto the IPv4 FTP server under FTP client view.

At login, you will be asked to enter the username and password for accessing the FTP server. If your input is correct, the login succeeds; otherwise, it fails.

This command is applicable to IPv4 networks.

Related command: **close**.

Example # In FTP client view, log onto the FTP server with the IP address of 192.168.1.50.

```
[ftp] open 192.168.1.50
Trying 192.168.1.50 ...
Press CTRL+K to abort
Connected to 192.168.1.50.
220 FTP service ready.
User(192.168.1.50:(none)):aa
```

```
331 Password required for aa.
Password:
230 User logged in.

[ftp]
```

open ipv6 (FTP client view)

Syntax **open ipv6** *server-address* [*service-port*] [**-i** *interface-type interface-number*]

View FTP client view

Parameter *server-address*: IP address or host name of the remote FTP server.

service-port: Port number of the remote FTP server, in the range 0 to 65535. The default value is 21.

-i *interface-type interface-number*: Specifies the egress interface by it type and number. This parameter can be used only in case that the FTP server address is the link local address and the specified egress interface must have a link local address (For the configuration of link local address, see "IPv6 Basics Configuration Commands" on page 283.

Description Use the **open ipv6** command to log onto IPv6 FTP server in FTP client view.

At login, you will be asked to enter the username and password for accessing the FTP server. If your input is correct, the login succeeds; otherwise, it fails.

This command is applicable to IPv6 networks.

Related command: **close**.

Example # Log onto the FTP server (with IPv6 address 3000::200) in FTP client view.

```
[ftp] open ipv6 3000::200
Trying 3000::200 ...
Press CTRL+K to abort
Connected to 3000::200.
220 Welcome!
User(3000::200:(none)): MY_NAME
331 Please specify the password.
Password:
230 Login successful.
```

passive (FTP client view)

Syntax **passive**

undo passive

View FTP client view

Parameter None

Description Use the **passive** command to set the data transmission mode to passive.

Use the **undo passive** command to set the data transmission mode to active.

The default transmission mode is passive.

Example # Set the data transmission mode to passive.

```
[ftp] passive
FTP: passive is on
```

put (FTP client view)

Syntax **put** *localfile* [*remotefile*]

View FTP client view

Parameter *localfile*: Local file name.

remotefile: Name of the file to be saved on the remote FTP server.

Description Use the **put** command to upload a file to the remote FTP server.

If no name is assigned to the file to be saved on the FTP server, the name of the source file is used by default.

Example # Upload source file cc.txt to the remote FTP server and save it as dd.txt.

```
[ftp] put cc.txt dd.txt
227 Entering Passive Mode (192,168,1,50,17,169).
125 ASCII mode data connection already open, transfer starting for dd.txt.
226 Transfer complete.
FTP: 9 byte(s) sent in 0.112 second(s), 80.00byte(s)/sec.
```

pwd (FTP client view)

Syntax **pwd**

View FTP client view

Parameter None

Description Use the **pwd** command to display the working directory on the remote FTP server.

Example # Display the working directory on the remote FTP server.

```
[ftp] pwd
257 "flash:/temp" is current directory.
```

quit (FTP client view)

Syntax **quit**

View FTP client view

Parameter None

Description Use the **quit** command to disconnect from the remote FTP server and exit to user view.

Example # Disconnect from the remote FTP server and exit to user view.

```
[ftp] quit
221 Server closing.

<Sysname>
```

remotehelp (FTP client view)

Syntax **remotehelp** [*protocol-command*]

View FTP client view

Parameter *protocol-command*: FTP command.

Description Use the **remotehelp** command to display the help information of FTP-related commands supported by the remote FTP server.

If no parameter is specified, FTP-related commands supported by the remote FTP server are displayed.

Example # Display FTP commands supported by the remote FTP server.

```
[ftp] remotehelp user
214-Here is a list of available ftp commands
    Those with '*' are not yet implemented.
   USER   PASS   ACCT*  CWD    CDUP   SMNT*  QUIT   REIN*
   PORT   PASV   TYPE   STRU*  MODE*  RETR   STOR   STOU*
   APPE*  ALLO*  REST*  RNFR*  RNTO*  ABOR*  DELE   RMD
   MKD    PWD    LIST   NLST   SITE*  SYST   STAT*  HELP
   NOOP*  XCUP   XCWD   XMKD   XPWD   XRMD
214 Direct comments to 3Com company.
```

Display the help information for the **user** command.

```
[ftp] remote user

214 Syntax: USER <sp> <username>.

[ftp]
```

Table 377 Field descriptions of the remotehelp command

Field	Description
214-Here is a list of available ftp commands	The following is an available FTP command list.
Those with '*' are not yet implemented.	Those commands with "*" are not yet implemented.
USER	Username
PASS	Password
CWD	Change the current working directory
CDUP	Change to parent directory
SMNT*	File structure setting
QUIT	Quit
REIN*	Re-initialization
PORT	Port number
PASV	Passive mode
TYPE	Request type
STRU*	File structure
MODE*	Transmission mode
RETR	Download a file
STOR	Upload a file
STOU*	Store unique
APPE*	Appended file
ALLO*	Allocation space
REST*	Restart
RNFR*	Rename the source
RNTO*	Rename the destination
ABOR*	Abort the transmission
DELE	Delete a file
RMD	Delete a folder
MKD	Create a folder
PWD	Print working directory
LIST	List files
NLST	List file description
SITE*	Orient a parameter
SYST	Display system parameters
STAT*	State
HELP	Help
NOOP*	No operation
XCUP	Extension command, the same meaning as CUP

Table 377 Field descriptions of the remotehelp command

Field	Description
XCWD	Extension command, the same meaning as CWD
XMKD	Extension command, the same meaning as MKD
XPWD	Extension command, the same meaning as PWD
XRMD	Extension command, the same meaning as RMD
Syntax: USER <sp> <username>.	Syntax of the **user** command: user (keyword) + space + *username*

rmdir (FTP client view)

Syntax **rmdir** *directory*

View FTP client view

Parameter *directory*: Directory name on the remote FTP server.

Description Use the **rmdir** command to remove a specified directory from the FTP server.

Note that only authorized users are allowed to use this command.

Note that:

- The directory to be deleted must be empty, meaning you should delete all files and the subdirectory under the directory before you delete a directory. For the deletion of files, refer to the **delete** command on page 1308.
- After you execute the **rmdir** command, the files in the remote recycle bin under the directory will be automatically deleted.

Example # Delete the flash:/temp1 directory from the FTP server.

```
[ftp] rmdir flash:/temp1
200 RMD command successful.
```

user (FTP client view)

Syntax **user** *username* [*password*]

View FTP client view

Parameter *username*: Other login username.

password: Login password.

Description Use the **user** command to relog onto the currently accessing FTP server with other username after you have logged onto the FTP server.

Before using this command, you must configure the corresponding username and password on the FTP server; otherwise, you login fails and the FTP connection is closed.

Example # User ftp1 has logged onto the FTP server and relogs onto the current FTP server with the username of ftp2. (Suppose username ftp2 and password 123123123123 have been configured on the FTP server).

```
[ftp] user ftp2
331 Password required for ftp2.
Password:
230 User logged in.

[ftp]
```

verbose (FTP client view)

Syntax **verbose**

undo verbose

View FTP client view

Parameter None

Description Use the **verbose** command to enable the verbose function to display detailed prompt information.

Use the **undo verbose** command to disable the verbose function.

By default, the verbose function is enabled.

Example # Enable the verbose function.

```
[ftp] verbose
FTP: verbose is on
```

91 TFTP CLIENT CONFIGURATION COMMANDS

display tftp client configuration

Syntax **display tftp client configuration**

View Any view

Parameter None

Description Use the **display tftp client configuration** command to display the configuration information of the TFTP client.

Related command: **tftp client source**.

Example # Display the current configuration information of the TFTP client.

```
<Sysname> display tftp client configuration
The source IP address is 192.168.0.123
```

Currently this command displays the source address configuration information. If the currently valid source address is the source IP address, the configured source IP address is displayed; if the currently valid address is the source interface, the configured source interface is displayed.

tftp-server acl

Syntax **tftp-server** [**ipv6**] **acl** *acl-number*

undo tftp-server [**ipv6**] **acl**

View System view

Parameter **ipv6**: References an IPv6 ACL. If it is not specified, an IPv4 ACL is referenced.

acl-number: Number of basic ACL, in the range 2000 to 2999.

Description Use the **tftp-server acl** command to reference an ACL to control access to the TFTP server. Users can use the configured rules in ACL to allow or prevent the use of TFTP server in a network.

Use the **undo tftp-server acl** command to remove the access restriction.

For more information about ACL, refer to the *ACL Configuration Commands.*

Example # Reference ACL 2000 to control access to the TFTP application in IPv4.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 1.1.1.1 0
[Sysname-acl-basic-2000] quit
[Sysname] tftp-server acl 2000
```

Associate IPv6 ACL 2001 with TFTP application in Ipv6.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2001
[Sysname-acl6-basic-2001] rule permit source 2030:5060::9050/64
[Sysname-acl6-basic-2001] quit
[Sysname] tftp-server ipv6 acl 2001
```

tftp

Syntax **tftp** *server-address* { **get** | **put** | **sget** } *source-filename* [*destination-filename*] [**source** { **ip** *source-ip-address* | **interface** *interface-type interface-number* }]

View User view

Parameter *server-address:* IP address or host name of a TFTP server.

source-filename: Source file name.

destination-filename: Destination file name.

get: Downloads a file in normal mode.

put: Uploads a file.

sget: Downloads a file in secure mode.

ip *source-ip-address:* Specifies a source IP address for transmitted TFTP packets. This source address must be the one that has been configured on the device.

interface *interface-type interface-number*: Specifies the source interface by its type and number. The primary IP address configured on the source interface is the source IP address of the packets sent by FTP. If no primary IP address is configured on the source interface, the transmission fails.

Description Use the **tftp** command to upload files from the local device to a TFTP server or download files from the TFTP server to the local device.

- If no destination file name is specified, the saved file uses the source file name.
- The priority of the source address specified with this command is higher than that with the **tftp client source** command. If you use the **tftp client source** command to specify the source address first and then with the **tftp** command, the latter one is adopted.

This command applies to IPv4 network.

Related command: **tftp client source**.

Example # Download the aaa.app file from the TFTP server with the IP address of 1.1.3.1 and save it as bbb.app.

```
<Sysname> tftp 1.1.3.1 get aaa.app bbb.app
```

Upload file cmwcfg.txt from the root directory of the storage device to the default path of the TFTP server with the IP address of 1.1.1.2 and save it as cmwcfg.bak.

```
<Sysname> tftp 1.1.1.2 put flash:/cmwcfg.txt cmwcfg.bak
```

tftp client source

Syntax **tftp client source** { **ip** *source-ip-address* | **interface** *interface-type interface-number* }

undo tftp client source

View System view

Parameter **ip** *source-ip-address:* The source IP address of the TFTP connection. It must be an IP address configured on the device.

interface *interface-type interface-number*: Specifies the source interface by its type and number. The primary IP address configured on the source interface is the source IP address of the packets sent by FTP. If no primary IP address is configured on the source interface, the transmission fails.

Description Use the **tftp client source** command to configure the source address of the TFTP packets from the TFTP client.

Use the **undo telnet client source** command to restore the default.

By default, a device uses the IP address of the interface determined by the routing protocol as the source IP address to communicate with a TFTP server.

Note that:

- The source address includes the source interface and the source IP, if you use the **tftp client source** command to specify the source interface and the source IP, the newly specified source IP overwrites the original one and vice versa.
- If the source address is specified with the **tftp client source** command and then with the **tftp** command, use the latter one.
- The source address specified with the **tftp client source** command is valid for all **tftp** connections and the source address specified with the **tftp** command is valid for the current **tftp** command.

Related command: **display tftp client configuration**.

Example # Specify the source IP address of the TFTP client to 2.2.2.2.

```
<Sysname> system-view
[Sysname] tftp client source ip 2.2.2.2
```

tftp ipv6

Syntax **tftp ipv6** *tftp-ipv6-server* [**-i** *interface-type interface-number*] { **get** | **put** } *source-file* [*destination-file*]

View User view

Parameter *tftp-ipv6-server*: IPv6 address or host name (a string of 1 to 46 characters) of a TFTP server.

-i *interface-type interface-number*: Specifies the egress interface by its type and number. This parameter can be used only in case that the TFTP server address is a link local address and the specified egress interface must have a link local address (For the configuration of link local address, see "IPv6 Basics Configuration Commands" on page 283.

get: Downloads a file.

put: Uploads a file.

source-filename: Source filename.

destination-filename: Destination filename. If not specified, this filename is the same as the source filename.

Description Use the **tftp ipv6** command to download a specified file from a TFTP server or upload a specified local file to a TFTP server.

This command applies to IPv6 network.

Example # Download filetoget.txt from TFTP server.

```
<Sysname> tftp ipv6 fe80::250:daff:fe91:e058 -i ethernet 1/0 get filetoget. txt

File will be transferred in binary mode
  Downloading file from remote tftp server, please wait...
  TFTP:       32 bytes received in 5 second(s).
  File downloaded successfully
```

92 SNMP CONFIGURATION COMMANDS

debugging snmp-agent

Syntax **debugging snmp-agent** { **header** | **packet** | **process** | **trap** }

undo debugging snmp-agent { **header** | **packet** | **process** | **trap** }

View User view

Parameter **header**: Enables SNMP packet header debugging.

packet: Enables SNMP packet debugging.

process: Enables SNMP packet process debugging.

trap: Enables trap packet debugging.

Description Use the **debugging snmp-agent** command to enable debugging for SNMP agent.

Use the **undo debugging snmp-agent** command to disable debugging for SNMP agent.

By default, debugging for SNMP agent is disabled.

Example # Enable debugging for SNMP packet header.

```
<Sysname> debugging snmp-agent header
```

display snmp-agent community

Syntax **display snmp-agent community** [**read** | **write**]

View Any view

Parameter **read**: Displays the information of communities with read-only access right.

write: Displays the information of communities with read and write access right.

Description Use the **display snmp-agent community** command to display community information for SNMPv1 or SNMPv2c.

Example # Display the information for all the current communities.

```
<Sysname> display snmp-agent community
   Community name:aa
       Group name:aa
       Acl:2001
       Storage-type: nonVolatile
   Community name:bb
       Group name:bb
       Storage-type: nonVolatile
```

Table 378 Descriptions on the fields of display snmp-agent community

Field	Description
Community name	Community name
Group name	SNMP group name
Acl	The number of the ACL in use
Storage-type	Storage type, which could be: ■ volatile: Information will be lost if the system is rebooted ■ nonVolatile: Information will not be lost if the system is rebooted ■ permanent: Modification permitted, but deletion forbidden ■ readOnly: Read only, that is, no modification, no deletion ■ other: Other storage types

display snmp-agent group

Syntax **display snmp-agent group** [*group-name*]

View Any view

Parameter *group-name*: Specifies the SNMP group name, a string of 1 to 32 characters, case sensitive.

Description Use the **display snmp-agent group** command to display information for the SNMP agent group, including group name, security model, MIB view, storage type, and so on. Absence of the *group-name* parameter indicates that information for all groups will be displayed.

Example # Display the information of all SNMP agent groups.

```
<Sysname> display snmp-agent group
   Group name: mygroup
       Security model: v1 noAuthnoPriv
       Readview: ViewDefault
       Writeview: <no specified>
       Notifyview:<no specified>
       Storage-type: nonVolatile
   Group name: managev3group
       Security model: v3 noAuthnoPriv
```

```
Readview: ViewDefault
Writeview: internet
Notifyview :<no specified>
Storage-type: nonVolatile
```

Table 379 Descriptions on the fields of the display snmp-agent group command

Field	Description
Group name	SNMP group name
Security model	Security model of the SNMP group, which can be: authPriv (authentication with privacy), authNoPriv (authentication without privacy), or noAuthNoPriv (no authentication no privacy).
Readview	The read only MIB view associated with the SNMP group
Writeview	The writable MIB view associated with the SNMP group
Notifyview	The notify MIB view associated with the SNMP group, the view with entries that can generate Trap messages
Storage-type	Storage type, which includes: volatile, nonVolatile, permanent, readOnly, and other. For detailed information, refer to Table 378.

display snmp-agent local-switch fabricid

Syntax **display snmp-agent local-switch fabricid**

View Any view

Parameter None

Description Use the **display snmp-agent local-switch fabricid** command to display the local SNMP agent switch fabric ID.

SNMP switch fabric ID uniquely identifies an SNMP entity within an SNMP domain. SNMP switch fabric is an indispensable part of an SNMP entity. It provides SNMP message allocation, message handling, authentication, and access control.

Example # Display the local SNMP agent switch fabric ID.

```
<Sysname> display snmp-agent local-switch fabricid
SNMP local EngineID: 000063A27F00000100006822
```

display snmp-agent mib-view

Syntax **display snmp-agent mib-view** [**exclude** | **include** | **viewname** *view-name*]

View Any view

Parameter **exclude**: Specifies to display SNMP MIB views of the "excluded" type.

include: Specifies to display SNMP MIB views of the "included" type.

viewname *view-name*: Name of the specified MIB view.

Description Use the **display snmp-agent mib-view** command to display SNMP MIB view information. Absence of the *view-name* parameter indicates that information for all MIB views will be displayed.

Example # Display the current SNMP MIB views.

```
<Sysname> display snmp-agent mib-view
   View name:ViewDefault
       MIB Subtree:iso
       Subtree mask:
       Storage-type: nonVolatile
       View Type:included
       View status:active

   View name:ViewDefault
       MIB Subtree:snmpUsmMIB
       Subtree mask:
       Storage-type: nonVolatile
       View Type:excluded
       View status:active

   View name:ViewDefault
       MIB Subtree:snmpVacmMIB
       Subtree mask:
       Storage-type: nonVolatile
       View Type:excluded
       View status:active

   View name:ViewDefault
       MIB Subtree:snmpModules.18
       Subtree mask:
       Storage-type: nonVolatile
       View Type:excluded
       View status:active
```

Table 380 Descriptions on the fields of the display snmp-agent mib-view command

Field	Description
View name	MIB view name
MIB Subtree	MIB subtree
Subtree mask	MIB subtree mask
Storage-type	Storage type
View Type	View type, which can be "included" or "excluded"
	Included indicates that all nodes of the MIB subtree are included in current view.
	Excluded indicates that not all nodes of the MIB subtree are included in current view.
View status	The status of MIB view

display snmp-agent statistics

Syntax **display snmp-agent statistics**

View Any view

Parameter None

Description Use the **display snmp-agent statistics** command to display SNMP statistics.

Example # Display the statistics on the current SNMP.

```
<Sysname> display snmp-agent statistics
  0 Messages delivered to the SNMP entity
  0 Messages which were for an unsupported version
  0 Messages which used a SNMP community name not known
  0 Messages which represented an illegal operation for the community supplied
  0 ASN.1 or BER errors in the process of decoding
  0 Messages passed from the SNMP entity
  0 SNMP PDUs which had badValue error-status
  0 SNMP PDUs which had genErr error-status
  0 SNMP PDUs which had noSuchName error-status
  0 SNMP PDUs which had tooBig error-status (Maximum packet size 1500)
  0 MIB objects retrieved successfully
  0 MIB objects altered successfully
  0 GetRequest-PDU accepted and processed
  0 GetNextRequest-PDU accepted and processed
  0 GetBulkRequest-PDU accepted and processed
  0 GetResponse-PDU accepted and processed
  0 SetRequest-PDU accepted and processed
  0 Trap PDUs accepted and processed
  0 Alternate Response Class PDUs dropped silently
  0 Forwarded Confirmed Class PDUs dropped silently
```

Table 381 Descriptions on the fields of the display snmp-agent statistics command

Field	Description
Messages delivered to the SNMP entity	Number of packets delivered to the SNMP agent
Messages which were for an unsupported version	Number of packets from a device with an SNMP version that is not supported by the current SNMP agent
Messages which used a SNMP community name not known	Number of packets that use an unknown community name
Messages which represented an illegal operation for the community supplied	Number of packets with operations that breach the access right of a community
ASN.1 or BER errors in the process of decoding	Number of packets with ASN.1 or BER errors
Messages passed from the SNMP entity	Number of packets sent by an SNMP Agent
SNMP PDUs which had badValue error-status	Number of SNMP PDUs with a badValue error
SNMP PDUs which had genErr error-status	Number of SNMP PDUs with a genErr error
SNMP PDUs which had noSuchName error-status	Number of PDUs with a noSuchName error
SNMP PDUs which had tooBig error-status (Maximum packet size 1500)	Number of PDUs with a tooBig error (the maximum packet size is 1,500 bytes)
MIB objects retrieved successfully	Number of MIB objects that have been successfully retrieved

Table 381 Descriptions on the fields of the display snmp-agent statistics command

Field	Description
MIB objects altered successfully	Number of MIB objects that have been successfully modified
GetRequest-PDU accepted and processed	Number of get requests that have been received and processed
GetNextRequest-PDU accepted and processed	Number of getNext requests that have been received and processed
GetBulkRequest-PDU accepted and processed	Number of getBulk requests that have been received and processed
GetResponse-PDU accepted and processed	Number of get responses that have been received and processed
SetRequest-PDU accepted and processed	Number of set requests that have been received and processed
Trap PDUs accepted and processed	Number of Trap messages that have been received and processed
Alternate Response Class PDUs dropped silently	Number of dropped response packets
Forwarded Confirmed Class PDUs dropped silently	Number of forwarded packets that have been dropped

display snmp-agent sys-info

Syntax **display snmp-agent sys-info** [**contact** | **location** | **version**] *

View Any view

Parameter **contact**: Displays the contact information of the current network administrator.

location: Displays the location information of the current device.

version: Displays the version of the current SNMP agent.

Description Use the **display snmp-agent sys-info** command to display the current SNMP system information.

If no keyword is specified, all SNMP agent system information will be displayed.

Example # Display the current SNMP agent system information.

```
<Sysname> display snmp-agent sys-info
   The contact person for this managed node:
           3Com Technology Co., Ltd.
   The physical location of this node:
           Hangzhou China
   SNMP version running in the system:
           SNMPv3
```

display snmp-agent trap-list

Syntax **display snmp-agent trap-list**

View Any view

Parameter None

Description Use the **display snmp-agent trap-list** command to display the modules that can send the Trap messages and whether their Trap sending is enabled or not. If a module comprises of multiple sub-modules, then as long as one sub-module has the sending of Trap messages enabled, the whole module will be displayed as being enabled with the Trap sending.

Related command: **snmp-agent trap enable**.

Example # Display the modules that can send the Trap messages and whether their Trap sending is enabled or not.

```
<Sysname> display snmp-agent trap-list

   bgp trap enable
   configuration trap enable
   flash trap enable
   isdn trap enable
   mpls trap enable
   ospf trap enable
   standard trap enable
   system trap enable
   vrrp trap enable

   Enable traps: 8; Disable traps: 0
```

In the above output, enable indicates that the module is enabled with the Trap sending whereas disable indicates the Trap sending is disabled. By default, Trap sending is enabled on all modules that can send Trap messages. Use the **snmp-agent trap enable** command to manually configure whether the Trap sending is enabled or not.

display snmp-agent usm-user

Syntax **display snmp-agent usm-user** [**switch fabricid** *switch fabricid* | **username** *user-name* | **group** *group-name*] *

View Any view

Parameter e*ngineid*: Displays SNMPv3 user information for a specified switch fabric ID.

user-name: Displays SNMPv3 user information for a specified user name. It is case sensitive.

group-name: Displays SNMPv3 user information for a specified SNMP group name. It is case sensitive.

Description Use the **display snmp-agent usm-user** command to display SNMPv3 user information.

Example # Display SNMPv3 information for the user aa.

```
<Sysname> display snmp-agent usm-user username aa
   User name: aa
   Group name: mygroupv3
       Engine ID: 800007DB0000000000006877
       Storage-type: nonVolatile
       UserStatus: active
```

Table 382 Descriptions on the fields of the display snmp-agent usm-user command

Field	Description
User name	SNMP user name
Group name	SNMP group name
Engine ID	Engine ID for an SNMP entity
Storage-type	Storage type
UserStatus	SNMP user status

enable snmp trap updown

Syntax **enable snmp trap updown**

undo enable snmp trap updown

View Interface view

Parameter None

Description Use the **enable snmp trap updown** command to enable the sending of Trap messages for interface state change (linkup/linkdown SNMP Trap messages).

Use the **undo enable snmp trap updown** command to disable the sending of linkup/linkdown SNMP Trap messages on an interface.

By default, the sending of linkup/linkdown SNMP Trap messages is enabled.

Note that:

To enable an interface to send SNMP Trap packets when its state changes, you need to enable the Link up/down Trap packet transmission function on an interface and globally. Use the **enable snmp trap updown** command to enable this function on an interface, and use the **snmp-agent trap enable** [**standard** [**linkdown** | **linkup**] *] command to enable this function globally.

Related command: **snmp-agent target-host**, **snmp-agent trap enable**.

Example # Enable the sending of linkup/linkdown SNMP Trap messages on the port Ethernet 6/1/1 and use the community name **public**.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable
[Sysname] snmp-agent target-host trap address udp-domain 10.1.1.1 pa
rams securityname public
[Sysname] interface ethernet 6/1/1
[Sysname-Ethernet6/1/1] enable snmp trap updown
```

snmp-agent

Syntax **snmp-agent**

undo snmp-agent

View System view

Parameter None

Description Use the **snmp-agent** command to enable SNMP agent.

Use the **undo snmp-agent** command to disable SNMP agent.

By default, SNMP agent is disabled.

Example # Disable the current SNMP agent.

```
<Sysname> system-view
[Sysname] undo snmp-agent
```

snmp-agent community

Syntax **snmp-agent community** { **read** | **write** } *community-name* [**acl** *acl-number* | **mib-view** *view-name*] *

undo snmp-agent community *community-name*

View System view

Parameter **read**: Indicates that the community has read only access right to the MIB objects, that is, the community can only inquire MIB information.

write: Indicates that the community has read and write access right to the MIB objects, that is, the community can configure MIB information.

community-name: Community name, a string of 1 to 32 characters.

view-name: MIB view name, a string of 1 to 32 characters. If no keyword is specified, the default view is ViewDefault (The view created by the system after SNMP Agent is enabled).

acl-number: ACL for the community name, in the range 2,000 to 2,999.

Description Use the **snmp-agent community** command to configure a new SNMP community. Parameters to be configured include access right, community name, ACL, and accessible MIB views.

Use the **undo snmp-agent community** command to delete a specified community.

The community name configured with this command is only valid for the SNMP v1 and v2c agent.

Example # Configure a community with the name of comaccess that has read-only access right.

```
<Sysname> system-view
[Sysname] snmp-agent community read comaccess
```

Delete the community comaccess.

```
<Sysname> system-view
[Sysname] undo snmp-agent community comaccess
```

snmp-agent group

Syntax The following syntax applies to SNMPv1 and SNMP v2c:

snmp-agent group { **v1** | **v2c** } *group-name* [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*] [**acl** *acl-number*]

undo snmp-agent group { **v1** | **v2c** } *group-name*

The following syntax applies to SNMPv3:

snmp-agent group v3 *group-name* [**authentication** | **privacy**] [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*] [**acl** *acl-number*]

undo snmp-agent group v3 *group-name* [**authentication** | **privacy**]

View System view

Parameter **v1**: SNMPv1.

v2c: SNMPv2c.

v3: SNMPv3.

group-name: Group name, a string of 1 to 32 characters.

authentication: Specifies the security model of the SNMP group to be authentication only (without privacy).

privacy: Specifies the security model of the SNMP group to be authentication and privacy.

read-view *read-view*: Read view, a string of 1 to 32 characters.

write-view *write-view:* Write view, a string of 1 to 32 characters.

notify-view *notify-view*: Notify view, for sending Trap messages, a string of 1 to 32 characters.

acl *acl-number*: Specifies an ACL by its number, in the range 2000 to 2999.

Description Use the **snmp-agent group** command to configure a new SNMP group and specify its access right.

Use the **undo snmp-agent group** command to delete a specified SNMP group.

By default, SNMP groups configured by the **snmp-agent group v3** command use a no-authentication-no-privacy security model.

Related command: **snmp-agent mib-view**, **snmp-agent usm-user**.

Example # Create an SNMP group group1 on an SNMPv3 enabled device, no authentication, no privacy.

```
<Sysname> system-view
[Sysname] snmp-agent group v3 group1
```

snmp-agent local-switch fabricid

Syntax **snmp-agent local-switch fabricid** *switch fabricid*

undo snmp-agent local-switch fabricid

View System view

Parameter *switch fabricid*: Engine ID, an even number of hexadecimal characters, in the range 10 to 64. Its length must not be an odd number, and the all-zero and all-F strings are invalid.

Description Use the **snmp-agent local-switch fabricid** command to configure a local switch fabric ID for an SNMP entity.

Use the **undo snmp-agent local-switch fabricid** command to restore the default local switch fabric ID.

By default, the switch fabric ID of a device is the combination of company ID and device ID. Note that if the newly configured switch fabric ID is not the same as the one used for creating the USM user, the user is invalid.

Related command: **snmp-agent usm-user**.

Example # Configure the local switch fabric ID to be 123456789A.

```
<Sysname> system-view
[Sysname] snmp-agent local-switch fabricid 123456789A
```

snmp-agent mib-view

Syntax **snmp-agent mib-view** { **included** | **excluded** } *view-name oid-tree* [**mask** *mask-value*]

undo snmp-agent mib-view *view-name*

View System view

Parameter **included**: Indicates that all nodes of the MIB tree are included in current view.

excluded: Indicates that not all nodes of the MIB tree are included in current view.

view-name: View name, a string of 1 to 32 characters.

oid-tree: MIB subtree. It can only be an OID string of 1 to 25 characters, such as 1.4.5.3.1, or an object name string, such as "system". OID is made up of a series of integers, which marks the position of the node in the MIB tree and uniquely identifies a MIB object.

mask *mask-value*: Mask for an object tree, in the range 1 to 32 hexadecimal digits.

Description Use the **snmp-agent mib-view** command to create or update MIB view information so that MIB objects can be specified.

Use the **undo snmp-agent mib-view** command to delete the current configuration.

By default, MIB view name is ViewDefault.

Related command: **snmp-agent group**.

Example # Create a MIB view mibtest, which includes all objects of the subtree mib2.

```
<Sysname> system-view
[Sysname] snmp-agent mib-view included mib2 1.3.6.1
```

snmp-agent packet max-size

Syntax **snmp-agent packet max-size** *byte-count*

undo snmp-agent packet max-size

View System view

Parameter *byte-count*: Maximum number of bytes of an SNMP packet that can be received or sent by an agent, in the range 484 to 17,940. The default value is 1,500 bytes.

Description Use the **snmp-agent packet max-size** command to configure the maximum number of bytes in an SNMP packet that can be received or sent by an agent.

Use the **undo snmp-agent packet max-size** command to restore the default packet size.

Example # Configure the maximum number of bytes that can be received or sent by an SNMP agent to 1,042 bytes.

```
<Sysname> system-view
[Sysname] snmp-agent packet max-size 1042
```

snmp-agent sys-info

Syntax **snmp-agent sys-info** { **contact** *sys-contact* | **location** *sys-location* | **version** { **all** | { **v1** | **v2c** | **v3** }* } }

undo snmp-agent sys-info { **contact** | **location** | **version** { **all** | { **v1** | **v2c** | **v3** }* } }

View System view

Parameter *sys-contact*: A string that describes the contact information for system maintenance.

sys-location: A string that describes the location of the device.

version: The SNMP version in use.

- **v1**: SNMPv1.
- **v2c**: SNMPv2c.
- **v3**: SNMPv3.
- **all**: Specifies SNMPv1, SNMPv2c, and SNMPv3.

Description Use the **snmp-agent sys-info** command to configure system information, including the contact information, the location, and the SNMP version in use.

Use the **undo snmp-agent sys-info** command to restore the default configuration.

By default, the location information is Hangzhou China, version is SNMPv3, and the contact is 3Com Technology Co., Ltd.

Related command: **display snmp-agent sys-info**.

Network maintenance switch fabricers can use the system contact information to get in touch with the manufacturer in case of network failures. The system

location information is a management variable under the system branch as defined in RFC 1213-MIB, it identifies the location of the managed object.

Example # Configure the contact information as "Dial System Operator at beeper # 27345".

```
<Sysname> system-view
[Sysname] snmp-agent sys-info contact Dial System Operator at beeper # 27345
```

snmp-agent target-host

Syntax **snmp-agent target-host trap address udp-domain** { *ip-address* | **ipv6** *ipv6-address* } [**udp-port** *port-number*] **params securityname** *security-string* [**v1** | **v2c** | **v3** [**authentication** | **privacy**]]

undo snmp-agent target-host { *ip-address* | **ipv6** *ipv6-address* } **securityname** *security-string*

View System view

Parameter **trap**: Specifies the host to be the Trap host.

address: Specifies the IP address of the target host for the SNMP messages.

udp-domain: Indicates that the Trap message is transmitted using UDP.

ip-address: The IPv4 address of the Trap host.

ipv6: Specifies that the target host that receives Trap messages uses the IPv6 address.

ipv6-address: The IPv6 address of the Trap host.

port-number: Specifies the number of the port that receives Trap packets.

params securityname *security-string*: Specifies authentication related parameters, which is SNMPv1 or SNMPv2c community name or an SNMPv3 user name, a string of 1 to 32 characters.

v1: SNMPv1.

v2c: SNMPv2c.

v3: SNMPv3.

authentication: Specifies the security model to be authentication without privacy.

privacy: Specifies the security model to be authentication with privacy.

Description Use the **snmp-agent target-host** command to configure the related settings for a Trap target host.

Use the **undo snmp-agent target-host** command to remove the current settings.

To enable the device to send Traps, you need to use the **snmp-agent target-host** command in combination with the **snmp-agent trap enable** and the **enable snmp trap updown** commands.

Related command: **enable snmp trap updown**, **snmp-agent trap enable**, **snmp-agent trap source**, **snmp-agent trap life**.

Example # Enable the device to send SNMP Traps to 10.1.1.1, using the community name of "public".

```
<Sysname> system-view
[Sysname] snmp-agent trap enable standard
[Sysname] snmp-agent target-host trap address udp-domain 10.1.1.1 pa
rams securityname public
```

snmp-agent trap enable

Syntax **snmp-agent trap enable** [**bgp** | **configuration** | **flash** | **mpls** | **ospf** [*process-id*] [*ospf-trap-list*] | **standard** [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**]* | **system** | **vrrp** [**authfailure** | **newmaster**]]

undo snmp-agent trap enable [**bgp** | **configuration** | **flash** | **mpls** | **ospf** [*process-id*] [*ospf-trap-list*] | **standard** [**authentication** | **coldstart** | **linkdown** | **linkup | warmstart**]* | **system** | **vrrp** [**authfailure** | **newmaster**]]

View System view

Parameter **bgp**: Enables the sending of BGP Trap packets.

configuration: Enables the sending of configuration Trap packets.

flash: Enables the sending of FLASH Trap packets.

mpls: Enables the sending of LSP Trap packets.

ospf [*process-id*] [*ospf-trap-list*]: Enables the sending of OSPF Trap packets. The parameter *process-id* is the process ID and *spf-trap-list* is the Trap packet list.

standard: Enables the sending of standard Trap packets.

- **authentication**: Enables the sending of authentication failure Trap packets in the event of authentication failure.
- **coldstart**: Sends coldstart Trap packets when the device restarts.
- **linkdown**: Sends linkdown Trap packets when the port is in a linkdown status. It should be configured globally.
- **linkup**: Sends linkup Trap packets when the port is in a linkup status. It should be configured globally.

warmstart: Sends warmstart Trap packets when the SNMP restarts.

system: Sends 3Com-SYS-MAN-MIB (a private MIB) Trap packets.

vrrp [**authfailure** | **newmaster**]: Sends VRRP Trap packets.

- **authfailure**: Sends authentication failure VRRP Trap packets.
- **newmaster**: Enables the sending of VRRP newmaster Trap packets when the device becomes the Master.

Description Use the **snmp-agent trap enable** command to enable the device to send Trap messages globally.

Use the **undo snmp-agent trap enable** command to disable the device from sending Trap messages.

By default, the device is enabled to send Trap messages.

Note that:

To enable an interface to send SNMP Trap packets when its state changes, you need to enable the Link up/down Trap packet transmission function on an interface and globally. Use the **enable snmp trap updown** command to enable this function on an interface, and use the **snmp-agent trap enable** [**standard** [**linkdown** | **linkup**] *] command to enable this function globally.

Related command: **snmp-agent target-host**, **enable snmp trap updown**.

Example # Enable the device to send SNMP authentication failure packets to 10.1.1.1, using the community name of "public".

```
<Sysname> system-view
[Sysname] snmp-agent target-host trap address udp-domain 10.1.1.1 pa
rams securityname public
[Sysname] snmp-agent trap enable standard authentication
```

snmp-agent trap life

Syntax **snmp-agent trap life** *seconds*

undo snmp-agent trap life

View System view

Parameter *seconds*: Time-out time, in the range 1 to 2,592,000 seconds.

Description Use the **snmp-agent trap life** command to configure the life time for Traps, which will be discarded when their life time expires.

Use the **undo snmp-agent trap life** command to restore the default life time for Trap packets.

By default, the life time for SNMP Traps is 120 seconds.

Related command: **snmp-agent trap enable**, **snmp-agent target-host**.

Example # Configure the life time for Trap packets as 60 seconds.

```
<Sysname> system-view
[Sysname] snmp-agent trap life 60
```

snmp-agent trap queue-size

Syntax **snmp-agent trap queue-size** *size*

undo snmp-agent trap queue-size

View System view

Parameter *size*: The queue size for the Trap messages, in the range 1 to 1,000.

Description Use the **snmp-agent trap queue-size** command to configure the size of the Trap queue.

Use the **undo snmp-agent trap queue-size** command to restore the default queue size.

By default, up to 100 Trap messages can be stored in the Trap queue.

Related command: **snmp-agent trap enable**, **snmp-agent target-host**, **snmp-agent trap life**.

Example # Configure the size of the Trap queue to 200.

```
<Sysname> system-view
[Sysname] snmp-agent trap queue-size 200
```

snmp-agent trap source

Syntax **snmp-agent trap source** { *interface-type interface-number* }

undo snmp-agent trap source

View System view

Parameter *interface type interface-number*: Interface type and interface number.

Description Use the **snmp-agent trap source** command to specify the source IP address contained in the Trap message.

Use the **undo snmp-agent trap source** command to restore the default.

By default, SNMP chooses the IP address of an interface to be the source IP address of the Trap message.

Use this command to trace a specific event by the source IP address of a Trap message.

Before you can configure the IP address of a particular interface as the source IP address of the Trap message, ensure that the interface already exists and that it has a legal IP address. Otherwise, it is likely that the configurations will either fail or be invalid.

Related command: snmp-agent trap enable, **snmp-agent target-host**.

Example # Configure the IP address for the port Ethernet 1/1/1 as the source address for Trap packets.

```
<Sysname> system-view
[Sysname] snmp-agent trap source ethernet 1/1/1
```

snmp-agent usm-user

Syntax The following syntax applies to SNMPv1 and SNMPv2c:

snmp-agent usm-user { **v1** | **v2c** } *user-name group-name* [**acl** *acl-number*]

undo snmp-agent usm-user { **v1** | **v2c** } *user-name group-name*

The following syntax applies to SNMPv3:

snmp-agent usm-user v3 *user-name group-name* [**authentication-mode** { **md5** | **sha** } *auth-password* [**privacy-mode** { **des56** | **aes128** } *priv-password*]] [**acl** *acl-number*]

undo snmp-agent usm-user v3 *user-name group-name* { **local** | **switch fabricid** *switch fabricid-string* }

View System view

Parameter **v1**: SNMPv1.

v2c: SNMPv2c.

v3: SNMPv3.

user-name: User name, a string of 1 to 32 characters. It is case sensitive.

group-name: Group name, a string of 1 to 32 characters. It is case sensitive.

authentication-mode: Specifies that the security mode is authentication.

md5: Specifies the authentication protocol to be HMAC-MD5-96.

sha: Specifies the authentication protocol to be HMAC-SHA-96.

auth-password: Authentication password, a string of 1 to 64 characters.

privacy: Specifies that the security mode is privacy.

des56: Specifies the privacy protocol to be data encryption standard (DES).

aes128: Specifies the privacy protocol to be advanced encryption standard (AES).

priv-password: The privacy password, a string of 1 to 64 characters.

acl-number: Basic ACL, in the range 2,000 to 2,999.

local: Represents a local SNMP entity user.

switch fabricid-string: The switch fabric ID string, an even number of hexadecimal characters, in the range 10 to 64. Its length must not be an odd number, and the all-zero and all-F strings are invalid.

Description Use the **snmp-agent usm-user** command to add a user to an SNMP group.

Use the **undo snmp-agent usm-user** command to delete a user from an SNMP group.

Engine ID is used in authentication after you configure a user for a remote agent. If the switch fabric ID is changed after a user is configured, the user corresponding to the original switch fabric ID is invalid.

Note that the validity of a user depends on the switch fabric ID of the SNMP agent. If the switch fabric ID used for creating the user is not identical to the current switch fabric ID, the user is invalid.

For SNMPv1 and SNMPv2c, this command means adding of a new SNMP group. For SNMPv3, this command adds a new user to an SNMP group.

Related command: **snmp-agent group**, **snmp-agent community**, **snmp-agent local-switch fabricid**.

Example # Add a user John to the SNMP group **Johngroup**. Configure the security mode as authentication, the authentication protocol as HMAC-MD5-96, and the authentication password as hello.

```
<Sysname> system-view
[Sysname] snmp-agent group v3 Johngroup
[Sysname] snmp-agent usm-user v3 John Johngroup authentication-mode md5 hello
```

Specify SNMPv2c users to access the SNMP agent through reading v2cReadCommunity.

```
<Sysname> system-view
[Sysname] snmp-agent usm-user v2c v2cReadCommunity v2cGroup
[Sysname] snmp-agent group v2c v2cGroup read-view internet
[Sysname] snmp-agent mib-view included internet internet
```

93 RMON CONFIGURATION COMMANDS

debugging rmon

Syntax **debugging rmon**

View User view

Parameter None

Description Use the **debugging rmon** command to enable RMON debugging.

Use the **undo debugging rmon** command to disable RMON debugging.

By default, RMON debugging is disabled.

Example # Enable RMON debugging.

```
<Sysname> debugging rmon
```

display rmon alarm

Syntax **display rmon alarm** [*entry-number*]

View Any view

Parameter *entry-number*: Index of an RMON alarm entry, in the range 1 to 65535. If no entry is specified, the configuration of all alarm entries is displayed.

Description Use the **display rmon alarm** command to display the configuration of the specified or all RMON alarm entries.

Related command: **rmon alarm**.

Example # Display the configuration of all RMON alarm table entries.

```
<Sysname> display rmon alarm
Alarm table 1 owned by user1 is VALID.
  Samples type              : absolute
  Variable formula          : 1.3.6.1.2.1.16.1.1.1.4.1 <etherStatsOctets.1>
  Sampling interval         : 10(sec)
  Rising threshold          : 50(linked with event 1)
  Falling threshold         : 5(linked with event 2)
```

```
When startup enables      : risingOrFallingAlarm
Latest value              : 0
```

Table 383 Field descriptions of the display rmon alarm command

Field	Description
Alarm table	Alarm entry index, 1 in this example
owned by	Owner of the entry, user1 in this example
VALID	Status of the entry identified by the index (VALID means the entry is valid, and UNDERCREATION means invalid. You can use the **display rmon** command to view the invalid entry and with the **display current-configuration** and **display this** commands you cannot view the corresponding **rmon** commands.)
Samples type	The sampling type (absolute in this example)
Variable formula	Formula for the sampling value
Sampling interval	Sampling interval
Rising threshold	Alarm rising threshold (When the sampling value is bigger than or equal to this threshold, a rising alarm is triggered.)
Falling threshold	Alarm falling threshold (When the sampling value is smaller than or equal to this threshold, a falling alarm is triggered.)
When startup enables	How can an alarm be triggered
Latest value	The last sampled value

display rmon event

Syntax **display rmon event** [*entry-number*]

View Any view

Parameter *entry-number*: Index of an RMON event entry, in the range 1 to 65535.

Description Use the **display rmon event** command to display the configuration of the specified or all RMON event entries.

Displayed information includes event index, event owner, event description, action triggered by the event (such as sending log or trap messages), and last time the event occurred (the elapsed time since system initialization/startup) in seconds.

If no entry is specified, the configuration of all event entries is displayed.

Related command: **rmon event**.

Example # Display the configuration of RMON event table.

```
<Sysname> display rmon event
Event table 1 owned by user1 is VALID.
  Description: null.
  Will cause log-trap when triggered, last triggered at 0days 00h:02m:27s.
```

Table 384 Field descriptions of the display rmon event command

Field	Description
Event table	Event entry number
owned by	Owner of the entry
VALID	Status of the entry identified by the index (VALID means the entry is valid, and UNDERCREATION means invalid. You can use the **display rmon** command to view the invalid entry and with the **display current-configuration** and **display this** commands you cannot view the corresponding **rmon** commands.)
Description	Description for the event
cause log-trap when triggered	The event will trigger logging and trapping.
last triggered at	Last time the event was triggered

display rmon eventlog

Syntax **display rmon eventlog** [*entry-number*]

View Any view

Parameter *entry-number*: Index of an event entry, in the range 1 to 65535.

Description Use the **display rmon eventlog** command to display log information for the specified or all event entries.

If you use the **rmon event** command to specify that the action of an entry includes logging, then when this event is triggered, the event log is retained in the RMON log list. You can use the **display rmon eventlog** command to display detailed log information including event index, current event state, time the event was logged (the elapsed time in seconds since system initialization/startup), and event description.

If no entry number is specified, the log information for all event entries is displayed.

Example # Display the RMON log information for event entry 1.

```
<Sysname> display rmon eventlog 1
Event table 1 owned by user1 is VALID.
Generates eventLog 1.1 at 0days 00h:01m:39s.
Description: The 1.3.6.1.2.1.16.1.1.1.4.1 defined in alarm table 1,
less than(or =) 100 with alarm value 0. Alarm sample type is absolute.
Generates eventLog 1.2 at 0days 00h:02m:27s.
Description: The alarm formula defined in private alarm table 1,
less than(or =) 100 with alarm value 0. Alarm sample type is absolute.
```

Table 385 Field descriptions of the display rmon eventlog command

Field	Description
Event table	Event index
owned by	Owner of the entry

Table 385 Field descriptions of the display rmon eventlog command

Field	Description
VALID	Status of the entry identified by the index (VALID means the entry is valid, and UNDERCREATION means invalid. You can use the **display rmon** command to view the invalid entry and with the **display current-configuration** and **display this** commands you cannot view the corresponding **rmon** commands.)
Generates eventLog at	Time the log was created
Description	Log description

display rmon history

Syntax **display rmon history** [*interface-type interface-number*]

View Any view

Parameter *interface-type interface-number*: Specifies an interface by its type and number.

Description Use the **display rmon history** command to display RMON history control entry and last history sampling information, including bandwidth utilization, number of bad packets, and total packet number.

Related command: **rmon history**.

Example # Display RMON history control entries and history sample information for interface Ethernet 2/1/1.

```
<Sysname> display rmon history ethernet 2/1/1
History control entry 1 owned by user1 is VALID
  Samples interface     : Ethernet2/1/1<ifEntry.642>
  Sampling interval     : 10(sec) with 10 buckets max
  Latest sampled values :
  Dropevents        :0         , octets               :0
  packets           :0         , broadcast packets    :0
  multicast packets :0         , CRC alignment errors :0
  undersize packets :0         , oversize packets     :0
  fragments         :0         , jabbers              :0
  collisions        :0         , utilization          :0
```

Table 386 Field descriptions of the display rmon history command

Field	Description
History control entry	Index of the history control entry for the interface, 1 in this example
owned by	Owner of the entry

Table 386 Field descriptions of the display rmon history command

Field	Description
VALID	Status of the entry identified by the index (VALID means the entry is valid, and UNDERCREATION means invalid. You can use the **display rmon** command to view the invalid entry and with the **display current-configuration** and **display this** commands you cannot view the corresponding **rmon** commands.)
Samples Interface	The sampled interface
Sampling interval	Sampling interval
buckets max	Maximum number of records that can be stored in the history control table.
Latest sampled values	The latest sampled values
Dropevents	Dropped packets during the sampling period
octets	Number of octets received during the sampling period
packets	Number of packets received during the sampling period
broadcastpackets	Number of broadcasts received during the sampling period
multicastpackets	Number of multicasts received during the sampling period
CRC alignment errors	Number of packets received with CRC alignment errors during the sampling period
undersize packets	Number of undersize packets received during the sampling period
oversize packets	Number of oversize packets received during the sampling period
fragments	Number of fragments received during the sampling period
jabbers	Number of jabbers received during the sampling period
collisions	Number of colliding packets received during the sampling period
utilization	Bandwidth utilization during the sampling period

Currently, the Switch 8800s do not support statistics on jabbers.

display rmon prialarm

Syntax **display rmon prialarm** [*entry-number*]

View Any view

Parameter *entry-number*: Private alarm entry index, in the range 1 to 65535. If no entry is specified, the configuration of all private alarm entries is displayed.

Description Use the **display rmon prialarm** command to display the configuration of the specified or all private alarm entries.

Related command: **rmon prialarm**.

Example # Display the configuration of all private alarm entries.

```
<Sysname> display rmon prialarm
Prialarm table 5 owned by user1 is UNDERCREATION.
  Samples type          : changeratio
  Variable formula      : ((.1.3.6.1.2.1.16.1.1.1.5.1-.1.3.6.1.2.1.1
6.1.1.1.6.1)*100/.1.3.6.1.2.1.16.1.1.1.5.1)
  Description           : ifUtilization.GigabitEthernet2/1/1
  Sampling interval     : 10(sec)
  Rising threshold      : 892340484(linked with event 1)
  Falling threshold     : 889783312(linked with event 2)
  When startup enables  : risingOrFallingAlarm
  This entry will exist : forever
  Latest value          : 0
```

Table 387 Field descriptions of the display rmon prialarm command

Field	Description
Prialarm table	Index of the prialarm table
owned by	Owner of the entry, user1 in this example
VALID	Status of the entry identified by the index (VALID means the entry is valid, and UNDERCREATION means invalid. You can use the **display rmon** command to view the invalid entry and with the **display current-configuration** and **display this** commands you cannot view the corresponding **rmon** commands.)
Samples type	Samples type
Variable formula	Variable formula
Sampling interval	Sampling interval
Rising threshold	Alarm rising threshold. An alarm event is triggered when the sampled value is greater than or equal to this threshold.
Falling threshold	Alarm falling threshold. An alarm event is triggered when the sampled value is less than or equal to this threshold.
linked with event	Event index associated with the prialarm
When startup enables	How can an alarm be triggered
This entry will exist	The lifetime of the entry, which can be forever or span the specified period
Latest value	The last sampled value

display rmon statistics

Syntax **display rmon statistics** [*interface-type interface-number*]

View Any view

Parameter *interface-type interface-number*: Specifies an interface by its type and number.

Description Use the **display rmon statistics** command to display RMON statistics.

The displayed statistics include statistics about network collisions, CRC alignment errors, undersize/oversize packets, broadcasts, multicasts, bytes received, packets received, and so on.

Related command: **rmon statistics**.

Currently, the Switch 8800s do not support statistics about oversize frames and bytes received.

Example # Display RMON statistics for interface Ethernet 2/1/1.

```
<Sysname> display rmon statistics ethernet 1/0
<Sysname>display rmon statistics GigabitEthernet 4/2/2
Statistics entry 1 owned by user1-rmon is VALID.
  Interface : GigabitEthernet4/2/2<ifIndex.157>
  etherStatsOctets         : 0         , etherStatsPkts          : 0
  etherStatsBroadcastPkts  : 0         , etherStatsMulticastPkts : 0
  etherStatsUndersizePkts  : 0         , etherStatsOversizePkts  : 0
  etherStatsFragments      : 0         , etherStatsJabbers       : 0
  etherStatsCRCAlignErrors : 0         , etherStatsCollisions    : 0
  etherStatsDropEvents (insufficient resources): 0
  Packets received according to length:
  64     : 0         ,  65-127  : 0         ,  128-255  : 0
  256-511: 0         ,  512-1023: 0         ,  1024-1518: 0
```

Table 388 Field descriptions of the display rmon statistics command

Field	Description
Statistics entry	Statistics table entry index
VALID	Status of the entry identified by the index (VALID means the entry is valid, and UNDERCREATION means invalid. You can use the **display rmon** command to view the invalid entry and with the **display current-configuration** and **display this** commands you cannot view the corresponding **rmon** commands.)
Interface	Interface on which statistics are gathered
etherStatsOctets	Number of octets received by the interface during the statistical period
etherStatsPkts	Number of packets received by the interface during the statistical period
etherStatsBroadcastPkts	Number of broadcast packets received by the interface during the statistical period
etherStatsMulticastPkts	Number of multicast packets received by the interface during the statistical period
etherStatsUndersizePkts	Number of undersize packets received by the interface during the statistical period
etherStatsOversizePkts	Number of oversize packets received by the interface during the statistical period
etherStatsFragments	Number of undersize packets with CRC errors received by the interface during the statistical period

Table 388 Field descriptions of the display rmon statistics command

Field	Description
etherStatsJabbers	Number of oversize packets with CRC errors received by the interface during the statistical period
etherStatsCRCAlignErrors	Number of packets with CRC errors received on the interface during the statistical period
etherStatsCollisions	Number of collisions received on the interface during the statistical period
etherStatsDropEvents	Total number of drop events received on the interface during the statistical period
Packets received according to length:	Statistics of packets received according to length during the statistical period

Currently, the Switch 8800s do not support statistics on etherStatsJabbers.

rmon alarm

Syntax **rmon alarm** *entry-number alarm-variable sampling-interval* { **absolute** | **delta** } **rising-threshold** *threshold-value1 event-entry1* **falling-threshold** *threshold-value2 event-entry2* [**owner** *text*]

undo rmon alarm *entry-number*

View System view

Parameter *entry-number*: Alarm entry index, in the range 1 to 65535.

alarm-variable: Alarm variable, a string of 1 to 256 characters, in dotted object identifier (OID) format, such as 1.3.6.1.2.1.2.1.10.1 (or ifInOctets.1). Only variables that can be parsed into INTEGER (INTEGER, Counter, Gauge, or Time Ticks) in the ASN.1 can be used for the *alarm-variable* argument.

sampling-interval: Sampling interval, in the range 5 to 65535 seconds.

absolute: Sets the sampling type to **absolute**.

delta: Sets the sampling type to **delta**.

threshold-value1: Rising threshold, in the range -2147483648 to +2147483647.

event-entry1: Index of the event triggered when the rising threshold is reached. It ranges from 0 to 65535.

threshold-value2: Falling threshold, in the range -2147483648 to +2147483647.

event-entry2: Index of the event triggered when the falling threshold is reached. It ranges from 1 to 65535.

owner *text*: Owner of the entry, a string of 1 to 127 characters. It is case sensitive and space is supported.

Description Use the **rmon alarm** command to create an entry in the RMON alarm table.

Use the **undo rmon alarm** command to remove a specified entry from the RMON alarm table.

This command defines alarms. The generation and notification of an alarm however, is controlled by the event entry associated with it.

The following is how the system handles alarm entries:

1. Samples the alarm variables at the specified interval.
2. Compares the sampled values with the predefined threshold and does the following:
   - If the rising threshold is reached, triggers the event specified by the *event-entry1* argument.
   - If the falling threshold is reached, triggers the event specified by the *event-entry2* argument.

- *Before creating an alarm entry, define the events to be referenced in the event table with the **rmon event** command.*
- *Rising threshold alarm and falling threshold alarm are alternate. That is, if a rising/falling threshold alarm occurs, next alarm must be a falling/rising threshold alarm.*
- *When you create an entry, if the values of the specified alarm variable (alarm-variable), sampling interval (sampling-interval), sampling type (**absolute** or **delta**), rising threshold (threshold-value1) and falling threshold (threshold-value2) are identical to those of the existing alarm entry, the system considers their configurations the same and the creation fails.*
- *You can create up to 60 alarm entries.*

Example # Add entry 1 in the alarm table and sample the node 1.3.6.1.2.1.16.1.1.1.4.1 at a sampling interval of 10 seconds in absolute sampling type. Generate event 1 when the sampled value is greater than or equal to the rising threshold of 50, and event 2 when the sampled value is lower than or equal to the falling threshold of 5. Set the owner of the entry to be user1.

```
<Sysname> system-view
[Sysname] rmon event 1 log
[Sysname] rmon event 2 none
[Sysname] interface Gigabitethernet 2/1/1
[Sysname-GigabitEthernet2/1/1] rmon statistics 1
[Sysname-GigabitEthernet2/1/1] quit
[Sysname] rmon alarm 1 1.3.6.1.2.1.16.1.1.1.4.1 10 absolute rising_t
hreshold 50 1 falling_threshold 5 2 owner user1
```

Remove the alarm table entry with the index of 15.

```
<Sysname> system-view
[Sysname] undo rmon alarm 15
```

rmon event

Syntax **rmon event** *entry-number* [**description** *string*] { **log** | **trap** *trap-community* | **log-trap** *log-trapcommunity* | **none** } [**owner** *text*]

undo rmon event *entry-number*

View System view

Parameter *entry-number*: Event entry index, in the range 1 to 65535.

description *string*: Event description, a string of 1 to 127 characters.

log: Logs the event when it occurs.

trap: Sends a trap when the event occurs.

trap-community: Network management station community to which traps are sent, a string of 1 to 127 characters.

log-trap: Performs both logging and trap sending when the event occurs.

log-trapcommunity: Community name of the network management station that receives trap messages, a string of 1 to 127 characters.

none: Performs no action when the event occurs.

owner *text*: Owner of the entry, a string of 1 to 127 characters. It is case sensitive and space is supported.

Description Use the **rmon event** command to create an entry in the RMON event table.

Use the **undo rmon event** command to remove the specified entry from the RMON event table.

When an event is triggered by its associated alarm in the alarm table, the event group allows you to log it, send a trap, do both, or do neither at all. This helps control the generation and notification of events.

- *When you create an entry, if the values of the specified event description (**description** string), event type (**log**, **trap**, **logtrap** or **none**), and community name (trap-community or log-trapcommunity) are identical to those of the existing event entry, the system considers their configurations the same and the creation fails.*
- *You can create up to 60 alarm entries.*

Example # Create event 10 in the RMON event table.

```
<Sysname> system-view
[Sysname] rmon event 10 log owner user1
```

rmon history

Syntax **rmon history** *entry-number* **buckets** *number* **interval** *sampling-interval* [**owner** *text*]

undo rmon history *entry-number*

View Ethernet interface view

Parameter *entry-number:* History control entry index, in the range 1 to 65535.

buckets *number*: History table size for the entry, in the range 1 to 65535. A Switch 8800 supports 10 buckets only.

interval *sampling-interval*: Sampling interval, in the range 5 to 3600 seconds.

owner *text-string*: Owner of the entry, a string of 1 to 127 characters. It is case sensitive and space is supported.

Description Use the **rmon history** command to create an entry in the RMON history control table.

Use the **undo rmon history** command to remove a specified entry from the RMON history control table.

This command enables RMON to periodically sample and save for an interface data such as bandwidth utilization, errors, and total number of packets for later retrieval.

- *When you create an entry, if the value of the specified sampling interval (**interval** sampling-interval) is identical to that of the existing history entry, the system considers their configurations the same and the creation fails.*
- *You can create up to 100 alarm entries.*

Related command: **display rmon history**.

Example # Create RMON history control entry 1 for interface Ethernet 2/1/1, the index is 1, table size is 10, and sampling interval is 5 seconds.

```
<Sysname> system-view
[Sysname] interface ethernet 2/1/1
[Sysname-Ethernet2/1/1] rmon history 1 buckets 10 interval 5 owner user1
```

Remove history control entry 15.

```
<Sysname> system-view
[Sysname] interface ethernet 2/1/1
[Sysname-Ethernet2/1/1] undo rmon history 15
```

rmon prialarm

Syntax **rmon prialarm** *entry-number prialarm-formula prialarm-des sampling-interval* { **absolute** | **changeratio** | **delta** } **rising_threshold** *threshold-value1 event-entry1* **falling_threshold** *threshold-value2 event-entry2* **entrytype** { **forever** | **cycle** *cycle-period* } [**owner** *text*]

undo rmon prialarm *entry-number*

View System view

Parameter *entry-number*: Index of a private alarm entry, in the range 1 to 65535.

prialarm-formula: Private alarm variable formula, a string of 1 to 256 characters. The variables in the formula must be represented in OID format that starts with a point ".", the formula (.1.3.6.1.2.1.2.1.10.1)*8 for example. You may perform the basic operations of addition, subtraction, multiplication, and division on these variables. The operations should yield a long integer. To prevent errors, make sure that the result of each calculating step falls into the value range for long integers.

prialarm-des: Private alarm entry description, a string of 1 to 127 characters.

sampling-interval: Sampling interval, in the range 10 to 65,535 seconds.

absolute | **changeratio** | **delta** : Sets the sampling type to absolute, delta, or change ratio.

threshold-value1: Rising threshold, in the range -2147483648 to +2147483647.

event-entry1: Index of the event triggered when the rising threshold is reached. It ranges from 0 to 65535.

threshold-value2: Falling threshold, in the range -2147483648 to +2147483647.

event-entry2: Index of the event triggered when the falling threshold is reached. It ranges from 0 to 65535.

forever: Indicates that the lifetime of the private alarm entry is infinite.

cycle *cycle-period*: Sets the lifetime period of the private alarm entry, in the range 0 to 2147483647 seconds.

owner *text*: Owner of the entry, a string of 1 to 127 characters. It is case sensitive and space is supported.

Description Use the **rmon prialarm** command to create an entry in the private alarm table of RMON.

Use the **undo rmon prialarm** command to remove a private alarm entry from the private alarm table of RMON.

The following is how the system handles private alarm entries:

1. Samples the private alarm variables in the private alarm formula at the specified sampling interval.
2. Performs calculation on the sampled values with the formula.
3. Compares the calculation result with the predefined thresholds and does the following:
   - If the rising threshold is reached, triggers the event specified by the *event-entry1* argument.
   - If the falling threshold is reached, triggers the event specified by the *event-entry2* argument.

- *Before creating a private alarm entry, define the events to be referenced in the event table with the* ***rmon event*** *command.*
- *When you create an entry, if the values of the specified alarm variable formula (prialarm-formula), sampling type (****absolute changeratio*** *or* ***delta****), rising threshold (threshold-value1) and falling threshold (threshold-value2) are identical to those of the existing alarm entry, the system considers their configurations the same and the creation fails.*
- *You can create up to 50 pri-alarm entries.*
- *For private alarms, the rising threshold alarm and falling threshold alarm are alternate.*

Example # Create entry 5 in the private alarm table. Calculate the private alarm variables with the (1.3.6.1.2.1.16.1.1.1.6.1*100/.1.3.6.1.2.1.16.1.1.1.5.1) formula and sample the corresponding variables at intervals of 10 seconds to get the percentage of broadcasts received on GigabitEthernet 1/1/5 in the total packets. When this ratio reaches or is bigger than the rising threshold of 50, trigger event 1; when this ratio reaches or drops under the falling threshold, trigger event 2. Set the lifetime of the entry to forever and owner to user 1.

```
<Sysname> system-view
[Sysname] rmon event 1 log
[Sysname] rmon event 2 none
[Sysname] interface Gigabitethernet 1/1/5
[Sysname-Gigabitethernet1/1/5] rmon statistics 1
[Sysname-Gigabitethernet1/1/5] quit
[Sysname] rmon prialarm 5 (.1.3.6.1.2.1.16.1.1.1.6.1*100/.1.3.6.1.2.
1.16.1.1.1.5.1) packet.Ethernet1/0 10 absolute rising-threshold 50 1
 falling-threshold 5 2 entrytype forever owner user1
```

Remove private alarm entry 10.

```
<Sysname> system-view
[Sysname] undo rmon prialarm 10
```

rmon statistics

Syntax **rmon statistics** *entry-number* [**owner** *text*]

undo rmon statistics *entry-number*

View Ethernet interface view

Parameter *entry-number*: Index of statistics entry, in the range 1 to 65535.

owner *text*: Owner of the entry, a string of 1 to 127 characters. It is case sensitive and space is supported.

Description Use the **rmon statistics** command to create an entry in the RMON statistics table.

Use the **undo rmon statistics** command to remove a specified entry from the RMON statistics table.

The RMON statistics group collects information on how a monitored port is being used and records errors. Statistics include number of collisions, CRC alignment errors, number of undersize or oversize packets, number of broadcasts, number of multicasts, number of bytes received, number of packets received.

To display information for the RMON statistics table, use the **display rmon statistics** command.

- *Currently, the Switch 8800s do not support statistics on oversize frames and bytes received.*
- *Only one statistics entry can be created on one interface.*
- *You can create up to 100 statistics entries.*

Example # Create an entry in the RMON statistics table for interface Ethernet 2/1/1. The index of the entry is 20.

```
<Sysname> system-view
[Sysname] interface ethernet 2/1/1
[Sysname-Ethernet2/1/1] rmon statistics 20 owner user1
```

94 NTP CONFIGURATION COMMANDS

debugging ntp-service

Syntax **debugging ntp-service** { **access** | **adjustment** | **all | authentication** | **event** | **filter** | **packet** | **parameter** | **refclock** | **selection** | **synchronization** | **validity** }

undo debugging ntp-service { **access** | **adjustment** | **all | authentication** | **event** | **filter** | **packet** | **parameter** | **refclock** | **selection** | **synchronization** | **validity** }

View User view

Parameter **access**: Enables debugging for NTP access control.

adjustment: Enables debugging for NTP clock adjustment.

all: Enables all NTP debugging.

authentication: Enables debugging for NTP authentication.

event: Enables debugging for NTP events.

filter: Enables debugging for NTP clock filtering.

packet: Enables debugging for NTP packets.

parameter: Enables debugging for NTP clock parameters.

refclock: Enables debugging for NTP reference clock.

selection: Enables debugging for NTP clock selection information.

synchronization: Enables debugging for NTP clock synchronization information.

validity: Enables debugging for NTP remote server validity.

Description Use the **debugging ntp-service** command to enable the corresponding NTP debugging function(s).

Use the **undo debugging ntp-service** command to disable the corresponding NTP debugging function(s).

By default, all NTP debugging is disabled.

***access** and **synchronization** debugging are for extension use.*

Table 389 Field descriptions of debugging ntp-service adjustment

Field	Description
NTP: gradual systime	Adjust system time by steps
NTP: step systime	Adjust system time in a single step
adj: *string*	Adjustment value of this time
residual: *string*	Residual value of last time
offset: *string*	Offset of single step adjustment

Table 390 Field descriptions of debugging ntp-service authentication

Field	Description
session_key	Session key
srcadr: *string*	Source IP address
dstadr: *string*	Destination IP address
keyid: *string*	Key ID
life: *string*	Life time of the key
auth_agekeys	State of the key life time
time: *string*	Current time of the key life time
trusted keynum: *string*	Number of trusted keys
expired keynum: *string*	Number of keys to be expired
Authentication keyID: *string*	Authentication key ID

Table 391 Field descriptions of the debugging ntp-service event command

Field	Description
NTP: control event	NTP control event
event: *string*	Event code
eventnum: *string*	Number of events
peer: *string*	IP address of the peer

Table 392 Field descriptions of the debugging ntp-service filter command

Field	Description
NTP: adj freq	Adjustment frequency
last clockoffset: *string*	Last clock offset
last drift_comp: *string*	Last frequency
new clockOffset: *string*	New clock offset
new drift_comp: *string*	New frequency
The offset *string* is larger than the value permitted, no adjustment.	Adjustment cannot be made, because the offset is larger than the value that can be adjusted.

Table 393 Field descriptions of the debugging ntp-service packet command

Field	Description
NTP: *titleAndTip* control packet from *sourceIPAddress* to *DestIPAddress*	*titleAndTip*: Title and prompt information *sourceIPAddress*: Source IP address of the control packet *DestIPAddress*: Destination IP address of the control packet
version: *string*	Protocol version in the control packet
r: *string*	Response bit in the control packet
e: *string*	Error bit in the control packet
m: *string*	Meet bit in the control packet
o: *string*	Operation code in the control packet
sequence: *string*	Sequence number in the control packet
status: *string*	Status word in the control packet
associationID: *string*	Association ID in the control packet
data: *string*	Data information in the control packet
authenticator: *string*	Message authenticator in the control packet
packet to *string*	Destination IP address of the packet sent
leap: *string*	Trap information in the packet
version: *string*	Protocol version in the packet
mode: *string*	Working mode in the packet
vrfindex: *string*	VPN index of the packets received or sent
stratum: *string*	Stratum in the packet
ppoll: *string*	Poll interval in the packet
precision: *string*	Precision in the packet
rdel: *string*	Root delay in the packet
rdsp: *string*	Root dispersion in the packet
refid: *string*	Reference clock identity in the packet
reftime: *string*	Reference timestamp in the packet
orgtime: *string*	Originate timestamp in the packet
rectime: *string*	Receive timestamp in the packet
xmttime: *string*	Transmit timestamp in the packet
inptime: *string*	Input timestamp
packet from *SourceIPAddress* to *DestIPAddress* on *InterfaceName*	*SourceIPAddress*: Source IP address of the packet *DestIPAddress*: Destination IP address of the packet *InterfaceName*: Name of the interface that receives the packet

Table 394 Field descriptions of debugging ntp-service parameter

Field	Description
NTP: popcorn spike: *string*	Popcorn spike of the offset when calculating time sample
NTP: discard: *string*	A new time sample is discarded when the new time sample is smaller than or equals the select time sample. The lifetime of the dropped sample is displayed here.

Table 394 Field descriptions of debugging ntp-service parameter

Field	Description
clock_filter(*PeerAddr, SampleOffset, SampleDelay, SampleDisp*)	Peer IP address, time sample offset, time sample delay, and time sample dispersion in clock filtering
offset: *string*	Peer offset
delay: *string*	Peer delay
dispersion: *string*	Peer dispersion
std: *string*	Peer jitter

Table 395 Field descriptions of the debugging ntp-service refclock command

Field	Description
Report Event:	Reference clock event
Clock: *string*	Reference clock IP address
Event: *string*	Description on the clock event
Code: *string*	Clock event code
RefClock Transmit: At *CurrentTime IPAddr*	Reference clock transmits analog information.
	CurrentTime: Current system time
	IPAddr: IP address of the reference clock.
RefClock Sample:	Time sample of the reference clock
sampleNum: *string*	Number of samples
offset: *string*	Offset
disp: *string*	Dispersion
std: *string*	Jitter
RefClock Receive: At *CurrentTime IPAddr*	Reference clock receives analog information.
	CurrentTime: Current system time
	IPAddr: IP address of the reference clock

Table 396 Field descriptions of the debugging ntp-service selection command

Field	Description
nlist: *string*	Number of candidate clocks in the candidate clock list
allow: *string*	Number of allowed candidate clocks
found: *string*	Number of dropped candidate clocks
low: *string*	Lower threshold of the sample time difference
high: *string*	Upper threshold of the sample time difference
candidate: *string*	IP address of a candidate clock
cdist: *string*	Synchronization distance of a candidate clock
disp: *string*	Dispersion of a candidate clock
survivor: *string*	IP address of the survivor (the candidate clock that has passed the checks)
offset: *string*	Offset of the survivor
cdist: *string*	Dispersion of the survivor
syspeer: *string*	IP address of the system select clock source
offset: *string*	Offset of the system select clock source

Table 397 Field descriptions of the debugging ntp-service validity command

Field	Description
NTP: packet from *SourceIPAddr*, *TestResult* validity tests *TestCode*	*SourceIPAddr*: Source IP address of the packet *TestResult*: Test result, succeed or fail *TestCode*: Code of the test item Description of specific test item codes: ■ 0x0001: Receives the copied information ■ 0x0002: Receives forged information ■ 0x0004: The information is not synchronized. ■ 0x0008: The peer delay/dispersion is out of range. ■ 0x0010: Peer authentication fails. ■ 0x0020: Peer clock is not synchronized ■ 0x0040: Peer stratum is out of range. ■ 0x0080: Root delay/dispersion is out of range. ■ 0x0100: Peer is not authenticated. ■ 0x0200: Access is denied.

Example # Two network devices Sysname A and Sysname B:

- The IP address of VLAN-interface 1 of Sysname A is 10.1.1.1.
- The IP address of VLAN-interface 1 of Sysname B is 10.1.1.2.
- There is a route between 10.1.1.1 and 10.1.1.2.
- Sysname B uses local clock as the reference clock, with the stratum of 8.
- Enable NTP packet debugging on Sysname A.
- Sysname A is synchronized to Sysname B in the symmetric peers mode.

```
<SysnameA> debugging ntp-service packet
<SysnameA> terminal debugging
<SysnameA> terminal monitor
<SysnameA> system-view
[SysnameA] ntp-service unicast-peer 10.1.1.2
```

After the above configuration, the following packet debugging information is displayed on Sysname A:

```
*0.91612291 Sysname A NTP/8/debug_NTP_packet_xmt:
 packet to 10.1.1.2
 leap: 3, version: 3, mode: 3, vrfindex: 0
 stratum: 0, ppoll: 64, precision: 2**18
 rdel: 0.000, rdsp: 0.000, refid: 0.0.0.0
 reftime: 03:43:57.233 UTC Jan 17 2001(BE0F937D.3BB2031C)
 orgtime: 00:00:00.000 UTC Jan 1 1900(00000000.00000000)
 rectime: 00:00:00.000 UTC Jan 1 1900(00000000.00000000)
 xmttime: 03:48:34.289 UTC Jan 17 2001(BE0F9492.4A273929)
```

// NTP module sends an NTP request to Sysname B, with the destination IP address being 10.1.1.2; the local clock trap bit (leap) is 3, local NTP version number is 3; working mode is 3; the VPN index of the packets sent is 0 (namely, the public

network); local clock stratum is 0; the polling interval is 64 seconds, clock precision is the eighteenth power of 1/2 seconds; local delay is 0.000; root dispersion is 0.000; reference source ID is 0.0.0.0, which indicates there is no reference source; the follow-up information includes reference timestamp, originate timestamp, receive timestamp, and transmit timestamp respectively.

```
%Jan 17 03:48:34:320 2001 Sysname A NTP/5/NTP_LOG:
System leap changes from 3 to 0 after clock update.
%Jan 17 03:48:34:331 2001 Sysname A NTP/5/NTP_LOG:
System stratum changes from 16 to 9 after clock update.
```

// Log information about system clock trap (leap) and stratum changes.

```
*0.91612341 Sysname A NTP/8/debug_NTP_packet_rcv:
 packet from 10.1.1.2 to 10.1.1.1 on Vlan-interface1
 leap: 0, version: 3, mode: 4, vrfindex: 0
 stratum: 8, ppoll: 64, precision: 2**18
 rdel: 0.000, rdsp: 10.941, refid: 127.127.1.0
 reftime: 03:48:08.827 UTC Jan 17 2001(BE0F9478.D3C69728)
 orgtime: 03:48:34.289 UTC Jan 17 2001(BE0F9492.4A273929)
 rectime: 03:48:34.287 UTC Jan 17 2001(BE0F9492.497A4617)
 xmttime: 03:48:34.287 UTC Jan 17 2001(BE0F9492.49983947)
 inptime: 03:48:34.302 UTC Jan 17 2001(BE0F9492.4D592D98)
```

// Sysname A receives the NTP response from Sysname B. IP address of VLAN-interface 1 of Sysname B is 10.1.1.2 and that of Sysname A is 10.1.1.1, and the packet ingress interface is VLAN-interface 1; Sysname B's trap bit (leap) is 0, indicating that Sysname B is synchronized; Sysname B's NTP version number is 3, working mode is 4, the VPN index of the packets sent is 0; the peer clock stratum is 8; the polling interval is 64 seconds; clock precision is the eighteenth power of 1/2 seconds, root delay is 0.000, root dispersion is 0.000, reference source ID is 127.127.1.0, which indicates the reference source is the local clock; the follow-up information includes reference timestamp, originate timestamp, receive timestamp, transmit timestamp, and the input timestamp (the timestamp when the packet is processed locally) respectively.

The example here just shows the information of the first two packets. Actually, the above packet interactive process will proceed for multiple times.

display ntp-service sessions

Syntax **display ntp-service sessions** [**verbose**]

View Any view

Parameter **verbose**: Displays the detailed information of all NTP sessions.

Description Use the **display ntp-service sessions** command to view the information of all NTP sessions. Without the **verbose** keyword, this command displays only the brief information of all NTP service sessions.

Example # View the brief information of NTP service sessions.

```
<Sysname> display ntp-service sessions
source         reference    stra reach  poll     now     offset delay disper
**************************************************************************
[12345]1.1.1.1  127.127.1.0  3   377        512  178  0.0   40.1      22.8
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
Total associations :  1
```

Table 398 Field descriptions of the display ntp-service sessions command

Field	Description
source	IP address of the clock source
reference	Reference clock ID of the clock source
	If the reference clock is the local clock, the value of this field is related to the value of the **stra** field: When the value of the **stra** field is 0 or 1, this field will be "LOCL"; when the **stra** field has another value, this filed will be the IP address of the local clock
	If the reference clock is the clock of another device on the network, the value of this field will be the IP address of that device.
stra	Stratum level of the clock source
reach	Reachability count of the clock source. 0 indicates that the clock source in unreachable
poll	Poll interval, namely the maximum interval between successive NTP messages.
now	The length of time from when the last NTP message was received or when the local clock was last updated to the current time
	The time is in second by default. If the time length is greater than 2048 seconds, it is displayed in minutes (m); if greater than 300 minutes, in hours (h); if greater than 96 hours, in days (d).
offset	The offset of the system clock relative to the reference clock, in milliseconds
delay	the roundtrip delay from the local device to the clock source, in milliseconds
disper	The maximum error of the system clock relative to the reference source.
[12345]	1: Clock source selected by the system, namely the current reference source, with a system clock stratum level of ≤ 15
	2: Stratum level of this system source is ≤ 15
	3: This clock source has passed the clock selection process
	4: This clock source is a candidate clock source
	5: This clock source was created by a configuration command
Total associations	Total number of associations

*When a device is working in the NTP broadcast/multicast server mode, the **display ntp-service sessions** command executed on the device will not display the NTP session information corresponding to the broadcast/multicast server, but the sessions will be counted in the total number of associations.*

display ntp-service status

Syntax **display ntp-service status**

View Any view

Parameter None

Description Use the **display ntp-service status** command to view the NTP service status information.

Example # View the NTP service status information.

```
<Sysname> display ntp-service status
Clock status: unsynchronized
 Clock stratum: 16
 Reference clock ID: none
 Nominal frequency: 100.0000 Hz
 Actual frequency: 100.0000 Hz
 Clock precision: 2^17
 Clock offset: 0.0000 ms
 Root delay: 0.00 ms
 Root dispersion: 0.00 ms
 Peer dispersion: 0.00 ms
 Reference time: 00:00:00.000 UTC Jan 1 1900(00000000.00000000)
```

Table 399 Field descriptions of the display ntp-service status command

Field	Description
Clock status	Status of the system clock
Clock stratum	Stratum level of the local clock
Reference clock ID	After the system clock is synchronized to a remote time server or a local reference source, this field indicates the address of the remote time server or the identifier of the local clock source (when the local clock has a stratum level of 1, the value of this field is "LOCL"; when the local clock has another value, the value of this filed is the IP address of the local clock)
Nominal frequency	The nominal frequency of the local system hardware clock
Actual frequency	The actual frequency of the local system hardware clock
Clock precision	The precision of the system clock.
Clock offset	The offset of the system clock relative to the NTP server
Root delay	The roundtrip delay from the local device to the primary reference clock
Root dispersion	The maximum error of the system clock relative to the primary reference clock.
Peer dispersion	The maximum error of the system clock relative to the reference clock
Reference time	Reference timestamp

display ntp-service trace

Syntax **display ntp-service trace**

View Any view

Parameter None

Description Use the **display ntp-service trace** command view the brief information of each NTP server along the NTP server chain from the local device back to the primary reference source.

The **display ntp-service trace** command is available only if the local device can ping through all the devices on the NTP server chain; otherwise, this command will fail to display all the NTP servers on the NTP chain due to timeout.

Example

```
<Sysname> display ntp-service trace
 server 127.0.0.1,stratum 2, offset -0.013500, synch distance 0.03154
 server 133.1.1.1,stratum 1, offset -0.506500, synch distance 0.03429
 refid LOCL
```

The information above shows an NTP server synchronization chain for the server 127.0.0.1: The server 127.0.0.1 is synchronized to the server 133.1.1.1, and the server 133.1.1.1 is synchronized to the local clock source.

Table 400 Field descriptions of the display ntp-service trace command

Field	Description
stratum	The stratum of the corresponding local clock reference
server	IP address of the NTP server
refid	Identifier of the primary reference source. When the stratum level of the primary reference clock is 0, it is displayed as LOCL; otherwise, it is displayed as the IP address of the primary reference clock.
offset	The clock offset relative to the upper-level clock reference
synch distance	The synchronization distance relative to the upper-level clock reference

ntp-service access

Syntax **ntp-service access** { **peer** | **query** | **server** | **synchronization** } *acl-number*

undo ntp-service access { **peer** | **query** | **server** | **synchronization** }

View System view

Parameter **peer**: Specifies to permit full access.

query: Specifies to permit control query.

server: Specifies to permit server access and query.

synchronization: Specifies to permit server access only.

acl-number: ACL number, in the range of 2000 to 2999

Description Use the **ntp-service access** command to configure the NTP service access-control right to the local device.

Use the **undo ntp-service access** command to remove the configured NTP service access-control right to the local device.

By default, the local NTP service access-control right is set to **peer**.

From the highest NTP service access-control right to the lowest one are **peer**, **server**, **synchronization**, and **query**. When a device receives an NTP request, it will perform an access-control right match and will use the first matched right.

- *The **ntp-service access** command provides only a minimum degree of security protection. A more secure method is identity authentication.*
- *Before specifying an ACL number in the **ntp-service access** command, make sure you have already created and configured this ACL.*

Example # Configure devices on the subnet 10.10.0.0/16 to have the full access right to the local device.

```
<Sysname> system-view
[Sysname] acl number 2001
[Sysname-acl-basic-2001] rule permit source 10.10.0.0 0.0.255.255
[Sysname-acl-basic-2001] quit
[Sysname] ntp-service access peer 2001
```

ntp-service authentication enable

Syntax **ntp-service authentication enable**

undo ntp-service authentication enable

View System view

Parameter None

Description Use the **ntp-service authentication enable** command to enable NTP authentication.

Use the **undo ntp-service authentication enable** command to disable NTP authentication.

By default, NTP authentication is disabled.

Example # Enable NTP authentication.

```
<Sysname> system-view
[Sysname] ntp-service authentication enable
```

ntp-service authentication-keyid

Syntax **ntp-service authentication-keyid** *keyid* **authentication-mode md5** *value*

undo ntp-service authentication-keyid *keyid*

View System view

Parameter *keyid*: Authentication key ID.

authentication-mode md5: Specifies to use the MD5 algorithm for key authentication.

value: Authentication key.

Description Use the **ntp-service authentication-keyid** command to set the NTP authentication key.

Use the **undo ntp-service authentication-keyid** command to remove the set NTP authentication key.

By default, no NTP authentication key is set.

CAUTION:

- *Presently the system supports only the MD5 algorithm for key authentication.*
- *You can set a maximum of 1,024 keys for each device.*

Example # Set an MD5 authentication key, with the key ID of 10 and key value of **BetterKey**.

```
<Sysname> system-view
[Sysname] ntp-service authentication-keyid 10 authentication-mode md5 BetterKey
```

ntp-service broadcast-client

Syntax **ntp-service broadcast-client**

undo ntp-service broadcast-client

View Interface view

Parameter None

Description Use the **ntp-service broadcast-client** command to configure the device to work in the NTP broadcast client mode.

Use the **undo ntp-service broadcast-client** command to remove the device as an NTP broadcast client.

Example # Configure the device to receive NTP broadcast messages on VLAN-interface 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ntp-service broadcast-client
```

ntp-service broadcast-server

Syntax **ntp-service broadcast-server** [**authentication-keyid** *keyid* | **version** *number*] *

undo ntp-service broadcast-server

View Interface view

Parameter **authentication-keyid** *keyid*: Specifies the key ID to be used for sending broadcast messages to broadcast clients. This keyword and argument combination is not needed if authentication is not required.

version *number*: Specifies the NTP version, where *number* defaults to 3.

Description Use the **ntp-service broadcast-server** command to configure the device to work in the NTP broadcast server mode.

Use the **undo ntp-service broadcast-server** command to remove the device as an NTP broadcast server.

Example # Configure the device to send NTP broadcast messages on VLAN-interface 1, using key 4 for encryption, and set the NTP version to 3.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ntp-service broadcast-server authenticatio
n-keyid 4 version 3
```

ntp-service max-dynamic-sessions

Syntax **ntp-service max-dynamic-sessions** *number*

undo ntp-service max-dynamic-sessions

View System view

Parameter *number*: Maximum number of dynamic NTP sessions to be set up.

Description Use the **ntp-service max-dynamic-sessions** command to set the maximum number of dynamic NTP sessions that allowed to be established locally.

Use the **undo ntp-service max-dynamic-sessions** command to restore the allowed maximum number of dynamic NTP sessions to the default.

By default, the number is 100.

Example # Set the maximum number of dynamic NTP sessions allowed to be established locally to 50.

```
<Sysname> system-view
[Sysname] ntp-service max-dynamic-sessions 50
```

ntp-service multicast-client

Syntax **ntp-service multicast-client** [*ip-address*]

undo ntp-service multicast-client [*ip-address*]

View Interface view

Parameter *ip-address*: Multicast IP address, which must be 224.0.1.1.

Description Use the **ntp-service multicast-client** command to configure the device to work in the NTP multicast client mode.

Use the **undo ntp-service multicast-client** command to remove the device as an NTP multicast client.

Example # Configure the device to work in the multicast client mode and receive NTP multicast messages on VLAN-interface 1, and set the multicast address to 224.0.1.1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ntp-service multicast-client 224.0.1.1
```

ntp-service multicast-server

Syntax **ntp-service multicast-server** [*ip-address*] [**authentication-keyid** *keyid* | **ttl** *ttl-number* | **version** *number*] *

undo ntp-service multicast-server [*ip-address*]

View Interface view

Parameter *ip-address*: Multicast IP address, which must be 224.0.1.1.

authentication-keyid *keyid*: Specifies the key ID to be used for sending multicast messages to multicast clients. This keyword and argument combination is not needed if authentication is not required.

ttl *ttl-number*: Specifies the TTL of NTP multicast messages, where *ttl-number* defaults to 16.

version *number*: Specifies the NTP version, where *number* defaults to 3.

Description Use the **ntp-service multicast-server** command to configure the device to work in the NTP multicast server mode.

Use the **undo ntp-service multicast-server** command to remove the device as an NTP multicast server.

Example # Configure the device to send NTP multicast messages on VLAN-interface 1 to the multicast address 224.0.1.1, using key 4 for encryption, and set the NTP version to 3.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ntp-service multicast-server 224.0.1.1 ver
sion 3 authentication-keyid 4
```

ntp-service refclock-master

Syntax **ntp-service refclock-master** [*ip-address*] [*stratum*]

undo ntp-service refclock-master [*ip-address*]

View System view

Parameter *ip-address*: IP address of the local reference clock, which is 127.127.1.u, where u is the NTP process ID. If you do not specify *ip-address*, it defaults to 127.127.1.0.

stratum: Stratum level of the local clock. The default value of this argument is 8.

Description Use the **ntp-service refclock-master** command to configure the local clock as a reference source for other devices.

Use the **undo ntp-service refclock-master** command to remove the local clock as a reference source.

The stratum level of a clock defines the clock accuracy. The value range is 1 to 16. The clock accuracy decreases from stratum 1 to stratum 16. A stratum 1 clock has the highest accuracy, and a stratum 16 clock is not synchronized and cannot be used as a reference clock.

Example # Specify the local clock as the NTP primary reference clock, with the stratum level of 3.

```
<Sysname> system-view
[Sysname] ntp-service refclock-master 3
```

ntp-service reliable authentication-keyid

Syntax **ntp-service reliable authentication-keyid** *keyid*

undo ntp-service reliable authentication-keyid *keyid*

View System view

Parameter *keyid*: Authentication key number.

Description Use the **ntp-service reliable authentication-keyid** command to specify that the authentication key is a trusted key. When NTP authentication enabled, a client can be synchronized only to a server that can provide the trusted authentication key.

Use the **ntp-service reliable authentication-keyid** command to cancel the configuration.

No trusted authentication key is configured by default.

Example # Enable NTP authentication, specify to use MD5 encryption algorithm, with the key ID of 37 and key value of "BetterKey", and specify that this key is a trusted key.

```
<Sysname> system-view
[Sysname] ntp-service authentication enable
[Sysname] ntp-service authentication-keyid 37 authentication-mode md5 BetterKey
[Sysname] ntp-service reliable authentication-keyid 37
```

ntp-service source-interface

Syntax **ntp-service source-interface** *interface-type interface-number*

undo ntp-service source-interface

View System view

Parameter *interface-type interface-number*: Interface type and interface number of the interface that sends the NTP messages.

Description Use the **ntp-service source-interface** command to specify a local interface for sending NTP messages.

Use the **undo ntp-service source-interface** command to remove the configured interface for sending NTP messages.

You can use this command to specify a particular interface for sending all NTP messages. In this case, the source address in all NTP messages is the primary IP address of this interface, so that IP addresses of other interfaces will not be the destination IP addresses of the NTP response messages.

Example # Specify that all NTP messages are to be sent out from VLAN-interface 1.

```
<Sysname> system-view
[Sysname] ntp-service source-interface vlan-interface 1
```

ntp-service in-interface disable

Syntax **ntp-service in-interface disable**

undo ntp-service in-interface disable

View Interface view

Parameter None

Description Use the **ntp-service in-interface disable** command to disable an interface from receiving NTP messages.

Use the **undo ntp-service in-interface disable** command to restore the default.

By default, all interfaces are enabled to receive NTP messages.

Example # Disable VLAN-interface 1 from receiving NTP messages.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ntp-service in-interface disable
```

ntp-service unicast-peer

Syntax **ntp-service unicast-peer** [**vpn-instance** *vpn-instance-name*] { *ip-address* | *peer-name* } [**authentication-keyid** *keyid* | **priority** | **source-interface** *interface-type interface-number* | **version** *number*] *

undo ntp-service unicast-peer [**vpn-instance** *vpn-instance-name*] { *ip-address* | *server-name* }

View System view

Parameter **vpn-instance** *vpn-instance-name*: Specifies a VPN instance by its name, where *vpn-instance-name* is a string of 1 to 31 characters.

ip-address: IP address of the symmetric-passive peer. It must be a host address, rather than a broadcast address, a multicast address or the IP address of the local clock.

peer-name: Host name of the symmetric-passive peer.

authentication-keyid *keyid*: Specifies the key ID to be used for sending NTP messages to the peer.

priority: Specifies the peer designated by *ip-address* or *peer-name* as the first choice.

source-interface *interface-type interface-number*: Specifies an interface for sending NTP messages. In an NTP message the local device sends to its peer, the source IP address is the primary IP address of this interface.

version *number*: Specifies the NTP version, where *number* defaults to 3.

Description Use the **ntp-service unicast-peer** command to designate a symmetric-passive peer for the device.

Use the **undo ntp-service unicast-peer** command to remove the symmetric-passive peer designated for the device.

No symmetric-passive peer is designated for the device by default.

- *If you specify a VPN instance name, this VPN must exist, and at least one local interface and the NTP server coexist in this VPN.*
- *If multiple VPNs have been configured on the PE and you want to synchronize the PE to a PE or CE in one of these VPNs, you need to provide* ***vpn-instance*** *vpn-instance-name in your command.*
- *If you include* ***vpn-instance*** *vpn-instance-name in the* ***undo ntp unicast-server*** *command, the command will remove the symmetric-passive peer with the IP address of ip-address in the specified VPN; if you do not include* ***vpn-instance*** *vpn-instance-name in this command, the command will remove the symmetric-passive peer with the IP address of ip-address in the public network.*

Example # Configure the local device to be synchronized to peer 128.108.22.44, and the peer also can be synchronized to the local device, and run NTPv3. Use the IP address of VLAN-interface 1 as the source IP address of the NTP messages.

```
<Sysname> system-view
[Sysname] ntp-service unicast-peer 128.108.22.44 version 3 source-in
terface vlan-interface 1
```

ntp-service unicast-server

Syntax **ntp-service unicast-server** [**vpn-instance** *vpn-instance-name*] { *ip-address* | *server-name* } [**authentication-keyid** *keyid* | **priority** | **source-interface** *interface-type interface-number* | **version** *number*] *

undo ntp-service unicast-server [**vpn-instance** *vpn-instance-name*] { *ip-address* | *server-name* }

View System view

Parameter **vpn-instance** *vpn-instance-name*: Specifies a VPN instance by its name.

ip-address: IP address of the NTP server. It must be a host address, rather than a broadcast address, a multicast address or the IP address of the local clock.

server-name: Host name of the NTP server.

authentication-keyid *keyid*: Specifies the key ID to be used for sending NTP messages to the NTP server.

priority: Specifies this NTP server as the first choice.

source-interface *interface-type interface-number*: Specifies an interface for sending NTP messages. In an NTP message the local device sends to the NTP server, the source IP address is the primary IP address of this interface.

version *number*: Specifies the NTP version, where *number* defaults to 3.

Description

Use the **ntp-service unicast-server** command to configure the NTP server for the local device. In this case, the local device acts as a client, and can be synchronized to the NTP server, but the NTP server cannot be synchronized to the local client.

Use the **undo ntp-service unicast-server** command to cancel the NTP server configuration.

No NTP server is configured for the local device by default.

- *The NTP version numbers of the devices to be synchronized must be the same; otherwise the synchronization may fail.*
- *If you specify a VPN instance name, this VPN must exist, and at least one local interface and the NTP server coexist in this VPN.*
- *If multiple VPNs have been configured on the PE and you want to synchronize the PE to a PE or CE in one of these VPNs, you need to provide* ***vpn-instance*** *vpn-instance-name in your command.*
- *If multiple VPNs have been configured on a PE (for example, VPN 1 and VPN 2), when configuring to synchronize the PE to other PE or CE in a VPN, you need to specify* ***vpn-instance*** *vpn-instance-name in the command.*
- *If you include* ***vpn-instance*** *vpn-instance-name in the* ***undo ntp unicast-server*** *command, the command will remove the NTP server with the IP address of ip-address in the specified VPN; if you do not include* ***vpn-instance*** *vpn-instance-name in this command, the command will remove the NTP server with the IP address of ip-address in the public network.*

Example

Configure the local device to be synchronized to the NTP server 128.108.22.44, and set the NTP version number to 3.

```
<Sysname> system-view
[Sysname] ntp-service unicast-server 128.108.22.44 version 3
```

95 NETSTREAM CONFIGURATION COMMANDS

display ip netstream cache

Syntax **display ip netstream cache**

View Any view

Parameter None

Description Use the **display ip netstream cache** command to view configuration and status information about the NetStream cache.

Example # Display information about the NetStream cache on the switch.

```
<Sysname> display ip netstream cache
Netstream cache information
  Stream active timeout(minute)       : 30
  Stream inactive timeout(second)     : 60
  IP active stream entry              : 0
  MPLS active stream entry            : 0
  IP stream entry been exported       : 0
  MPLS stream entry been exported     : 0
  Last clearing of statistics never

 Protocol           Total   Packets   Stream   Packets Active(sec)   Idle(sec)
                   Streams     /Sec     /Sec   /stream     /stream     /stream
 ------------------------------------------------------------------------------
 Total                  0         0         0         0           0           0
```

Table 401 Field descriptions of the display ip netstream cache command

Field	Description
Stream active timeout(minute)	Active aging timer for NetStream cache entries
Stream inactive timeout(second)	Inactive aging time for NetStream cache entries
IP Active stream entry	Number of active NetStream IP streams
MPLS Active stream entry	Number of active NetStream MPLS streams
IP Stream entry been exported	Number of free NetStream IP streams that are counted
MPLS Stream entry been exported	Number of free NetStream MPLS streams that are counted
Last clearing of statistics never	The statistics have never been cleared.
Protocol Total Streams Packets /Sec Stream /Sec Packets /stream Active(sec) /stream Idle(sec) /stream	Packet statistics differentiated by protocol type: protocol, total number of streams, number of packets per second, number of streams per second, active time for each stream, inactive time for each stream

display ip netstream export

Syntax **display ip netstream export**

View Any view

Parameter None

Description Use the **display ip netstream export** command to view statistics about exported NetStream statistics packets.

Example # Display information about the NetStream cache on the switch.

```
<Sysname> display ip netstream export
Version 5 IP export information
  Stream source interface                       : Vlan-interface1000
  Stream destination IP(UDP)                    : 192.168.1.200(9991)
  Exported stream number                        : 20
  Exported UDP datagram number(failed number)   : 2(0)
 Version 9 MPLS export information
  Stream source interface                       : Vlan-interface1000
  Stream destination IP(UDP)                    : 192.168.1.200(9991)
  Exported stream number                        : 0
  Exported UDP datagram number(failed number)   : 0(0)
 Version 8 AS aggregation information
  Stream source interface                       :
  Stream destination IP(UDP)                    : 192.168.1.200(9991)
  Exported stream number                        : 0
  Exported UDP datagram number(failed number)   : 0(0)
```

Table 402 Field descriptions of the display ip netstream export command

Field	Description
Version 5 IP export information	Statistics for exported version 5 statistics packets
Stream source interface	Source interface of exported UDP packets
Stream destination IP(UDP)	Destination address and port number of exported UDP packets
Exported stream number	Number of exported streams
Exported UDP datagram number(failed number)	Number of exported UDP packets (number of failed sending attempts)
Version 8 AS aggregation export information	Statistics for exported version 8 AS aggregation UDP packets. Displayed only when NetStream aggregation is enabled.
Version 9 MPLS export information	Statistics for exported version 9 MPLS packets

enable

Syntax **enable**

undo enable

View NetStream aggregation view

Parameter None

Description Use the **enable** command to enable current aggregation mode.

Use the **undo enable** command to disable current aggregation mode.

By default, no aggregation mode is enabled.

Related command: **ip netstream aggregation**.

Example # Enable NetStream AS aggregation.

```
<Sysname> system-view
[Sysname] ip netstream aggregation as
[Sysname-aggregation-as] enable
```

interface net-stream

Syntax **interface net-stream** *interface-number*

View System view

Parameter *interface-number:* Specifies a NetStream interface by its number.

Description Use the **interface net-stream** command to enter specified NetStream interface view.

An L3 + I/O Module (line processing unit) is needed for the execution of this command.

Example # Enter specified NetStream interface view.

```
<Sysname> system-view
[Sysname] interface net-stream 1/0/2
[Sysname-Net-Stream1/0/2]
```

ip netstream

Syntax **ip netstream** { **inbound** | **outbound** }

undo ip netstream { **inbound** | **outbound** }

View Ethernet interface view

Parameter **inbound**: Enables NetStream statistics in the inbound direction of a port.

outbound: Enables NetStream statistics in the outbound direction of a port.

Description Use the **ip netstream** command to enable NetStream statistics in the inbound or outbound direction of the current port.

Use the **undo ip netstream** command to disable Netstream statistics in the inbound or outbound direction of the current port.

By default, NetStream statistics is disabled in both directions of a port.

- *Currently, the Switch 8800s support the **ip netstream inbound** command only.*
- *The execution of the **ip netstream** command occupies mirroring resources of inbound interface. If the resources are insufficient, IP NetStream cannot be configured.*

Example # Enable NetStream statistics in the inbound direction of port Ethernet 1/1/1.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1/1
[Sysname-Ethernet1/1/1] ip netstream inbound
```

ip netstream aggregation

Syntax **ip netstream aggregation** { **as** | **destination-prefix** | **prefix** | **prefix-port** | **protocol-port** | **source-prefix** | **tos-as** | **tos-destination-prefix** | **tos-prefix** | **tos-protocol-port** | **tos-source-prefix** }

View System view

Parameter **as**: AS aggregation by combination of source AS number, destination AS number, inbound interface index, and outbound interface index.

destination-prefix: Destination-prefix aggregation by destination AS number, destination address mask length, destination prefix, and outbound interface index.

prefix: Source and destination prefix aggregation by combination of source AS number, destination AS number, source address mask length, destination address mask length, source prefix, destination prefix, inbound interface index, and outbound interface index.

prefix-port: Prefix-port aggregation by combination of source prefix, destination prefix, source address mask length, destination address mask length, ToS, protocol number, source port, destination port, inbound interface index, and outbound interface index.

protocol-port: Protocol-port aggregation by combination of protocol number, source port, and destination port.

source-prefix: Source-prefix aggregation by combination of source AS number, source address mask length, source prefix, and inbound interface index.

tos-as: ToS-AS aggregation by combination of ToS, source AS number, destination AS

number, inbound interface index, and outbound interface index.

tos-destination-prefix: ToS-destination-prefix aggregation by ToS, destination AS number, destination address mask length, destination prefix, and outbound interface index.

tos-prefix: ToS-prefix aggregation by combination of ToS, source AS number, source prefix, source address mask length, destination AS number, destination address mask length, destination prefix, inbound interface index, and outbound interface index.

tos-protocol-port: ToS-protocol-port aggregation by combination of ToS, protocol number, source port, destination port, inbound interface index, and outbound interface index.

tos-destination-prefix: ToS-source-prefix aggregation by ToS, source AS number, source prefix, source address mask length, and inbound interface index.

Description Use the **ip netstream aggregation** command to enter NetStream aggregation view.

In NetStream aggregation view, you can enable or disable the aggregation mode, set information about source interface, destination IP address and destination port number for version 8 UDP packets.

Related command: **enable, ip netstream export host**, **ip netstream export source**.

Example # Enter NetStream AS aggregation view.

```
<Sysname> system-view
[Sysname] ip netstream aggregation as
[Sysname-aggregation-as]
```

ip netstream binding interface

Syntax **ip netstream binding interface** *interface-type interface-number*

undo ip netstream binding interface *interface-type interface-number*

View NetStream interface view

Parameter *interface-type interface-number*: Specifies an interface by its type and number. *interface-type* can be Ethernet, GigabitEthernet and Ten-GigabitEthernet.

Description Use the **ip netstream binding interface** command to associate the interface on the NetStream I/O Module with the specified interface.

Use the **undo ip netstream binding interface** command to cancel the association.

By default, no interface is bound.

Note that:

- The command can enable the NetStream statistics function only when it is executed together with the **ip netstream inbound** command.
- Multiple interfaces can be bound on a NetStream I/O Module.

An 3C17542 I/O Module is needed for the execution of this command.

Related command: **ip netstream**.

Example # Associate the interface GigabitEthernet 6/1/2 with the interface NetStream 3/0/2 on the NetStream I/O Module.

```
<Sysname> system-view
[Sysname] interface net-stream 3/0/2
[Sysname-NetStream3/0/2] ip netstream binding interface GigabitEthernet6/1/2
```

ip netstream export host

Syntax **ip netstream export host** *ip-address udp-port*

undo ip netstream export host [*ip-address*]

View System view, NetStream aggregation view

Parameter *ip-address*: Destination IP address for NetStream UDP packets.

udp-port: Destination port number for NetStream UDP packets.

Description Use the **ip netstream export host** command to set the destination IP address and port number for NetStream UDP packets.

Use the **undo ip netstream export host** command to restore the default.

By default, no destination IP address and port number are configured in system view and the IP address and port number in aggregation view are those configured by users in system view.

Note that:

- Different destination hosts can be configured in different aggregation views.
- You can configure up to two different destination hosts in one aggregation view. Statistics packets for a single stream are sent to all destination hosts configured in system view. Aggregation statistics packets are sent to all destination hosts configured in the aggregation view corresponding to the aggregation type.

Related command: **ip netstream aggregation**, **ip netstream export source**.

Example # Configure the destination IP address and port number for NetStream statistics packet as 172.16.105.48 and 5000 respectively.

```
<Sysname> system-view
[Sysname] ip netstream export host 172.16.105.48 5000
```

ip netstream export source interface

Syntax **ip netstream export source interface** *interface-type interface-number*

undo ip netstream export source

View System view, NetStream aggregation view

Parameter *interface-type interface-number*: Specifies a source interface for NetStream statistics packets by its type and number.

Description Use the **ip netstream export source interface** command to configure the source interface for NetStream statistics packets. The IP address of this interface is used as the source address of UDP packets.

Use the **undo ip netstream export source** command to remove the configured source interface.

By default, the source interface is the interface of statistics packets, that is, the source address of NetStream statistics packets is used as the IP address for the layer 3 interface that sends packets.

Different source interface addresses can be configured in different aggregation views.

Related command: **ip netstream aggregation**, **ip netstream export destination**.

Example # Configure the source interface for NetStream statistics packets as POS 3/1/1.

```
<Sysname> system-view
[Sysname] ip netstream export source interface pos 3/1/1
```

ip netstream export v9-template refresh-rate packet

Syntax **ip netstream export v9-template refresh-rate packet** *packets*

undo ip netstream export v9-template refresh-rate packet

View System view

Parameter *packets*: Packet refresh rate of version 9 templates. It is the number of reported packets.

Description Use the **ip netstream export v9-template refresh-rate packet** command to configure the packet refresh rate of version 9 templates.

Use the **undo ip netstream export v9-template refresh-rate packet** command to restore the default packet refresh rate of version 9 templates, that is, 20.

Because of its limited capacity, XLog does not save all version 9 templates for ever; therefore, version 9 templates must be refreshed periodically. You can configure the packet refresh rate of version 9 templates to refresh them on time.

Related command: **ip netstream export v9-template refresh-rate time**.

Example # Set the packet refresh rate for version 9 templates to 100.

```
<Sysname> system-view
[Sysname] ip netstream export v9-template refresh-rate packet 100
```

ip netstream export v9-template refresh-rate time

Syntax **ip netstream export v9-template refresh-rate time** *minutes*

undo ip netstream export v9-template refresh-rate time

View System view

Parameter *minutes*: Specifies the interval to send version 9 templates for NetStream statistics packets, in minutes.

Description Use the **ip netstream export v9-template refresh-rate time** command to configure the interval to send version 9 templates for NetStream statistics packets.

Use the **undo ip netstream export version** command to restore the default interval, that is, 30 minutes.

Because of its limited capacity, XLog cannot save all version 9 templates for ever; therefore, version 9 templates must be refreshed periodically. You can configure the interval to send version 9 templates to refresh them on time.

Related command: **ip netstream export v9-template refresh-rate packet**.

Example # Set the interval to send version 9 templates to 60 minutes.

```
<Sysname> system-view
[Sysname] ip netstream export v9-template refresh-rate time 60
```

ip netstream export version

Syntax **ip netstream export version** *version-number* [**origin-as** | **peer-as**]

undo ip netstream export version

View System view

Parameter *version-number*: Version number for NetStream statistics packets.

origin-as: Sets the type of AS number recorded in NetStream cache entries to origin.

peer-as: Sets the type of AS number recorded in NetStream cache entries to peer.

Description Use the **ip netstream export version** command to configure the type of AS numbers to be recorded in NetStream cache entries and the version of NetStream statistics packets.

Use the **undo ip netstream export version** command to restore the default.

By default, a single stream is sent in version 5 UDP packets, aggregation statistics information is sent in version 8 UDP packets, and MPLS stream information is sent in version 9 UDP packets and the AS option is **peer-as**.

Note that the AS numbers for the source and destination IP addresses of a stream are recorded in the statistics information. And each IP address corresponds with two AS numbers (origin and peer), the system records the AS numbers according to the AS option configured by users.

Example # Set the NetStream statistics packet version number to 5 and the AS option to **origin-as**.

```
<Sysname> system-view
[Sysname] ip netstream export version 5 origin-as
```

ip netstream timeout active

Syntax **ip netstream timeout active** *minutes*

undo ip netstream timeout active

View System view

Parameter *minutes*: Sets the length of the active aging timer for NetStream cache entries, in minutes.

Description Use the **ip netstream timeout active** command to set the active aging timer for NetStream cache entries.

Use the **undo ip netstream timeout active** command to restore the default.

The active aging timer for NetStream cache entries is 30 minutes by default.

CAUTION: *You can configure the active aging timer and inactive aging timer at the same time. When either of them times out, the entry ages out.*

Related command: **ip netstream timeout inactive**.

Example # Set the active aging timer to 60 minutes.

```
<Sysname> system-view
[Sysname] ip netstream timeout active 60
```

ip netstream timeout inactive

Syntax **ip netstream timeout inactive** *seconds*

undo ip netstream timeout inactive

View System view

Parameter *seconds*: Sets the length of the inactive aging timer for NetStream cache entries, in seconds.

Description Use the **ip netstream timeout inactive** command to set the inactive aging timer for NetStream cache entries.

Use the **undo ip netstream timeout inactive** command to restore the default.

The inactive aging timer for NetStream cache entries is 60 seconds by default.

CAUTION: *You can configure the active aging timer and inactive aging timer at the same time. When either of them times out, the entry ages out.*

Related command: **ip netstream timeout active**.

Example # Set the inactive aging timer to 60 seconds.

```
<Sysname> system-view
[Sysname] ip netstream timeout inactive 60
```

reset ip netstream statistics

Syntax **reset ip netstream statistics**

View User view

Parameter None

Description Use the **reset ip netstream statistics** command to age and export all stream statistics to clear the NetStream cache.

Example # Age and export all stream statistics to clear the NetStream cache.

```
<Sysname> reset ip netstream statistics
```

96 NQA CONFIGURATION COMMANDS

count (NQA test group view)

Syntax **count** *times*

undo count

View NQA test group view

Parameter *times*: Number of probes in a test, in the range 1 to 15.

Description Use the **count** command to configure the number of probes in a test.

Use the **undo count** command to restore the default.

By default, one probe is performed in a test.

For a TCP test, one probe means one connection; for a Jitter test, the number of packets sent in one probe depends on the **jitter-packetnum** command; for an SNMP test, three packets are sent in one probe; for other types of tests, one packet is sent for one probe.

If the number of probes in a test is greater than 1, the system sends a second packet after it sends the first packet and receives a response packet. If the system does not receive a response packet, the system waits for the test timer to expire before sending a second test packet. The process is repeated until the specified probes are completed.

Example # Configure the number of probes in a test to 10.

```
<Sysname> system-view
[Sysname] nqa administrator test
[Sysname-nqa-administrator-test] count 10
```

datafill

Syntax **datafill** *text*

undo datafill

View NQA test group view

Parameter *text*: String of fill characters of a test packet, in the range 1 to 200.

Description Use the **datafill** command to configure the string of fill characters for a test packet.

Use the **undo datafill** command to restore the default.

By default, the string of fill characters of an ICMP packet is the string corresponding with the ASCII code 00 to 09 and that for a UDP packet is the string corresponding with the ASCII code 00 to FF.

The fill data of an NQA test packet can be any string of characters. If the test packet is smaller than the fill data, the system uses only the first part of the character string to encapsulate the packet. If the test packet is larger than the fill data, the system fills the character string cyclically to encapsulate the test packet until the packet is full. For example, when the fill data is "abcd" and the size of a test packet is 3 byte, "adc" is used to fill. When the test packet size is 6 byte, "abcdab" is used to fill.

Because the first byte of a UDP packet has some specific usage, the configured character string is used to fill the remaining bytes in the packet.

Note that the **datafill** command is valid for an ICMP test and a UDP test.

Example # Configure the string of fill characters of a test packet to "abcd".

```
<Sysname> system-view
[Sysname] nqa administrator test
[Sysname-nqa-administrator-test] datafill abcd
```

datasize

Syntax **datasize** *size*

undo datasize

View NQA test group view

Parameter *size*: Size of a test packet in bytes, in the range of 1 to 8100.

Description Use the **datasize** command to configure the size of a test packet, namely, an echo request packet (IP header and ICMP header excluded).

Use the **undo datasize** command to restore the size of a test request packet to the default value.

By default, the size of an ICMP test packet is 56 bytes and that of a UDP test packet is 100 bytes.

Note that:

- The **datasize** command is valid only for ICMP and UDP tests.

- For an ICMP test, if the value of the *size* argument is less than 20, the system automatically fills ICMP test packets to 20 bytes with a string of fill characters.
- When you perform a UDP test, the size of test packets is subject to the configuration.

Related command: **datafill**.

Example # Configure the size of a test packet as 50 bytes.

```
<Sysname> system-view
[Sysname] nqa administrator test
[Sysname-nqa-administrator-test] datasize 50
```

debugging nqa

Syntax **debugging nqa** { **all | error | event** }

undo debugging nqa { **all | error | event** }

View User view

Parameter **all**: Enables all debugging for NQA.

error: Enables error debugging for NQA.

event: Enables event debugging for NQA.

Description Use the **debugging nqa** command to enable NQA debugging.

Use the **undo debugging nqa** command to disable NQA debugging.

By default, NQA debugging is disabled.

Example # Enable NQA event debugging.

```
<Sysname> terminal debugging
<Sysname> debugging nqa event
```

description (NQA test group view)

Syntax **description** *text*

undo description

View NQA test group view

Parameter *text*: Descriptive string of characters for a test group, in the range 1 to 200.

Description Use the **description** command to give a brief description of a test group, usually, the test type or test purpose of a test group.

Use the **undo description** command to remove the description information.

By default, no descriptive string is available for a test group.

Example # Configure a descriptive string for a test group as "icmp-test".

```
<Sysname> system-view
[Sysname] nqa administrator test
[Sysname-nqa-administrator-test] description icmp-test
```

destination-ip

Syntax **destination-ip** *ip-address*

undo destination-ip

View NQA test group view

Parameter *ip-address*: Destination IP address of a test request packet.

Description Use the **destination-ip** command to configure a destination IP address for a test request packet.

Use the **undo destination-ip** command to remove the destination IP address.

By default, no destination IP address is configured for a test request packet.

Related command: **destination-port**.

Example # Set the destination IP address of a test request packet to 10.1.1.1.

```
<Sysname> system-view
[Sysname] nqa administrator test
[Sysname-nqa-administrator-test] destination-ip 10.1.1.1
```

destination-port

Syntax **destination-port** *port-number*

undo destination-port

View NQA test group view

Parameter *port-number*: Destination port number of a test request packet, in the range 1 to 65535.

Description Use the **destination-port** command to configure a destination port number for a test request packet.

Use the **undo destination-port** command to remove the destination port number.

By default, no destination port number is configured for a test request packet.

Related command: destination-ip

- *The **destination-port** command is applicable to only jitter, TCP-Private, and UDP-Private tests.*
- *You are not recommended to perform a TCP, UDP, or jitter test on port from 1 to 1023 (known ports). Otherwise, the NQA test will fail or the corresponding services of this port will be unavailable.*

Example # Set the destination port number of a test request packet to 9000.

```
<Sysname> system-view
[Sysname] nqa administrator test
[Sysname-nqa-administrator-test] destination-port 9000
```

display nqa

Syntax **display nqa** { **results** | **history** | **jitter** } [*admin-name operation-tag*]

View Any view

Parameter **results**: Displays the results of the last test.

history: Displays the history records of tests.

jitter: Displays the recorded delay jitter of UDP packet transmission in the last NQA jitter test.

admin-name: Name of the administrator who creates NQA test groups, a string of 1 to 32 characters.

operation-tag: Operation tag, a string of 1 to 32 characters.

Description Use the **display nqa** command to display results of an NQA test or tests.

If neither of the test group arguments (*admin-name* and *operation-tag*) is specified, results of all test groups are displayed. Otherwise, results of only the specified test group(s) are displayed.

Related command: **test-enable**.

Example # Display the results of the last test.

```
<Sysname> display nqa results administrator icmp
  NQA entry(admin administrator, tag icmp) test result:
```

```
    Destination ip address: 169.254.10.2
    Send operation times: 10            Receive response times: 10
    Min/Max/Average Round Trip Time: 1/2/1
    Square-Sum of Round Trip Time: 13
    Last succeeded test time: 2004-11-25 16:28:55.0
  Extend result:
    Packet lost in test: 0%
    Failures due to Timeout: 0
    Failures due to System Busy: 0
    Failures due to Disconnect: 0
    Failures due to No Connection: 0
    Failures due to Sequence Error: 0
    Failures due to Internal Error: 0
    Failures due to Other Errors: 0
```

Table 403 Field descriptions of the display nqa results command

Field	Description
Destination ip address	IP address of the destination
Send operation times	Number of probe packets sent
Receive response times	Number of response packets received
Min/Max/Average Round Trip Time	Minimum/maximum/average roundtrip time
Square-Sum of Round Trip Time	Square sum of roundtrip time
Last succeeded test time	Completion time of the last successful test
SD Maximal delay	Maximum delay from the source to the destination
DS Maximal delay	Maximum delay from the destination to the source
Packet lost in test	Average packet loss ratio
Disconnect operation number	Number of disconnections by the peer
Failures due to Timeout	Number of time-out occurrences in a test
Failures due to System Busy	Number of test failures owing to the system being busy
Failures due to Disconnect	Number of disconnections by the peer
Failures due to No Connection	Number of failures to connect with the peer
Failures due to Sequence Error	Number of failures owing to out-of-sequence packets
Failures due to Internal Error	Number of failures owing to internal errors
Failures due to Other Errors	Number of failures owing to other errors

Display the history records of tests.

```
<Sysname> display nqa history administrator test
  NQA entry(admin administrator, tag test) history record:
    Index     Response    Status      LastRC      Time
       1            1         1           0    2004-11-25 16:28:55.0
       2            1         1           0    2004-11-25 16:28:55.0
       3            1         1           0    2004-11-25 16:28:55.0
       4            1         1           0    2004-11-25 16:28:55.0
       5            1         1           0    2004-11-25 16:28:55.0
       6            2         1           0    2004-11-25 16:28:55.0
       7            1         1           0    2004-11-25 16:28:55.0
       8            1         1           0    2004-11-25 16:28:55.0
       9            1         1           0    2004-11-25 16:28:55.9
      10            1         1           0    2004-11-25 16:28:55.9
```

Table 404 Field descriptions of the display nqa history command

Field	Description
Index	History record number
Response	Roundtrip delay of a test packet in the case of a successful test, time-out time in the case of time-out, or 0 in the case of a test failure (in milliseconds)
Status	Status value of test results, including: 1: responseReceived 2: unknown 3: internalError 4: requestTimedOut 5: unknownDestinationAddress 6: noRouteToTarget 7: interfaceInactiveToTarget 8: arpFailure 9: maxConcurrentLimitReached 10: unableToResolveDnsName 11: invalidHostAddress
LastRC	Temporarily, this field is not supported.
Time	Time when the test is completed

Display the recorded delay jitter of UDP packet transmission in the last NQA jitter test.

```
<Sysname> display nqa jitter admin jitter

  NQA entry(admin admin, tag jitter) test jitter result:
      RTT Number: 10
      SD Maximal delay: 2                  DS Maximal delay: 2
      Min Positive SD: 1                   Min Positive DS: 1
      Max Positive SD: 1                   Max Positive DS: 1
      Positive SD Number: 4                Positive DS Number: 2
      Positive SD Sum: 4                   Positive DS Sum: 2
      Positive SD average: 1               Positive DS average: 1
      Positive SD Square Sum: 4            Positive DS Square Sum: 2
      Min Negative SD: 1                   Min Negative DS: 1
      Max Negative SD: 2                   Max Negative DS: 1
      Negative SD Number: 2                Negative DS Number: 3
      Negative SD Sum: 3                   Negative DS Sum: 3
      Negative SD average: 2               Negative DS average: 1
      Negative SD Square Sum: 5            Negative DS Square Sum: 3
      SD lost packets number: 0            DS lost packet number: 0
      Unknown result lost packet number: 0
```

Table 405 Field descriptions of the display nqa jitter command

Field	Description
RTT Number	Number of received response packets
SD Maximal delay	Maximum delay from the source to the destination

Table 405 Field descriptions of the display nqa jitter command

Field	Description
DS Maximal delay	Maximum delay from the destination to the source
Min Positive SD	Minimum positive jitter delay from the source to the destination
Min Positive DS	Minimum positive jitter delay from the destination to the source
Max Positive SD	Maximum positive jitter delay from the source to the destination
Max Positive DS	Maximum positive jitter delay from the destination to the source
Positive SD Number	Number of positive jitter delays from the source to the destination
Positive DS Number	Number of positive jitter delays from the destination to the source
Positive SD Sum	Sum of positive jitter delays from the source to the destination
Positive DS Sum	Sum of positive jitter delays from the destination to the source
Positive SD average	Average of positive jitter delays from the source to the destination
Positive DS average	Average of positive jitter delays from the destination to the source
Positive SD Square Sum	Sum of the square of positive jitter delays from the source to the destination
Positive DS Square Sum	Sum of the square of positive jitter delays from the destination to the source
Min Negative SD	Minimum absolute value of negative jitter delays from the source to the destination
Min Negative DS	Minimum absolute value of negative jitter delays from the destination to the source
Max Negative SD	Maximum absolute value of negative jitter delays from the source to the destination
Max Negative DS	Maximum absolute value of negative jitter delays from the destination to the source
Negative SD Number	Number of negative jitter delays from the source to the destination
Negative DS Number	Number of negative jitter delays from the destination to the source
Negative SD Sum	Sum of absolute values of negative jitter delays from the source to the destination
Negative DS Sum	Sum of absolute values of negative jitter delays from the destination to the source
Negative SD average	Average of negative jitter delays from the source to the destination
Negative DS average	Average of negative jitter delays from the destination to the source
Negative SD Square Sum	Sum of the square of negative jitter delays from the source to the destination
Negative DS Square Sum	Sum of the square of negative jitter delays from the destination to the source

Table 405 Field descriptions of the display nqa jitter command

Field	Description
SD lost packets number	Number of lost packets from the source to the destination
DS lost packet number	Number of lost packets from the destination to the source
Unknown result lost packet number	Number of lost packets for unknown reasons

filename

Syntax **filename** *file-name*

undo filename

View NQA test group view

Parameter *file-name*: Name of the file transferred between the FTP server and the FTP client, a string of 1 to 200 characters.

Description Use the **filename** command to specify a file to be transferred between the FTP server and the FTP client.

Use the **undo filename** command to cancel the file.

By default, no file is specified.

Note that the **filename** command is valid only for FTP tests.

Related command: **username**, **password**, and **ftp-operation**.

Example # Specify the config.txt file to be transferred between the FTP server and the FTP client.

```
<Sysname> system-view
[Sysname] nqa administrator test
[Sysname-nqa-administrator-test] filename config.txt
```

frequency

Syntax **frequency** *interval*

undo frequency

View NQA test group view

Parameter *interval*: Interval of performing a cyclic test in seconds, in the range 1 to 65535.

Description Use the **frequency** command to configure the interval of performing a cyclic test. After you execute the **test-enable** command to start an NQA test, the test will be performed at intervals.

Use the **undo frequency** command to restore the default.

By default, no cyclic test is performed.

Note that the **frequency** command is invalid for the DHCP test.

Related command: **test-enable**.

Example # Configure the interval of performing a cyclic test to 10 seconds.

```
<Sysname> system-view
[Sysname] nqa administrator test
[Sysname-nqa-administrator-test] frequency 10
```

ftp-operation

Syntax **ftp-operation** { **get** | **put** }

undo ftp-operation

View NQA test group view

Parameter **get**: Obtains a file from the FTP server.

put: Transfers a file to the FTP server.

Description Use the **ftp-operation** command to configure the FTP operation type.

Use the **undo ftp-operation** command to restore the default.

By default, the FTP operation type is "get" (obtain a file from the FTP server).

Note that the **ftp-operation** command is valid only for FTP tests.

Related command: **username** and **password**.

Example # Obtain a file from the FTP server.

```
<Sysname> system-view
[Sysname] nqa administrator test
[Sysname-nqa-administrator-test] ftp-operation get
```

history-records

Syntax **history-records** *number*

undo history-records

View NQA test group view

Parameter *number*: Maximum number of history records that can be saved in a test group, in the range 0 to 50.

Description Use the **history-records** command to configure the maximum number of history records that can be saved in a test group.

Use the **undo history-records** command to restore the default.

By default, the maximum number of records that can be saved in a test group is 50.

If the history records exceed the predefined maximum number, the first test result will be discarded.

Example # Configure the maximum number of history records that can be saved in a test group to 10.

```
<Sysname> system-view
[Sysname] nqa administrator test
[Sysname-nqa-administrator-test] history-records 10
```

http-operation

Syntax **http-operation** { **get** | **post** }

undo http-operation

View NQA test group view

Parameter **get**: Obtains data from the HTTP server.

post: Transfers data to the HTTP server.

Description Use the **http-operation** command to configure the HTTP operation type.

Use the **undo http-operation** command to restore the default.

By default, the HTTP operation type is "get" (obtain data from the HTTP server).

Note that the **http-operation** command is valid only for HTTP tests.

Related command: **http-string**.

Example # Obtain data from the HTTP server.

```
<Sysname> system-view
[Sysname] nqa administrator test
[Sysname-nqa-administrator-test] http-operation get
```

http-string

Syntax **http-string** *string version*

undo http-string

View NQA test group view

Parameter *string*: HTTP operation string, which specifies a webpage to be accessed. The length of the *string* argument plus that of the *version* argument must be less than 200 characters.

version: HTTP version. Currently, it can only be "HTTP/1.0", where HTTP must be capital.

Description Use the **http-string** command to configure an HTTP operation string and version information.

Use the **undo http-string** command to remove the configuration of the HTTP operation string and version information.

By default, no HTTP operation string or version information is configured.

Note that the **http-string** command is valid only for HTTP tests.

Related command: **http-operation**.

Example # Set the web page accessible through HTTP to / index.htm and the HTTP version to HTTP/1.0.

```
<Sysname> system-view
[Sysname] nqa administrator test
[Sysname-nqa-administrator-test] http-string /index.htm HTTP/1.0
```

nqa (System view)

Syntax **nqa** *admin-name operation-tag*

undo nqa *admin-name operation-tag*

View System view

Parameter *admin-name*: Name of the administrator who creates NQA test groups, a string of 1 to 32 characters.

operation-tag: Tag of a test operation, a string of 1 to 32 characters.

Description Use the **nqa** command to create an NQA test group and enter its view. If the test group already exists, you will directly enter NQA test group view when you execute the **nqa** command.

Use the **undo nqa** command to remove the test group.

Example # Create an NQA test group whose administrator name is "administrator" and whose operation tag is "test" and enter NQA test group view.

```
<Sysname> system-view
[Sysname] nqa administrator test
[Sysname-nqa-administrator-test]
```

nqa-agent enable

Syntax **nqa-agent enable**

undo nqa-agent enable

View System view

Parameter None

Description Use the **nqa-agent enable** command to enable the NQA client.

Use the **undo nqa-agent enable** command to disable the NQA client.

By default, the NQA client is disabled.

Note that you can perform tests only after the NQA client is enabled.

Related command: **nqa-server enable**.

Example # Enable the NQA client.

```
<Sysname> system-view
[Sysname] nqa-agent enable
```

nqa-agent max-requests

Syntax **nqa-agent max-requests** *max-number*

undo nqa-agent max-requests

View System view

Parameter *max-number*: Maximum number of tests that the NQA client can simultaneously perform, in the range 1 to 5.

Description Use the **nqa-agent max-requests** command to configure the maximum number of tests that the NQA client can simultaneously perform.

Use the **undo nqa-agent max-requests** command to restore the default.

By default, the maximum number of tests that the NQA client can simultaneously perform is five.

Example # Specify the NQA client to simultaneously perform four tests at most.

```
<Sysname> system-view
[Sysname] nqa-agent max-requests 4
```

jitter-interval

Syntax **jitter-interval** *interval*

undo jitter-interval

View NQA test group view

Parameter *interval*: Interval for sending jitter test packets in milliseconds, in the range 10 to 1,000.

Description Use the **jitter-interval** command to configure the interval of sending jitter test packets.

Use the **undo jitter-interval** command to restore the default.

By default, the interval for sending jitter test packets is 20 milliseconds.

Note that the **jitter-interval** command is valid only for a jitter test.

Related command: **jitter-packetnum**.

Example # Set the interval of sending jitter test packets to 30 milliseconds.

```
<Sysname> system-view
[Sysname] nqa administrator test
[Sysname-nqa-administrator-test] jitter-interval 30
```

jitter-packetnum

Syntax **jitter-packetnum** *number*

undo jitter-packetnum

View NQA test group view

Parameter *number*: Number of test packets sent in a probe, in the range 10 to 100.

Description Use the **jitter-packetnum** command to configure the number of jitter test packets sent in a probe.

Use the **undo jitter-packetnum** command to restore the default.

By default, the number of test packets sent in a probe is 10.

Note that the **jitter-packetnum** command is valid only for a jitter test.

Related command: **jitter-interval**.

Example # Set the number of packets sent in a probe to 30.

```
<Sysname> system-view
[Sysname] nqa administrator test
[Sysname-nqa-administrator-test] jitter-packetnum 30
```

password (NQA test group view)

Syntax **password** *password*

undo password

View NQA test group view

Parameter *password*: Password used to log on to the FTP server, a string of 1 to 32 characters.

Description Use the **password** command to configure a password used to log onto the FTP server.

Use the **undo password** command to remove the password.

By default, no password is configured.

Note that the **password** command is valid only for an FTP test.

Related command: **username** and **ftp-operation**.

Example # Set the login password to nqa.

```
<Sysname> system-view
[Sysname] nqa administrator test
[Sysname-nqa-administrator-test] test-type ftp
[Sysname-nqa-administrator-test] username aaa
[Sysname-nqa-administrator-test] password nqa
```

probe-failtimes

Syntax **probe-failtimes** *times*

undo probe-failtimes

View NQA test group view

Parameter *times*: Number of consecutive probe failures in a test, in the range 1 to 15.

Description Use the **probe-failtimes** command to configure the number of consecutive probe failures in an NQA test before a trap message is sent to the network management server to indicate a probe failure.

Use the **undo probe-failtimes** command to restore the default.

By default, a Trap message is sent to the network management (NM) server once one probe fails in an NQA test.

One test may involve multiple probes.

Example # Configure the system to send a Trap message after three consecutive probe failures in an NQA test.

```
<Sysname> system-view
[Sysname] nqa administrator test
[Sysname-nqa-administrator-test] probe-failtimes 3
```

send-trap

Syntax **send-trap** { **all** | { **probefailure** | **testcomplete** | **testfailure** }* }

undo send-trap { **all** | { **probefailure** | **testcomplete** | **testfailure** }* }

View NQA test group view

Parameter **probefailure:** Sends a Trap message when a probe fails.

testcomplete: Sends a Trap message when a test is completed.

testfailure: Sends a Trap message when a test fails (the number of probe failures in a test is greater than or equal to the number configured by the **test-failtimes** command). For a test, only one trap message is sent.

all: Sends a Trap message in any of the above cases.

Description Use the **send-trap** command to enable the Trap debugging (A Trap message is sent to the network management server).

Use the **undo send-trap** command to disable the Trap debugging (No Trap message is sent to the network management server).

By default, no trap message is sent to the network management server.

Example # Send a Trap message when a test is completed.

```
<Sysname> system-view
[Sysname] nqa administrator test
[Sysname-nqa-administrator-test] send-trap testcomplete
```

sendpacket passroute

Syntax **sendpacket passroute**

undo sendpacket passroute

View NQA test group view

Parameter None

Description Use the **sendpacket passroute** command to enable the routing table bypass function to test the direct connectivity to the destination.

Use the **undo sendpacket passroute** command to disable the routing table bypass function.

By default, the routing table bypass function is disabled.

After this function is enabled, the routing table is not searched, and the packet is directly sent to the destination in a directly connected network. If the destination is not in the directly connected network, an error will be prompted.

Note that the **sendpacket passroute** command is invalid for DHCP tests.

Example # Enable the routing table bypass function.

```
<Sysname> system-view

[Sysname] nqa administrator test
[Sysname-nqa-administrator-test] sendpacket passroute
```

source-interface

Syntax **source-interface** *interface-type interface-number*

undo source-interface

View NQA test group view

Parameter *interface-type interface-number*: Specifies the interface by its type and number.

Description Use the **source-interface** command to specify the IP address of an interface as the source IP address of ICMP test request packets or specify an interface for a DHCP test.

Use the **undo source-interface** command to remove the configuration.

By default, no interface address is specified as the source IP address of ICMP test request packets, or no interface is specified for a DHCP test.

Note that:

- For a DHCP test, the **source-interface** command is required, for an ICMP test, it is optional, and for other tests, it is invalid.
- For an ICMP test, if a source IP address is configured by using the **source-ip** command, the configuration by using the **source-interface** command is invalid.
- The interface specified by the **source-interface** command can only be a pos interface or VLAN interface.
- The interface specified by the command must be up. Otherwise, the test will fail.

Example # Specify Vlan-interface12 as the source interface for sending test requests.

```
<Sysname> system-view
[Sysname] nqa administrator test
[Sysname-nqa-administrator-test] test-type dhcp
[Sysname-nqa-administrator-test] source-interface Vlan-interface 12
```

source-ip

Syntax **source-ip** *ip-address*

undo source-ip

View NQA test group view

Parameter *ip-address*: Source IP address of a test request packet.

Description Use the **source-ip** command to configure a source IP address for a test request packet.

Use the **undo source-ip** command to remove the configured source address. That is, the IP address of the interface sending a test request packet serves as the source IP address of the test request packet.

By default, no source IP address is specified. If a source interface is specified, the IP address of the source interface serves as the source IP address of a test request packet.

Note that:

- For an FTP test, the source-ip command is required, for a DHCP test, it is invalid, and for other tests, it is optional.
- The source IP address in the command must be the IP address of an interface on the device and the interface must be up. Otherwise, the test will fail.

Example # Configure the source IP address of a test request packet to 10.1.1.1.

```
<Sysname> system-view
[Sysname] nqa administrator test
[Sysname-nqa-administrator-test] source-ip 10.1.1.1
```

source-port

Syntax **source-port** *port-number*

undo source-port

View NQA test group view

Parameter *port-number*: Source port number for a test request packet, in the range 1 to 50000.

Description Use the **source-port** command to configure a source port number for a test request packet.

Use the **undo source-port** command to remove the configured port number.

By default, no source port number is specified.

Note that this command is valid only for jitter, UDP, and SNMP tests.

Example # Configure the source port number of a test request packet to 8000.

```
<Sysname> system-view
[Sysname] nqa administrator test
[Sysname-nqa-administrator-test] source-port 8000
```

test-type

Syntax **test-type** *test-type*

undo test-type

View NQA test group view

Parameter *test-type*: Type of a test, including the following keywords:

- **dhcp**: DHCP test.
- **dlsw**: DLSw test.
- **ftp**: FTP test.
- **http**: HTTP test.
- **icmp**: ICMP test.
- **jitter**: Analyzes and tests the delay jitter of UDP packet transmission.
- **snmpquery**: SNMP test.

- **tcpprivate**: Tests the TCP connection to a specified port.
- **tcppublic**: Tests the TCP connection to port 7.
- **udpprivate**: Tests the UDP connection to a specified port.
- **udppublic**: Tests the UDP connection to port 7.

Description Use the **test-type** command to configure the test type.

Use the **undo test-type** command to restore the default.

By default, the test type is ICMP.

Example # Set the test type to FTP.

```
<Sysname> system-view
[Sysname] nqa administrator test
[Sysname-nqa-administrator-test] test-type ftp
```

test-enable

Syntax **test-enable**

undo test-enable

View NQA test group view

Parameter None

Description Use the **test-enable** command to enable the NQA test.

Use the **undo test-enable** command to disable the NQA test.

Test results will not be displayed after you enable the NQA test. In this case, you need to execute the **display nqa** command to display the test results.

Related command: display nqa.

Example # Enable the NQA test.

```
<Sysname> system-view
[Sysname] nqa-agent enable
[Sysname] nqa administrator test
[Sysname-nqa-administrator-test] test-enable
```

test-failtimes

Syntax **test-failtimes** *times*

undo test-failtimes

View NQA test group view

Parameter *times*: Minimum number of probe failures in a test before a Trap message is sent to indicate a test failure, in the range 1 to 15.

Description Use the **test-failtimes** command to configure the minimum number of probe failures in a test before a Trap message is sent to the network management server to indicate a test failure.

Use the **undo test-failtimes** command to restore the default.

By default, a Trap message is sent to the NM server once a probe fails in a test.

One test may involve multiple probes.

Example # Configure the system to send a Trap message to indicate a test failure after three probe failures in an NQA test.

```
<Sysname> system-view
[Sysname] nqa administrator test
[Sysname-nqa-administrator-test] test-failtimes 3
```

timeout

Syntax **timeout** *time*

undo timeout

View NQA test group view

Parameter *time*: Time-out time in one probe, in the range 1 to 60 seconds.

Description Use the **timeout** command to configure the time-out time in one probe. If no response packet is received within the time-out time of a request packet, the probe fails.

Use the **undo timeout** command to restore the default.

By default, the time-out time in one probe is three seconds.

Example # Configure the time-out time in one probe to 10 seconds.

```
<Sysname> system-view
[Sysname] nqa administrator test
[Sysname-nqa-administrator-test] timeout 10
```

tos

Syntax **tos** *value*

undo tos

View NQA test group view

Parameter *value*: Value of the ToS field in the IP header in an NQA test packet, in the range 0 to 15.

Description Use the **tos** command to configure the value of the ToS field in the IP header in an NQA test packet.

Use the **undo tos** command to restore the default.

By default, the ToS field in the IP header of an NQA test packet is 0.

Note that the **tos** command is invalid for DHCP tests.

Example # Set the ToS field in a IP packet header in an NQA test packet to 1.

```
<Sysname> system-view
[Sysname] nqa administrator test
[Sysname-nqa-administrator-test] tos 1
```

ttl

Syntax **ttl** *number*

undo ttl

View NQA test group view

Parameter *number*: Maximum number of hops a test request packet traverses in the network, in the range 1 to 255.

Description Use the **ttl** command to configure the maximum number of hops a test request packet traverses in the network.

Use the **undo ttl** command to restore the maximum number of hops to the default.

By default, the maximum number of hops that a test request packet can traverse in a network is 20.

- *The **ttl** command is invalid for DHCP tests.*
- *After you configure the **sendpacket passroute** command, the maximum number of hops a test request packet traverses in the network is 1.*

Example # Configure the maximum number of hops a test request packet traverses in the network to 16.

```
<Sysname> system-view
[Sysname] nqa administrator test
[Sysname-nqa-administrator-test] ttl 16
```

username

Syntax **username** *name*

undo username

View NQA test group view

Parameter *name*: Username used to log on to the FTP server, a string of 1 to 32 characters.

Description Use the **username** command to configure a username used to log onto the FTP server.

Use the **undo username** command to remove the configured username.

By default, no username is configured.

Note that the **username** command is valid only for FTP tests.

Related command: **password** and **ftp-operation**.

Example # Set the login username to administrator.

```
<Sysname> system-view
[Sysname] nqa administrator test
[Sysname-nqa-administrator-test] test-type ftp
[Sysname-nqa-administrator-test] username administrator
```

vpninstance

Syntax **vpninstance** *name*

undo vpninstance

View NQA test group view

Parameter *name*: VPN instance name, a string of 1 to 31 characters.

Description Use the **vpninstance** command to specify a VPN instance. If there are multiple VPNs, you need to use this command to specify a VPN for test.

Use the **undo vpninstance** command to remove the specified VPN instance.

By default, no VPN instance is specified.

Note that the **vpninstance** command is valid only for ICMP tests.

*The support for the **vpninstance** command depends on the device model.*

You can only use this command to specify an existing VPN instance.

Example # Specify the VPN instance vpn1.

```
<Sysname> system-view
[Sysname] nqa administrator test
[Sysname-nqa-administrator-test] vpninstance vpn1
```

97 NQA SERVER COMMANDS

You only need to configure the NQA server for jitter, TCP, and UDP tests.

nqa-server enable

Syntax **nqa-server enable**

undo nqa-server enable

View System view

Parameter None

Description Use the **nqa-server enable** command to enable the NQA server.

Use the **undo nqa-server enable** command to disable the NQA server.

By default, the NQA server is disabled.

Related command: **nqa-agent enable**, **nqa-server tcpconnect**, and **nqa-server udpecho**.

Example # Enable the NQA server.

```
<Sysname> system-view
[Sysname] nqa-server enable
```

nqa-server tcpconnect

Syntax **nqa-server tcpconnect** *ip-address port-number*

undo nqa-server tcpconnect *ip-address port-number*

View System view

Parameter *ip-address*: IP address specified for the TCP listening service on the NQA server.

port-number: Port number specified for the TCP listening service on the NQA server, in the range 1 to 50000. For a TCP-Public test, the port number must be 7.

Description Use the **nqa-server tcpconnect** command to create a TCP listening service on the NQA server.

Use the **undo nqa-server tcpconnect** command to remove the TCP listening service from the NQA server.

Note that:

- You need to configure the **nqa-server tcpconnect** command on the NQA server only for the TCP-Private and TCP-Public tests.
- The IP address and port number must be consistent with those on the NQA client and must be different from those for an existing listening service.
- The IP address must be that of an interface on the NQA server. Otherwise, the configuration will be invalid.

Related command: **nqa-server enable**.

Example # Create a TCP listening service by using the IP address 169.254.10.2 and port 9000.

```
<Sysname> system-view
[Sysname] nqa-server tcpconnect 169.254.10.2 9000
```

nqa-server udpecho

Syntax **nqa-server udpecho** *ip-address port-number*

undo nqa-server udpecho *ip-address port-number*

View System view

Parameter *ip-address*: IP address specified for the UDP listening service on the NQA server.

port-number: Port number specified for the UDP listening service on the NQA server, in the range 1 to 50000. For the UDP-Public test, the port number must be 7.

Description Use the **nqa-server udpecho** command to create a UDP listening service on the NQA server.

Use the **undo nqa-server udpecho** command to remove the UDP connection.

Note that:

- You need to configure the **nqa-server udpecho** command on the NQA server only for the jitter, UDP-Private, and UDP-Public tests.
- The IP address and port number must be consistent with those of the NQA client and must be different from those of an existing listening service.
- The IP address must be that of an interface on the NQA server and must not be 0.0.0.0. Otherwise, the configuration will be invalid.

Related command: **nqa-server enable**.

Example # Create a UDP listening service by using the IP address 169.254.10.2 and port 9000.

```
<Sysname> system-view
[Sysname] nqa-server udpecho 169.254.10.2 9000
```

98 HIGH AVAILABILITY CONFIGURATION COMMANDS

debugging ha

Syntax **debugging ha** { **all** | **error** | **event** | **message** | **state** }

undo debugging ha { **all** | **error** | **event** | **message** | **state** }

View User view

Parameter **all**: Enables all debugging.

error: Enables error debugging for switchover between the active module and the standby module.

event: Enables event debugging for switchover between the active module and the standby module.

message: Enables message debugging for switchover between the active module and the standby module.

state: Enables event debugging for switchover between the active module and the standby module.

Description Use the **debugging ha** command to enable HA debugging.

Use the **undo debugging ha** command to disable HA debugging.

Example # Enable state debugging for switchover between the active module and the standby module.

```
<Sysname> debugging ha state
```

debugging haxbar

Syntax **debugging haxbar** [**slot** *slot-id*]

undo debugging haxbar [**slot** *slot-id*]

View User view

Parameter **slot** *slot-id*: Slot ID of the active module or standby module.

Description Use the **debugging haxbar** command to enable HA Xbar debugging.

Use the **undo debugging haxbar** command to disable HA Xbar debugging.

Example # Enable debugging for the HA Xbar module of the module in slot 1.

```
<Sysname> debugging haxbar slot 1
```

display fullmesh-enhance

Syntax **display fullmesh-enhance**

View Any view

Parameter None

Description Use the **display fullmesh-enhance** command to display the configuration information forwarded in Full Mesh mode.

CAUTION: *Only when the active module and standby module work in load balancing mode can the system activate Full Mesh enhance mode.*

Example # Display information of the Full Mesh enhance mode of the system.

```
<Sysname> display fullmesh-enhance
Configuration status: Enabled
Operation status: Active
```

Table 406 Field descriptions of the display fullmesh-enhance command

Field	Description
Configuration status	Configuration status: Enabled means Full Mesh enhance mode is configured and Disabled means Full Mesh enhance mode is not configured.
Operation status	Operation status: Active means Full Mesh enhance mode is activated and Inactive means Full Mesh enhance is not activated.

display switchover state

Syntax **display switchover state** [*slot-id*]

View Any view

Parameter *slot-id*: Slot ID of the active module or standby module.

Description Use the **display switchover state** command to display the switchover state.

This command displays the switchover state on the active module or the standby module depending on the slot number specified. The switchover state of the active module will be displayed if no slot number is specified.

Example # Display the switchover state on the active module.

```
<Sysname> display switchover state
HA FSM State(master): Slave is absent.
```

Table 407 Descriptions on the fields of display switchover state

Field	Description
Slave is absent	The standby module is not in the slot.
Waiting batch backup request from slave	Waiting for the backup requests from the standby module
Batch backup	Backup state
Realtime and routine backup to slave	Real-time or routine backup state
Receiving realtime and routine data	Receives realtime or routine data.

fullmesh-enhance

Syntax **fullmesh-enhance** { **enable** | **disable** }

View System view

Parameter **enable**: Enables Full Mesh enhance mode.

disable: Disables Full Mesh enhance mode.

Description Use the **fullmesh-enhance enable** command to set the Full Mesh forwarding mode to enhance mode.

Use the **fullmesh-enhance disable** command to remove the Full Mesh enhance mode.

By default, the Full Mesh enhance mode is disabled.

CAUTION:

- *If only the active module or the standby module is in the slot, the Full Mesh enhance mode does not take effect.*
- *The Switch 8807 series switches do not support this command.*

Example # Set the Full Mesh forwarding mode to enhance mode.

```
<Sysname> system-view
[Sysname] fullmesh-enhance enable
```

Remove the Full Mesh enhance mode and return to a normal mode.

```
[Sysname] fullmesh-enhance disable
```

slave restart

Syntax **slave restart**

View System view

Description Use the **slave restart** command to manually configure the standby module to restart.

When the backup system program operates abnormally and needs to be reloaded, you can manually restart the standby module.

Example # Restart the standby module.

```
<Sysname> system-view
[Sysname] slave restart
The slave will reset! Continue?[Y/N]:y
```

slave switchover (System view)

Syntax **slave switchover**

View System view

Parameter None

Description Use the **slave switchover** command to manually configure the switchover between the active module and standby module.

Related command: **slave switchover**.

Example # Manually configure the switchover between the active module and the standby module.

```
<Sysname> system-view
[Sysname] slave switchover
Caution!!! Confirm switch slave to master?[Y/N] y
Starting.....
RAM Line....OK
```

slave switchover (System view)

Syntax **slave switchover** { **enable** | **disable** }

View System view

Parameter **enable**: Enables manual configuration of the switchover between active module and standby module.

disable: Disables manual configuration of the switchover between active module and standby module.

Description Use the **slave switchover** command to configure manual switchover function between active module and standby module.

By default, manual configuration of the switchover between active module and standby module is enabled.

Related command: **slave switchover**.

Example # Enable manual configuration of the switchover between active module and standby module.

```
<Sysname> system-view
[Sysname] slave switchover enable
```

99 INFORMATION CENTER CONFIGURATION COMMANDS

display channel

Syntax **display channel** [*channel-number* | *channel-name*]

View Any view

Parameter *channel-number*: Specifies a channel number, in the range 0 to 9.

channel-name: Specifies a channel name, which could be a default name or one that is defined by the user. The user needs to specify a channel name first before using it as a self-defined channel name. For more information, refer to the **info-center channel name** command on page 1453.

Table 408 Information channels for different output directions

Output direction	Information channel number	Default channel name
Console	0	console
Monitor terminal	1	monitor
Log host	2	loghost
Trap buffer	3	trapbuffer
Log buffer	4	logbuffer
SNMP NMS	5	snmpagent
Log file	9	channel9

Description Use the **display channel** command to display channel information.

If no channel is specified, information for all channels is displayed.

Example # Display information for channel 0.

```
<Sysname> display channel 0
channel number:0, channel name:console
MODU_ID  NAME     ENABLE LOG_LEVEL     ENABLE TRAP_LEVEL    ENABLE DEBUG_LEVEL
ffff0000 default  Y      warnings      Y      debugging     Y      debugging
```

Table 409 Field descriptions of the display channel command

Field	Description
channel number	A specified channel number, in the range 0 to 9.

Table 409 Field descriptions of the display channel command

Field	Description
channel name	A specified channel name, which varies with user's configuration. For more information, refer to the **info-center channel name** command on page 1453.
MODU_ID	The ID of the module to which the information permitted through the current channel belongs
NAME	The name of the module to which the information permitted through the current channel belongs.
ENABLE	Indicates whether to enable or disable the output of log information, which could be Y or N.
LOG_LEVEL	The severity level of log information, refer to Table 411 for details.
ENABLE	Indicates whether to enable or disable the output of trap information, which could be Y or N.
TRAP_LEVEL	The severity level of trap information, refer to Table 411 for details.
ENABLE	Indicates whether to enable or disable the output of debug information, which could be Y or N.
DEBUG_LEVEL	The severity level of debug information, refer to Table 411 for details.

The above information indicates to output log information with the severity level from 0 to 4, trap information with the severity level from 0 to 7 and debug information with the severity level from 0 to 7 to the console. The source module is default.

display info-center

Syntax **display info-center**

View Any view

Parameter None

Description Use the **display info-center** command to display configurations for all channels (except channel 6 to 8) of the information center.

Example # Display configurations for all channels.

```
<Sysname> display info-center
Information Center:enabled
Log host:
Console:
    channel number : 0, channel name : console
Monitor:
    channel number : 1, channel name : monitor
SNMP Agent:
```

```
    channel number : 5, channel name : snmpagent
Log buffer:
    enabled,max buffer size 1024, current buffer size 512,
    current messages 512, dropped messages 0, overwritten messages 191
    channel number : 4, channel name : logbuffer
Trap buffer:
    enabled,max buffer size 1024, current buffer size 256,
    current messages 50, dropped messages 0, overwritten messages 0
    channel number : 3, channel name : trapbuffer
logfile:
    channel number:9, channel name:channel9, language English
Information timestamp setting:
    log - date, trap - date, debug - date,
    loghost - date

Sent messages = 752, Received messages = 752

IO Reg messages = 0 IO Sent messages = 0
```

Table 410 Field descriptions of the display info-center command

Field	Description
Information Center	The current state of the information center, which could be enabled or disabled.
Log host	The information of the log host channel, including IP address of the log host, the channel number(s) and channel name(s) used, the language mode and logging facility used.
Console	The Console channel information, including the channel number(s) and channel name(s) used.
Monitor	The monitor channel information, including the channel number(s) and channel name(s) used
SNMP Agent	The NMS channel information, including the channel number(s) and channel name(s) used
Log buffer	The information of the log buffer channel, including whether it is enabled or disabled, the maximum capacity, the current capacity, the current number of messages, the number of dropped messages, the number of messages that have been overwritten, and the channel number(s) and channel name(s) used.
Trap buffer	The information of the trap buffer channel, including whether it is enabled or disabled, the maximum capacity, the current capacity, the current number of messages, the number of dropped messages, the number of messages that have been overwritten, and the channel number(s) and channel name(s) used.
logfile	The logfile configurations information, including the channel number(s), channel name(s), and language mode used.
Information timestamp setting	The time stamp configurations, specifying the time stamp format for log, trap, debug, and log host information.

display logbuffer

Syntax **display logbuffer** [**level** *severity* | **size** *buffersize* | **slot** *slotnum*] * [| { **begin** | **exclude** | **include** } *text*]

View Any view

Parameter *severity*: Information level, in the range 0 to 7.

Table 411 Severity description

Severity	Value	Description
emergencies	0	The system is unavailable
alerts	1	Information that requires prompt reaction
critical	2	Critical information
errors	3	Error information
warnings	4	Warnings
notifications	5	Normal errors with important information
informational	6	Informational information to be recorded
debugging	7	Debugging information

buffersize: Specifies the number of the latest log messages to display in the log buffer, in the range 1 to 1,024.

slot *slotnum*: Slot number.

|: The output log information filtered by a regular expression.

begin: Displays log information beginning with the specified text.

exclude: Displays log information that does not contain the specified text.

include: Displays log information that contains the specified text.

text: Regular expression.

Table 412 Meanings of characters in text

Character	Meaning	Remarks
^	Starting sign, the string following it appears only at the beginning of a line.	Regular expression "^user" matches a string begins with "user", not "Auser".
$	Ending sign, the string following it appears only at the end of a line.	Regular expression "user$" matches a string ends with "user", not "userA".
.	Full stop, a wildcard used in place of any character, including blank	None
*	Asterisk, used to match a subexpression before it zero or multiple times	zo* can map to "z" and "zoo".
+	Addition, used to match a subexpression before it one or multiple times	zo+ can map to "zo" and "zoo", but not "z".

Table 412 Meanings of characters in text

Character	Meaning	Remarks
-	Hyphen. It connects two values (the smaller one before it and the bigger one after it) to indicate a range together with [ ].	For example, "1-9" means numbers from 1 to 9 (inclusive); "a-h" means from a to h (inclusive).
[ ]	Selects one character from the group.	For example, [1-36A] can match only one character among 1, 2, 3, 6, and A.
( )	A group of characters. It is usually used with "+" or "*".	For example, (123A) means a string "123A"; "408(12)+" can match 40812 or 408121212. But it cannot match 408. That is, "12" can appear continuously and it must at least appear once.

Description

Use the **display logbuffer** command to display the state of the log buffer and the log information recorded. Absence of the **size** *buffersize* argument indicates that all log information recorded in the log buffer is displayed.

Example

Display the state of the log buffer and the log information recorded on a Switch 8800.

```
<Sysname> display logbuffer
Logging buffer configuration and contents:enabled
Allowed max buffer size : 1024
Actual buffer size : 512
Channel number : 4 , Channel name : logbuffer
Dropped messages : 0
Overwritten messages : 0
Current messages : 452
%Mar 24 11:51:41:188 2006 Sysname-wvrp IC/7/SYS_RESTART:
System restarted --
3Com Versatile Routing Platform Software
Copyright (c) 2003-2004 by VMW Team Hangzhou Institute 3Com Tech, Inc
%Mar 24 11:51:58:4328 2006 Sysname CFM/5/CFM_LOG:
 **Type system(59) Section system(Mod4)
%Mar 24 11:51:58:4344 2006 Sysname CFM/5/CFM_LOG:
 **Type system(59) Section system(BDR4)
%Mar 24 11:51:58:4344 2006 Sysname CFM/5/CFM_LOG:
 **Type mpls(6) Section mpls(Mod2)
%Mar 24 11:51:58:4344 2006 Sysname CFM/5/CFM_LOG:
 **Type mpls(6) Section mpls(BDR2)
%Mar 24 11:51:58:4344 2006 Sysname CFM/5/CFM_LOG:
 **Type post-system(24) Section post-system(Mod2)
%Mar 24 11:51:58:4344 2006 Sysname CFM/5/CFM_LOG:
 **Type post-system(24) Section post-system(BDR2)
%Mar 24 11:52:02:516 2006 Sysname HTTPD/5/Log:Starting HTTP server.
%Mar 24 11:53:08:625 2006 Sysname SHELL/5/LOGIN: Console login from con0
%Mar 24 12:01:41:109 2006 Sysname HWCM/5/TRAPLOG:
          1.3.6.1.4.1.2011.10.2.4.2.1 configure changed:
          EventIndex=1,CommandSource=2,ConfigSource=4,ConfigDestination=2
```

Table 413 Descriptions on the fields of the display logbuffer command

Field	Description
Logging buffer configuration and contents	Indicates the current state of the log buffer and its contents, which could be enabled or disabled.

Table 413 Descriptions on the fields of the display logbuffer command

Field	Description
Allowed max buffer size	The maximum buffer size allowed
Actual buffer size	The actual buffer size
Channel number	The channel number of the log buffer, defaults to 4
Channel name	The channel name of the log buffer, defaults to logbuffer
Dropped messages	The number of dropped messages
Overwritten messages	The number of overwritten messages (when the buffer size is not big enough to hold all messages, the latest messages overwrite the old ones).
Current messages	The number of the current messages

display logbuffer summary

Syntax **display logbuffer summary** [**level** *severity* | **slot** *slotnumber*] *

View Any view

Parameter *severity*: Information level, in the range 0 to 7.

slot *slotnumer*: Slot number.

Description Use the **display logbuffer summary** command to display the summary of the log buffer.

Example # Display the summary of the log buffer on a Switch 8800.

```
<Sysname> display logbuffer summary
  SLOT EMERG ALERT  CRIT ERROR  WARN NOTIF  INFO DEBUG
     0     0     0     0     0     0     0     0     0
     1     0     0     0     0     0     0     0     0
     2     0     0     0     0     0     0     0     0
     3     0     0     0     0    16     0     1     0
```

Table 414 Descriptions on the fields of the display logbuffer summary command

Field	Description
SLOT	Slot number
EMERG	Represents emergencies, refer to Table 411 for details
ALERT	Represents alerts, refer to Table 411 for details
CRIT	Represents critical, refer to Table 411 for details
ERROR	Represents errors, refer to Table 411 for details
WARN	Represents warnings, refer to Table 411 for details
NOTIF	Represents notifications, refer to Table 411 for details

Table 414 Descriptions on the fields of the display logbuffer summary command

Field	Description
INFO	Represents informational, refer to Table 411 for details
DEBUG	Represents debugging, refer to Table 411 for details

display logfile buffer

Syntax **display logfile buffer**

View Any view

Parameter None

Description Use the **display logfile buffer** command to display contents of the log file buffer.

Example # Display the contents of the log file buffer.

```
<Sysname> display logfile buffer
%@27222%Mar 12 02:01:03 2006 Sysname %%10IC/7/SYS_RESTART:
System restarted --
3Com Versatile Routing Platform Software
Copyright (c) 2003-2004 by CMW Team Hangzhou Institute 3Com Tech, Inc
%@27224%Mar 12 02:02:06:124 2006 Sysname CFM/5/CFM_LOG:
 Module 60c0000 Func 131baa0 using old API installing Buildrun in mfr
%@27225%Mar 12 02:02:06:124 2006 Sysname CFM/5/CFM_LOG:
 Module 60c0000 Func 131baa0 using old API installing Buildrun in mp-group
%@27226%Mar 12 02:02:06:125 2006 Sysname RM/4/RMLOG:
 RM notify Memory shortage notification
%@27227%Mar 12 02:02:06:125 2006 Sysname RM/4/RMLOG:RIP: System memory low V
OS notification received
%@27228%Mar 12 02:02:06:125 2006 Sysname RM/4/RMLOG:RIPng: System memory low
 VOS notification received
```

display logfile summary

Syntax **display logfile summary**

View Any view

Parameter None

Description Use the **display logfile summary** command to display the configuration of the log file.

Example # Display the configuration of the log file.

```
[Sysname]display logfile summary
  Log file is enabled.
  Language mode : english
```

```
Channel number : 9
Log file size quota : 0 MB (0 for unlimited)
Log file directory : flash:/logfile
Writing frequency : 0 hour 0 min 10 sec
```

Table 415 Descriptions on the fields of the display logfile summary command

Field	Description
Log file is	The current state of a log file, which could be enabled or disabled.
Language mode	Language of logfile: Chinese or English
Channel number	The channel number of a log file, defaults to 9.
Log file size quota	The maximum storage space reserved for a log file
Log file directory	Log file directory
Writing frequency	Log file writing frequency

display trapbuffer

Syntax **display trapbuffer** [**size** *buffersize*]

View Any view

Parameter *buffersize*: Specifies the number of the latest trap messages in a trap buffer, in the range 1 to 1,024.

Description Use the **display trapbuffer** command to display the state and the trap information recorded.

Absence of the **size** *buffersize* argument indicates that all trap information is displayed.

Example # Display the state of the trap buffer and the trap information recorded.

```
<Sysname> display trapbuffer
Trapping buffer configuration and contents:enabled
Allowed max buffer size : 1024
Actual buffer size : 256
Channel number : 3 , channel name : trapbuffer
Dropped messages : 0
Overwritten messages : 0
Current messages : 1

#Nov 21 10:57:24:568 2006 Sysname DEV/1/BOARD INSERTED:
 Trap 1.3.6.1.4.1.2011.2.23.1.12.1.9: frameIndex is 0, slotIndex 0.4
```

Table 416 Descriptions on the fields of the display trapbuffer command

Field	Description
Trapping buffer configuration and contents	Indicates the current state of the trap buffer and its contents, which could be enabled or disabled.
Allowed max buffer size	The maximum buffer size allowed
Actual buffer size	The actual buffer size

Table 416 Descriptions on the fields of the display trapbuffer command

Field	Description
Channel number	The channel number of the trap buffer, defaults to 3
Channel name	The channel name of the trap buffer, defaults to trapbuffer
Dropped messages	The number of dropped messages
Overwritten messages	The number of overwritten messages (when the buffer size is not big enough to hold all messages, the latest messages overwrite the old ones).
Current messages	The number of the current messages

info-center channel name

Syntax **info-center channel** *channel-number* **name** *channel-name*

undo info-center channel *channel-number*

View System view

Parameter *channel-number*: Specifies a channel number, in the range 0 to 9.

channel-name: Specifies a channel name, a string of 1 to 30 characters. It should not start with a number, an underscore (-), a forward slash (/), or a backward slash (\). The channel name is not case sensitive.

Description Use the **info-center channel name** command to name a channel with a specified channel number.

Use the **undo info-center channel** command to restore the default name for a channel with a specified channel number.

Refer to Table 408 for details of default channel names and channel numbers.

Example # Name channel 0 as abc.

```
<Sysname> system-view
[Sysname] info-center channel 0 name abc
```

info-center console channel

Syntax **info-center console channel** { *channel-number* | *channel-name* }

undo info-center console channel

View System view

Parameter *channel-number*: Specifies a channel number, in the range 0 to 9.

channel-name: Specifies a channel name, which could be a default name or one that is defined by the user. The user needs to specify a channel name first before using it as a self-defined channel name. For related configuration, refer to the **info-center channel name** command on page 1453.

Description Use the **info-center console channel** command to specify the channel to output system information to the console.

Use the **undo info-center console channel** command to restore the default output channel to the console.

By default, output of information to the console is enabled with channel 0 as the default channel (known as console).

Note that the **info-center console channel** command takes effect only after the information center is enabled first with the **info-center enable** command.

Example # Set channel 0 to output system information to the console.

```
<Sysname> system-view
[Sysname] info-center console channel 0
```

info-center enable

Syntax **info-center enable**

undo info-center enable

View System view

Parameter None

Description Use the **info-center enable** command to enable information center.

Use the **undo info-center enable** command to disable the information center.

The system outputs information to the log host or the console only after the information center is enabled first.

By default, the information center is enabled.

Example # Enable the information center.

```
<Sysname> system-view
[Sysname] info-center enable
% Information center is enabled
```

info-center logbuffer

Syntax **info-center logbuffer** [**channel** { *channel-number* | *channel-name* } | **size** *buffersize*] *

undo info-center logbuffer [**channel** | **size**]

View System view

Parameter *buffersize*: Specifies the maximum number of log messages in a log buffer, in the range 0 to 1,024 with 512 as the default value.

channel-number: A specified channel number, in the range 0 to 9.

channel-name: Specifies a channel name, which could be a default name or one that is defined by the user. The user needs to specify a channel name first before using it as a self-defined channel name. For related configuration, refer to the **info-center channel name** command on page 1453.

Description Use the **info-center logbuffer** command to enable information output to a log buffer and set the corresponding parameters.

Use the **undo info-center logbuffer** command to disable information output to a log buffer.

By default, information output to the log buffer is enabled with channel 4 (logbuffer) as the default channel and a maximum buffer size of 512.

Note that the **info-center logbuffer** command takes effect only after the information center is enabled with the **info-center enable** command.

Example # Enable the system to output information to the log buffer with a default buffer size of 50.

```
<Sysname> system-view
[Sysname] info-center logbuffer size 50
```

info-center logfile enable

Syntax **info-center logfile enable**

undo info-center logfile enable

View System view

Parameter None

Description Use the **info-center logfile enable** command to enable the output of system information to the log file.

Use the **undo info-center logfile enable** command to disable the output of system information to the log file.

By default, the output of system information to the log file is enabled.

Example # Enable the log file feature.

```
<Sysname> system-view
[Sysname] info-center logfile enable
```

info-center logfile frequency

Syntax **info-center logfile frequency** *freq-sec*

undo info-center logfile frequency

View System view

Parameter *freq-sec*: Frequency with which the system saves the log file, in the range 1 to 86400, in seconds.

Description Use the **info-center logfile frequency** command to configure the frequency with which the system saves the log file.

Use the **undo info-center logfile frequency** command to restore the default frequency.

By default, the frequency with which a Switch 8800 saves the log file is 60 seconds.

Example # Configure the frequency with which the system saves the log file as 60,000 seconds.

```
<Sysname> system-view
[Sysname] info-center logfile frequency 60000
```

info-center logfile language

Syntax **info-center logfile language** { **chinese** | **english** }

undo info-center logfile language

View System view

Parameter **chinese**: Specifies to record log information in Chinese.

english: Specifies to record log information in English.

Description Use the **info-center logfile language** command to set the language of log files.

Use the **undo info-center logfile language** command to restore the language of log files to the default.

By default, the log files are in English.

Example # Set the language of the log files to Chinese.

```
<Sysname> system-view
[Sysname] info-center logfile language chinese
```

info-center logfile size-quota

Syntax **info-center logfile size-quota** *size*

undo info-center logfile size-quota

View System view

Parameter *size:* The maximum capacity of a disk, in MB. The value cannot be smaller than 1 MB and larger than 10 MB.

Description Use the **info-center logfile size-quota** command to set the maximum storage space reserved for a log file.

Use the **undo info-center logfile size-quota** command to restore the default maximum storage space reserved for a log file.

Example # Set the maximum storage space reserved for a log file to 6 MB.

```
<Sysname> system-view
[Sysname] info-center logfile size-quota 6
```

info-center logfile switch-directory

Syntax **info-center logfile switch-directory** *dir-name*

View System view

Parameter *dir-name*: The name of the directory where a log file is saved, a string of 1 to 64 characters.

Description Use the **info-center logfile switch-directory** command to configure the directory where a log file is saved. Ensure that the directory is created first before saving a log file into it.

By default, the directory to save a log file is the logfile directory under the root directory of the storage device.

Note that this command can be used to manually configure the directory to which a log file can be saved. The configuration will lose after system restarts or primary/backup switchover.

Example # Create a directory with the name test under flash root directory.

```
<Sysname> mkdir test
%Created dir flash:/test.
```

Set the directory to save the log file to flash:/test.

```
<Sysname> system-View
[Sysname] info-center logfile switch-directory flash:/test
```

info-center loghost

Syntax **info-center loghost** *host-ip* [**channel** { *channel-number* | *channel-name* } **facility** *local-number* | **language** { **chinese** | **english** }] *

undo info-center loghost *host-ip*

View System view

Parameter *host-ip*: The IP address of the log host.

channel: Specifies the channel through which system information can be output to the log host.

channel-number: Specifies a channel number, in the range 0 to 9.

channel-name: Specifies a channel name, which could be a default name or one that is defined by the user. The user needs to specify a channel name first before using it as a self-defined channel name. For related configuration, refer to the **info-center channel name** command on page 1453.

facility *local-number*: The logging facility of the log host. The value can be local0 to local7.

language: Sets the language mode of the log files. The default language is English.

- **chinese**: Sets the language to Chinese.
- **english**: Sets the language to English.

Description Use the **info-center loghost** command to specify a log host and to configure the related parameters.

Use the **undo info-center loghost** command to restore the default configurations on a log host.

By default, output of system information to the log host is disabled. When it is enabled, the default channel name will be loghost and the default channel number will be 2.

Note that:

- The **info-center loghost** command takes effect only after the information center is enabled with the **info-center enable** command.

- Ensure that the IP address input is correct while using the **info-center loghost** command to configure the IP address for a log host. System will prompt an invalid address if the loopback address (127.0.0.1) is input.
- A maximum number of 4 hosts (different) can be designated as the log host.

Example # Set to output log information to a Unix station with the IP address being 202.10.10.1/16.

```
<Sysname> system-view
[Sysname] info-center loghost 202.10.10.1
```

info-center loghost source

Syntax **info-center loghost source** *interface-type interface-number*

undo info-center loghost source

View System view

Parameter *interface-type interface-number*: Specifies a source interface by its type and number.

Description Use the **info-center loghost source** command to configure the source interface to output log information to the log host.

Use the **undo info-center loghost source** command to remove the source interface to output log information to the log host.

By default, no source interface is configured to output log information to the log host, and the system selects an interface as the source interface.

Note that the **info-center loghost source** command takes effect only after the information center is enabled with the **info-center enable** command.

Example # Configure the interface M-Ethernet 6/0/0 as the source interface to output log information to the log host.

```
<Sysname> system-view
[Sysname] info-center loghost source M-Ethernet 6/0/0
```

info-center monitor channel

Syntax **info-center monitor channel** { *channel-number* | *channel-name* }

undo info-center monitor channel

View System view

Parameter *channel-number*: Specifies a channel number, in the range 0 to 9.

channel-name: Specifies a channel name, which could be a default name or one that is defined by the user. The user needs to specify a channel name first before using it as a self-defined channel name. For more information, refer to the **info-center channel name** command on page 1453.

Description Use the **info-center monitor channel** command to configure the channel to output system information to the monitor.

Use the **undo info-center monitor channel** command to restore the default channel to output system information to the monitor.

By default, output of system information to the monitor is enabled with a default channel name of monitor and a default channel number of 1.

Note that the **info-center monitor channel** command takes effect only after the information center is enabled with the **info-center enable** command.

Example # Set to output system information to the monitor through channel 0.

```
<Sysname> system-view
[Sysname] info-center monitor channel 0
```

info-center snmp channel

Syntax **info-center snmp channel** { *channel-number* | *channel-name* }

undo info-center snmp channel

View System view

Parameter *channel-number*: Specifies a channel number, in the range 0 to 9.

channel-name: Specifies a channel name, which could be a default name or one that is defined by the user. The user needs to specify a channel name first before using it as a self-defined channel name. For more information, refer to the **info-center channel name** command on page 1453.

Description Use the **info-center snmp channel** command to configure the channel to output system information to the SNMP NMS.

Use the **undo info-center snmp channel** command to restore the default channel to output system information to the SNMP NMS.

By default, output of system information to the SNMP NMS is enabled with a default channel name of snmpagent and a default channel number of 5.

For more information, refer to the **display snmp-agent** command in the "SNMP Configuration Commands" on page 1347.

Example # Set to output system information to the SNMP NMS through channel 6.

```
<Sysname> system-view
[Sysname] info-center snmp channel 6
```

info-center source

Syntax **info-center source** { *module-name* | **default** } **channel** { *channel-number* | *channel-name* } [**debug** { **level** *severity* | **state** *state* } * | **log** { **level** *severity* | **state** *state* } * | **trap** { **level** *severity* | **state** *state* } *] *

undo info-center source { *module-name* | **default** } **channel** { *channel-number* | *channel-name* }

View System view

Parameter *module-name*: Specifies the source modules of the system information. For example, if you want to output the system information of the ARP module, set the argument to ARP. **default**: Allows all the modules to output the system information. The modules that are allowed to output system information vary with devices.

debug: Debug information.

log: Log information.

trap: Trap information.

severity: Specifies the severity of system information, refer to Table 411 for details.

state: The state of system information, which could be **on** or **off**.

channel-number: Specifies a channel number, in the range 0 to 9.

channel-name: Specifies a channel name, which could be a default name or one that is defined by the user. The user needs to specify a channel name first before using it as a self-defined channel name. For more information, refer to the **info-center channel name** command.

Description Use the **info-center source** command to specify the information source of the specified information channel, making the information output to the corresponding direction through the specified information channel.

Use the **undo info-center source** command to restore the default.

By default, the system assigns an information channel for each output direction. See Table 408.

This command can be used to filter and redirect system information.

For example, the user can set to output log information with severity higher than warnings to the log host, and information with severity higher than informational to the log buffer. The user can also set to output trap information of the IP module to a specified output direction.

Example # Set the output channel for the log information of VLAN module to snmpagent and to output information with severity being emergencies.

```
<Sysname> system-view
[Sysname] info-center source VLAN channel snmpagent log level emergencies
```

info-center synchronous

Syntax **info-center synchronous**

undo info-center synchronous

View System view

Parameter None

Description Use the **info-center synchronous** command to enable synchronous information output.

Use the **undo info-center synchronous** command to disable the synchronous information output.

By default, the synchronous information output is disabled.

- *Under the current command line prompt, if the user's input is interrupted by system output such as log information, then after the completion of system output the system will not display command line prompt.*
- *When users need to input some interactive information (non Y/N confirmation information) if the user's input is interrupted by system information, then after the completion of system output the system will not display command line prompt but just print the user's input.*

Example # Enable synchronous information output.

```
<Sysname> system-view
[Sysname] info-center synchronous
% Info-center synchronous output is on
```

The user receives trap messages when he/she is about to display the configurations for an Ethernet interface by inputting the **display interface ethernet** command. After the system has finished its output of trap messages, it will display the user's original input, which is "display interface ethernet" in this case.

```
<Sysname> display interface ethernet
%Apr  2 17:33:48:986 2000 Sysname L2INF/5/PORT LINK STATUS CHANGE:- 1 -
 Ethernet1/1/4: is UP

<Sysname> display interface Ethernet
```

info-center timestamp

Syntax **info-center timestamp** { **log** | **trap** | **debugging** } { **boot** | **date** | **none** }

undo info-center timestamp { **log** | **trap** | **debugging** }

View System view

Parameter **log**: Log information.

trap: Trap information.

debugging: Debug information.

boot: The time taken to boot up the system, in the format of xxxxxx.yyyyyy, in which xxxxxx represents the most significant 32 bits of the time taken to boot up the system (in milliseconds) whereas yyyyyy is the least significant 32 bits.

date: The current system date and time, in the format of "Mmm dd hh:mm:ss:sss yyyy".

- Mmm: The abbreviations of the months in English, which could be Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, or Dec.
- dd: The date, starting with a space if less than 10, for example " 7".
- hh:mm:ss:sss: The local time, with hh ranging from 00 to 23, mm and ss ranging from 00 to 59, and sss ranging from 0 to 999.
- yyyy: Represents the year.

none: Indicates no time information is provided.

Description Use the **info-center timestamp** command to configure the time stamp format.

Use the **undo info-center timestamp** command to restore the default.

By default, the time stamp format for log, trap and debug information is **date**.

Example # Configure the time stamp for debug information as boot.

```
<Sysname> system-view
[Sysname] info-center timestamp debugging boot
```

info-center timestamp loghost

Syntax **info-center timestamp loghost** { **date** | **no-year-date** | **none** }

undo info-center timestamp loghost

View System view

Parameter **date**: Indicates the current system date and time, the format of which depends on the log host.

no-year-date: Indicates the current system date and time (year exclusive).

none: Indicates that no time stamp information is provided.

Description Use the **info-center timestamp loghost** command to configure the time stamp format of the log information sent to the log host.

Use the **undo info-center timestamp loghost** command to restore the default.

By default, the time stamp format for log information sent to the log host is **date.**

Example # Set not to include the year information in the output information to the log host.

```
<Sysname> system-view
[Sysname] info-center timestamp loghost no-year-date
```

info-center trapbuffer

Syntax **info-center trapbuffer** [**channel** { *channel-number* | *channel-name* } | **size** *buffersize*] *

undo info-center trapbuffer [**channel** | **size**]

View System view

Parameter *buffersize*: Specifies the maximum number of trap messages in a trap buffer, in the range 0 to 1,024 with 256 as the default value.

channel-number: Specifies a channel number, in the range 0 to 9.

channel-name: Specifies a channel name, which could be a default name or one that is defined by the user. The user needs to specify a channel name first before using it as a self-defined channel name. For more information, refer to the **info-center channel name** command on page 1453.

Description Use the **info-center trapbuffer** command to enable information output to the trap buffer and set the corresponding parameters.

Use the **undo info-center trapbuffer** command to disable information output to the trap buffer.

By default, information output to the trap buffer is enabled with channel 3 (trapbuffer) as the default channel and a maximum buffer size of 256.

Note that the **info-center trapbuffer** command takes effect only after the information center is enabled with the **info-center enable** command.

Example # Enable system to output information to the trap buffer with a default buffer size of 30.

```
<Sysname> system-view
[Sysname] info-center trapbuffer size 30
```

logfile save

Syntax **logfile save**

View Any view

Parameter None

Description Use the **logfile save** command to manually save the log buffer contents into the log file.

By default, the system automatically saves the log file based on a frequency configured by the **info-center logfile frequency** command into a directory configured by the **info-center logfile switch-directory** command.

Example # Set to manually save the log buffer contents into the log file.

```
<Sysname> logfile save
```

reset logbuffer

Syntax **reset logbuffer**

View User view

Parameter None

Description Use the **reset logbuffer** command to reset the log buffer contents.

Example # Reset the log buffer contents.

```
<Sysname> reset logbuffer
```

reset trapbuffer

Syntax **reset trapbuffer**

View User view

Parameter None

Description Use the **reset trapbuffer** command to reset the trap buffer contents.

Example # Reset the trap buffer contents.

```
<Sysname> reset trapbuffer
```

terminal debugging

Syntax **terminal debugging**

undo terminal debugging

View User view

Parameter None

Description Use the **terminal debugging** command to enable the display of debug information on the current terminal.

Use the **undo terminal debugging** command to disable the display of debug information on the current terminal.

By default, the display of debug information on the current terminal is disabled.

Note that the debug information is displayed (using the **terminal debugging** command) only after the monitoring of system information is enabled on the current terminal first (using the **terminal monitor** command).

Example # Enable the display of debug information on the current terminal.

```
<Sysname> terminal debugging
% Current terminal debugging is on
```

terminal logging

Syntax **terminal logging**

undo terminal logging

View User view

Parameter None

Description Use the **terminal logging** command to enable the display of log information on the current terminal.

Use the **undo terminal logging** command to disable the display of log information on the current terminal.

By default, the display of log information on the current terminal is disabled.

Note that the log information is displayed (using the **terminal logging** command) only after the monitoring of system information is enabled on the current terminal first (using the **terminal monitor** command).

Example # Disable the display of log information on the current terminal.

```
<Sysname> undo terminal logging
% Current terminal logging is off
```

terminal monitor

Syntax **terminal monitor**

undo terminal monitor

View User view

Parameter None

Description Use the **terminal monitor** command to enable the monitoring of system information on the current terminal.

Use the **undo terminal monitor** command to disable the monitoring of system information on the current terminal.

- Note that the **terminal monitor** command must be configured first before the log, trap, and debug information can be displayed using the corresponding commands.
- Configuration of the **undo terminal monitor** command automatically disables the monitoring of log, trap, and debug information.

By default, the monitoring of the console is enabled and the monitoring of the terminal is disabled.

Example # Enable the monitoring of system information on the current terminal.

```
<Sysname> terminal monitor
% Current terminal monitor is on
```

terminal trapping

Syntax **terminal trapping**

undo terminal trapping

View User view

Parameter None

Description Use the **terminal trapping** command to enable the display of trap information on the current terminal.

Use the **undo terminal trapping** command to disable the display of trap information on the current terminal.

By default, the display of trap information on the current terminal is enabled.

Note that the trap information is displayed (using the **terminal trapping** command) only after the monitoring of system information is enabled on the current terminal first (using the **terminal monitor** command).

Example #Enable the display of trap information on the current terminal.

```
<Sysname> terminal trapping
% Current terminal trapping is on
```

Alphabetical Listing of Commands

A B C D E F G H I J K L M N O P Q R S T U V W X

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X