3Com® Switch 8800 Family
Command Reference Guide

Switch 8807
Switch 8810
Switch 8814

www.3Com.com
Part No. 10015595, Rev. AA
Published: January 2007

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

3Com Corporation reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Corporation to provide notification of such revision or change.

3Com Corporation provides this documentation without warranty, term, or condition of any kind, either implied or expressed, including, but not limited to, the implied warranties, terms or conditions of merchantability, satisfactory quality, and fitness for a particular purpose. 3Com may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If there is any software on removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the hard copy documentation, or on the removable media in a directory file named LICENSE.TXT or !LICENSE.TXT. If you are unable to locate a copy, please contact 3Com and a copy will be provided to you.

UNITED STATES GOVERNMENT LEGEND

If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following:

All technical data and computer software are commercial in nature and developed solely at private expense. Software is delivered as "Commercial Computer Software" as defined in DFARS 252.227-7014 (June 1995) or as a "commercial item" as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in 3Com's standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this User Guide.

Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not be registered in other countries.

3Com and the 3Com logo are registered trademarks of 3Com Corporation.

Cisco is a registered trademark of Cisco Systems, Inc.

Funk RADIUS is a registered trademark of Funk Software, Inc.

Aegis is a registered trademark of Aegis Group PLC.

Intel and Pentium are registered trademarks of Intel Corporation. Microsoft, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation. Novell and NetWare are registered trademarks of Novell, Inc. UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company, Ltd.

IEEE and 802 are registered trademarks of the Institute of Electrical and Electronics Engineers, Inc.

All other company and product names may be trademarks of the respective companies with which they are associated.

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.

Alphabetical Listing of Commands

CONTENTS

ABOUT THIS GUIDE

This guide describes the 3Com® Switch 8800 and how to install hardware, configure and boot software, and maintain software and hardware. This guide also provides troubleshooting and support information for your switch.

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.

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
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.”

Table 2 Text Conventions

Convention	Description
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 Command Reference Guide* — Provides detailed descriptions of command line interface (CLI) commands, that you require to manage your Switch 8800.
- *Switch 8800 Configuration Guide*— 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 3Com World Wide Web site:

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

1 Command Line Interface Commands

Command Line Interface Commands

command-privilege level

Syntax

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

undo command-privilege view *view command*

View

System view

Parameter

level: Specifies the command level, ranging from 0 to 3.

view: Specifies the command view, which can be any of the views supported by the switch.

command: Specifies the command to be configured.

Description

Use the **command-privilege level** command to configure the priority of the specifically command of the specifically view.

Use the **undo command-privilege view** command to restore the default command priority.

The command levels include visit, monitoring, configuration, and management, which are identified as 0 through 3 respectively. An administrator assigns authorities as per user requirements and allows them to operate in corresponding views. When a user logs in to the switch, the command level that it can access depends on two points. One is the command level that the user itself can access, the other is the set command level of this user interface. If the two levels are different, the former will be taken. For example, the command level of VTY 0 user interface is 1, however, user Tom has the right to access commands of level 3; if Tom logs in from VTY 0 user interface, he can access commands of level 3 and lower.

By default, **ping**, **tracert**, and **telnet** are at visit level (0); **display** and **debugging** are at monitoring level (1); all the configuration commands are at configuration level (2); and FTP, TFTP and commands for file system operations are at management level (3).

Example

Configure the precedence of the command "interface" as 0.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] command-privilege level 0 view system interface
```

display history-command

Syntax

display history-command [*Command-Number*] [| { **begin** | **include** | **exclude** } *Match-string*]

View

Any view

Parameter

Command-Number: The number of history commands the user wants to query. The value range is 1 to 256.

|: Operator, indicating that a regular expression follows.

begin: Displays all commands starting from the one that matches the match string.

include: Displays only the command that matches the string.

exclude: Displays only the commands that do not match the match string.

Match-string: The regular expression to match.

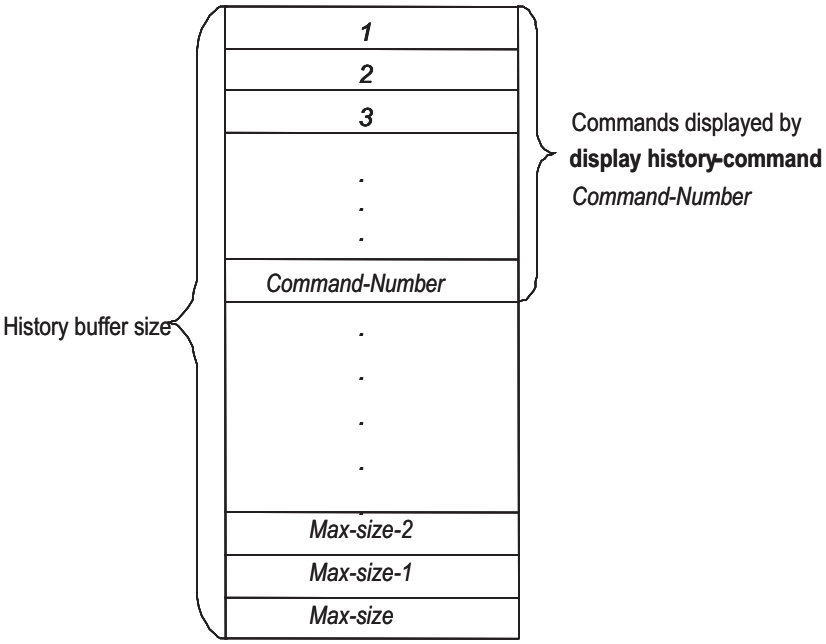
Description

The **display history-command** command is used to query selectively the history commands. All the history commands are stored in the history command buffer. When the history command buffer is full, the oldest information in the buffer will be replaced by new information.

The number of history commands obtained through the **display history-command** command, *Command-Number*, depends on the size of the history command buffer set through the **history-command max-size** command, and *Command-Number* should not be bigger than the size of the history command buffer *Max-size*. If the specified *Command-Number* is bigger than the *Max-size*, all the commands in the history command buffer will be queried.

Refer to Figure 1.

Figure 1 Relation between history buffer size and Command-Number



You can either specify the number of commands to be queried (*Command-Number*) or input a string to query commands that match the string. You can the two methods separately or in combination.

- If you only specify *Command-Number*, the *Command-Number* pieces of commands executed recently will be displayed.
- If you specify a regular expression "| { **begin** | **include** | **exclude** } *Match-string*", all the commands that have been successfully executed by the user and that match the regular expression.
- If you specify both the number of commands *Command-Number* and a regular expression "| { **begin** | **include** | **exclude** } *Match-string*", the system will display the commands that match the regular expression among the *Command-Number* pieces of commands executed recently.

Related command: **history-command max-size**.

Example

Display all history commands in the buffer.

```
<SW8800>display history-command
  system-view
  user-interface vty 0
  user-interface vty 0 4
  history-command max-size 100
  quit
  display vlan
  display vlan all
  acl name lc
  interface Vlan-interface 1
  ip address 10.11.113.14 24
  quit
  quit
```

Display five commands executed recently in the history command buffer.

```
<SW8800>display history-command 5
  acl name lc
  interface Vlan-interface 1
  ip address 10.11.113.14 24
  quit
  quit
```

Display all the buffered history commands that match the specified regular expression.

```
<SW8800>display history-command | begin ip
  ip address 10.11.113.14 24
  quit
  quit
  display history-command
```

Display all the buffered history commands that do not match the specified regular expression.

```
<SW8800>display history-command | exclude ip
  system-view
  user-interface vty 0
  user-interface vty 0 4
  history-command max-size 100
  quit
  display vlan
  display vlan all
  acl name lc
  interface Vlan-interface 1
  quit
  quit
  display history-command
  display history-command 5
  display history-command | include 10.11.113.14
  displ
```

super

Syntax

super [*level*]

View

User view

Parameter

level: User level, ranging 0 to 3. The default value is 3.

Description

Use the **super** command to enable the user to change to user level from the current user level. If the user has set the **super password** [**level** *level*] { **simple** | **cipher** } *password*, then user password of the higher level is needed, or the former user level will not change.

Login users are classified into four levels that correspond to the four command levels respectively. After users of different levels log in, they can only use commands at the levels that are equal to or lower than its own level.

Related command: **super password**, **quit**.

Example

change to user level 3 from the current user level.

```
<SW8800> super 3
Password:
```

super password

Syntax

super password [**level** *level*] { **simple** | **cipher** } *password*

undo super password [**level** *level*]

View

System view

Parameter

level: Specifies the entering password of the specified priority, ranging from 1 to 3. The default value is 3, i.e. do not specify user level. It means the password to be set is used for entering level 3.

simple: Displays the current password with plain text.

cipher: Displays the current password with cipher text.

password: If the authentication is in the **simple** mode, the password must be in plain text. If the authentication is in the **cipher** mode, the password can either be in encrypted text or in plain text. The result is determined by the input. A plain text password is a sequential character string of no more than 16 digits, for example, 3com918. The length of an encrypted password must be 24 digits and in encrypted text, for example, _(TT8F]Y5SQ=^Q‘MAF4<1!!.

Description

Use the **super password** command to configure the password for changing the user from a lower level to a higher level. In order to prevent unauthorized users from illegal intrusion, user ID authentication is performed when users switch from a lower level to a higher level. For the sake of confidentiality, on the screen the user cannot see the password that he entered. Only when correct password is input for three times, can the user switch to the higher level. Otherwise, the original user level will remain unchanged. Use the **undo super password** command to cancel the current settings.

The password in plain text is required when performing authentication, regardless whether the configuration is plain text or encrypted text.

Example

Configure the password to zbr for changing the user from the current level to level 3.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] super password level 3 simple zbr
```

2 COMMANDS USED TO LOG IN TO SWITCH

Logging in to Switch Commands

authentication-mode

Syntax

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

View

User interface view

Parameter

password: Performs local password authentication.

scheme: Performs local or remote authentication of username and password.

command-authorization: Specifies that the commands available to users logging into a switch are defined on the server end (instead of an Switch 8800 Family switch).

none: Does not authenticate users trying to log into a switch.

Description

Use the **authentication-mode** command to configure the authentication method for login user.

Use the **authentication-mode none** command to configure no authentication.

This command with the **password** parameter indicates to perform local password authentication, that is, you need to configure a login password using the **set authentication password** { **cipher** | **simple** } *password* command.

This command with the **scheme** parameter indicates to perform authentication of local or remote username and password. The type of the authentication depends on your configuration. For detailed information, see "Security" section.

By default, terminal authentication is not required for local users log in via the Console port. However, password authentication is required for local users and remote Modem users to log in via the AUX port, and for Telnet users and VTY users to log in through Ethernet port.

If the Console port is configured for local password authentication, the user can directly log in to the system even without a password configured; if other user

interfaces, such as the AUX port and VTY interface, are configured for local password authentication, users cannot log in to the system without a password.

Example

Configure local password authentication.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] user-interface aux 0
[3Com-ui-aux0] authentication-mode password
```

auto-execute command

Syntax

auto-execute command *text*

undo auto-execute command

View

User interface view

Parameter

text: Specifies the command to be run automatically.

Description

Use the **auto-execute command** command to configure to automatically run a specified command. When a user logs in, the command configured will be executed automatically. The user will be disconnected after that.

Use the **undo auto-execute command** command to configure not to run the command automatically.

This command is usually used to configure the **telnet** command on the terminal, which will connect the user to a designated device automatically.

By default, auto run is disabled.

CAUTION:

- If you execute this command, the user-interface can no longer be used to perform routine configurations on the local system. Therefore use caution when using this command.
- Ensure that you will be able to log in to the system in some other way to cancel the configuration, before you configure the **auto-execute command** command and save the configuration.

Example

Configure to automatically execute **telnet 10.110.100.1** after the user logs in via VTY 0.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] user-interface vty 0
[3Com-ui-vty0] auto-execute command telnet 10.110.100.1
```

databits

Syntax

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

undo databits

View

User interface view

Parameter

7: Sets 7 data bits.

8: Sets 8 data bits.

Description

Use the **databits** command to configure the data bits for the user interface.

Use the **undo databits** command to restore the default bits of the user interface.

This command can only be performed in Console and AUX user interface view.

By default, the value is 8.

Example

Configure the data bits of AUX port to 7 bits.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] user-interface aux 0
[3Com-ui-aux0] databits 7
```

display user-interface

Syntax

display user-interface [*type number* | *number*] [**summary**]

View

Any view

Parameter

type: Specifies the type of a user interface.

number: Specifies the number of a user interface.

Summary: Displays the summary of a user interface.

Description

Use the **display user-interface** command to view the relational information of the user interface. This command without the **summary** parameter displays user interface type, absolute/relative index, transmission speed, priority, authentication methods, and physical location. This command with the **summary** parameter displays one user interface in use totally and user interface name etc.

Example

Display the relational information of user interface 0.

```
<SW8800> 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: Authenticate use AAA.
  N: Current UI need not authentication.
  P: Authenticate use current UI's password.
```

Table 3 Description on the fields of the display user-interface command

Field	Description
+	Current user interface is in use
F	Current user interface is in use and work in asynchronous mode
Idx	Absolute index of user interface
Type	Type and relative index of user interface
Tx/Rx	User interface speed
Modem	Modem operation mode
Privi	Which levels of commands can be used after logging in from the user interface
Auth	User interface authentication method
Int	The physical location of user interfaces

Display the summary information of user interface 0.

```
<SW8800> display user-interface 0 summary
          0: U

    1 character mode users.     (U)
    1 total UIs in use.
    UI's name: con0
```

Table 4 Description on the fields of the display the user-interface summary command

Field	Description
0: U	User interface type
1 character mode users.	One type user interface
1 total UIs in use.	One user interface in use totally
UI's name	User interface name

display users

Syntax

display users [**all**]

View

Any view

Parameter

all: Displays the information of all user interfaces.

Description

Use the **display users** command to view the information of the user interface.

Example

Display the information of the current user interface.

```
<SW8800> display users
UI     Delay      Type    Ipaddress      Username
+ 0    CON 0    00:00:00
```

Table 5 Description on the fields of the display users command

Field	Description
+	Current user interface is in use and work in asynchronous mode.
UI	Number of the first list is the absolute number of user interface. Number of the second list is the relative number of user interface.
Delay	Indicates the interval from the latest input till now in seconds.
Type	User type
IPaddress	Displays initial connection location, namely the host IP address of the incoming connection.
Username	Display the name of the user using this user interface, namely the login username of the user.

flow-control

Syntax

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

undo flow-control

View

User interface view

Parameter

hardware: Configures to perform hardware flow control.

none: Configures no flow control.

software: Configures to perform software flow control.

Description

Use the **flow-control** command to configure the flow control mode on the user interface.

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

By default, the value is **none**. That is, no flow control will be performed.

This command can only be performed in Console and AUX user interface view.

Example

Configure software flow control on AUX port.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
```

```
[SW8800] user-interface aux 0
[3Com-ui-aux0] flow-control software
```

free user-interface

Syntax

free user-interface [*type*] *number*

View

User view

Parameter

type: Specifies the user interface type.

number: Specifies the absolute/relative number of the user interface. Configured together with the *type*, it will specify the user interface number of the corresponding type. If the *type* is not specified, *number* will specify an absolute user interface number.

Description

Use the **free user-interface** command to release a specified user interface. The user interface will be disconnected after the command is executed.

Note that the current user interface cannot be release.

Example

Release user interface 1 after logged in to the switch via user interface 0.

```
<SW8800> free user-interface 1
```

After the command is executed, user interface 1 will be disconnected. It will not be connected to the switch until you log in via the user interface 1 for the next time.

header

Syntax

header [**shell** | **incoming** | **login**] *text*

undo header [**shell** | **incoming** | **login**]

View

System view

Parameter

login: Login information in case of authentication. It is displayed before the user is prompted to enter user name and password.

shell: User conversation established header, the information output after user conversation has been established. If authentication is required, it is prompted after the user passes authentication.

incoming: Login header, the information output after a Modem user logs in. If authentication is required, it is prompted after the user passes authentication. In this case, no **shell** information is output.

text: Specifies the title text. If you do not choose any keyword in the command, the system displays the login information by default. The system supports two types of input modes: one is to input all the text in one line, and altogether 256 characters, including command key word, can be input; the other is to input all the text in several lines using the <Enter> key, and altogether 1024 characters, excluding command key word, can be input. The text starts and ends with the first character. After inputting the end character, press the <Enter> key to exit the interact process.

Description

Use the **header** command to configure to display header when user login.

Use the **undo header** command to configure not to display the header.

When the user logs in to the switch, if a connection is activated, the **login** header will be displayed. After the user successfully logs in to the switch, the **shell** header will be displayed.

Note that if you press <Enter> after typing any of the three keywords **shell**, **login** and **incoming** in the command, then what you type after the word header is the contents of the login information, instead of identifying header type.

You can judge whether the initial character can be used as the header contents this way:

1 Input texts in multiple lines. You need to enter only one character in the first line. The character and the last character of the string entered serve as the identifiers of the header content and must be the same. For example,

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] header shell 0
Input banner text, and quit with the character '0'.
Welcome !0
```

(The starting and ending characters must be the same, and press the <Enter> key to finish a line)

When you log in to the switch again, the preset session establishment header "welcome!" is displayed on the terminal screen.

The initial character 0 is not header contents.

For another example,

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] header shell 0
Input banner text, and quit with the character '0'.
Hello,
Welcome!0
```

(The starting and ending characters must be the same, and press the <Enter> key to finish a line)

When you log in to the switch again, the preset session establishment header "Hello, welcome!" is displayed on the terminal screen. The initial character 0 is not header content.

2 You can also input the header content in a single line. In this case, the beginning and the end character serve as the identifiers and must be the same. For example,

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] header shell 0welcome,my friend!0
```

(The starting and ending characters must be the same. Press the <Enter> key to finish a line)

When you log in to the switch again, the preset session establishment header "welcome, my friend!" appears on the terminal screen. The beginning and the end characters, that is, character 0, are not displayed.

3 Finally, you can input the header content in multiple lines, with multiple characters contained in the first line. The initial character is different from the ending one and the initial character pairs with the ending one. The initial character is the text contents, for example,

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] header shell hello
Input banner text, and quit with the character 'h'.
my friend !
h
```

(The starting and ending characters must be the same, and press the <Enter> key to finish a line)

When you log in to the switch again, the preset session establishment header "hello, my friend!" is displayed on the terminal screen. The initial character "h" is the header contents.

Example

Set the header for the switch.

Option 1: Input in one line

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] header shell %SHELL: Hello! Welcome%
```

(The starting and ending characters must be the same, and press the <Enter> key to finish a line.)

When you log in to the switch again, the terminal displays the header you set.

```
[SW8800] quit
<SW8800> quit
Please press ENTER
SHELL: Hello! Welcome
```

(The character "%" is not displayed.)

```
<SW8800>
```

Option 2: Input in multiple lines

```
[SW8800] header shell % SHELL:
```

(After you press the <Enter> key, the system prompts the following message.)

```
Input banner text, and quit with the character '%'.
```

Go on inputting the rest text and end your input with the first letter:

```
Hello! Welcome %
```

(Press the <Enter> key)

```
[SW8800]
```

When you log in to the switch again, the following is displayed.

```
[SW8800] quit
<SW8800> quit
Please press ENTER
%SHELL:
```

(The character "%" is contained in the header.)

```
Hello! Welcome
<SW8800>
```

history-command max-size

Syntax

history-command max-size *value*

undo history-command max-size

View

User interface view

Parameter

value: Defines the size of the history buffer, ranging from 0 to 256. By default, the size is 10, that is, 10 history commands can be saved.

Description

Use the **history-command max-size** command to configure the size of the history command buffer.

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

Example

Set the history buffer to 20, namely saving 20 history commands.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
```

```
[SW8800] user-interface aux 0
[3Com-ui-aux0] history-command max-size 20
```

idle-timeout

Syntax

idle-timeout *minutes* [*seconds*]

undo idle-timeout

View

User interface view

Parameter

minutes: Specifies the minute, ranging from 0 to 35791.

seconds: Specifies the second, ranging from 0 to 59.

Description

Use the **idle-timeout** command to configure the timeout function. If there is no user operation performed before idle-timeout expires, the user interface will be disconnected.

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

idle-timeout 0 means disabling idle-timeout.

By default, idle-timeout is set to 10 minutes.

Example

Configure the timeout value to 1 minute on the AUX user interface.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] user-interface aux 0
[3Com-ui-aux0] idle-timeout 1 0
```

language-mode

Syntax

language-mode { **chinese** | **english** }

View

User view

Parameter

chinese: Configures the language environment of command line interface as Chinese.

english: Configures the language environment of command line interface as English.

Description

Use the **language-mode** command to switch between different language environments of command line interface for convenience of different users.

By default, the value is English.

Example

Switch from English mode to Chinese mode.

```
<SW8800> language-mode chinese
```

lock

Syntax

lock

View

User view

Parameter

None

Description

Use the **lock** command to lock the user interface to prevent unauthorized user from operating it.

Example

Lock the current user interface.

```
<SW8800> lock
Password: xxxx
Again: xxxx
```

modem

Syntax

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

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

View

User interface view

Parameter

call-in: Configures to allow call-in.

both: Configures to allow call-in and call-out.

Description

Use the **modem** command to configure the call-in and call-out attributes of the Modem. Use the **undo modem** command to cancel the configuration of Modem call-in and call-out attributes.

The **modem** command without parameters is used to allow call-in and call-out.

The **undo modem** command without parameters is used to ban call-in and call-out.

This command can only be performed in AUX user interface view.

Example

Configure to allow call-in and call-out of Modem on the AUX port.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] user-interface aux 0
[3Com-ui-aux0] modem both
```

modem auto-answer

Syntax

modem auto-answer

undo modem auto-answer

View

User interface view

Parameter

None

Description

Use the **modem auto-answer** command to configure the answer mode as auto-answer.

Use the **undo modem auto-answer** command to configure the answer mode as manual answer.

By default, the mode is set to manual answer.

This command can only be performed in AUX user interface view.

Example

Configure the answer mode of the Modem on the AUX port as auto-answer.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] user-interface aux 0
[SW8800] user-interface aux 0
[3Com-ui-aux0] modem auto-answer
```

modem timer answer

Syntax

modem timer answer *seconds*

undo modem timer answer

View

User interface view

Parameter

seconds: Specifies the timer answer in seconds, ranging from 1 to 60.The default value is 30s.

Description

Use the **modem timer answer** command to configure the timer answer from off-hook to carrier detected when establishing the call in connection.

Use the **undo modem timer answer** command to restore the default timeout value.

This command can only be performed in AUX user interface view.

Example

Set the timer answer of AUX 0 to 45s.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] user-interface aux 0
[3Com-ui-aux0] modem timer answer 45
```

parity

Syntax

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

undo parity

View

User interface view

Parameter

even: Configures to perform even parity.

mark: Configures to perform mark parity.

none: Configures not to perform parity.

odd: Configures to perform odd parity.

space: Configures to perform space parity.

Description

Use the **parity** command to configure the parity mode on the user interface.

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

This command can only be performed in Console and AUX user interface view.

By default, the mode is set to none.

Example

Set mark parity on the AUX port.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] user-interface aux 0
[3Com-ui-aux0] parity mark
```

protocol inbound

Syntax

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

View

User interface view

Parameter

all: Specifies to support all the protocols including Telnet and SSH.

ssh: Specifies to support SSH protocol only.

telnet: Specifies to support Telnet protocol only.

Description

Use the **protocol inbound** command to set the protocols to be used when logging in.

By default, all the protocols are set to be used for user login

Note that only the VTY type of user interfaces support protocol setting.

Related command: **user-interface vty**.

Example

Set the Telnet protocol to be used for user login.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] user-interface vty 0
[3Com-ui-vty0] protocol inbound telnet
```

quit

Syntax

quit

View

Any view

Parameter

None

Description

Use the **quit** command to return to the lower level view from the current view. If the current view is user view, you can quit the system.

There are three levels of views, which are listed from low to high as follows:

- User view
- System view
- VLAN view, Ethernet port view, and so on.

Related command: see **return**, **system-view**.

Example

Return to user view from system view.

```
[SW8800] quit
<SW8800>
```

return

Syntax

return

View

System view or above

Parameter

None

Description

Use the **return** command to return to user view from a view other than user view.

Combination key <Ctrl+Z> performs the same function with the **return** command.

Related command: **quit**.

Example

Return to user view from system view.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800]vlan 2
[3Com-vlan2] return
<SW8800>
```

screen-length

Syntax

screen-length *screen-length*

undo screen-length

View

User interface view

Parameter

screen-length: Specifies how many lines can be displayed on a screen, ranging from 0 to 512. The default value is 24.

Description

Use the **screen-length** command to configure how many lines that can be displayed on a screen of the terminal.

Use the **undo screen-length** command to restore the default number of terminal information lines displayed on the terminal screen.

By default, 24 lines (including the multi-screen identifier lines) are displayed in one screen when the multi-screen display function is enabled.

The **screen-length** 0 command is used to disable this function.

Example

Configure the lines that can be displayed on a screen as 20 lines.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] user-interface aux 0
[3Com-ui-aux0] screen-length 20
```

send

Syntax

send { **all** | *number* | *type number* }

View

User view

Parameter

all: Configures to send message to all user interfaces.

type: Specifies the user interface type, which can be console, aux or vty.

number: Specifies the absolute/relative number of the user interface. If it follows *type*, it is a relative number. For Aux or Console user types, it can be 0 only. For VTY user type, it ranges from 0 to 4. If the *type* is not specified, it is an absolute number, which ranges from 0 to 6.

Description

Use the **send** command to send messages between different user interfaces.

Example

Send message to all the user interfaces.

```
<SW8800> send all
```

service-type telnet

Syntax

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

undo service-type telnet

View

Local-user view

Parameter

level: Specifies which level of command a user can use after login, ranging from 0 to 3 and defaults to level 2.

Description

Use the **service-type telnet** command to configure which level of command a user can use after login.

Use the **undo service-type telnet** command to restore the default level of command a user can use after login.

Commands are classified into four levels, namely visit level, monitoring level, configuration level and management level. They are introduced as follows:

- Visit level: Commands of this level involve command of network diagnosis tool (such as **ping** and **tracert**), command of switch between different language environments of user interface (**language-mode**), and **telnet** command etc. The operation of saving configuration file is not allowed on this level of commands.
- Monitoring level: Commands of this level, including the **display** command and the **debugging** command, are used for system maintenance, service fault diagnosis, etc. The operation of saving the configuration file is not allowed on this level of commands.
- Configuration level: Service configuration commands, including routing command and commands on each network layer, are used to provide direct network service to the user.
- Management level: These are commands that influence the basic operation of the system and system support module, which plays a supporting role on service. Commands of this level involve file system commands, FTP commands, TFTP commands, XModem downloading commands, user management commands, and level setting commands.

Example

Configure the user zbr to use commands at level 0 after login.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] local-user zbr
[3Com-luser-zbr] service-type telnet level 0
```

set authentication password

Syntax

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

undo set authentication password

View

User interface view

Parameter

cipher: Displays the current password with cipher text.

simple: Displays the current password with plain text.

password: If the authentication is in the **simple** mode, the password must be in plain text. If the authentication is in the **cipher** mode, the password can be either in encrypted text or in plain text. The result is determined by the input. A plain text password is a sequential character string of no more than 16 digits, for example, 3com918. The length of an encrypted password must be 24 digits and in encrypted text, for example, _(TT8F]Y5SQ=^Q‘MAF4<1!!.

Description

Use the **set authentication password** command to configure the password for local authentication.

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

The password in plain text is required when performing authentication, regardless whether the configuration is plain text or encrypted text.

By default, password is required to be set for authenticating local users and remote Modem users log in via the AUX port, and Telnet users log in through Ethernet port. If no password has been set, the following prompt will be displayed "Login password has not been set."

Example

Configure the local authentication password on VTY 0 to aaa.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] user-interface vty 0
[3Com-ui-vty0] set authentication password simple aaa
```

shell

Syntax

shell

undo shell

View

User interface view

Parameter

None

Description

Use the **shell** command to enable terminal service of a user interface.

Use the **undo shell** command to disable the terminal service of a user interface.

By default, terminal service is enabled.

When using the **undo shell** command, note the following points.

- The **undo shell** command can only be used on the user interfaces other than the Console user interface.
- You cannot use this command on the user interface via which you log in.
- You will be asked to confirm before executing this command on any legal user interface.

Example

Disable terminal service on the vty user interface 0 to 4 after logging in to the switch via user interface 0.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] user-interface vty 0 4
[3Com-ui-vty0-4] undo shell
```

speed

Syntax

speed *speed-value*

undo speed

View

User interface view

Parameter

speed-value: Specifies the transmission rate on the user interface in bps, which can be 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600, or 115200. The default rate is 9600 bps.

Description

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

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

This command can only be performed in Console and AUX user interface view.

Note that AUX user interface does not support the transmission rate: 57600 bps and 115200 bps.

Example

Configure the transmission speed on the AUX port as 4800 bps.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] user-interface aux 0
[3Com-ui-aux0] speed 4800
```

stopbits

Syntax

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

undo stopbits

View

User interface view

Parameter

1: Sets 1 stop bit.

1.5: Sets 1.5 stop bits.

2: Sets 2 stop bits.

Description

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

Use the **undo stopbits** command to restore the default stop bits.

This command can only be performed in Console and AUX user interface view.

By default, the value is 1.

Note that setting 1.5 stop bits is not available on 3Com Switch 8800 Family Series Routing Switches at present.

Example

Set stop bits to 2.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] user-interface aux 0
[3Com-ui-aux0] stopbits 2
```

sysname

Syntax

sysname *text*

undo sysname

View

System view

Parameter

text: Specifies the hostname with a character string, ranging from 1 to 30 characters. The default name is 3Com.

Description

Use the **sysname** command to configure the hostname of the switch.

Use the **undo sysname** command to restore the default hostname.

Changing the hostname of the switch will affect the prompt of command line interface. For example, if the hostname of the switch is 3Com, the prompt in user view will be <SW8800>.

Example

Configure the hostname of switch to Switch.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] sysname Switch
[Switch]
```

system-view

Syntax

system-view

View

User view

Parameter

None

Description

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

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

Example

Enter system view from user view.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z..
[SW8800]
```

telnet

Syntax

telnet [**vpn-instance** *vpn-instance-name*] { *hostname* | *ip-address* } [*service-port*]

View

User view

Parameter

vpn-instance *vpn-instance-name*: Specifies vpn-instance of MPLS VPN.

hostname: Specifies the host name of the remote system. It is configured using the **ip host** command.

ip-address: Specifies the IP address of the remote switch.

service-port: Designates the TCP port on the remote switch providing Telnet service, ranging from 0 to 65535.

Description

Use the **telnet** command to log in to another switch from the current one via telnet for remote management. To terminate the Telnet login, press <Ctrl+K>.

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

Related command: **display tcp status** and **ip host**.

Example

Log in to switch 3Com2 at 129.102.0.1 from the current 3Com1 switch.

```
<3Com1> telnet 129.102.0.1
Trying 129.102.0.1...
Press CTRL+K to abort
Connected to 129.102.0.1...
<3Com2>
```

user-interface

Syntax

user-interface [*type*] *first-number* [*last-number*]

View

System view

Parameter

type: Specifies the user interface type, which can be aux, console or vty.

first-number: Specifies the number of the first user interface to be configured. It must be an integer in the range of 0 to 6.

last-number: Specifies the number of the last user interface to be configured. It must be an integer in the range of 1 to 6 and it must be greater than the value of *first-number*.

Description

Use the **user-interface** command to enter single user interface view to configure the corresponding user interfaces.

Example

Enter vty 0 user interface view for configuration.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] user-interface vty 0
[3Com-ui-vty0]
```

user privilege level

Syntax

user privilege level *level*

undo user privilege level

View

User interface view

Parameter

level: Specifies which level of command a user can use after login from the specifically user interface, ranging from 0 to 3.

Description

Use the **user privilege level** command to configure which level of command a user can use after login from the specifically user interface, so that a user can use all the available commands at this level.

Use the **undo user privilege level** command to restore the default level of command a user can use after login from the specifically user interface.

By default, a user can access the commands at Level 3 after logging in through the Console user interface, and the commands at Level 0 after logging in through the AUX or VTY user interface.

Example

Configure to use commands level 0 after logging in from VTY 0 user interface.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] user-interface vty 0
[3Com-ui-vty0] user privilege level 0
```

After you telnet from VTY 0 user interface to the switch, you will view the terminal only displays commands at level 0.

```
<SW8800> ?
User view commands:
  debugging         Enable system debugging functions
  language-mode     Specify the language environment
  ping              Ping function
  quit              Exit from current command view
  super             Privilege current user a specified priority level
  telnet             Establish one TELNET connection
  tracert            Trace route function
undo                Cancel current setting
```

3 CONFIGURATION FILE MANAGEMENT COMMANDS

Configuration File Management Commands

display current-configuration

Syntax

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

View

Any view

Parameter

controller: Views the configuration information of controllers.

interface: Views the configuration information of interfaces.

interface-type: Type of the interface, including Aux, Ethernet, GigabitEthernet, NULL, Vlan-interface, M-Ethernet, LoopBack.

interface-number: Number of the interface.

configuration *configuration*: Views the pre-positive and post-positive configuration information. The value of *configuration* is the key word of the configuration, such as:

- **system**: Views the host name.
- **timerange**: Views the configuration information of time range.

|: Filters the configuration information to be output by regular expression.

begin: Begins with the line that matches the regular expression.

exclude: Excludes lines that match the regular expression.

include: Includes lines that match the regular expression.

regular-expression: Defines the regular expression.

Table 6 Special characters in the regular expression

Special characters	Description	Restriction
_	Underscore, similar to a wildcard and can stand for these characters: (^|$|[,()\{\}]) A space, the beginning of the input string, the end of the input string	If the first character in the regular expression is not a underscore, then there is no restriction on the number of the underscore (but it is restricted by the command length). If the first character in the regular expression is an underscore, then there should be less than five consecutive underscores. If the underscores in a command are discrete, on the first group of underscores are filtered for the output information, but not the subsequent underscores.
(	Left parenthesis, push flag in program	It is recommended not to use this character in the regular expression.

Description

Use the **display current-configuration** command to display the currently effective configuration parameters of the switch.

If some running configuration parameters are the same with the default operational parameters, they will not be displayed.

If a user needs to authenticate whether the configurations are correct after finishing a set of configuration, the **display current-configuration** command can be used to display the running parameters. Although the user has configured some parameters, but the related functions are not effective, they are not displayed.

When there is much configuration information, you can use the regular expression to filter the output information. For specific rules about the regular expression, refer to the corresponding operation manual.

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

Example

View the running configuration parameters of the switch.

```
<SW8800> display current-configuration
#
 sysname 3Com
#
radius scheme system
 server-type nec
 primary authentication 127.0.0.1 1645
 primary accounting 127.0.0.1 1646
 user-name-format without-domain

domain system
 radius-scheme system
 access-limit disable
```

```
 state active
 idle-cut disable

 domain default enable system
#
 local-server nas-ip 127.0.0.1 key 3com
#
 router id 2.2.2.2
#
 stp timer hello 500
#
vlan 1
#
vlan 2
#
interface Vlan-interface1
#
interface Vlan-interface2
 ip address 10.1.1.2 255.255.255.0
#
interface Aux0/0
interface Aux0/0/1
#
interface M-Ethernet0/0/0
#
interface Ethernet4/1/1
#
interface Ethernet4/1/2
#
interface Ethernet4/1/3
#
interface Ethernet4/1/4
#
interface Ethernet4/1/5
#
interface Ethernet4/1/6
#
interface Ethernet4/1/7
...
#
interface NULL0
#
ospf
 #
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
#
user-interface aux 0
user-interface vty 0 4
#
return
```

View the lines containing the character string "10*.110" in the configuration information. The "*" indicates that the "0" before it can appear 0 times or multiple consecutive times.

```
<SW8800> display current-configuration | include 10*.110
primary authentication 127.0.0.1 1645
 primary accounting 127.0.0.1 1646
 local-server nas-ip 127.0.0.1 key 3com
vlan 1
interface Vlan-interface1
 ip address 10.1.1.2 255.255.255.0
interface Ethernet4/1/1
 speed 1000
interface Ethernet4/1/2
interface Ethernet4/1/3
interface Ethernet4/1/4
interface Ethernet4/1/5
  network 10.1.1.0 0.0.0.255
```

View configuration information begin with "user".

```
<SW8800> display current-configuration | include ^user
user-interface aux 0
user-interface vty 0 4
```

View the pre-positive and post-positive configuration information.

```
<SW8800> display current-configuration configuration
#
 sysname 3Com
#
radius scheme system
 server-type nec
 primary authentication 127.0.0.1 1645
 primary accounting 127.0.0.1 1646
 user-name-format without-domain

domain system
 radius-scheme system
 access-limit disable
 state active
 idle-cut disable

 domain default enable system
#
 local-server nas-ip 127.0.0.1 key 3com
#
 router id 2.2.2.2
#
 stp timer hello 500
#
ospf
 #
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
#
user-interface aux 0
user-interface vty 0 4
#
return
```

display saved-configuration

Syntax

display saved-configuration

View

Any view

Parameter

None

Description

Use the **display saved-configuration** command to view the configuration files in the flash memory or CF card of Switch.

If the the switch works abnormally after electrified, execute the **display saved-configuration** command to view the startup configuration of the Switch.

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

Example

Display configuration files in flash memory or CF card of the switch.

```
<SW8800> display saved-configuration
#
 sysname 3Com
#
local-user abc password simple abc
#
 tcp window 8
#
interface Aux7/1/1
 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 12/1/0
#
user-interface con 0
user-interface aux 0
user-interface vty 0 4
 authentication-mode none
#
return
```

The displayed information is global, port and user configurations.

display this

Syntax

display this

View

Any view

Parameter

None

Description

Use the **display this** command to display the running configuration of the current view. If you need to authenticate whether the configurations is correct after you have finished a set of configurations under a view, you can use the **display this** command to view the running parameters.

Some effective parameters are not displayed if they are the same with the default ones, while some parameters, though have been configured by the user, if their related functions are not effective, are not displayed either. For example, if X.25 is encapsulated at the data link layer on an interface, you can configure PPP parameter on the interface, but cannot view the configuration information when executing the **display this** command.

Associated configuration of the interface is displayed when executing the command in different interface views; related configuration of the protocol view is displayed when executing this command in different protocol views; and all the configuration of the protocol view is displayed when executing this command in protocol sub-views.

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

Example

Display the running configuration parameters for the current view of the switch system.

```
<SW8800> display this
```

display startup

Syntax

display startup

View

Any view

Parameter

None

Description

Use the **display startup** command to display the related system software and configuration filenames used for the current and the next start-ups.

This command is used to display the following information: the filename of the system software for the current enabling configured by the user, the filename of

the system software actually used for the current enabling, the filename of the system software configured for the next enabling, the configuration filename used for the current enabling, the configuration filename configured for the next enabling.

Related command: **startup saved-configuration**.

Example

Display the filenames related to the current and the next enabling.

```
<SW8800> display startup
MainBoard:
  Startup saved-configuration file:          flash:/8500.cfg
  Next startup saved-configuration file:     flash:/8500.cfg
```

reset saved-configuration

Syntax

reset saved-configuration

View

User view

Parameter

None

Description

Use the **reset saved-configuration** command to erase configuration files from the flash memory of the switch.

Perform this command with cautious. It is suggested to consult technical support personnel first.

Generally, this command is used in the following situations:

- After upgrade of software, configuration files in flash memory may not match the new version's software. Perform the **reset saved-configuration** command to erase the old configuration files.
- If a used switch is applied to the new circumstance and the original configuration files cannot meet the new requirements, the switch should be configured again. Erase the original configuration files for reconfiguration.

If the configuration files do not exist in the flash memory when the switch is electrified and initialized, it will enter setup switch view automatically.

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

Example

Erase the configuration files from the flash memory of the switch.

```
<SW8800> reset saved-configuration
The saved configuration will be erased.
Are you sure?[Y/N]
```

save

Syntax

save [*file-name*]

View

User view

Parameter

file-name: Name of the configuration file with the extension .cfg. It is a character string of 5 to 56 characters.

Description

Use the **save** command to save the current configuration files to Flash memory.

After finishing a group of configurations and achieving corresponding functions, user should remember to get the current configuration files stored in the flash memory.

Even if the problems like reboot and power-off occur during saving, the configuration can be still saved to Flash.

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

Example

Get the current configuration files stored in the flash memory.

```
<SW8800> save
The configuration will be written to the device.
Are you sure?[Y/N]y
Now saving current configuration to the device.
Saving configuration flash:/8500.cfg. Please wait..
Configuration is saved to flash memory successfully.
```

startup saved-configuration

Syntax

startup saved-configuration *cfgfile*

View

User view

Parameter

cfgfile: Name of the configuration file. It is a string with a length of 5 to 56 characters.

Description

Use the **startup saved-configuration** command to configure the configuration file used for enabling the system for the next time.

The configuration file must have ".cfg" as its extension name and must be saved under the root directory of the Flash. By default, the configuration file will be saved under the root directory of Flash.

The extension of configuration file must be .cfg, and the startup configuration file must be saved under the directory where the memory resides. The memory is Flash.

Related command: **display startup**.

Example

Configure the configuration file for the next start-up

```
<SW8800> startup saved-configuration vrpcfg.cfg
```

4 VLAN CONFIGURATION COMMANDS

VLAN Configuration Commands

description

Syntax

description *string*

undo description

View

VLAN view, VLAN interface view

Parameter

string: Description character string of current VLAN or VLAN interface. For VLAN, it ranges from 1 to 32 characters. For VLAN interface, it ranges from 1 to 64 characters. The default description character string of current VLAN is VLAN ID of the VLAN, e.g. VLAN 0001. The default description character string of VLAN interface is the interface name, e.g., "Vlan-interface1 interface".

Description

Use the **description** command to configure a description for the current VLAN or VLAN interface.

Use the **undo description** command to restore the default description of current VLAN or VLAN interface.

Related command: **display vlan**, **display interface vlan-interface**.

Example

Specify a description character string "RESEARCH" for the current VLAN.

```
[3Com-vlan1] description RESEARCH
```

display trap-to-cpu

Syntax

display trap-to-cpu

View

Any view

Parameter

None

Description

Use the **display trap-to-cpu** command to view the related information about the CPU port.

Example

Display related information about the CPU port

```
<SW8800> display trap-to-cpu
trap-to-cpu disable vlan 2 10 14 to 15
```

display interface Vlan-interface

Syntax

display interface Vlan-interface [*vlan-id*]

View

Any view

Parameter

vlan-id: Specifies VLAN ID.

Description

Use the **display interface Vlan-interface** command to view the related information about specified or all VLAN interfaces, including physical protocol status and link protocol status of VLAN interface, Ethernet sending frame format, MAC address, IP address and sub-net mask, description character string and MTU, etc.

With *vlan-id* specified, only the information about the specified VLAN interface will be displayed. If no *vlan-id* is specified, the information about all the existing VLAN interfaces will be displayed.

Related command: **interface vlan-interface**.

Example

Display related information about VLAN-interface 1.

```
<SW8800> display interface Vlan-interface 1
Vlan-interface1 current state : DOWN
Line protocol current state : DOWN
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 00e
0-fc07-4101
Internet Address is 10.1.1.1/24 Primary
Description : Vlan-interface1 Interface
The Maximum Transmit Unit is 1500
```

Table 7 Description on the fields of the display interface Vlan-interface command

Field	Description
Vlan-interface1 current state	Current state of the VLAN interface
Line protocol current state	Current state of the Line protocol
IP Sending Frames' Format	Format of the IP sending frames
Hardware address	Corresponding MAC address of the VLAN interface
Internet Address	IP address
Description	Description of the VLAN interface

Table 7 Description on the fields of the display interface Vlan-interface command

Field	Description
The Maximum Transmit Unit	Maximum Transmit Unit (MTU)

display vlan

Syntax

display vlan [*vlan-id* **to** *vlan-id* | **all** | **static** | **dynamic**]

View

Any view

Parameter

vlan-id: Displays information of the specified VLAN.

all: Displays information of all VLANs.

static: Displays information of VLANs created statically by the system.

dynamic: Displays information of VLANs created dynamically by the system.

Description

Use the **display vlan** command to view related information about the specified or all VLANs.

If *vlan-id* or **all** is specified, information of specified VLAN or all VLANs is displayed. It includes: VLAN ID, VLAN type (dynamic or static), whether the routing function has been enabled on this VLAN (if enabled, the main IP address and mask will be displayed), VLAN description, and the ports VLAN contains.

If parameter is not specified, information of the VLANs that has been created is displayed. If the parameter dynamic or static is selected, information of VLANs created dynamically or statically by the system is displayed.

Related command: **vlan**.

Example

Display the information about VLAN2.

```
[SW8800] display vlan 2
VLAN ID: 2
VLAN Type: static
ARP proxy disabled
Route interface: not configured
Description: VLAN 0002
Tagged   Ports: none
Untagged Ports:
    Ethernet2/1/1  Ethernet2/1/2  Ethernet2/1/3
```

Table 8 Description on the fields of the display vlan 2 command

Field	Description
VLAN ID	VLAN ID
VLAN Type	Configuration type of VLAN: either dynamic or static
Route interface	Whether the route interface exists

Table 8 Description on the fields of the display vlan 2 command

Field	Description
ARP proxy disabled	The ARP proxy function of the VLAN is disabled
Description	VLAN description
Tagged Ports	The ports on which VLAN packets need tag
Untagged Ports	The ports on which VLAN packets need not tag

interface vlan-interface

Syntax

interface vlan-interface *vlan-id*

undo interface vlan-interface *vlan-id*

View

System view

Parameter

vlan-id: ID of VLAN interface, ranging from 1 to 4094.

Description

Use the **interface vlan-interface** command to configure VLAN interface or enter VLAN interface view.

Use the **undo interface vlan-interface** command to cancel one VLAN interface.

Related command: **display interface vlan-interface**.

Example

Enter the view of the VLAN-interface 1.

```
[SW8800] interface vlan-interface 1
```

name

Syntax

name *string*

undo name

View

VLAN view

Parameter

string: Name of the current VLAN, a string of 1 to 32 characters. The default value is the VLAN ID of the VLAN.

Description

Use the **name** command to name the current VLAN.

Use the **undo name** command to restore the default name of the current VLAN.

By default, the name of the current VLAN is the VLAN ID of the VLAN.

Example

Name the current VLAN 2 "hello".

```
[3Com-vlan2] name hello
```

shutdown

Syntax

shutdown

undo shutdown

View

VLAN interface view

Parameter

None

Description

Use the **shutdown** command to disable the VLAN interface.

Use the **undo shutdown** command to enable the VLAN interface.

By default, when all the Ethernet ports in a VLAN are in the Down state, this VLAN interface is also Down. When there are one or more Ethernet ports in the Up state, this VLAN interface is also Up.

This command can be used to start interface after the related parameters and protocols of VLAN interface are set. Or when the VLAN interface fails, the interface can be shut down first and then restarted. In this way, the interface may be restored to normal status.

Shutting down or bringing up a VLAN interface will not affect any Ethernet port of this VLAN.

Example

Shut down Vlan-interface 2.

```
[3Com-Vlan-interface1] shutdown
```

trap-to-cpu disable

Syntax

trap-to-cpu disable

undo trap-to-cpu disable

View

VLAN view

Parameter

None

Description

Use the **trap-to-cpu disable** command to move the CPU port out of a VLAN.

Use the **undo trap-to-cpu disable** command to move the CPU port into a VLAN.

By default, a VLAN contains a CPU port.

Example

Move the CPU port out of VLAN 2.

```
[3Com-vlan2] trap-to-cpu disable
Warning : CPU port will exit the designated VLAN.
Broadcast & multicast packets cannot forward to CPU!
```

trap-to-cpu disable vlan

Syntax

trap-to-cpu disable vlan { *vlan-list* | **all** }

undo trap-to-cpu disable vlan { *vlan-list* | **all** }

View

System view

Parameter

vlan-list: Specifies the list of VLANs that contain a CPU port, expressed in form of *vlan-list* = { *vlan-id* [**to** *vlan-id*] } &<1-10>. The *vlan-id* before the keyword **to** must be larger than or equal to the *vlan-id* after **to**. &<1-10> means that the preceding parameter can be repeated up to 10 times.

all: All VLANs.

Description

Use the **trap-to-cpu disable vlan** command to move the CPU port out of the specified VLANs.

Use the **undo trap-to-cpu disable vlan** command to move the CPU port into the specified VLANs.

Example

Move the CPU port out of VLAN 5 and VLANs 20 to 30.

```
[SW8800] trap-to-cpu disable vlan 5 20 to 30
```

vlan

Syntax

vlan *vlan-id-list*

undo vlan { *vlan-id* [**to** *vlan-id*] | **all** }

View

System view

Parameter

vlan-id-list: *vlan-id-list* = [*vlan-id1* [**to** *vlan-id2*]]&<1-10>, specifies the range of VLANs to be created. The value range of *vlan-id* is 1 to 4094. &<1-10> means that the preceding parameter can be repeated up to 10 times.

all: Deletes all VLANs.

Description

Use the **vlan** *vlan-id-list* command to enter VLAN view or to create a range of VLANs.

Use the **undo vlan** command to delete the specified VLAN.

If only one VLAN is created, the system will automatically enter the view of the VLAN just created.

Related command: **display vlan**.

Example

Create VLANs 5, 20, 21, 22, 23, 24, 400, 1002, 1003, 1004, and 2000.

```
<SW8800> system-view
[SW8800] vlan 5 20 to 24 400 1002 to 1004 2000
```

CAUTION:

- VLAN 1 is the system-default VLAN and cannot be removed.
- VLANs with their ports being VLAN VPN-enabled cannot be removed.
- A Guest VLAN cannot be deleted.
- A protocol-enabled VLAN cannot be deleted.

Port-Based VLAN Configuration Commands

port

Syntax

port *interface-list*

undo port *interface-list*

View

VLAN view

Parameter

interface-list: List of Ethernet ports, expressed as *interface-list*= { *interface-type interface-number* [**to** { *interface-type interface-number*] }&<1-10>. *interface-type* is interface type, *interface-number* is interface number. The interface number after the keyword **to** must be larger than or equal to the interface number before **to**. &<1-10> represents that the preceding parameter can be repeated up to 10 times.

Description

Use the **port** command to add one port or one group of ports to VLAN.

Use the **undo port** command to cancel one port or one group of ports from VLAN.

Note that you can add/delete trunk port and hybrid port to/from VLAN by the **port** and **undo port** commands in Ethernet port view, but not in VLAN view.

Related command: **display vlan**.

Example

Add Ethernet2/1/1 through Ethernet2/1/3 to VLAN 2.

```
[3Com-vlan2] port ethernet2/1/1 to ethernet2/1/3
```

Protocol-Based VLAN Configuration Commands

display protocol-vlan interface

Syntax

display protocol-vlan interface { *interface-list* | **all** }

View

Any view

Parameter

interface-list: Displays the protocol information of a specified interface, in the form of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] }. *interface-type* is interface type, *interface-number* is interface number. The interface number after the keyword **to** must be larger than or equal to the interface number before **to**.

all: Displays the protocol information of all ports.

Description

Use the **display protocol-vlan interface** command to view the protocol information and protocol index configured on the specific port, to which you can refer when you use the protocol-based VLAN and add/delete a protocol.

Related command: **display interface**.

Example

Display the protocol information and protocol index configured on Ethernet2/1/1.

```
<SW8800> display protocol-vlan interface ethernet2/1/1
 Interface: Ethernet2/1/1
      Vlan-ID  Index    Type              Value
      10        0         at
      10        1         ethernetii      etype 0x0600
      10        2         llc              dsap 0x01 ssap 0x02
      10        3         snap             etype 0x0700
      10        4         ipx ethernetii
      10        5         ipx llc
      10        6         ipx raw
      10        7         ipx snap
```

display vlan-protocol-vlan vlan

Syntax

display protocol-vlan vlan { *vlan-list* | **all** }

View

Any view

Parameter

vlan-list: Specifies a VLAN list. It is expressed in the form of *vlan-list* = { *vlan-id* [**to** *vlan-id*] }, where the *vlan-id* after the keyword **to** must be larger than or equal to the *vlan-id* before **to**.

all: Displays the protocol information of all VLANs.

Description

Use the **display protocol-vlan vlan** command to view the protocol information and protocol index configured for a VLAN, to which you can refer when you use the protocol-based VLAN and add/delete a protocol.

Related command: **display vlan**.

Example

Display the protocol information and protocol index configured on the VLAN 522.

```
<SW8800> display protocol-vlan vlan 522
VLAN ID: 522
 VLAN Type: Protocol-based VLAN
      Index              Type              Value
      0                   at
      1                   ethernetii        etype 0x0600
      2                   llc                dsap 0x1 ssap 0x02
      3                   snap               etype 0x0700
      4                   ipx ethernetii
      5                   ipx llc
      6                   ipx raw
      7                   ipx snap
```

port hybrid protocol-vlan vlan

Syntax

port hybrid protocol-vlan vlan *vlan-id* { *vlan-protocol-list* | **all** }

undo port hybrid protocol-vlan vlan { *vlan-id* { *vlan-protocol-list* | **all** } | **all** }

View

Ethernet port view

Parameter

vlan-id: ID of the VLAN which a protocol is added to or deleted from.

{ *vlan-protocol-list* | **all** }*: vlan-protocol represents* the VLAN protocol list to be added to or deleted from a certain port, in the form of *vlan-protocol-list* = { *protocol-index* [*to protocol-end*] }. *protocol-index* indicates the initial value of protocol index; *protocol-end* indicates the end value of protocol index.

all: Adds/deletes all protocols to/from a port.

Description

Use the **port hybrid protocol-vlan vlan** command to add a protocol VLAN or protocol VLANs to a specified port.

Use the **undo port hybrid protocol-vlan vlan** command to delete a protocol VLAN or protocol VLANs from the port.

Use the **undo port hybrid protocol-vlan vlan all** command to delete all the configured protocol VLANs from the port.

- Only Hybrid ports support this feature at present.
- The specified port must belong to the VLAN before a protocol VLAN can be added to it.

Related command: **display protocol-vlan vlan** { *vlan-list* | **all** }.

Example

Add protocol VLANs 4 to 7 to Ethernet1/1/1.

```
[3Com-Ethernet1/1/1] port hybrid protocol-vlan vlan 3 4 to 7
```

protocol-vlan

Syntax

protocol-vlan [*protocol-index*] { **at** | **ipx** { **ethernetii** | **llc** | **raw** | snap } | **mode** { **ethernetii** [**etype** *etype-id*] | **llc** [**dsap** *dsap-id*] [**ssap** *ssap-id*] | **snap** [**etype** *etype-id*] } }

undo protocol-vlan { *protocol-index* [**to** *protocol-end*] | **all** }

View

VLAN view

Parameter

protocol-index: Initial value of protocol index, ranging from 0 to 7. It must be smaller than *protocol-end*.

protocol-end: End value of protocol index, ranging from 0 to 7

at: AppleTalk-based VLAN. Encapsulation format is EthernetII, and the Ethernet type is 0x809B.

ipx: IPX-based protocol VLAN, encapsulated in three formats: Ethernetii, LLC, and SNAP.

ethernetii: Encapsulation format is EthernetII, and the Ethernet type is 0x8137.

llc: Encapsulation format is LLC, DSAP=SSAP=0xE0.

snap: Encapsulation format is SNAP, and the Ethernet type is 0x8137.

raw: LLC-encapsulated IPX packet format of Novell, DSAP=SSAP=0xFF.

mode: Specifies the VLAN based on other protocols.

The following protocols can be supported:

Protocol mode	Parameter	Description
Ethernet II-based VLAN	**ethernetii etype** *etype-id*	*etype-id*: Indicates the Ethernet type of an inbound packet, in the range of 600 to FFFF
etype-id: Indicates the Ethernet type of an inbound packet, in the range of 600 to FFFF	**llc dsap** *dsap-id* **ssap** *ssap-id*	*dsap-id*: Indicates a destination service access point, in the range of 0 to FF *ssap-id*: Indicates a source service access point, in the range of 0 to FF
SNAP-based protocol	**snap etype** *etype-id*	*etype-id*: Indicates the Ethernet type of an inbound packet, in the range of 600 to FFFF

all: Supports all the protocols.

Description

Use the **protocol-vlan** command to specify the parameters of VLANs based on AppleTalk, IPX, and so on.

Use the **undo vlan-type protocol** command to cancel this configuration.

Related command: **display protocol-vlan vlan**.

Example

Specify VLAN 5 based on AppleTalk.

```
[3Com-vlan5] protocol-vlan at
```

IP Subnet-Based VLAN Configuration Commands

display vlan-ip vlan

Syntax

display vlan-ip vlan { *vlan-list* | **all** }

View

Any view

Parameter

vlan-list: Displays the information of a specified IP subnet-based VLAN, in the form of *vlan-list* = { *vlan-id* [**to** *vlan-id*] }.

all: Displays the protocol information and indexes of all the IP subnet-based VLANs.

Description

Use the **display vlan-ip vlan** command to display the information and index of the IP subnet-based VLAN configured on the specified VLAN. You can refer to this command for using an IP subnet-based VLAN and adding/deleting an IP subnet-based VLAN.

Related command: **display vlan-ip interface**

Example

Display the information and indexes of IP subnet-based VLANs configured on VLAN 10 and VLAN 11.

```
<SW8800> display vlan-ip vlan 10 to 11
 VLAN ID: 10
 VLAN Type: IP-based VLAN
      Index             Type              Value
      0                  IPv4              1.2.3.0 255.255.255.0
      1                  IPv4              1.2.4.0 255.255.255.0
      2                  IPv4              1.2.5.0 255.255.255.0
      3                  IPv4              1.2.6.0 255.255.255.0
      4                  IPv4              1.2.7.0 255.255.255.0
      5                  IPv4              1.2.8.0 255.255.255.0
      6                  IPv4              1.2.9.0 255.255.255.0
      7                  IPv4              1.2.10.0 255.255.255.0
 VLAN ID: 11
 VLAN Type: IP-based VLAN
      Index             Type              Value
      0                  IPv4              2.2.7.0 255.255.255.0
      1                  IPv4              2.2.8.0 255.255.255.0
      2                  IPv4              2.2.9.0 255.255.255.0
      3                  IPv4              2.2.10.0 255.255.255.0
      4                  IPv4              2.2.3.0 255.255.255.0
      5                  IPv4              2.2.4.0 255.255.255.0
      6                  IPv4              2.2.5.0 255.255.255.0
      7                  IPv4              2.2.6.0 255.255.255.0
```

display vlan-ip interface

Syntax

display vlan-ip interface { *interface-list* | **all** }

View

Any view

Parameter

interface-list: Displays the protocol information of the IP subnet-based VLAN on the specified port, in the form of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] }. *interface-type* indicates a port type and *interface-number* indicates a port number. The port number after the keyword **to** must be greater than or equal to that before **to**.

all: Displays the protocol information of the IP subnet-based VLANs on all the ports.

Description

Use the **display vlan-ip interface** command to display the information of the IP subnet-based VLAN configured on a specified port. You can refer to this command for using an IP subnet-based VLAN and adding/deleting an IP subnet-based VLAN.

Related command: **display interface**.

Example

Display the information of the IP subnet-based VLANs configured on all the ports.

```
<SW8800> display vlan-ip interface all
 Interface: GigabitEthernet2/1/1
      Vlan-ID  Index    Type              Value
      11        0         IPv4              2.2.7.0 255.255.255.0
      11        1         IPv4              2.2.8.0 255.255.255.0
      11        2         IPv4              2.2.9.0 255.255.255.0
      11        3         IPv4              2.2.10.0 255.255.255.0
      11        4         IPv4              2.2.3.0 255.255.255.0
      11        5         IPv4              2.2.4.0 255.255.255.0
      11        6         IPv4              2.2.5.0 255.255.255.0
      11        7         IPv4              2.2.6.0 255.255.255.0
 Interface: Ethernet6/1/1
      Vlan-ID  Index    Type              Value
      10        0         IPv4              1.2.3.0 255.255.255.0
      10        1         IPv4              1.2.4.0 255.255.255.0
      10        2         IPv4              1.2.5.0 255.255.255.0
      10        3         IPv4              1.2.6.0 255.255.255.0
      10        4         IPv4              1.2.7.0 255.255.255.0
      10        5         IPv4              1.2.8.0 255.255.255.0
      10        6         IPv4              1.2.9.0 255.255.255.0
      10        7         IPv4              1.2.10.0 255.255.255.0
```

port hybrid ip-vlan vlan

Syntax

port hybrid ip-vlan vlan *vlan-id*

undo port hybrid ip-vlan vlan *vlan-id*

View

Ethernet port view

Parameter

vlan-id: Specifies the ID of the IP subnet-based VLAN to be delivered or deleted.

Description

Use the **port hybrid ip-vlan vlan** command to associate a specified port with an IP subnet-based VLAN.

Use the **undo port hybrid ip-vlan vlan** command to dissociate a specified port from an IP subnet-based VLAN.

Related command: **display vlan-ip vlan** { *vlan-list* | **all** }.

Example

Associate the port Ethernet1/1/1 with the IP subnet-based VLAN on VLAN 2.

```
[3Com-Ethernet1/1/1] port hybrid ip-vlan vlan 2
```

vlan-type ip-subnet

Syntax

vlan-type ip-subnet ip *ip-address* { [*net-mask* | *net-mask-length*] }

undo vlan-type ip-subnet { *index-begin* [**to** *index-end*] | **all** }

View

VLAN view

Parameter

ip-address: IP address

net-mask: Mask of an IP address. If no mask is specified, the default mask is 255.255.255.0.

net-mask-length: Mask length of an IP address

index-begin: Initial value of an IP subnet-based VLAN index, ranging from 0 to 11. The value must be less than *index-end*.

index-end: End value of an IP subnet-based VLAN index, ranging from 0 to 11.

Description

Use the **vlan-type ip-subnet** command to configure an IP subnet-based VLAN.

Use the **undo vlan-type ip-subnet** command to remove the configuration.

Related command: **display vlan-ip vlan**.

Example

Configure IP subnet 192.168.1.0/24-based VLAN 5.

[3Com-vlan5] vlan-type ip-subnet ip 192.168.1.0 24

5 SUPER VLAN CONFIGURATION COMMANDS

Super VLAN Configuration Commands

display supervlan

Syntax

display supervlan [*supervlan-id*]

View

Any view

Parameter

supervlan-id: VLAN ID of a configured super VLAN. This argument ranges from 1 to 4094.

Description

Use the **display supervlan** command to display mapping relationship between a specified super VLAN and sub VLANs, and the ports that identify the mapping relationship.

Related command: **supervlan**, **subvlan**.

Example

Display the mapping relationship between the super VLAN and the sub VLAN.

```
[SW8800] display supervlan 2
Supervlan ID :  2
 Subvlan ID :  3-5
 Subvlan in which arp proxy is disabled: None
```

Display detailed information about the super VLAN and the sub VLANs displayed above.

```
[SW8800]display vlan 2
 VLAN ID: 2
 VLAN Type: static
 It is a Super VLAN.
 Route Interface: configured
 IP Address: 10.153.1.41
 Subnet Mask: 255.255.255.0
 Description: VLAN 0002
 Tagged   Ports: none
 Untagged Ports: none
[SW8800]display vlan 3
 VLAN ID: 3
```

```
 VLAN Type: static
 It is a Sub VLAN. And the Super VLAN is VLAN 2
 ARP proxy enabled.
 Route Interface: not configured
 Description: VLAN 0003
 Tagged   Ports: none
 Untagged Ports:
      Ethernet5/1/1
[SW8800]display vlan 4
 VLAN ID: 4
 VLAN Type: static
 It is a Sub VLAN. And the Super VLAN is VLAN 2
 ARP proxy enabled.
 Route Interface: not configured
 Description: VLAN 0004
 Tagged   Ports: none
 Untagged Ports:
      Ethernet5/1/2
[SW8800]display vlan 5
 VLAN ID: 5
 VLAN Type: static
 It is a Sub VLAN. And the Super VLAN is VLAN 2
 ARP proxy enabled.
 Route Interface: not configured
 Description: VLAN 0005
 Tagged   Ports: none
 Untagged Ports:
      Ethernet5/1/3
```

subvlan

Syntax

subvlan *sub-vlan-list*

undo subvlan [*sub-vlan-list*]

View

VLAN view of super VLAN

Parameter

sub-vlan-list: List of sub VLANs. It is expressed in the form of *sub-vlan-list* = { *vlan-id* [**to** *vlan-id* }&<*1-10*>. The *vlan-id* after the keyword **to** must be larger than or equal to that before **to**. &<1-10> means that the preceding parameter can be repeated up to 10 times.

Description

Use the **subvlan** command to associate a specified super VLAN to sub VLANs.

Use the **undo subvlan** command to cancel the mapping relationship between the super VLAN and sub VLANs.

Note that:

- The VLANs configured to be the sub VLANs of a super VLAN must be existing VLANs.

- You can still add/remove ports to/from a VLAN after the mapping relationship is established.
- The **undo subvlan** command cancels all mapping relationships between the specified super VLAN and all sub VLANs. If you do not specify the *sub-vlan-list* argument. Otherwise, this command cancels the mapping relationship between the specified sub VLAN and the specified super VLAN.

Related command: **display supervlan**.

Example

Establish mapping relationship between super VLAN 10 and sub VLANs with VLAN IDs of 3, 4, 5 and 9.

```
[3Com-vlan10] subvlan 3 to 5 9
```

supervlan

Syntax

supervlan

undo supervlan

View

VLAN view

Parameter

None

Description

Use the **supervlan** command to set a VLAN to be a super VLAN.

Use the **undo supervlan** command to cancel the super VLAN type of a VLAN.

By default, no type is configured for a VLAN.

Note that:

- You cannot add ports to a super VLAN.
- The ARP proxy of the interfaces of a VLAN are enabled automatically and cannot be disabled when the VLAN is set to be a super VLAN.
- The default VLANs cannot be super VLANs.

Related command: **display supervlan**.

Example

Set VLAN 2 to be a super VLAN.

```
[3Com-vlan2] supervlan
```

6 ISOLATE-USER-VLAN CONFIGURATION COMMANDS

Isolate-user-vlan Configuration Commands

display isolate-user-vlan

Syntax

display isolate-user-vlan [*isolate-user-vlan-num*]

View

Any view

Parameter

isolate-user-vlan-num: VLAN ID of an isolate-user-VLAN.

Description

Use the **display isolate-user-vlan** command to view the mapping relationships between isolate-user-VLANs and Secondary VLANs and the ports identifying the mapping relationships between isolate-user-vlan and Secondary VLAN.

Related command: **isolate-user-vlan enable**, **isolate-user-vlan**.

Example

Display the mapping relationships between isolate-user-VLANs and Secondary VLANs.

```
[SW8800] display isolate-user-vlan
 Isolate-user-VLAN VLAN ID : 5
 Secondary VLAN ID : 3-4

 VLAN ID: 5
 VLAN Type: static
 Isolate-user-VLAN type : isolate-user-VLAN
 ARP proxy disabled.
 Route Interface: not configured
 Description: VLAN 0005
 Name: VLAN 0005
 Tagged   Ports: none
 Untagged Ports:
      Ethernet2/1/3           Ethernet2/1/4

 VLAN ID: 3
 VLAN Type: static
 Isolate-user-VLAN type : secondary
 ARP proxy disabled.
 Route Interface: not configured
```

```
Description: VLAN 0003
Name: VLAN 0003
Tagged   Ports: none
Untagged Ports:
     Ethernet2/1/3

VLAN ID: 4
VLAN Type: static
Isolate-user-VLAN type : secondary
ARP proxy disabled.
Route Interface: not configured
Description: VLAN 0004
Name: VLAN 0004
Tagged   Ports: none
Untagged Ports:
     Ethernet2/1/4
```

Table 9 Description on the fields of the display isolate-user-vlan command

Field	Description
Isolate-user-VLAN Vlan ID	VLAN ID of Isolate-user-VLAN
Secondary Vlan ID	VLAN ID of Secondary VLAN
Vlan ID	VLAN ID
Vlan Type	VLAN configuration type (static or dynamic configuration)
Isolate-user-VLAN type	VLAN type is Isolate-user-VLAN or Secondary VLAN.
ARP proxy disabled	ARP proxy is disabled.
Route Interface	Whether VLAN has route function
Description	VLAN description
Tagged Ports	Identifies the ports on which the VLAN packets are to be tagged
Untagged Ports	Identifies the ports on which the VLAN packets are not to be tagged

isolate-user-vlan

Syntax

isolate-user-vlan *isolate-user-vlan-num* **secondary** *secondary-vlan-numlist*

undo isolate-user-vlan *isolate-user-vlan-num* [**secondary** *secondary-vlan-numlist*]

View

System view

Parameter

isolate-user-vlan-num: VLAN ID of isolate-user-VLAN.

Secondary-vlan-numlist: VLAN ID of Secondary vlan. *secondary-vlan-numlist* = { *secondary-vlan-num* [**to** *secondary-vlan-num*] }&<1-10>. The *secondary-vlan-num* parameter after the keyword **to** cannot be smaller than that before the keyword. &<1-10> indicates you can repeatedly input the preceding parameter up to 10 times.

Description

Use the **isolate-user-vlan** command to establish the mapping relationship between isolate-user-vlan and Secondary VLAN.

Use the **undo isolate-user-vlan** command to cancel the mapping relationship.

By default, there is no mapping relationship between isolate-user-vlan and Secondary VLAN.

Before you execute the **isolate-user-vlan** command, the VLAN can include hybrid ports, access ports, or no ports. After this command is executed, the mapping relationship between isolate-user-vlan and Secondary VLAN is established.

The actual operation include: for access ports or hybrid ports whose PVIDs are the same as isolate-user-VLAN IDs and join to isolate-user-vlans in the untagged mode, add the ports of isolate-user-VLAN to every Secondary VLAN and add the ports of all Secondary VLANs to isolate-user-VLAN.

After **undo isolate-user-vlan** command is executed, the mapping relationship between isolate-user-vlan and Secondary VLAN will be canceled. The actual operation include: delete the ports included in isolate-user-vlan from Secondary VLAN and delete the ports included in Secondary VLAN from isolate-user-vlan.

Related command: **display isolate-user-vlan**.

Example

Map isolate-user-VLAN 10 to Secondary VLAN 2, 3, 4, 5, and 9.

```
[SW8800] isolate-user-vlan 10 secondary 2 to 5 9
```

isolate-user-vlan enable

Syntax

isolate-user-vlan enable

undo isolate-user-vlan enable

View

VLAN view

Parameter

None

Description

Use the **isolate-user-vlan enable** command to set a VLAN as an isolate-user-VLAN.

Use the **undo isolate-user-vlan enable** command to cancel the configuration.

An isolate-user-VLAN is allowed to contain multiple ports, including upstream ports connecting to other switches. However, the VLAN can only contain access or hybrid ports, not trunk ports.

Related command: **display isolate-user-vlan**.

- You cannot configure VLAN 1 as an isolate-user-VLAN or Secondary VLAN.
- You cannot directly configure isolate-user-VLAN as other types of VLAN than common VLAN, such as Secondary VLAN, multicast VLAN, Super VLAN/Sub VLAN, Guest VLAN and VLAN running L2VPN services. You cannot directly configure Secondary VLAN as other type of VLAN than common VLAN, such as isolate-user-VLAN, multicast VLAN, super VLAN/sub VLAN, guest VLAN and VLAN running L2VPN services.
- When you configure common VLAN as isolate-user-VLAN or Secondary VLAN, the VLAN cannot contain trunk ports. Otherwise, the configuration will fail.

- One isolate-user-vlan can be mapped to up to 64 Secondary VLANs.
- You can configure up to 32 isolate-user-VLANs for the system.
- You can configure up to 1024 Secondary VLANs for the system.
- You cannot configure the same MAC address in the Secondary VLAN corresponding to an isolate-user-VLAN.

Example

Configure VLAN 5 as isolate-user-VLAN.

```
[3Com-vlan5] isolate-user-vlan enable
```

7 IP Address Configuration Commands

IP Address Configuration Commands

display ip host

Syntax

display ip host

View

Any view

Parameter

None

Description

Use the **display ip host** command to display all the host names and the corresponding IP addresses.

Example

Display all host names and the corresponding IP addresses of the hosts.

```
<SW8800> display ip host
Host         Age     Flags       Address
My           0       static      1.1.1.1
Aa           0       static      2.2.2.4
```

Table 10 Description on the fields of the display ip host command

Field	Description
Host	Host name
Age	Valid period
Flags	Indicates the relationship between the host name and the IP address. If you configure the host name by using the **ip host** command, the relationship between the host name and the IP address is static. If you resolve the host name through DNS, the relationship between the host name and the IP address is dynamic.
Address	Host IP address

display ip interface

Syntax

display ip interface *interface-type interface-number*

View

Any view

Parameter

interface-type interface-number: *interface-type* refers to the interface type, and *interface-number* refers to the interface number. Refer to the **interface** command in *Port Command Manual* for more information.

Description

Use the **display ip interface** command to display information about an interface.

Example

Display the information about interface VLAN-interface 1.

```
<SW8800> display ip interface vlan-interface 1
Vlan-interface1 current state : DOWN
Line protocol current state : DOWN
Internet Address is 1.1.1.1/8 Primary
Broadcast address : 1.255.255.255
The Maximum Transmit Unit : 1500 bytes
input packets : 0, bytes : 0, multicasts : 0
output packets : 0, bytes : 0, multicasts : 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 11 Description on the fields of the display ip interface command

Field	Description
Vlan-interface1 current state	Current state of the VLAN interface 1
Line protocol current state	Current state of the Line protocol
Internet Address	IP address
Broadcast address	Broadcast address
The Maximum Transmit Unit	Maximum transmission unit
input packets : 0, bytes : 0, multicasts : 0 output packets : 0, bytes : 0, multicasts : 0	The number of the input/output unicast packets, bytes and broadcast packets are all 0
TTL invalid packet number	The number of the received packets with invalid TTLs

Table 11 Description on the fields of the display ip interface command

Field	Description
ICMP packet input number	Total received ICMP packets, including:
Echo reply:	Echo reply packets, unreachable packets, source quench packets, routing redirect packets, echo request packets, route advertisement packets, route solicitation packets, packets that exceed the time, packets with bad IP headers, timestamp request packets, timestamp reply packets, information request packets, information reply packets, netmask request packets, netmask reply packets and unknown packets.
Unreachable:	
Source quench:	
Routing redirect:	
Echo request:	
Router advert:	
Router solicit:	
Time exceed:	
IP header bad:	
Timestamp request:	
Timestamp reply:	
Information request:	
Information reply:	
Netmask request:	
Netmask reply:	
Unknown type:	
DHCP packet deal mode	DHCP packet processing mode

ip address

Syntax

ip address *ip-address* { *mask* | *mask-length* } [**sub**]

undo ip address [*ip-address* { *mask* | *mask-length* } [**sub**]]

View

VLAN interface view, loopback interface view, or console view

Parameter

ip-address: IP address of VLAN interface in dotted decimal format.

mask: Corresponding subnet mask in dotted decimal format.

mask-length: Mask length. That is, the number of bits with a value of 1.

sub: Specifies the IP address to be configured to be the secondary IP address of the VLAN interface/loopback interface.

Description

Use the **ip address** command to assign an IP address and the corresponding subnet mask to the VLAN interface/loopback interface/console interface.

Use the **undo ip address** command to remove the IP address and the corresponding subnet mask assigned to the VLAN interface/loopback interface/console interface.

By default, a VLAN interface/loopback interface/console interface does not have an IP address configured.

Normally, a VLAN interface/loopback interface/console interface only needs to be configured with one IP address. But you can also assign up to 21 IP addresses to a VLAN interface/loopback interface/console interface to enable it to connect to multiple subnets. Of all the IP addresses assigned to a VLAN interface/loopback interface/console interface, one is the primary IP address, and the other are secondary IP addresses. The relationship between primary and secondary addresses is:

- When you configure a primary IP address for an interface already has a primary IP address configured, the newly configured one replaces the old one.
- If you execute the **undo ip address** command without providing any parameter, the switch removes both primary and secondary IP addresses of the interface. The **undo ip address** [*ip-address* { *mask* | *mask-length* } command can be used to delete the primary IP address, while the **undo ip address** [*ip-address* { *mask* | *mask-length* } **sub** command can be used to delete the secondary IP address.

*When you use the **ip address** command to configure IP addresses of VLAN interfaces, the system will prompts if you continue if the IP address you configure is in different network segment from the existing IP address. If you do continue, the IP address of the VLAN interface will be modified. In addition, if the ARP entries (including dynamic ARP entries and static ARP entries) in the original network segment match the new network segment, they will not be removed; otherwise, the ARP entries in the original network segment will be removed.*

Related command: **display ip interface**.

Example

Assign 129.12.0.1 to VLAN interface 1, with a subnet mask of 255.255.255.0.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface vlan-interface 1
[3Com-Vlan-interface1] ip address 129.12.0.1 255.255.255.0
```

Assign 129.12.0.10 to Ethernet4/0/0, with a 24-bit subnet mask.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface M-Ethernet4/0/0
[3Com-M-Ethernet4/0/0] ip address 129.12.0.10 24
```

ip host

Syntax

ip host *hostname ip-address*

undo ip host *hostname* [*ip-address*]

View

System view

Parameter

hostname: Name of the host. It is a character string that consists of 1 to 20 characters, including letters, numbers, "_", or ",", and it must contain at least one letter.

ip-address: Host IP address (the corresponding IP address to the host name) in dotted decimal notation.

Description

Use the **ip host** command to configure the host name and the host IP address.

Use the **undo ip host** command to cancel the host name and the host IP address.

By default, host name and corresponding IP address are null.

Related command: **display ip host**.

Example

Set Lanswtich1's IP address to be 10.110.0.1.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] ip host Lanswitch1 10.110.0.1
```

ip icmp-time-exceed enable

Syntax

ip icmp-time-exceed enable

undo ip icmp-time-exceed enable

View

System view

Parameter

None

Description

Use the **ip icmp-time-exceed enable** command to enable the switch to send the ICMP message "time exceeded" to the network management system when the switch receives an IP packet whose TTL is less than or equal to 1, thus preventing the switch from keeping sending unreachable packets to the sending end.

Use the **undo ip icmp-time-exceed enable** command to remove the configuration. As a result, the switch sends an unreachable packet to the sending end.

By default, the switch sends the ICMP message "time exceeded" to the network management system

Example

Configure that the switch sends the ICMP message "time exceeded" to the network management system when the switch receives an IP packet whose TTL is less than or equal to 1.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] ip icmp-time-exceed enable
```

ip-protect enable

Syntax

ip-protect enable

undo ip-protect

View

VLAN interface view

Parameter

None

Description

Use the **ip-protect enable** command to enable IP address protection.

Use the **undo ip-protect** command to disable IP address protection.

After IP address protection is enabled, the current interface will no longer dynamically learn ARP mapping entries, and existing dynamic ARP mapping entries will be removed. At the same time, the switch will enable the MAC address auto filling function, so that the user can configure static ARP entries that have only IP address.

By default, IP address protection is disabled.

You can use the **display this** command to view the status of IP address protection (enabled/disabled) for the current VLAN interface.

Example

Enable IP address protection for Vlan-interface 2.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800]interface Vlan-interface 2
[3Com-Vlan-interface2]ip-protect enable
```

8 IP PERFORMANCE CONFIGURATION COMMANDS

IP Performance Configuration Commands

display fib

Syntax

display fib

View

Any view

Parameter

None

Description

Use the **display fib** command to view the entries of the forwarding information base. Each line outputs indicates a FIB entry. The information includes destination address/mask length, next hop, current flag, timestamp and outbound interface.

Example

Display the entries of the Forwarding Information Base.

```
<SW8800> display fib
Destination/Mask    Nexthop          Flag TimeStamp    Interface
10.153.17.0/24      10.153.17.99     U    t[0]         Vlan-interface1
10.153.18.88/32     127.0.0.1        GHU  t[0]         InLoopBack0
10.153.18.0/24      10.153.18.88     U    t[0]         LoopBack0
10.153.17.99/32     127.0.0.1        GHU  t[0]         InLoopBack0
127.0.0.0/8         127.0.0.1        U    t[0]         InLoopBack0
```

Table 12 Description on the fields of the display fib command

Field	Description
Destination/Mask	Destination address/Mask length
Nexthop	The forwarding next hop address

Table 12 Description on the fields of the display fib command

Field	Description
Flag	The flag options include: B - Blackhole route D - Dynamic route G - Gateway route H - Local host route S - Static route U - Route in UP status R - Unreachable route L - Route generated by ARP or ISIS
Timestamp	Timestamp
Interface	The forwarding interface

display fib ip-address

Syntax

display fib [*ip-address1* { *mask1* | *mask-length1* } [*ip-address2* { *mask2* | *mask-length2* } | **longer**] | **longer**]

View

Any view

Parameter

ip-address1, *ip-address2*: Destination IP address, in dotted decimal format. *ip-address1* and *ip-address2* jointly define an address range. The FIB entries in this address range are displayed.

mask1, *mask2:* IP address mask, in dotted decimal format.

mask-length1, mask-length2: An integer in the range of 0 to 32 to represent the mask length.

longer: Specifies to display the FIB entries that match the specified IP address/subnet mask pairs.

Description

Use the **display fib** *ip-address* command to view the FIB entries matching the destination IP address (range). Each line outputs a FIB entry and the display contents for each entry include destination address/mask length, next hop, current flag, timestamp and outbound interface.

Example

Display the FIB entries whose destination addresses match 169.253.0.0 in the natural mask range or which match most of 169.253.0.0..

```
<SW8800> display fib 169.253.0.0
  Route Entry Count: 1
Destination/Mask    Nexthop     Flag        TimeStamp   Interface
169.253.0.0/16      2.1.1.1         U       t[0]            Vlan-interface1
```

Display the FIB entries whose destination addresses are in the range of 169.254.0.0/16 to 169.254.0.6/16.

```
<SW8800> display fib 169.254.0.0 255.255.0.0 169.254.0.6 255.255.0.0
  Route Entry Count: 1
Destination/Mask    Nexthop     Flag        TimeStamp   Interface
169.254.0.1/16  2.1.1.1     U       t[0]            Vlan-interface1
```

For the descriptions of the displayed fields, refer to Table 12.

display fib acl

Syntax

display fib acl { *number* | *name* }

View

Any view

Parameter

number: ACL in number form, in the range 2000 to 2999

name: ACL in name form, a string of 1 to 32 characters.

Description

Use the **display fib** command to view the FIB entries matching a specific ACL.

Example

Display the FIB entries matching ACL 2000.

```
<SW8800> display fib acl 2000
Route entry matched by access-list 2000:
Summary counts: 1
Destination/Mask        Nexthop     Flag        TimeStamp   Interface
127.0.0.0/8         127.0.0.1   U       t[0]            InLoopBack0
```

For the descriptions of the displayed fields, refer to Table 12.

display fib |

Syntax

display fib | { { **begin** | **include** | **exclude** } *text* }

View

Any view

Parameter

begin: Displays the FIB entries from the first one containing the character string *text*.

include: Displays only those FIB entries containing the character string *text*.

exclude: Displays only those FIB entries excluding the character string *text*.

text: Character string.

Description

Use the **display fib |** command to view the FIB entries which are output from the buffer according to regular expression and related to the specific character string.

Example

Display the lines starting from the first one containing the string 169.254.0.0

```
<SW8800> display fib | begin 169.254.0.0
Destination/Mask    Nexthop     Flag        TimeStamp   Interface
169.254.0.0/16  2.1.1.1     U       t[0]            Vlan-interface1
2.0.0.0/16      2.1.1.1     U       t[0]            Vlan-interface1
```

For the descriptions of the displayed fields, refer to Table 12.

display fib ip-prefix

Syntax

display fib ip-prefix *listname*

View

Any view

Parameter

listname: Prefix list name, a string of 1 to 19 characters in length.

Description

Use the **display fib** command to view the FIB entries matching the specific prefix list.

Example

Display the FIB entries matching the prefix list abc0.

```
<SW8800> display fib ip-prefix abc0
Route Entry matched by prefix-list abc0:
Summary count: 3
Destination/Mask    Nexthop     Flag        TimeStamp   Interface
127.0.0.0/8     127.0.0.1   U       t[0]            InLoopBack0
127.0.0.1/32        127.0.0.1   U       t[0]            InLoopBack0
169.0.0.0/8     2.1.1.1     SU      t[0]            Vlan-interface1
```

For the descriptions of the displayed fields, refer to Table 12.

display fib statistics

Syntax

display fib statistics

View

Any view

Parameter

None

Description

Use the **display fib statistics** command to view the total number of FIB entries.

Example

Display the total number of FIB entries.

```
<SW8800> display fib statistics
Route Entry Count : 30
```

display icmp statistics

Syntax

display icmp statistics

View

Any view

Parameter

None

Description

Use the **display icmp statistics** command to view the statistics information about ICMP packets.

Related command: **display ip interface**, **reset ip statistics**.

Example

View statistics about ICMP packets.

```
<SW8800> 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 13 Description on the fields of the display icmp statistics command

Field	Description
bad formats	Number of input packets in bad format
bad checksum	Number of input packets with wrong checksum
echo	Number of input/output echo request packets
destination unreachable	Number of input/output packets with unreachable destination
source quench	Number of input/output source quench packets
redirects	Number of input/output redirected packets
echo reply	Number of input/output echo reply packets
parameter problem	Number of input/output packets with parameter problems
timestamp	Number of input/output timestamp packets
information request	Number of input information request packets

Table 13 Description on the fields of the display icmp statistics command

Field	Description
mask requests	Number of input/output mask request packets
mask replies	Number of input/output mask reply packets
information reply	Number of output information reply packets
time exceeded	Number of packets that exceeds the time

display ip socket

Syntax

display ip socket [**socktype** *sock-type*] [*task-id socket-id*]

View

Any view

Parameter

sock-type: The type of a socket (tcp:1, udp: 2, raw ip: 3).

task-id: The ID of a task, with the value ranging from 1 to 100.

socket-id: The ID of a socket, with the value ranging from 0 to 3072.

Description

Use the **display ip socket** command to display the information about the sockets in the current system.

Example

Display the information about the socket of TCP type.

```
<SW8800> display ip socket socktype 1
SOCK_STREAM:
Task = VTYD(18), socketid = 1, Proto = 6,
LA = 0.0.0.0:23, FA = 0.0.0.0:0,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_ACCEPTCONN SO_KEEPALIVE SO_SENDVPNID SO_SETKEEPALIVE,
socket state = SS_PRIV SS_ASYNC

Task = VTYD(18), socketid = 2, Proto = 6,
LA = 10.153.17.99:23, FA = 10.153.17.56:1161,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_KEEPALIVE SO_OOBINLINE SO_SENDVPNID SO_SETKEEPALIVE,
socket state = SS_ISCONNECTED SS_PRIV SS_ASYNC

Task = VTYD(18), socketid = 3, Proto = 6,
LA = 10.153.17.99:23, FA = 10.153.17.82:1121,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_KEEPALIVE SO_OOBINLINE SO_SENDVPNID SO_SETKEEPALIVE,
socket state = SS_ISCONNECTED SS_PRIV SS_ASYNC
```

Table 14 Description on the fields of the display ip socket command

Field	Description
SOCK_STREAM	The socket type
Task	The ID of a task
socketid	The ID of a socket
Proto	The protocol number used by the socket
sndbuf	The sending buffer size of the socket

Table 14 Description on the fields of the display ip socket command

Field	Description
rcvbuf	The receiving buffer size of the socket
sb_cc	The current data size in the sending buffer. The value makes sense only for the socket of TCP type, because only TCP is able to cache data
rb_cc	The current data size in the receiving buffer
socket option	The option of the socket
socket state	The state of the socket

display ip statistics

Syntax

display ip statistics

View

Any view

Parameter

None

Description

Use the **display ip statistics** command to view the statistics information about IP packets.

Related command: **display ip interface**, **reset ip statistics**.

Example

View statistics about IP packets.

```
<SW8800> display ip statistics
  Input:   sum            7120            local             112
           bad protocol   0               bad format        0
           bad checksum   0               bad options       0
  Output:  forwarding     0               local             27
           dropped        0               no route          2
           compress fails 0
  Fragment:input          0               output            0
           dropped        0
           fragmented     0               couldn't fragment 0
  Reassembling:sum        0               timeouts          0
```

Table 15 Description on the fields of the display ip statistics command

Field		Description
Input:	sum	Sum of input packets
	local	Number of received packets whose destination is the local device
	bad protocol	Number of packets with wrong protocol number
	bad format	Number of packets in bad format
	bad checksum	Number of packets with wrong checksum
	bad options	Number of packets that have wrong options
	forwarding	Number of forwarded packets
Output:	local	Number of packets that are sent by the local device
	dropped	Number of dropped packets during transmission
	no route	Number of packets that cannot be routed
	compress fails	Number of packets that cannot be compressed
Fragment:	input	Number of input fragments
	output	Number of output fragments
	dropped	Number of dropped fragments
	fragmented	Number of packets that are fragmented
	couldn't fragment	Number of packets that cannot be fragmented
Reassembling:	sum	Number of packets that are reassembled
	timeouts	Number of packets that time out

display tcp statistics

Syntax

display tcp statistics

View

Any view

Parameter

None

Description

Use the **display tcp statistics** command to view the statistics information about TCP packets.

For the related commands, see **display tcp status**, **reset tcp statistics**.

Example

View statistics about TCP packets.

```
<SW8800> display tcp statistics
Received packets:
 Total: 753
 packets in sequence: 412 (11032 bytes)
 window probe packets: 0, window update packets: 0
 checksum error: 0, offset error: 0, short error: 0
 duplicate packets: 4 (88 bytes), partially duplicate packets: 5 (7 bytes)
 out-of-order packets: 0 (0 bytes)
 packets of data after window: 0 (0 bytes)
 packets received after close: 0
 ACK packets: 481 (8776 bytes)
 duplicate ACK packets: 7, too much ACK packets: 0

Sent packets:
 Total: 665
 urgent packets: 0
 control packets: 5 (including 1 RST)
 window probe packets: 0, window update packets: 2
 data packets: 618 (8770 bytes) data packets retransmitted: 0 (0 bytes)
 ACK-only packets: 40 (28 delayed)

Retransmitted timeout: 0, connections dropped in retransmitted timeout: 0
Keepalive timeout: 0, keepalive probe: 0, Keepalive timeout, so connections
disconnected : 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 16 Description on the fields of the display tcp statistics command

Field	Description
Received packets	Information followed is about received packets
Total:753	Total number of received packets: 753
packets in sequence: 412 (11032 bytes)	Up to 412 packets (total of 11,032 bytes) arrive in sequence
window probe packets: 0, window update packets: 0	Number of window probe packets: 0
	Number of window update packets: 0
checksum error: 0, offset error: 0, short error: 0	Number of checksum errors: 0
	Number of offset errors: 0
	Number of short errors: 0
duplicate packets: 4 (88 bytes), partially duplicate packets: 5 (7 bytes)	Number of duplicate packets: 4 (total of 88 bytes)
	Number of partially duplicate packets: 5 (total of 7 bytes)
out-of-order packets: 0 (0 bytes)	Number of out-of-order packets: 0 (0 byte)
packets of data after window: 0 (0 bytes)	Number of packets out of receiving window: 0 (0 byte)
packets received after close: 0	Number of packets received after the connection closed: 0
ACK packets: 481 (8776 bytes)	Number of ACK packets: 481 (total of 8776 bytes of data acknowledged)
duplicate ACK packets: 7, too much ACK packets: 0	Number of duplicate ACK packets: 7
	Number of too-much ACK packets: 0 (ACK packets that acknowledge data not sent)

Table 16 Description on the fields of the display tcp statistics command

Field	Description
Sent packets	Information followed is about sent packets
Total: 665	Total number of sent packets: 665
urgent packets: 0	Number of urgent packets: 0
control packets: 5 (including 1 RST)	Number of control packets: 5 (including 1 RST packet)
window probe packets: 0, window update packets: 2	Number of window probe packets: 0
	Number of window update packets: 2
data packets: 618 (8770 bytes) data packets retransmitted: 0 (0 bytes)	Number of data packets: 618 (total of 8770 bytes)
	Number of data packets retransmitted: 0 (0 byte)
ACK-only packets: 40 (28 delayed)	Number of ACK packets: 40 (28 of which delayed)
Retransmitted timeout: 0, connections dropped in retransmitted timeout: 0	Number of retransmitted timeout events: 0
	Number of connections dropped due to the number of retransmitted timeout events exceeding the specified value: 0
Keepalive timeout: 0, keepalive probe: 0, Keepalive timeout, so connections	Number of keepalive timeout events: 0
	Number of keepalive probe packets sent: 0
disconnected : 0	Number of connections disconnected when keepalive probes fail: 0
Initiated connections: 0, accepted connections: 0, established connections: 0	Number of initiated connections: 0
	Number of accepted connections: 0
	Number of established connection: 0
Closed connections: 0 (dropped: 0, initiated dropped: 0)	Number of closed connection: 0
	Number of dropped connections (after SYN messages received): 0
	Number of connections initiated drooped: 0
Packets dropped with MD5 authentication: 0	Number of packets dropped with MD5 authentication: 0
Packets permitted with MD5 authentication: 0	Number of packets permitted with MD5 authentication: 0

display tcp status

Syntax

display tcp status

View

Any view

Parameter

None

Description

Use the **display tcp status** command to view all TCP connection states. This helps user monitor TCP connection at any time.

Example

Display the state of all TCP connections.

```
<SW8800> display tcp status
TCPCB       Local Add:port      Foreign Add:port        State
03e37dc4    0.0.0.0:4001            0.0.0.0:0           Listening
04217174    100.0.0.204:23      100.0.0.253:65508   Established
```

The displayed information indicates that a TCP connection is established. The local IP address of this TCP connection is 100.0.0.204, and the local port number is 23. The remote IP address is 100.0.0.253, and the remote port number is 65508. In addition, there is a local server process which listens to the port 4001.

display udp statistics

Syntax

display udp statistics

View

Any view

Parameter

None

Description

Use the **display udp statistics** command to view UDP traffic statistic information.

It displays the statistic information of all current UDP connections. The statistics information about UDP packets are divided into two major kinds which are received packets and sent packets. The packets are further divided into different types such as check packets and error packets. There are also some statistics related closely to the connections, such as the number of broadcast packets. All these displayed information are measured in packets.

Related command: **reset udp statistics**.

Example

Display the UDP traffic statistic information.

```
<SW8800> display udp statistics
Received packet:
Total:0
checksum error:0
shorter than header:0, data length larger than packet:0
no socket on port:0
broadcast:0
not delivered, input socket full:0
input packets missing pcb cache:0
Sent packet:
Total:0
```

Table 17 Description on the fields of the display udp statistics command

Field	Description
Received packet: Total: 0	Total received UDP packets: 0

Table 17 Description on the fields of the display udp statistics command

Field	Description
checksum error: 0	Number of checksum errors: 0
shorter than header: 0, data length larger than packet: 0	Cases that the length of the packets is shorter than the header: 0
	Cases that the data length exceeds the packet length: 0
no socket on port: 0	Cases that there is no socket on port: 0
broadcast: 0	Number of broadcast packets: 0
not delivered, input socket full: 0	Cases that the packets are not forwarded because the socket buffer is full: 0
input packets missing pcb cache: 0	Cases that the packets cannot find pcb: 0
Sent packet:	Total sent UDP packets: 0
Total: 0	

reset ip statistics

Syntax

reset ip statistics

View

User view

Parameter

None

Description

Use the **reset ip statistics** command to clear the IP statistics information.

Related command: **display ip interface**, **display ip statistics**.

Example

Clear the IP statistics information.

```
<SW8800> reset ip statistics
```

reset tcp statistics

Syntax

reset tcp statistics

View

User view

Parameter

None

Description

Use the **reset tcp statistics** command to clear the TCP statistics information.

Related command: **display tcp statistics**.

Example

Clear the TCP statistics information.

```
<SW8800> reset tcp statistics
```

reset udp statistics

Syntax

reset udp statistics

View

User view

Parameter

None

Description

Use the **reset udp statistics** command to can clear the UDP statistics information.

Example

Clear the UDP traffic statistics information.

```
<SW8800> reset udp statistics
```

tcp timer fin-timeout

Syntax

tcp timer fin-timeout *time-value*

undo tcp timer fin-timeout

View

System view

Parameter

time-value: TCP finwait timer value in second, with the value ranging from 76 to 3600; By default, it is 675 seconds.

Description

Use the **tcp timer fin-timeout** command to configure the TCP finwait timer.

Use the **undo tcp timer fin-timeout** command to restore the default value of the TCP finwait timer.

When the TCP connection state changes from FIN_WAIT_1 to FIN_WAIT_2, the finwait timer is enabled. If the switch does not receive FIN packets before the finwait timer times out, the TCP connection is terminated.

Related command: **tcp timer syn-timeout**, **tcp window**.

Example

Configure the TCP finwait timer value as 800 seconds.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] tcp timer fin-timeout 800
```

tcp timer syn-timeout

Syntax

tcp timer syn-timeout *time-value*

undo tcp timer syn-timeout

View

System view

Parameter

time-value: TCP synwait timer value measured in seconds, whose value ranges from 2 to 600. The default *time-value* is 75 seconds.

Description

Use the **tcp timer syn-timeout** command to configure the TCP synwait timer.

Use the **undo tcp timer syn-timeout** command to restore the default value of the timer.

TCP enables the synwait timer if a SYN packet is sent. The TCP connection is terminated if the response packet is not received.

Related command: **tcp timer fin-timeout**, **tcp window**.

Example

Configure the TCP synwait timer value as 80 seconds.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] tcp timer syn-timeout 80
```

tcp window

Syntax

tcp window *window-size*

undo tcp window

View

System view

Parameter

window-size: The size of the sending and receiving buffers measured in kilobytes (KB), whose value ranges from 1 to 32. By default, the *window-size* is 8KB.

Description

Use the **tcp window** command to configure the size of the sending and receiving buffers of the connection-oriented Socket.

Use the **undo tcp window** command to restore the default size of the buffer.

Related command: **tcp timer fin-timeout**, **tcp timer syn-timeout**.

Example

Configure the size of the sending and receiving buffers as 3KB.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] tcp window 3
```

9 GARP&GVRP CONFIGURATION COMMANDS

GARP Configuration Commands

display garp statistics

Syntax

display garp statistics [**interface** *interface-list*]

View

Any view

Parameter

interface-list: List of Ethernet ports to be displayed, expressed as *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>. *interface-type* is interface type, and *interface-number* is interface number. The interface number after the keyword **to** must be larger than or equal to that before **to**. &<1-10> represents that the preceding parameter can be repeated up to 10 times.

Description

Use the **display garp statistics** command to view the GARP statistics information, including the number of packets received/sent and discarded by GVRP/GMRP.

Example

Display the GARP statistics information on Ethernet port Ethernet2/1/1.

```
<SW8800> display garp statistics interface ethernet2/1/1
  GARP statistics on port Ethernet2/1/1
        Number Of GMRP Frames Received          : 0
        Number Of GVRP Frames Received          : 0
        Number Of GMRP Frames Transmitted       : 0
        Number Of GVRP Frames Transmitted       : 0
        Number Of Frames Discarded               : 0
```

The information above indicates that the number of received/sent packets and the number of packets discarded by GVRP/GMRP on Ethernet2/1/1 are all 0.

display garp timer

Syntax

display garp timer [**interface** *interface-list*]

View

Any view

Parameter

interface-list: List of Ethernet ports of which the GRRP timer information is to be displayed, expressed as *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>. *interface-type* is interface type, and *interface-number* is interface number. The interface number after the keyword **to** must be larger than or equal to that before **to**. &<1-10> means that the preceding parameter can be repeated up to 10 times.

Description

Use the **display garp timer** command to view the value of GARP timer, including Hold timer, Join timer, Leave timer and LeaveAll timer.

Related command: **garp timer**, **garp timer leaveall**.

Example

Display GARP timer on Ethernet2/1/1.

```
<SW8800> display garp timer interface ethernet2/1/1
      GARP timers on port Ethernet2/1/1
                GARP JoinTime           : 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 port view

Parameter

hold: GARP Hold timer. After receiving certain registration information, the GARP application entity will not send Join Message at once. Instead, it starts the Hold timer. All the registration information received within duration of the Hold timer will be transmitted in the same frame after the Hold timer times out, thereby saving the bandwidth resource.

join: GARP Join timer. GARP application entity will send out Join message after the Join timer goes timeout to make other GARP application entity register its own information.

leave: GARP Leave timer . When a GARP application entity wants to deregister certain attribute information, it sends Leave message. The GARP application entity receiving the message starts Leave timer. If the entity receives no Join message before the timer goes timeout, it will deregister the attribute information.

timer-value: Value of GARP hold timer, join timer and leave timer in centiseconds. The step is five centiseconds. By default, Hold timer is 10 centiseconds, Join timer is 20 centiseconds, Leave timer is 60 centiseconds.

The range conforms to the following rule:

- The value of Join timer should be no less than the doubled value of Hold timer.
- The value of Leave timer should be greater than the doubled value of Join timer and smaller than the Leaveall timer value.
- The minimal value of Join timer is 10 centiseconds.

Description

Use the **garp timer** command to set the value of GARP timer (including Hold timer, Join timer and Leave timer) of the port.

Use the **undo garp timer** command to restore the default value of GARP timer.

The value range of a timer varies with the values of other timers. So if the value of a timer you want to set is not within the available value range, you can change the value range by changing the values of other related timers.

- The lower limit of Hold timer is 10 centiseconds. You can change its upper limit by changing the value of Join timer.
- You can change the lower limit and upper limit of Join timer by changing the value of Hold timer and Leave timer respectively.
- You can change the lower limit and upper limit of Leave timer by changing the value of Join timer and LeaveAll timer respectively.
- The upper limit of LeaveAll timer is 32765 centiseconds. You can change its lower limit by changing the value of Leave timer.

Related command: **display garp timer**.

Example

Set Join timer of GARP to 300ms.

```
[3Com-Ethernet2/1/1] garp timer join 30
```

garp timer leaveall

Syntax

garp timer leaveall *timer-value*

undo garp timer leaveall

View

System view

Parameter

timer-value: Value of GARP LeaveAll timer in centiseconds, ranging from 65 to 32765. The step is five centiseconds. The value of LeaveAll timer should be greater than the value of Leave timer.

By default, the value of LeaveAll timer is 1000 centiseconds, i.e., 10s.

Description

Use the **garp timer leaveall** command to configure GARP LeaveAll timer.

Use the **undo garp timer leaveall** command to restore the default value.

After every GARP application entity is started, the LeaveAll timer will be started simultaneously. The GARP application entity will send LeaveAll message after the timer times out to make other application entities re-register all attribute information on the entities themselves. Then, the LeaveAll timer is started and the new cycle begins.

Related command: **display garp timer**.

Example

Set GARP LeaveAll timer to 1s.

```
[SW8800] garp timer leaveall 100
```

reset garp statistics

Syntax

reset garp statistics [**interface** *interface-list*]

View

User view

Parameter

interface-list: Specifies a list of Ethernet ports on which the GARP statistics information will be cleared, expressed as *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-num*] }&<1-10>. *interface-type* is interface type, and *interface-number* is interface number. The *interface-number* after the keyword **to** must be larger than or equal to that before **to**. &<1-10> means that the preceding parameter can be repeated up to 10 times.

Description

Use the **reset garp statistics** command to reset the GARP statistics information (such as the packets received/sent and discarded by GVRP/GMRP). If the command has no parameter, it will clear the GARP statistics information of all the ports.

Related command: **display garp statistics**.

Example

Clear GARP statistics information.

```
<SW8800> reset garp statistics
```

GVRP Configuration Commands

display gvrp statistics

Syntax

display gvrp statistics [**interface** *interface-list*]

View

Any view

Parameter

Interface-list: List of Ethernet ports on which the GVRP statistics information is to be displayed, expressed as *interface-list* = { *interface-type interface-number* } [**to**

interface-type interface-number] }&<1-10>. *interface-type* is interface type, and *interface-number* is interface number. The *interface-number* after the keyword **to** must be larger than or equal to that before **to**. &<1-10> means that the preceding parameter can be repeated up to 10 times.

Description

Use the **display gvrp statistics** command to view the GVRP statistics information of all the Trunk ports, including GVRP status information, failed GVRP registration entries and the last GVRP data unit origin.

Example

Display the GVRP statistics information on Ethernet2/1/1.

```
<SW8800> display gvrp statistics interface ethernet2/1/1
       GVRP statistics on port Ethernet2/1/1
                GVRP Status                    : Enabled
                GVRP Failed Registrations        : 0
                GVRP Last Pdu Origin            : 0000-0000-0000
                GVRP Registration Type          : Normal
```

Table 18 Description on the fields of the display gvrp statistics command

Field	Description
GVRP Status	GVRP status, that is, enabled or disabled
GVRP Failed Registrations	Failed GVRP registration entries
GVRP Last Pdu Origin	The source of the last GVRP data unit. If GVRP data unit is not received, the system displays 0000-0000-0000; if received from a device, the GVRP data unit received last time is regarded as coming from this MAC address of this device.
GVRP Registration Type	GVRP registration type, that is, fixed, forbidden or normal

display gvrp status

Syntax

display gvrp status

View

Any view

Parameter

None

Description

Use the **display gvrp status** command to view the global GVRP status information.

Example

Display the global status information about GVRP.

```
<SW8800> display gvrp status
     GVRP is enabled
```

The above information means that the global GVRP is enabled.

gvrp

Syntax

gvrp

undo gvrp

View

System view/Ethernet port view

Parameter

None

Description

Use the **gvrp** command to enable GVRP.

Use the **undo gvrp** command to disable GVRP.

By default, GVRP is disabled.

This command can be used to enable/disable global GVRP in system view or enable/disable port GVRP in Ethernet port view.

Before enabling port GVRP, you must enable global GVRP first. In addition, port GVRP must be enabled/disabled on Trunk ports.

Related command: **display gvrp status**.

Example

Enable global GVRP.

```
[SW8800] gvrp
```

gvrp registration

Syntax

gvrp registration { **fixed** | **forbidden** | **normal** }

undo gvrp registration

View

Ethernet port view

Parameter

fixed: Enables to create or register VLAN on the port manually and disables to register or deregister VLAN dynamically.

forbidden: Deregisters all VLANs except VLAN 1 and disables to create or register any other VLAN on the port.

normal: Enables to create, register and deregister VLAN on the port manually or dynamically.

Description

Use the **gvrp registration** command to configure GVRP registration type.

Use the **undo gvrp registration** command to restore the default type.

By default, the registration type is **normal**.

This command can be only used on Trunk port.

Related command: **display gvrp statistics**.

Example

Set the GVRP registration type of Ethernet2/1/1 as **fixed**.

```
[3Com-Ethernet2/1/1] gvrp registration fixed
```

10 ETHERNET PORT CONFIGURATION COMMANDS

Ethernet Port Configuration Commands

broadcast-suppression

Syntax

broadcast-suppression { *ratio* | **bandwidth** *bandwidth* }

undo broadcast-suppression

View

Ethernet port view

Parameter

ratio: Specifies the maximum wire speed ratio of the broadcast traffic allowed on the port. The value range is 1 to 100, and the default value is 50. The smaller the ratio is, the smaller the broadcast traffic is allowed.

bandwidth: Specifies broadcast suppression bandwidth on the port. The value range is 1 to the maximum value of port bandwidth.

Description

Use the **broadcast-suppression** command to set the broadcast suppression ratio or broadcast suppression bandwidth.

Use the **undo broadcast-suppression** command to disable the broadcast suppression function.

The default broadcast suppression ratio is 50%.

You can use the **broadcast-suppression** command repeatedly. The effective broadcast suppression ratio value is the one last updated.

CAUTION:

- You cannot enable both broadcast suppression and multicast suppression simultaneously on the same card. Namely, once you have enabled broadcast suppression on some ports of a card, you cannot enable multicast suppression on the other ports of the card, and vice versa.
- If multicast suppression is enabled, broadcast packets are also suppressed at the same time, while broadcast suppression does not work on multicast packets.

- No distinction is made between known multicast and unknown multicast for multicast suppression.

Related command: **multicast-suppression**.

Example

Set the broadcast suppression ratio to 40.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface Ethernet 2/1/1
[3Com-Ethernet2/1/1] broadcast-suppression 40
```

Set the broadcast suppression bandwidth to 40Mbit.

```
[3Com-Ethernet2/1/1] broadcast-suppression bandwidth 40
```

Disable broadcast suppression.

```
[3Com-Ethernet2/1/1] undo broadcast-suppression
```

copy configuration

Syntax

copy configuration source { *interface-type interface-number* | *interface-name* | **aggregation-group** *agg-id* } **destination** { *interface-list* [**aggregation-group** *agg-id*] | **aggregation-group** *agg-id* }

View

System view

Parameter

interface-type: Source port type.

interface-number: Source port number.

interface-list: Destination port list, *interface-list* = *interface-type interface-number* [**to** *interface-type interface-number*] *&<1-10>*. &<1-10> indicates that the former parameter can be input 10 times repeatedly at most.

agg-id: Source or destination aggregation group ID. If it is a source aggregation group, the port with minimum port number is the source port; if it is a destination aggregation group, the configurations of all its member ports change to be consistent with that of the source.

Description

Use the **copy configuration** command to copy the configuration of a specific port to other ports, to ensure consistent configuration.

Example

Copy the configuration of aggregation group 1 to aggregation group 2.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] copy configuration source aggregation-group 1 destination
aggregation-group 2
```

description

Syntax

description *text*

undo description

View

Ethernet port view

Parameter

text: Port description character string, with 64 characters at most.

Description

Use the **description** command to configure the description character string for Ethernet port.

Use the **undo description** command to cancel the port description character string.

By default, the port description character string is null.

Example

Configure the description character string of Ethernet port Ethernet2/1/1 as lanswitch-interface.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface Ethernet 2/1/1
[3Com-Ethernet2/1/1] description lanswitch-interface
```

display counters

Syntax

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

View

Any view

Parameter

rate: Displays the rate information of the ports in the Up state during the latest sampling period. If this keyword is not specified in the command, the system displays packet counts.

inbound: Displays the import statistic information.

outbound: Displays the export statistic information.

interface-type: Specifies the port type; either Ethernet or Gigabit Ethernet.

Description

Use the **display counters** command to view the statistics on the ports of the specified types. If the port type is not specified, the system displays statistics orderly on all the ports.

Example

Display the inbound statistics on the GigabitEthernet ports.

```
<SW8800> display counters inbound interface GigabitEthernet
Interface    Total(pkts)  BroadCast(pkts)  MultiCast(pkts) Err(pkts)
GE3/2/1   12,345,678,912,345   OverFlow 12,345,678,912,345 1,234,567
GE3/2/2               0             0             0               0
GE3/2/3               0             0             0               0
GE3/2/4               0             0             0               0
 OverFlow :more than 14 decimal digits(7 digits for column "Err").
:not supported.
```

Statistic values are comma-separated decimal numbers. For the Total, BroadCast and MultiCast items, decimal numbers of 14 digits can be displayed at most, and those of more than 14 digits are indicated with "OverFlow"; for the Err item, decimal numbers of 7 digits can be displayed at most, and those of more than 7 digits are indicated with "OverFlow".

display interface

Syntax

display interface [*interface-type* | *interface-type interface-number* [*packets*]]

View

Any view

Parameter

interface-type: Specifies the port type.

interface-number: Specifies the port number.

For parameter description, refer to the **interface** command.

Description

Use the **display interface** command to view the configuration information on the port.

If the port type and number are not specified when displaying the port information, the information of all the ports will be displayed. If only the port type is specified, all the information of the ports of this type will be displayed. If both port type and port number are specified, the information of the designated port will be displayed.

Example

Display configuration information of Ethernet2/1/1.

```
<SW8800> display interface ethernet2/1/1
Ethernet2/1/1 current state : UP
 IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is
00e0-fc00-85ff
 The Maximum Transmit Unit is 1500
 Media type is twisted pair, loopback not set
 Port hardware type is 100_BASE_TX
 100Mbps-speed mode, full-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%
```

```
Allow jumbo frame to pass
MixInsert-Port VPN status:not enable MixInsert access
PVID: 48
Mdi type: auto
Port link-type: access
 Tagged   VLAN ID : none
 Untagged VLAN ID : 48
Last 300 seconds input:  0 packets/sec 61 bits/sec       1%
Last 300 seconds output:  0 packets/sec 0 bits/sec       1%
Input(total):  54 packets, 7465 bytes
         42 broadcasts, 5 multicasts
Input(normal):  54 packets, 7465 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): 1 packets, 64 bytes
         0 broadcasts, 0 multicasts, 0 pauses
Output(normal): 1 packets, 64 bytes
         - broadcasts, - multicasts, 0 pauses
Output: 0 output errors,  - underruns, - buffer failures
         0 aborts, 0 deferred, - collisions, 0 late collisions
         - lost carrier, - no carrier
Receive Packet Peak Value Info: 7215 bytes, happened at 03:30:35 3-7-2001
Transmit Packet Peak Value Info: 64 bytes, happened at 03:30:35 3-7-2001
```

Table 19 Description on the fields of the display interface command

Field	Description
Ethernet2/1/1 current state	The current status of Ethernet port (enabled or disabled)
IP Sending Frames' Format	Ethernet frame format
Hardware address	Port hardware address
The Maximum Transmit Unit	Maximum transmit unit
Media type	Type of media
loopback not set	Port loopback test status
Port hardware type	Port hardware type
100 Mbps-speed mode, full-duplex mode Link speed type is autonegotiation, link duplex type is autonegotiation	Both the duplex mode and the rate are set to auto-negotiation. The rate of 100 Mbps and the mode of full-duplex are adopted after negotiating with its peer
Flow-control is not enabled	Port flow control status
The Maximum Frame Length	Maximum length of the Ethernet frames that can pass the port
Broadcast MAX-ratio	Port broadcast storm suppression ratio
Allow jumbo frame to pass	Jumbo frame is allowed to pass the port
Port VPN status	Port VPN status (enable or not VPN access)
PVID	Port default VLAN ID
Mdi type	Cable type
Port link-type	Port link type
Tagged VLAN ID	The VLANs with packets tagged
Untagged VLAN ID	The VLANs with packets untagged
Last 300 seconds input: 0 packets/sec 0 bits/sec Last 300 seconds output: 0 packets/sec 0 bits/sec	The input/output rate and the passing packet number on this port in the last 300 seconds.

Table 19 Description on the fields of the display interface command

Field	Description
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	The statistics information of input/output packets and errors on this port. "-" indicates that the item doesn't supported by the switch.

display jumboframe configuration

Syntax

display jumboframe configuration

View

Any view

Parameter

None

Description

Use the **display jumboframe configuration** command to view the Jumbo frame configuration on all cards. The supported Jumbo frame length ranges, as well as the default values, may vary from card to card.

Example

Display the current Jumboframe configuration in the system.

```
<SW8800>system-view
[SW8800] display jumboframe configuration
The jumboframe configuration at present:
Slot 2:
 Allow jumbo frame to pass
 The Maximum Frame Length is 1552
```

display port

Syntax

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

View

Any view

Parameter

hybrid: Displays Hybrid port.

trunk: Displays Trunk port.

Description

Use the **display port** command to view the ports in the current system, whose link type is Hybrid or Trunk. If there is any such port, display the corresponding port name and the information about passing VLANs.

Example

Display the Hybrid ports in the current system and the information about passing VLANs.

```
<SW8800> display port hybrid
 Interface                 VLAN passing:
Ethernet3/1/1            Tagged  : 3, 5, 7, 9, 11
                            Untagged: 1-2, 4, 6,
Ethernet3/1/2            Tagged  : none
                            Untagged: 1
```

The information above shows that the current system has two hybrid ports: Ethernet 3/1/1 and Ethernet 3/1/2. The tagged VLANs that pass Ethernet3/1/1 are 3, 5, 7, 9, and 11, and the untagged VLANs that pass it are 1, 2, 4, and 6. No tagged VLAN passes Ethernet3/1/2, and untagged VLAN 1 passes Ethernet 3/1/2.

Display the Trunk ports in the current system.

```
<SW8800> display port trunk
Interface                 VLAN passing
Ethernet3/1/3            1, 3-5, 10
Ethernet3/1/4            none
Ethernet3/1/7            1
```

The information above shows that the current system has three Trunk ports: Ethernet 3/1/3, Ethernet 3/1/4, Ethernet2/1/7. The VLANs that pass Ethernet 3/1/3 are 1, 3, 4, 5, and 10. No VLAN passes Ethernet 3/1/4. VLAN 1 passes Ethernet 3/1/3.

duplex

Syntax

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

undo duplex

View

Ethernet port view

Parameter

auto: Port auto-negotiation attribute.

full: Port full-duplex attribute.

half: Port half-duplex attribute.

Description

Use the **duplex** command to configure the duplex attribute of the Ethernet port.

Use the **undo duplex** command to restore the duplex attribute of the port to default auto-negotiation mode.

By default, the duplex attribute is **auto**.

Related command: **speed**.

Example

Configure the Ethernet port Ethernet2/1/1 as auto-negotiation attribute.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface Ethernet 2/1/1
[3Com-Ethernet2/1/1] duplex auto
```

flow-control

Syntax

flow-control

undo flow-control

View

Ethernet port view

Parameter

None

Description

Use the **flow-control** command to enable flow control feature on the Ethernet port to avoid discarding data packets due to congestion.

Use the **undo flow-control** command to disable flow control feature.

By default, flow control on the Ethernet port is disabled.

Example

Enable flow control on Ethernet2/1/1.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface Ethernet 2/1/1
[3Com-Ethernet2/1/1] flow-control
```

flow-interval

Syntax

flow-interval *interval*

undo flow-interval

View

Ethernet port view

Parameter

interval: Interval of performing statistics on ports in seconds. It is 300 seconds by default.

Description

Use the **flow interval** command to set the interval of performing statistics on ports. The switch performs the statistics about the average speed during the interval.

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

Related command: **display interface**.

Example

Set the interval of performing statistics on Ethernet3/1/1 to 100 seconds.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800]interface Ethernet 3/1/1
[3Com-Ethernet3/1/1] flow-interval 100
```

Restore the interval o f performing statistics on Ethernet 3/1/1 to the default value.

```
[3Com-Ethernet3/1/1] undo flow-interval
```

link-status hold

Syntax

link-status hold *hold-time*

undo link-status hold

View

System view

Parameter

hold-time: Sets time interval (in seconds) for port suppression. The value 0 indicates that port suppression is not enabled. By default, the time interval is 3 seconds.

Description

Use the **link-status hold** *hold-time* command to set port hold time. If the Down/Up operation is implemented on ports too frequently, the switch may fail. Therefore, the function is provided to prohibit frequent change of the port status.

Use the **undo link-status hold** command to restore the default port hold time, 3 seconds.

Related command: **display interface**.

Example

Set the port hold time to 5 seconds.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] link-status hold 5
```

interface

Syntax

interface *interface-type interface-number*

View

System view

Parameter

interface-type: Specifies the port type. It can be Aux, Ethernet, Loopback, M-Ethernet, NULL, VLAN-interface, GigabitEthernet or 10-GigabitEthernet.

interface-number: Specifies the port number. It adopts *slot-number/subslot-number/ port-number* format. *slot-number* specifies the I/O Module slot number of the port. For Switch 8807, it ranges from 2 to 6. For Switch 8810, it ranges from 0 to 3 and 6 to 9 (slot number 4 and 5 are Fabric). For Switch 8814, it ranges from 0 to 5 and 8 to 13 (slot number 6 and 7 are Fabric). *subslot-number* specifies the sub-slot number of the port and ranges from 1 to 3. *port-number* specifies the port number on the daughter card. It is 1 or ranges from 1 to 12, 20, or 48, depending on the module type. M-Ethernet is used to update and maintain. It ranges from 0/0/0.

Description

Use the **interface** command to enter various types of Ethernet port views.

Before you can configure the related parameters of a type of Ethernet port, you must first use this command to enter the Ethernet port view of this type.

Example

Enter the Ethernet2/1/1 port view.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface ethernet2/1/1
```

jumboframe enable

Syntax

jumboframe enable [*jumboframe-value*] **slot** *slot-num*

undo jumboframe enable

View

System view

Parameter

slot-num: Specifies the slot number of the card.

jumboframe-value: specifies the maximum size of jumbo frames permitted to pass the card.

Description

Use the **jumboframe enable** command to permit jumbo frames to pass the card on the specified slot and set the maximum size of Jumbo frames.

Use the **jumboframe disable slot** command to prohibit jumbo frames from passing the card on the specified slot.

By default, jumbo frame is permitted to pass cards.

Related command: **display jumboframe configuration**.

The system supports discrete values of Jumbo frame lengths ranging from 1536 to 10240. However, effective Jumbo frame values fall into several sections: the effective Jumbo frame value for the 1536-1552 section is 1552, that for the 1553-9022 section is 9022, that for the 9023-9192 section is 9192, and that for the 9193-10240 section is 10240.

Example

Permit jumbo frames to pass the card on slot 6 and set the maximum size of Jumbo frames to 9022 .

```
<SW8800>system-view
[SW8800] jumboframe enable 9022 slot 6
```

loopback

Syntax

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

undo loopback

View

Ethernet port view

Parameter

external: Ethernet port in external loop mode. Presently, the Ethernet ports of the 3Com Switch 8800 Family Series Routing Switches do not support this mode.

internal: Ethernet port in internal loop mode.

Description

Use the **loopback** command to set the Ethernet port in loop mode.

Use the **undo loopback** command to cancel the loop setting.

By default, the Ethernet port is not in loop mode.

Example

Configure Ethernet2/1/1 in internal loop mode.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800]interface ethernet2/1/1
[3Com-Ethernet2/1/1] loopback internal
```

mdi

Syntax

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

undo mdi

View

Ethernet port view

Parameter

across: Network cable type is cross-over cable.

auto: Network cable will be recognized whether it is straight-through cable or cross-over cable.

normal: Network cable of the port is straight-through cable.

Description

Use the **mdi** command to configure the network cable type of the Ethernet ports. Use the **undo mdi** command to restore the default type.

By default, the network cable type will be recognized automatically.

Note that the settings only take effect on the 10/100 Mbps and 10/100/1000 Mbps electrical ports.

Example

Configure the network cable type of Ethernet port Ethernet2/1/1 as auto.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface ethernet2/1/1
[3Com-Ethernet2/1/1] mdi auto
```

multicast-suppression

Syntax

multicast-suppression { *ratio* | **bandwidth** *bandwidth* }

undo multicast-suppression

View

Ethernet port view

Parameter

ratio: Specifies the maximum wire speed ratio of the multicast traffic allowed on the Ethernet port. The value range is 1 to 100, and the default value is 50. The smaller the ratio is, the smaller the multicast traffic is allowed.

bandwidth: Specifies multicast suppression bandwidth on the port. The value range is 1 to the maximum value of port bandwidth.

Description

Use the **multicast-suppression** command to set the multicast suppression ratio or broadcast suppression bandwidth.

Use the **undo multicast-suppression** command to disable the broadcast suppression function.

The default multicast suppression ratio is 100%.

You can use the **multicast-suppression** command repeatedly. The effective multicast suppression ratio value is the one last updated.

CAUTION:

- You cannot enable both multicast suppression and broadcast suppression simultaneously on the same card. Namely, once you have enabled broadcast suppression on some ports of a card, you cannot enable multicast suppression on the other ports of the card, and vice versa. Although the commands are based on ports, the mutual exclusion between these two commands is based on cards.
- If multicast suppression is enabled, broadcast packets are also suppressed at the same time, while broadcast suppression does not work on multicast packets.
- No distinction is made between known multicast and unknown multicast for multicast suppression.

Related command: **broadcast-suppression**.

Example

Set the multicast suppression ratio to 40%.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800]interface Ethernet 2/1/1
[3Com-Ethernet2/1/1] multicast-suppression 40
```

Set the multicast suppression bandwidth to 40Mbit.

```
[3Com-Ethernet2/1/1] multicast-suppression bandwidth 40
```

Disable the multicast suppression function.

```
[3Com-Ethernet2/1/1] undo multicast-suppression
```

port access vlan

Syntax

port access vlan *vlan-id*

undo port access vlan

View

Ethernet port view

Parameter

vlan-id: VLAN ID defined in IEEE802.1Q, ranging from 2 to 4094.

Description

Use the **port access vlan** command to add the access port into a specified VLAN.

Use the **undo port access vlan** command to cancel the access port from the VLAN.

The condition for using this command is that the VLAN indicated in *vlan-id* must exist.

Example

Join Ethernet2/1/1 port to VLAN3 (VLAN3 has existed).

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface ethernet2/1/1
[3Com-Ethernet2/1/1] port access vlan 3
```

port hybrid pvid vlan

Syntax

port hybrid pvid vlan *vlan-id*

undo port hybrid pvid

View

Ethernet port view

Parameter

vlan-id: VLAN ID defined in IEEE802.1Q, ranging from 1 to 4094 and the default *vlan-id* is 1.

Description

Use the **port hybrid pvid vlan** command to configure the default VLAN ID of the local hybrid port.

Use the **undo port hybrid pvid** command to restore the default VLAN ID of the local hybrid port.

The default VLAN ID of local hybrid port shall be consistent with that of the peer one, otherwise, the packet cannot be properly transmitted.

Related command: **port link-type**.

Example

Configure the default VLAN of the hybrid port Ethernet2/1/1 to 100.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface ethernet2/1/1
[3Com-Ethernet2/1/1] 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 port view

Parameter

vlan-id-list: *vlan-id-list* = [*vlan-id1* [**to** *vlan-id2*]]&<1-10>: Specifies which VLAN the hybrid port will be added to. It can be discrete. The *vlan-id* ranges from 1 to 4,094. &<1-10> indicates that the former parameter can be input 10 times repeatedly at most.

tagged: Packet of specified VLAN will have tag.

untagged: Packet of specified VLAN will not have tag.

Description

Use the **port hybrid vlan** command to join the hybrid port to specified existing VLAN.

Use the **undo port hybrid vlan** command to cancel the hybrid port from the specified VLAN.

Hybrid port can belong to multiple VLANs. If the **port hybrid vlan** *vlan-id-list* { **tagged** | **untagged** } command is used for many times, the VLANs carried by the hybrid port is the set of *vlan-id-list*.

This command can be used on condition that the VLAN specified with *vlan-id must have been existed.*

Related command: **port link-type**.

Example

Join hybrid port Ethernet2/1/1 to VLAN of 2, 4 and 50-100, and these VLAN will have tags.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface ethernet2/1/1
[3Com-Ethernet2/1/1] 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 port view

Parameter

access: Configures the port as access port.

hybrid: Configures the port as hybrid port.

trunk: Configures the port as trunk port

Description

Use the **port link-type** command to configure the link type of Ethernet port.

Use the **undo port link-type** command to restore the port as default status, i.e. access port.

You can configure three types of ports concurrently on the same switch, but you cannot switch between trunk port and hybrid port. You must turn it first into access port and then set it as other type. For example, you cannot configure a trunk port directly as hybrid port, but first set it as access port and then as hybrid port.

By default, the link type of the port is Access port.

Example

Configure Ethernet port Ethernet2/1/1 as trunk port.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface ethernet2/1/1
[3Com-Ethernet2/1/1] port link-type trunk
```

port-mode

Syntax

port-mode { **wan** | **lan** }

undo port-mode

View

Ethernet port view

Parameter

wan: Configures the port works in WAN mode, and then only common data exchange can be implemented on the port.

lan: Configures the port works in LAN mode, and then data can be transferred on the port.

Description

Use the **port-mode** command to configure network mode available on the port. Most ports adopt the LAN mode for general data exchange. The port must work in WAN mode, however, if it needs to transfer data (such as in fiber transmission).

Use the **undo port-mode** command to restore the default mode of the port.

By default, Ethernet ports work in LAN mode. 10GE ports support WAN mode.

Example

Set port GigabitEthernet2/1/1 to work in WAN mode.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface GigabitEthernet2/1/1
[3Com-GigabitEthernet2/1/1] port-mode wan
```

Restore the default (LAN) mode on port GigabitEthernet2/1/1.

```
[3Com-GigabitEthernet2/1/1] undo port-mode
```

port trunk permit vlan

Syntax

port trunk permit vlan { *vlan-id-list* | **all** }

undo port trunk permit vlan { *vlan-id-list* | **all** }

View

Ethernet port view

Parameter

vlan-id-list: vlan-id-list = [*vlan-id1* [**to** *vlan-id2*]]&<1-10> is the VLAN range joined by the trunk port. It can be discrete. The vlan-id ranges from 2 to 4,094. &<1-10> indicates that the former parameter can be input 10 times repeatedly at most.

all: Joins the trunk port to all VLANs.

Description

Use the **port trunk permit vlan** command to join trunk port to specified VLAN.

Use the **undo port trunk permit vlan** command to cancel trunk port from specified VLAN.

Trunk port can belong to multiple VLANs. If the **port trunk permit vlan** command is used many times, then the VLAN enabled to pass on trunk port is the set of these *vlan-id-list*.

Related command: **port link-type**.

Example

Remove the trunk port from the default VLAN.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface Ethernet2/1/1
[3Com-Ethernet2/1/1] undo port trunk permit vlan 1
```

Add the trunk port to all VLANs.

```
[3Com-Ethernet2/1/1] port trunk permit vlan all
```

port trunk pvid vlan

Syntax

port trunk pvid vlan *vlan-id*

undo port trunk pvid

View

Ethernet port view

Parameter

vlan-id: VLAN ID defined in IEEE802.1Q, ranging from1 to 4,094 and the default *vlan-id* is 1.

Description

Use the **port trunk pvid vlan** command to configure the default VLAN ID of trunk port.

Use the **undo port trunk pvid** command to restore the default VLAN ID of the port.

The default VLAN ID of local trunk port should be consistent with that of the peer one, otherwise, the packet cannot be properly transmitted.

Related command: **port link-type**.

Example

Configure the default VLAN of the trunk port Ethernet2/1/1 to 100.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface Ethernet2/1/1
[3Com-Ethernet2/1/1] port trunk pvid vlan 100
```

reset counters interface

Syntax

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

View

User view

Parameter

interface-type: Specifies the port type.

interface-number: Specifies the port number.

For parameter description, refer to the **interface** command.

Description

Use the **reset counters interface** command to reset the statistical information on the port and count the related information again on the port for the user.

If the port type and number are not specified when clearing the port information, information of all ports on the switch will be cleared. If only the port type is specified, all the information on the ports of this type will be cleared. If both port type and port number are specified, the information on the designated port will be cleared.

You cannot clear statistics on the 802.1x-enabled port.

Example

Clear the statistical information of Ethernet port Ethernet2/1/1.

```
<SW8800> reset counters interface ethernet2/1/1
```

shutdown

Syntax

shutdown

undo shutdown

View

Ethernet port view

Parameter

None

Description

Use the **shutdown** command to disable the Ethernet port.

Use the **undo shutdown** command to enable the Ethernet port.

By default, the Ethernet port is enabled.

Example

Enable Ethernet port Ethernet2/1/1.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface Ethernet2/1/1
[3Com-Ethernet2/1/1] undo shutdown
```

speed

Syntax

speed { **10** | **100** | **1000** | **10000** | **auto** }

undo speed

View

Ethernet port view

Parameter

10: Speed on the port is 10 Mbps.

100: Speed on the port is 100 Mbps.

1000: Speed on the port is 1000 Mbps.

10000: Speed on the port is 10 Gbps.

auto: Port speed is in peer auto-negotiation status.

Description

Use the **speed** command to configure the port speed.

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

The optional parameters of this command are determined by the port types and duplex modes. For example, the 10/100/1000 Mbps electrical ports support three optional parameters including 10 Mbps, 100 Mbps, and 1000 Mbps. You can select proper port speed as you require. But when the duplex mode is changed into half duplex mode, the port speed can be set to 1000 Mbps or **auto**.

By default, the speed is **auto**.

Related command: **duplex**.

Example

Configure Ethernet port Ethernet2/1/1 port speed as 100 Mbps.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface Ethernet2/1/1
[3Com-Ethernet2/1/1] speed 100
```

vlan-vpn enable

Syntax

vlan-vpn enable

undo vlan-vpn

View

Ethernet port view

Parameter

None

Description

Use the **vlan-vpn enable** command to enable port VLAN VPN.

Use the **undo vlan-vpn** command to disable port VLAN VPN.

Note that if anyone of GComware, STP, NTP or 802.1x has been enabled on a port, VLAN VPN cannot be enabled on it.

By default, the port VLAN VPN is disabled.

Example

Enable VLAN VPN on Ethernet2/1/1.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface Ethernet2/1/1
[3Com-Ethernet2/1/1] vlan-vpn enable
```

11 ETHERNET LINK AGGREGATION CONFIGURATION COMMANDS

Ethernet 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

System view

Parameter

interface *interface-type interface-number* [**to** *interface-type interface-number*]: Specifies a port or ports. The command without the parameter **to** specifies one port, while the command with the parameter **to** specifies several contiguous ports. *interface-type* indicates port type. *interface-number* indicates port number. For more information, see the parameter description of the **interface** command.

Description

Use the **debugging lacp packet** command to enable LACP packet debugging for the port. If you do not specify a port, the command enables packet debugging on all LACP-enabled ports.

Use the **undo debugging lacp packet** command to disable LACP packet debugging for the port.

Example

Enable LACP packet debugging for Ethernet port Ethernet1/1/1.

```
<SW8800> debugging lacp packet interface ethernet1/1/1
```

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

Parameter

interface *interface-type interface-number* [**to** *interface-type interface-number*]: Specifies a port or ports. The command without the parameter **to** specifies one port, while the command with the parameter **to** specifies several contiguous ports. *interface-type* indicates port type. *interface-number* indicates port number. For more information, see the parameter description of the **interface** command.

actor-churn: Actor-churn state machine debugging switch.

mux: MUX state machine debugging switch.

partner-churn: Partner-churn state machine debugging switch.

ptx: PTX state machine debugging switch.

rx: RX state machine debugging switch.

all: debugging switch of all state machines.

Description

Use the **debugging lacp state** command to enable LACP state machine debugging for the port.

Use the **undo debugging lacp state** command to disable LACP state machine debugging for the port.

Example

Enable debugging of all LACP state machines.

```
<SW8800> debugging lacp state all
```

debugging link-aggregation error

Syntax

debugging link-aggregation error

undo debugging link-aggregation error

View

User view

Parameter

None

Description

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

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

Example

Enable link aggregation error debugging.

```
<SW8800> debugging link-aggregation error
```

debugging link-aggregation event

Syntax

debugging link-aggregation event

undo debugging link-aggregation event

View

User view

Parameter

None

Description

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

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

Example

Enable link aggregation event debugging.

```
<SW8800> debugging link-aggregation event
```

display lacp system-id

Syntax

display lacp system-id

View

Any view

Parameter

None

Description

Use the **display lacp system-id** command to display the device ID of local system, including system priority and system MAC address.

Related command: **link-aggregation**.

Example

Display the device ID of the local system.

```
<SW8800> display lacp system-id
 Actor System ID: 0x8000, 00e0-fc00-0100
```

Table 20 Description on the fields of the display lacp system-id command

Field	Description
Actor System ID	The device ID of the local system, including system priority and system MAC address.

display link-aggregation summary

Syntax

display link-aggregation summary

View

Any view

Parameter

None

Description

Use the **display link-aggregation summary** command to view summary information of all aggregation groups, including local device ID, aggregation group ID, aggregate group type, peer device ID, number of Selected ports, number of Standby ports, load sharing type and master port number.

Example

Display summary information of all aggregation information.

```
<SW8800> display link-aggregation summary
Aggregation Group Type:D -- Dynamic, S -- Static , M -- Manual
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Actor ID: 0x8000, 00e0-fc23-0d90

  AL  AL   Partner ID            Select Standby Share Master
  ID  Type                       Ports  Ports   Type  Port
------------------------------------------------------------------------
------------
  1   M    none             2      0       Shar  GigabitEthernet3/1/1
  3   M    none             4      0      Shar  Ethernet4/1/45
```

Table 21 Description on the fields of the display link-aggregation summary command

Field	Description
Actor ID	Local device ID
AL ID	Aggregation group ID
AL Type	Aggregation group type
Partner ID	Peer device ID
Select Ports	Number of selected ports
Standby Ports	Number of standby ports
Share Type	Load sharing type
Master Port	Master port number

display link-aggregation verbose

Syntax

display link-aggregation verbose [*agg-id*]

View

Any view

Parameter

agg-id: Aggregation group ID, which must be existing ones, in the range of 1 to 920. IDs 1 through 31 indicate manual or static aggregation groups; IDs 32 through 64 are reserved; IDs 65 through 192 are Routed Trunks; IDs 193 through 920 indicate dynamic aggregation groups.

Description

Use the **display link-aggregation verbose** command to view detailed information of a designated port, including aggregation group ID, aggregation group type, load sharing type, aggregation group description and detailed local information (system ID, member ports, port status, port priority, flag, operation key, link status) and detailed remote information (local port, indexes of remote ports, port priority, flag, operation key and system ID, here local and remote are in a relative sense).

Note that since the manual aggregation group cannot get the information of the peer end, every item of the peer end is displayed as 0, which does not indicate the actual status of the peer system.

Example

Display the detailed information of aggregation group 5.

```
<SW8800>display link-aggregation verbose 5
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing

Aggregation ID: 5, AggregationType: Manual,   Loadsharing Type: Shar
Aggregation Description:
System ID: 0x0, 00e0-fc00-1312
Port Status: S -- Selected,  T -- sTandby,  U -- Unselected
Local:
    Port                  Status  Priority Flag Oper-Key Link-Status
------------------------------------------------------------------------
------------
    Ethernet9/1/9           S       32768    0x00 8        Down
    Ethernet9/1/10          S       32768    0x00 8        Down
Remote:
    Actor                   Partner Priority Flag Oper-Key SystemID
------------------------------------------------------------------------
------------
    Ethernet9/1/9     0     0       0x00 0        0x0,0000-0000-0000
    Ethernet9/1/10    0     0       0x00 0        0x0,0000-0000-0000
```

Table 22 Description on the fields of the display link-aggregation verbose command

Field	Description
Aggregation ID	Aggregation group ID
Aggregation Type	Aggregation group type, which can be dynamic, static and manual
Loadsharing Type	Load sharing type
Aggregation Description	Aggregation group description
System ID	Local device ID

Table 22 Description on the fields of the display link-aggregation verbose command

Field	Description
Port State	Port state
Local: Port Status Priority Flag Oper-key Link-Status	Other information of the local end, including member ports, port state, port priority, flag bit , operation key and link status.
Remote: Actor Partner Priority Flag Oper-key SystemID	Detailed information about the peer device, including local port, peer port index, port priority, flag, operation key and device ID

display link-aggregation interface

Syntax

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

View

Any view

Parameter

interface { *interface-type interface-number* [**to** *interface-type interface-number*]: Specifies a port or ports. Without the parameter **to**, one port is specified. You can specify multiple contiguous ports with the parameter **to**. *interface-type* specifies port type and *interface-number* specifies port number. For more information, see the parameter item for the **interface** command.

Description

Use the **display link-aggregation interface** command to view detailed link aggregation information at a designated port, including aggregation group ID for the port, port priority, operation key, flag, peer information (system ID, port number, port priority, operation key, flag).

Note that since the manual aggregation group cannot get the information of the peer end, every item of the peer end is displayed as 0, which does not indicate the actual status of the peer system.

Example

Display detailed link aggregation information of link aggregation group.

```
<SW8800> display link-aggregation interface ethernet2/1/1
 Ethernet2/1/1:
   Attached AggID: 1
   Local:
     Port-Priority: 32768, Oper key: 1, Flag: 0x00
   Remote:
     System ID: 0x0, 0000-0000-0000
     Port Number: 0, Port-Priority: 0, Oper-key: 0, Flag: 0x00
Received LACP Packets: 0 packet(s), Illegal: 0 packet(s)
   Sent LACP Packets: 0 packet(s)
```

Table 23 Description on the fields of the display link-aggregation interface command

Field	Description
Attached AggID	Aggregation group ID for the specified port

Table 23 Description on the fields of the display link-aggregation interface command

Field	Description
Local: Port-Priority: 32768, Oper key: 1, Flag: 0x00	Port priority, operation key, LACP state flag of the local end
Remote: System ID: 0x0, 0000-0000-0000 Port Number: 0, Port-Priority: 0, Oper-key: 0, Flag: 0x00	Device ID, port priority, operation key, LACP state flag of the remote end
Received LACP Packets: 0 packet(s), Illegal: 0 packet(s)	Received LACP packets
Sent LACP Packets: 0 packet(s)	Sent LACP packets

lacp enable

Syntax

lacp enable

undo lacp enable

View

Ethernet port view

Parameter

None

Description

Use the **lacp enable** command to enable LACP.

Use the **undo lacp enable** command to disable LACP.

Example

Enable LACP for Ethernet port Ethernet1/1/1.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface Ethernet1/1/1
[3Com-Ethernet1/1/1] lacp enable
```

lacp port-priority

Syntax

lacp port-priority *port-priority-value*

undo lacp port-priority

View

Ethernet port view

Parameter

port-priority-value: Port priority, in the range of 0 to 65,535. By default, it is 32,768.

Description

Use the **lacp port-priority** command to configure port priority.

Use the **undo lacp port-priority** command to restore the default port priority.

Related command: **display link-aggregation verbose** and **display link-aggregation interface**.

Example

Set port priority to 64.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface Ethernet1/1/1
[3Com-Ethernet1/1/1] lacp port-priority 64
```

lacp system-priority

Syntax

lacp system-priority *system-priority-value*

undo lacp system-priority

View

System view

Parameter

system-priority-value: System priority, in the range of 0 to 65,535. By default, it is 32,768.

Description

Use the **lacp system-priority** command to configure system priority.

Use the **undo lacp system-priority** command to restore the default system priority.

Related command: **display lacp system-id**.

Example

Set system priority to 64.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] lacp system-priority 64
```

link-aggregation

Syntax

link-aggregation *interface-name1* **to** *interface-name2* [**both**]

View

System view

Parameter

interface-name1: Starting range value of Ethernet port joined the Ethernet link aggregation.

interface-name2: Last range value of Ethernet port joined the Ethernet link aggregation.

both: Specifies the aggregation group to balance load for inbound and outbound packets.

Description

Use the **link-aggregation** command to configure a series of ports to aggregation port.

Related command: **link-aggregation group** *agg-id* **mode**, **port link-aggregation group**.

When a port is added into an aggregation group, the original ARP information of the port will be lost.

Example

Configure to balance load for inbound and outbound packets.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] link-aggregation ethernet2/1/1 to ethernet2/1/2 both
```

link-aggregation group agg-id description

Syntax

link-aggregation group *agg-id* **description** *alname*

undo link-aggregation group *agg-id* **description**

View

System view

Parameter

agg-id: Aggregation group ID, in the range of 1 to 920. IDs 1 though 31 indicate manual or static aggregation groups; IDs 32 through 64 are reserved; IDs 65 though 192 indicate Routed Trunks; IDs 193 through 920 indicate dynamic aggregation groups.

alname: Aggregation group name, character string with 1 to 32 characters.

Description

Use the **link-aggregation group** *agg-id* **description** command to configure description for an aggregation group.

Use the **undo link-aggregation group** *agg-id* **description** command to delete aggregation group description.

Note that you cannot configure the description for a dynamic aggregation group.

Related command: **display link-aggregation verbose**.

Example

Configure myal1 as the description of aggregation group 22.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] link-aggregation group 22 description myal1
```

link-aggregation group agg-id mode

Syntax

link-aggregation group *agg-id* **mode** { **manual** | **static** }

undo link-aggregation group *agg-id*

View

System view

Parameter

agg-id: Aggregation group ID, in the range of 1 to 920. IDs 1 though 31 indicate manual or static aggregation groups; IDs 32 through 64 are reserved; IDs 65 though 192 indicate Routed Trunks; IDs 193 through 920 indicate dynamic aggregation groups.

Description

Use the **link-aggregation group** *agg-id* **mode** command to create an aggregation group.

Use the **undo link-aggregation group** command to delete an aggregation group.

Related command: **display link-aggregation summary**.

Port aggregation includes manual aggregation, static aggregation and dynamic aggregation.

- In the manual aggregation mode, ports working at different rates can be aggregated. Manual aggregation can be load balancing aggregation if the aggregation resource is available. In this case, if the traffic rate shared by a low-rate port exceeds the maximum rate of the port, packets may be lost.
- In the static aggregation mode, ports working at different rates can also be aggregated. However, the Selected/Standby state of statically aggregated ports is determined by the transmission rate. Only the ports with the maximum rate and in full-duplex mode can be selected to forward traffic, while other standby ports do not forward traffic.

Example

Create manual aggregation group 22.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] link-aggregation group 22 mode manual
```

port link-aggregation group

Syntax

port link-aggregation group *agg-id*

undo port link-aggregation group

View

Ethernet port view

Parameter

agg-id: Aggregation group ID, in the range of 1 to 920. IDs 1 though 31 indicate manual or static aggregation groups; IDs 32 through 64 are reserved; IDs 65 though 192 indicate Routed Trunks; IDs 193 through 920 indicate dynamic aggregation groups.

Description

Use the **port link-aggregation group** command to add an Ethernet port into a manual or static aggregation group. Use the **undo port link-aggregation group** command to delete an Ethernet port from an aggregation group.

Related command: **display link-aggregation verbose**.

When a port is added into an aggregation group, the original ARP information of the port will be lost.

Example

Add Ethernet2/1/1 into aggregation group 22.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface Ethernet2/1/1
[3Com-Ethernet2/1/1] port link-aggregation group 22
```

reset lacp statistics

Syntax

reset lacp statistics [**interface** *interface-type interface-number* [**to** *interface-type interface-number*]]

View

System view

Parameter

interface *interface-type interface-number* [**to** *interface-type interface-number*]: Specifies a port or ports. The command without the parameter **to** specifies one port, while the command with the parameter **to** specifies several contiguous ports. *interface-type* indicates port type. *interface-number* indicates port number. For more information, refer to the parameter description of the **interface** command.

Description

Use the **reset lacp statistics** command to clear LACP statistics for the port. If you do not specify a port, the command clears LACP statistics for all the ports.

Related command: **display link-aggregation interface**.

Example

Clear LACP statistics for all Ethernet ports.

```
<SW8800> reset lacp statistics
```

12 MAC ADDRESS TABLE MANAGEMENT COMMANDS

MAC Address Table Management Commands

display mac-address aging-time

Syntax

display mac-address aging-time

View

Any view

Parameter

None

Description

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

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

Example

Display the aging time of the dynamic entry in the MAC address table.

```
<SW8800> display mac-address aging-time
mac-address aging-time: 300s
```

The above information indicates that the aging time of the dynamic entry in the MAC address is 300s.

display mac-address

Syntax

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

View

Any view

Parameter

mac-addr: Specifies the MAC address.

vlan-id: Specifies the VLAN ID.

static: Static table entry, that is no aging, If the configuration is saved, it can be restored after the switch is reset.

dynamic: Dynamic table entry, which will be aged.

interface-type: Specifies the interface type.

interface-number: Specifies the interface number.

count: the display information will only contain the sum number of MAC addresses in the MAC address table if user choice this parameter when using this command.

Description

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

When managing the Layer-2 addresses of the switch, the administrator can perform this command to view such information as the Layer-2 address table, address status (static or dynamic), Ethernet port of the MAC address, VLAN of the address, and system address aging time.

Related command: mac-address, mac-address timer.

Example

Show the information of the entry with MAC address at 00e0-fc01-0101

```
<SW8800> display mac-address 00e0-fc01-0101
MAC ADDR          VLAN ID  STATE          PORT INDEX    AGING TIME(s)
00e0-fc01-0101  1        Learned         Ethernet1/1/1     300
```

Table 24 Description on the fields of the display mac-address command on display

Field	Description
MAC ADDR	The destination MAC address
VLAN ID	The VLAN of the MAC address
STATE	The state of the item, which can be Learned, Config static
PORT INDEX	The forwarding port
AGING TIME(s)	The aging time

mac-address

Syntax

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

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

View

System view

Parameter

static: Static table entry, lost after resetting switch.

dynamic: Dynamic table entry, which will be aged.

mac-addr: Specifies the MAC address.

For detailed description on *interface-type* and *interface-number* see Port Configuration section of this manual.

vlan-id: Specifies the VLAN ID.

Description

Use the **mac-address** command to add/modify the MAC address table entry.

Use the **undo mac-address** command to cancel the MAC address table entry

If the input address has been existed in the address table, the original entry will be modified. That is, replace the interface pointed by this address with the new interface and the entry attribute with the new attribute (dynamic entry, static entry and permanent entry).

All the (MAC unicast) addresses on a certain interface can be deleted. User can choose to delete any of the following addresses: address learned by system automatically, dynamic address configured by user, static and permanent addresses configured by user.

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

Example

Configure the port number corresponding to the MAC address 00e0-fc01-0101 as Ethernet2/1/1 in the address table, and sets this entry as static entry.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] mac-address static 00e0-fc01-0101 interface ethernet 2/1/1 vlan 2
```

mac-address max-mac-count

Syntax

mac-address max-mac-count *count*

undo mac-address max-mac-count

View

Ethernet port view

Parameter

count: Maximum number of MAC addresses learned by a port, ranging from 0 to 14,336, the value of 0 means that address learning is disabled.

Description

Use the **mac-address max-mac-count** command to set the maximum number of MAC addresses learned by an Ethernet port.

Use the **undo mac-address max-mac-count** command to remove the limit on the maximum number of MAC addresses learned by an Ethernet port.

By default, a port can learn as many MAC addresses as on an I/O Module. You can change the default value by using this command: if you set the value to *count*, and when the number of MAC addresses learned by the port reaches this value,

this port will no longer learn any more MAC addresses; and you can use the **undo mac-address max-mac-count** command to remove the limit on the number.

- The maximum number of MAC addresses on an I/O Module ranges from 12 K to 16 K depending on various software versions and module types.
- The aforementioned number of MAC addresses includes only the MAC addresses learned by the switch dynamically, and excludes those configured by the user.
- When executing the **mac-address max-mac-count** command, if the current number of MAC addresses exceeds the threshold value, the switch neither delete the present MAC address entries nor learn new MAC address until the number of entries less than the threshold value after some entries are aged out.

Related command: **mac-address** and **mac-address timer**.

Example

Set the maximum number of MAC addresses learned by Ethernet port Ethernet3/1/3 to 600.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface Ethernet3/1/3
[3Com-Ethernet3/1/3] mac-address max-mac-count 600
```

mac-address max-mac-count enable

Syntax

mac-address max-mac-count enable { **alarm** | **forward** }*

undo mac-address max-mac-count enable { **alarm** | **forward** }*

View

Ethernet port view

Parameter

None

Description

Use the **mac-address max-mac-count enable** { **alarm** | **forward** }* command to enable the switch to send alarms to the network administrator and forward the packets whose source MAC addresses are not learned by the port when the number of MAC addresses automatically learned by the port reaches the threshold value.

Use the **undo mac-address max-mac-count enable** { **alarm** | **forward** }* command to disable the function.

Use the **mac-address max-mac-count enable forward** command to enable the switch to forward the packets whose source MAC addresses are not learned by the port when the number of MAC addresses automatically learned by the port reaches the threshold value.

Use the **undo mac-address max-mac-count enable forward** command to enable the switch to drop the packets whose source MAC addresses are not learned by the port when the number of MAC addresses automatically learned by the port reaches the threshold value.

Use the **mac-address max-mac-count enable alarm** command to enable the switch to send alarms to the network administrator when the number of MAC addresses automatically learned by the port reaches the threshold value.

Use the **undo mac-address max-mac-count enable alarm** command to remove this configuration.

By default, the switch forwards the packets whose source MAC addresses are not learned by the port when the number of MAC addresses automatically learned by the port reaches the threshold value.

After the **mac-address max-mac-count enable** { **alarm** | **forward** }***** command is executed, if the MAC addresses learned by a port reach the maximum number of MAC addresses that the port can learned, the port will send an alarm to network administrator to prompt that the port will no longer learn any MAC addresses.

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

- The maximum number of MAC addresses on an I/O Module ranges from 12 K to 16 K depending on various software versions and module types.
- The aforementioned number of MAC addresses includes only the MAC addresses learned by the switch dynamically, and excludes those configured by the user.
- When executing the **mac-address max-mac-count** command, if the current number of MAC addresses exceeds the threshold value, the switch neither delete the present MAC address entries nor learn new MAC address until the number of entries less than the threshold value after some entries are aged out.

Example

Set the maximum number of MAC addresses learned by Ethernet port Ethernet3/1/3 to 600, and the switch will give an alarm to the network administrator and forward the packets when the number of MAC addresses learned exceeds 600.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface Ethernet3/1/3
[3Com-Ethernet3/1/3] mac-address max-mac-count 600
[3Com-Ethernet3/1/3] mac-address max-mac-count enable forward alarm
```

Set the maximum number of MAC addresses learned by Ethernet3/1/3 to 600. When the number of MAC addresses exceeds this value, the switch drops the packets whose MAC addresses are not learned by the port.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
```

```
[SW8800] interface Ethernet3/1/3
[3Com-Ethernet3/1/3] mac-address max-mac-count 600
```

[3Com-Ethernet3/1/3] undo mac-address max-mac-count enable forward

Cancel the alarm function

```
[3Com-Ethernet3/1/3] undo mac-address max-mac-count enable alarm
```

mac-address max-mac-count max-mac-num

Syntax

mac-address max-mac-count *max-mac-num*

undo mac-address max-mac-count

View

VLAN view

Parameter

max-mac-num: Maximum number of MAC addresses that can be learned in a VLAN. This argument ranges from 0 to 4,294,967,295. Value of 0 disables MAC address learning.

Description

Use the **mac-address max-mac-count** command to set the maximum number of MAC addresses that can be learned in VLAN.

Use the **undo mac-address max-mac-count** command to cancel the configuration.

If you have set the maximum number, MAC addresses will not be learned in the VLAN when the maximum number is reached.

By default, the number of learned MAC addresses is not limited in a VLAN.

If you execute this command with the max-mac-num argument less than the current number of MAC addresses learned, the switch does not remove the existing MAC address entries, neither does it learns new MAC addresses. The switch resumes MAC address learning when the number of MAC addresses learned is less than the value specified by the max-mac-num argument.

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

Example

Set the maximum number of learned MAC addresses in a VLAN 100 to 600.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] vlan 100
[3Com-vlan100] mac-address max-mac-count 600
```

mac-address timer

Syntax

mac-address timer { **aging** *age* | **no-aging** }

undo mac-address timer aging

View

System view

Parameter

aging *age*: Specifies the aging time (measured in seconds) of the Layer-2 dynamic address table entry, ranging from 10 to 630. By default, the aging time is 300 seconds.

no-aging : No aging time.

Description

Use the **mac-address timer** command to configure the aging time of the Layer-2 dynamic address table entry.

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

If aging time is too short, the MAC address might be deleted before the switch gets the address information. That way the switch broadcasts the received packets to all the ports within the VLAN. This will affect the switch operation performance.

If aging time is too long, the switch will store a great number of out-of-date MAC address tables. This will consume MAC address table resources and the switch will not be able to update MAC address table according to the network change.

CAUTION: *The aging of dynamic MAC address is completed during the second aging cycle that has been configured.*

Example

Configure the entry aging time of Layer-2 dynamic address table to be 500 seconds.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] mac-address timer aging 500
```

reset mac-address

Syntax

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

View

User view

Parameter

all: Clears all of the MAC address entries.

dynamic: Clears all dynamic MAC address entries.

static: Cleasr all static MAC address entries.

interface-type is the type of the port, *and interface-number* is the number of the interface.

Vlan *vlan-id*: Clears all of the MAC address entries in the specified VLAN. For the range of the *vlan-id* argument, see the introduction to the **interface** command in the port module of the command manual.

Description

Use the **reset mac-address** command to clear corresponding MAC address entries.

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

Example

Clear all MAC address entries.

```
<SW8800> reset mac-address all
```

13 MSTP CONFIGURATION COMMANDS

MSTP Configuration Commands

active region-configuration

Syntax

active region-configuration

View

MST region view

Parameter

None

Description

Use the **active region-configuration** command to activate the configurations of MST region.

This command is used for manually activate the configurations of MST region. Configuring the related parameters, especially the VLAN mapping table, of the MST region, will lead to the recalculation of spanning tree and network topology flapping. To bate such flapping, MSTP applies the configured parameters and launches recalculation of the spanning tree only when you activate the configured MST region parameters or enable MSTP.

After you entered this command, MSTP will apply the MST region parameters you have configured to the system and recalculate the spanning tree.

Related command: **instance**, **region-name**, **revision-level**, **vlan-mapping modulo**, **check region-configuration**.

Example

Manually activate MST region configurations.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800]stp region-configuration
[3Com-mst-region] active region-configuration
```

check region-configuration

Syntax

check region-configuration

View

MST region view

Parameter

None

Description

Use the **check region-configuration** command to view the configuration information (including switch region name, revision level, and VLAN mapping table) to be activated.

MSTP defines that the user must ensure the correct region configurations, especially the VLAN mapping table configuration. The switches can be configured in the same region only if their region names, VLAN mapping tables, and MSTP revision levels are configured exactly the same. The switch may not be configured in the expected region due to any slight deviation. You can use this command to display the MST region configuration information to be activated to know to which MST regions the switch belongs and check if the MST region configurations are correct.

Related command: **instance**, **region-name**, **revision-level**, **vlan-mapping modulo**, **active region-configuration**.

Example

Display the configuration information about the region.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800]stp region-configuration
[3Com-mst-region] check region-configuration
Admin. Configuration
   Format selector :0
   Region name     :00b010000001
   Revision level  :0

   Instance   Vlans Mapped
      0       1 to 9, 11 to 4094
     16       10
```

Table 25 Description on the fields of the check region-configuration command

Field	Description
Format selector	The selector defined by MSTP
Region name	Region name of MST region
Revision level	Revision level of MST region
Instance Vlans Mapped	VLAN mapping table of MST region

debugging stp

Syntax

debugging stp { **global-error** | **global-event** | **all** | **event** [**flush | packetdrop | port**] | **instance** *instance-id* | **lacp-key** | **packet** | **state-machine** [{ **pim | prs | prt | pst | tcm** } [**instance** *instance-id*] **|** [ppm | ptx | tcpm]] | **interface** *interface-type interface-number* { **lacp-key** | **packet** | **event** } }

undo debugging stp { **global-error** | **global-event** | **all** | **event** [**flush | packetdrop | port**] | **instance** *instance-id* | **lacp-key** | **packet** | **tc-protectionstate-machine** [{ **pim | prs | prt | pst | tcm** } [**instance** *instance-id*

] **|** [ppm | ptx | tcpm]] | **interface** *interface-type interface-number* { **lacp-key** | **packet** | **event** } }

View

User view

Parameter

None

Description

Use the **debugging stp** { **global-error** | **global-event** } command to enable STP global error or event debugging.

Use the **undo debugging stp** { **global-error** | **global-event** } command to disable STP global error or event debugging.

Use the **debugging stp all** command to enable global debugging.

Use the **undo debugging stp all** command to disable global debugging.

Use the **debugging stp event** command to enable event debugging of MSTP.

Use the **undo debugging stp event** to disable event debugging of MSTP.

Use the **debugging stp packet** command to enable packet debugging of MSTP.

Use the **undo debugging stp packet** command to disable packet debugging of MSTP.

Use the **debugging stp instance** *instance-id* command to enable specified instance debugging of MTSP.

Use the **undo debugging stp instance** *instance-id* command to disable specified instance debugging of MTSP.

Use the **debugging stp lacp-key** command to enable MD5 summary information debugging of LACP protocol.

Use the **undo debugging stp lacp-key** command to disable MD5 summary information debugging of LACP protocol.

Use the **debugging stp state-machine** command to enable debugging of the state machine.

Use the **undo debugging stp state-machine** command to disable debugging of the state machine.

Use the **debugging stp state-machine pim** command to enable debugging of the port information state machine.

Use the **undo debugging stp state-machine pim** command to disable debugging of the port information state machine.

Use the **debugging stp state-machine prs** command to enable debugging of the state machine for port role selection. Use the **undo debugging stp state-machine prs** command to disable debugging of the state machine for port role selection.

Use the **debugging stp state-machine prt** command to enable debugging of the state machine for port role transition.

Use the **undo debugging stp state-machine prt** command to disable debugging of the state machine for port role transition.

Use the **debugging stp state-machine pst** command to enable debugging of the state machine for port state transition.

Use the **undo debugging stp state-machine pst** command to disable debugging of the state machine for port state transition.

Use the **debugging stp state-machine tcm** command to enable debugging of the topology change state machine.

Use the **undo debugging stp state-machine tcm** command to disable debugging of the topology change state machine.

Use the **debugging stp state-machine ppm** command to enable debugging of the state machine for port protocol transition. Use the **undo debugging stp state-machine ppm** command to disable debugging of the state machine for port protocol transition.

Use the **debugging stp state-machine ptx** command to enable debugging of the port transport state machine.

Use the **undo debugging stp state-machine ptx** command to disable debugging of the port transport state machine.

Use the **debugging stp state-machine tcpm** command to enable debugging of the state machine for topology change protection. Use the **undo debugging stp state-machine tcpm** command to disable debugging of the state machine for topology change protection.

Use the **debugging stp interface** *interface-type interface-number* { **lacp-key** | **packet** | **event** } command to enable specified port debugging of MSTP.

Use the **undo debugging stp interface** *interface-type interface-number* { **lacp-key** | **packet** | **event** } command to disable specified port debugging of MSTP.

Example

Enable STP global event debugging.

```
<SW8800> debugging stp global-event
```

display stp

Syntax

display stp [**instance** *instance-id*] [**interface** *interface-list* | **slot** *slot-num*] [**brief**]

View

Any view

Parameter

instance-id: Specifies the spanning tree instance ID, ranging from 0 to 48. Instance 0 represents CIST.

interface-list: Ethernet port list, containing multiple Ethernet ports and expressed as *interface-list* = { { *interface-type interface-num* | *interface-name* } [**to** { *interface-type interface-num* | *interface-name* }] }&<1-10>. For detail descriptions of *interface-type*, *interface-num* and *interface-name* parameters, refer to the corresponding descriptions in *Port Command Manual*. &<1-10> means that the preceding parameters can be entered up to 10 times.

slot *slot-num*: Displays STP information about a specified slot.

brief: Displays only port state, port protection type and port role in the corresponding instance.

Description

Use the **display stp** command to view the state information and statistics information of the spanning tree.

The MSTP state and statistics information can help analyze and maintain the network topology and maintain the normal operation of MSTP.

If no spanning tree instance ID or port list is specified, the command will display the spanning tree information of all the instances on all the ports in port number order. If the instance ID is specified, the command will display the spanning tree information of the specified instance on all the port in port number order. If only the port list is specified, the command will display the information about all the MSTIs on the port in port number order. If both instance ID and port list are specified, the command will display the spanning tree information of the specified instance and port according to the port list of the instance ID.

If there is an aggregation port, the command will only display the instance information on the master port.

MSTP state information includes:

1. Global CIST parameter: Protocol operation mode, switch priority in the CIST instance, MAC address, Hello Time, Max Age, Forward Delay, Max Hops, CIST common root, external path cost of the switch to the CIST common root, region root, internal path cost of the switch to the region root, CIST root port of the switch, and whether to enable BPDU protection; Number of received TC/TCN packets, time interval for receiving packets. If you specify the relationship between a master root and one or multiple slave roots, the global CIST parameters can also be displayed in CIST Root Type.
2. CIST port parameter: Port state, role, priority, path cost, path cost standard designated bridge, designated port, edge port/non-edge port, whether connected to the point-to-point link, port transit limit, whether to enable Root protection, whether being a region edge port, Hello Time, Max Age, Forward Delay,

Message-age time, and Remaining-hops; Num of VLANs Mapped, number of sent BPDU packets, and number of received BPDU packets.

3 Global MSTIs parameter: MSTI instance ID, bridge priority of the instance, region root, internal path cost, MSTI root port, MASTER bridge, path cost to region root and number of the received TC packets. If you specify the relationship between master roots and slave roots in an instance, the global MSTI parameters can also be displayed in MSTI Root Type.

4 MSTIs port parameter: Port state, role, priority, path cost, path cost standard, designated bridge, designated port, and remaining hops. You can view Num of VLANs Mapped in port view.

Statistics information: Count of TCN, CONFIG BPDU, RST, and MST BPDU transmitted/received via the port.

Related command: **reset stp**.

Example

Display the state and statistics information about the spanning tree.

```
<SW8800> display stp instance 0 interface Ethernet 2/1/1 to Ethernet 2/1/4
  GigabitEthernet 3/2/1 to GigabitEthernet 3/2/4 GigabitEthernet 3/3/1 brief
  MSTID      Port                  Role  STP State     Protection
    0        Ethernet2/1/1         ALTE  DISCARDING      LOOP
    0        Ethernet2/1/2         DESI  FORWARDING      NONE
    0        Ethernet2/1/3         DESI  FORWARDING      NONE
    0        Ethernet2/1/4         DESI  FORWARDING      NONE
    0        GigabitEthernet3/2/1  DESI  FORWARDING      NONE
    0        GigabitEthernet3/2/2  DESI  FORWARDING      NONE
    0        GigabitEthernet3/2/3  DESI  FORWARDING      NONE
    0        GigabitEthernet3/2/4  DESI  FORWARDING      NONE
    0        GigabitEthernet3/3/1  ROOT  FORWARDING      NONE
```

Table 26 Description on the fields of the display stp command

Field	Description
MSTID	MST instance ID in a MST region
Port	Port number, corresponding to the related MST instance
Role	Role of the port
STP State	Port STP state, including enabled status and disabled status, and also monitoring and learning status during transition
Protection	Protection type on the port

display stp region-configuration

Syntax

display stp region-configuration

View

Any view

Parameter

None

Description

Use the **display stp region-configuration** command to view the effective MST region configurations.

MST region configuration information includes: region name, region revision level, and associations between VLANs and MSTIs. All these configurations together determine to which MST region a switch belongs.

Related command: **stp region-configuration**.

Example

Display the MST region configuration information.

```
<SW8800> display stp region-configuration
Oper Configuration
   Format selector :0
   Region name     :3com
   Revision level  :0

   Instance   Vlans Mapped
      0       21 to 4094
      1       1 to 10
      2       11 to 20
```

Table 27 Description on the fields of the display stp region-configuration command

Field	Description
Format selector	Selector defined by MSTP
Region name	Region name of MST region
Revision level	Revision level of MST region
Instance Vlans Mapped	VLAN mapping table of MST region

display stp tc

Syntax

display stp [**instance** *instanceid*] tc { **all** | **detected** | **received** | **sent** }

View

Any view

Parameter

instance *instanceid*: Instance to be displayed. By default, TC (Topology Change) statistics of all the instances will be displayed.

detected: TC statistics detected by the bridge.

received: TC statistics received at the bridge.

sent: TC statistics sent from the bridge.

all: All TC statistics, including those detected, received and sent by the bridge.

Description

Use the **display stp tc** command to view TC (transaction capabilities) statistics.

Example

Display all TC statistics.

```
<SW8800> dis stp tc all
 ---------- Stp Instance 0 tc or tcn received count ----------
```

```
Port Ethernet3/1/1              0
Port Ethernet3/1/9              1
---------- Stp Instance 0 tc or tcn detected count ----------
Port Ethernet3/1/1              1
Port Ethernet3/1/9              0
---------- Stp Instance 0 tc or tcn sent count ----------
Port Ethernet3/1/1              1
Port Ethernet3/1/9              0
```

The topology changes and notification information of Instance 0 will be recorded in the log.

instance

Syntax

instance *instance-id* **vlan** *vlan-list*

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

View

MST region view

Parameter

instance-id: Specifies the spanning tree instance ID, ranging from 0 to 48. The value 0 indicates a CIST.

vlan *vlan-list*: Specifies the VLAN list, ranging from 1 to 4094. *vlan-list* = { *vlan-id* [**to** *vlan-id*] }&<1-10>. Where, &<1-10> represents that you can input *vlan-id*s up to 10 times

Description

Use the **instance** command to map the specified VLAN list to the specified MSTI.

Use the **undo instance** command to cancel the specified VLAN list from the specified MSTI, and the removed VLAN will then be mapped to the CIST (i.e., the Instance 0). If no VLAN is specified in the **undo** command, all the VLANs associated with the specified MSTI will be mapped to CIST.

By default, all the VLANs are mapped to CIST, i.e., the Instance 0.

MSTP describes the association between VLANs and MSTIs with the VLAN mapping table. You can use this command to configure this table. Every VLAN can be mapped to an MSTI as per your configuration.

You cannot map one VLAN to different instances, while you can map multiple VLANs to one instance. When you remap the mapped VLAN to a different instance, the original mapping relation is removed automatically. The mapping relationship of VLANs and instances in the same MSTP domain must be correct. The data will be transmitted according to the spanning tree topology structure of the instance the VLAN maps to.

Related command: **region-name**, **revision-level**, **check region-configuration**, **vlan-mapping modulo**, **active region-configuration**.

Example

Map VLAN 2 to MSTI 1.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800]stp region-configuration
[3Com-mst-region] instance 1 vlan 2
```

Map VLAN5-10 to MSTI 3.

```
[3Com-mst-region] instance 3 vlan 5 6 7 8 9 10
```

region-name

Syntax

region-name *name*

undo region-name

View

MST region view

Parameter

name: Specifies the MST region name of the switch with a character string not exceeding 32 bytes.

Description

Use the **region-name** command to configure the MST region name of a switch.

Use the **undo region-name** command to restore the default MST region name.

By default, the MST region name of the switch is the switch MAC address in hexadecimal notation.

The switch region name, together with VLAN mapping table of the MST region and MSTP revision level, is used for determining the region to which the switch belongs.

Related command: **instance**, **revision-level**, **check region-configuration**, **vlan-mapping modulo**, **active region-configuration**.

Example

Set the MST region name of the switch as abcde.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800]stp region-configuration
[3Com-mst-region] region-name abcde
```

reset stp

Syntax

reset stp [**interface** *interface-list*]

View

User view

Parameter

interface-list: Ethernet port list, containing multiple Ethernet ports and expressed as *interface-list* = { *interface-type interface-number* [**to** { *interface-type interface-number*] }&<1-10>. For detail descriptions of *interface-type*, *interface-number* parameters, refer to the corresponding descriptions in *Port Command Manual*. &<1-10> means that the preceding parameters can be entered up to 10 times.

Description

Use the **reset stp** command to reset the spanning tree statistics information.

The spanning tree statistics information includes TCN, Config BPDU, RST, and MST BPDU, received and transmitted on the port. Among them, STP BPDU and TCN BPDU are counted on CIST.

If you specify a port list, the command clears the spanning tree statistics information of the specified port. If you do not specify any port, the command clears the spanning tree statistics information of all ports.

Related command: **display stp**.

Example

Clear the statistics information on the ports from Ethernet2/1/1 through Ethernet2/1/3

```
<SW8800> reset stp interface Ethernet 2/1/1 to Ethernet 2/1/3
```

revision-level

Syntax

revision-level *level*

undo revision-level

View

MST region view

Parameter

level: Specifies the MSTP revision level, ranging from 0 to 65535. By default, MSTP revision level takes 0.

Description

Use the **revision-level** command to configure MSTP revision level of the switch.

Use the **undo revision-level** command to restore the default revision level.

MSTP revision level, together with region name and VLAN mapping table, is used for determining the MST region to which the switch belongs.

Related command: **instance**, **region-name**, **check region-configuration**, **vlan-mapping modulo** and **active region-configuration**.

Example

Set the MSTP revision level of the switch MST region to 5.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800]stp region-configuration
[3Com-mst-region] revision-level 5
```

stp **Syntax**

stp { **enable** | **disable** }

undo stp

View

System view, Ethernet port view

Parameter

enable: Enables global or port MSTP.

disable: Disables global or port MSTP.

Description

Use the **stp** command to enable or disable MSTP on a device or a port.

Use the **undo stp** command to restore the default MSTP state on a device or a port.

By default, MSTP is disabled on the switch.

After MSTP is enabled, the switch determines to run MSTP in STP-compatible mode or MSTP mode as per your configurations. The switch serves as a transparent bridge after MSTP is disabled.

After MSTP is enabled, it will dynamically maintain the spanning tree state of the corresponding VLAN according to the received configuration BPDU until it is disabled. After MSTP is disabled, it will not maintain the state.

By default, global and port MSTP are disabled. When you enable MSTP on a device or a port, both global and port MSTP are enabled; if you do not enable MSTP globally, you will fail to use the **stp enable** command on a port.

Related command: **stp mode, stp interface**.

Example

Enable MSTP globally.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] stp enable
```

Disable MSTP on Ethernet 2/1/1

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface Ethernet 2/1/1
[3Com-Ethernet 2/1/1] stp disable
```

stp bpdu-protection

Syntax

stp bpdu-protection

undo stp bpdu-protection

View

System view

Parameter

None

Description

Use the **stp bpdu-protection** command to enable the BPDU protection on the switch. Use the **undo stp bpdu-protection** command to restore the default state of BPDU protection.

By default, BPDU protection is disabled.

Generally, the access ports of the access layer devices are directly connected to user terminals (such as PC) or file servers. In this case, the access ports are set to edge ports to implement fast state transition. However, when such access ports receive configuration BPDU, the system will automatically set them to non-edge ports and recalculate the spanning tree, which makes the network topology flap. These ports will not receive any STP configuration BPDU in normal cases. Anyway, if someone maliciously attacks the switch with fake configuration BPDU, the network will flap.

MSTP provides BPDU protection function to avoid such attack: After configured with BPDU protection, the switch will disable the edge port through MSTP, which receives a BPDU, and notify the network manager at same time. These ports can be resumed by the network manager only.

Example

Enable BPDU protection on the switch.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z
[SW8800] stp bpdu-protection
```

stp bridge-diameter

Syntax

stp bridge-diameter *bridgenum*

undo stp bridge-diameter

View

System view

Parameter

bridgenum: Ranges from 2 to 7 and defaults to 7.

Description

Use the **stp bridge-diameter** command to configure the switching network diameter. Use the **undo stp bridge-diameter** command to restore the default network diameter.

The definition of network diameter: Maximum count of switches between the farthest communication ends.

The **stp bridge-diameter** command configures the switching network diameter and determines the three time parameters of MSTP accordingly. This configuration takes effect on CIST only but makes no sense for MSTI.

The spanning tree convergence can be speeded up, when Hello Time, Forward Delay, and Max Age are well configured. These parameters are related to the network scale.

You can configure the network scale to get the time parameters. When users configure the bridge-diameter parameter of the switch, MSTP will automatically set Hello Time, Forward Delay, and Max Age to moderate values. When bridge-diameter defaults to 7, the time parameters also take their respective default values.

Related command: **stp timer forward-delay**, **stp timer hello**, **stp timer max-age**.

*The **stp bridge-diameter** command configures the switching network diameter and determines the three MSTP time parameters (Hello Time, Forward Delay, and Max Age) accordingly.*

Example

Set the diameter of the switching network to 5.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] stp bridge-diameter 5
```

stp compliance

Syntax

stp compliance { **legacy** | **dot1s** | **auto** }

View

Ethernet port view

Parameter

legacy: Indicates that the port sends and receives private MSTP packets.

dot1s: Indicates that the port sends and receives standard MSTP packets.

auto: Indicates the port has the auto-sensing function. The port can automatically adjust the format of the packet to be sent based on the format of the received packet.

Description

Use the **stp compliance** command to set the format of the packets that the current port sends and receives. You can configure the format to **legacy**, **dot1s**, or **auto**.

By default, the port sends the packets in the **legacy** format.

Example

Set Ethernet2/1/1 to the **auto** mode.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface Ethernet2/1/1
[3Com-Ethernet2/1/1] stp compliance auto
```

stp cost

Syntax

stp [**instance** *instance-id*] **cost** *cost*

undo stp [**instance** *instance-id*] **cost**

View

Ethernet port view

Parameter

instance *instance-id*: Specifies the spanning tree instance ID, ranging from 0 to 48. The Instance 0 represents CIST.

cost *cost*: Port path cost. Its range depends on the selected standard of path cost.

Description

Use the **stp instance cost** command to configure the port path cost on the specified MSTI for the current port.

Use the **undo stp instance cost** command to restore the path cost on the specified MSTI.

By default, switch calculates the path costs of a port on different MSTIs.

You may specify the *instance-id* parameter as 0 to configure CIST path cost of the port. The path cost has effect on the port role selection. A port can be configured with different path costs on different MSTIs. Thus the traffic from different VLANs can run over different physical links, thereby implementing the VLAN-based load-balancing. MSTP will recalculate the port role and transit its state, upon the port path cost changes.

Related command: **stp interface instance cost**.

Example

Set the path cost of Ethernet 2/1/3 on MSTI 2 to 200.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface Ethernet 2/1/3
[3Com-Ethernet2/1/3] stp instance 2 cost 200
```

stp edged-port

Syntax

stp edged-port { **enable** | **disable** }

undo stp edged-port

View

Ethernet port view

Parameter

enable: Configures the current port as an edge port.

disable: Configures the current port as a non-edge port.

Description

Use the **stp edged-port enable** command to configure the current Ethernet port as an edge port.

Use the **stp edged-port disable** command to configure the current Ethernet port as a non-edge port.

Use the **undo stp edged-port** command to restore the default state, i.e., non-edge port.

By default, all the switch ports are configured as non-edge ports.

If the current Ethernet port is connected to other switch, you can use the **stp** edged-port **disable** or **no stp** edged-port command to configure it as a non-edge port. The **stp** edged-port **enable** command is used for configuring the port as an edge port.

A port is considered as an edge port when it is directly connected to the user terminal, instead of any other switches or shared network segments. The edge port will not cause loop upon network topology changes. Accordingly, you can configure a port as an edge port, so that it can transit to forwarding state fast. For this purpose, configure the Ethernet port directly connected to the user terminal as an edge port.

Because the edge port is not connected to any other switches, it will not receive the configuration BPDUs from them.

CAUTION: *If the STP function has been enabled on the downstream equipment of the switch, do not configure edge port on the equipment. Otherwise the system will fail to delete the MAC address table entries and ARP address table entries on the port.*

Related command: **stp interface edged-port**.

Example

Configure Ethernet 2/1/1 as a non-edge port.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface Ethernet 2/1/1
[3Com-Ethernet2/1/1] stp edged-port disable
```

stp instance root primary

Syntax

stp [**instance** *instance-id*] **root primary** [**bridge-diameter** *bridgenum* [**hello-time centi-senconds**]]

undo stp [**instance** *instance-id*] **root**

View

System view

Parameter

instance-id: Specifies the spanning tree instance ID, ranging from 0 to 48. Specify it as 0 to configure the root bridge of CIST.

root primary: Configures the current switch as the primary root of the specified MSTI.

bridge-diameter *bridgenum*: Specifies the network diameter of the spanning tree, ranging from 2 to 7.

hello-time *centi-senconds*: Specifies the Hello Time of the spanning tree, which is in the range from 100 to 1000 and measured in centiseconds.

Description

Use the **stp root primary** command to configure the current switch as the primary root of the specified MSTI.

Use the **undo stp root** command to cancel the current switch for the primary root of the designated MSTI.

If you execute these commands without using the **instance** *instance-id* option, your configuration takes effect only on the CIST instance.

When you set the *instance-id* parameter to 0, its following parameter setting takes effect.

By default, the switch does not server as a root bridge.

You can specify one root bridge for each MSTI regardless of the switch priority. When setting a root bridge, you can use this command to specify the switching network diameter and determine the three time parameters (Hello time, Forward Delay and Max Age). Because the switch calculates inaccurate Hello time value, you can specify the switching network diameter and the Hello Time for the root bridge, and thus determine other two parameter values for the root bridge. In general, you are recommended to determine the other two time parameter values by setting the network diameter.

CAUTION: *In a switching network, you can configure only one root bridge for each MSTI and one or more secondary switches. Do not configure more than one root bridge for an MSTI at the same time. Otherwise, the calculation result will be unpredictable.*

After a switch is configured as a primary root bridge or a secondary root bridge, users cannot modify the bridge priority of the switch.

Example

Designate the current switch as the root bridge of MSTI 0 and specify the diameter of the switching network as 4 and the Hello Time as 500 centiseconds.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] stp instance 0 root primary bridge-diameter 4 hello-time 50
0
```

stp interface

Syntax

stp interface *interface-list* { **enable** | **disable** }

View

System view

Parameter

interface-list: Ethernet port list, containing multiple Ethernet ports and expressed as *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>. For detail descriptions of *interface-type* and *interface-number* parameters, refer to the corresponding descriptions in *Port Command Manual*. &<1-10> means that the preceding parameters can be entered up to 10 times.

enable: Enables MSTP on the port.

disable: Disables MSTP on the port.

Description

Use the **stp interface** command to enable/disable MSTP on a switch port in system view.

By default, if MSTP is enabled globally, it is enabled on every port. If MSTP is disabled globally, it is also disabled on every port.

When MSTP is disabled, the corresponding port stays in forwarding state and does not take part in any MSTI calculation.

CAUTION: *If you disable MSTP on a port, a loop may be generated.*

Related command: **stp mode, stp**.

Example

Enable MSTP on Ethernet 2/1/1 in system view.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z
[SW8800] stp interface Ethernet 2/1/1  enable
```

stp interface instance cost

Syntax

stp interface *interface-list* [**instance** *instance-id*] **cost** *cost*

undo stp interface *interface-list* [**instance** *instance-id*] **cost**

View

System view

Parameter

interface-list: Ethernet port list, containing multiple Ethernet ports and expressed as *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>. For detail descriptions of *interface-type* and i*nterface-number* parameters, refer to the corresponding descriptions in *Port Command Manual*. &<1-10> means that the preceding parameters can be entered up to 10 times.

instance-id: Specifies the spanning tree instance ID, ranging from 0 to 48. The instance 0 represents CIST.

cost: Port path cost. Its range depends on the selected standard of path cost.

Description

Use the **stp interface cost** command to configure the path cost of the specified port on the specified MSTI in system view.

Use the **undo stp interface cost** command to restore the path cost of the specified port on the specified MSTI to the default value in system view.

By default, switch automatically calculates the path costs of a port on different MSTIs based on corresponding standard.

You may specify the *instance-id* parameter as 0 to configure CIST path cost of the port. The path cost has effect on the port role selection. You can configure different path costs for different MSTIs on a port. Thus the traffic from different VLANs can run over different physical links, thereby implementing the VLAN-based load-balancing. MSTP will recalculate the port role and transit its state, upon the port path cost changes.

Related command: **stp cost.**

Example

Set the path cost of Ethernet 2/1/3 on MSTI 2 to 400 in system view.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] stp interface Ethernet 2/1/3 instance 2 cost 400
```

stp interface edged-port

Syntax

stp interface *interface-list edged-port* {**enable** | **disable** }

undo stp interface *interface-list* **edged-port**

View

System view

Parameter

interface-list: Ethernet port list, containing multiple Ethernet ports and expressed as *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>. For detail descriptions of *interface-type* and i*nterface-number* parameters, refer to the corresponding descriptions in *Port Command Manual*. &<1-10> means that the preceding parameters can be entered up to 10 times.

enable: Configures the current port as an edge port.

disable: Configures the current port as a non-edge port.

Description

Use the **stp interface edged-port enable** command to configure a port as an edge port in system view.

Use the **stp interface edged-port disable** command to configure a port as a non-edge port in system view.

Use the **undo stp interface edged-port** command to restore the port to the default type (that is, non-edge port) in system view.

By default, all the switch ports are configured as non-edge ports.

If the current Ethernet port is connected to other switches, you can use the **stp interface edged-port disable** or **undo stp interface edged-port** command to configure it as a non-edge port. The **stp interface edged-port enable** command is used for configuring the port as an edge port.

A port is considered as an edge port when it is directly connected to the user terminal, instead of any other switches or shared network segments. The edge port will not cause loop upon network topology changes. Accordingly, you can configure a port as an edge port, so that it can transit to forwarding state fast. For this purpose, configure the Ethernet port directly connected to the user terminal as an edge port.

Because the edge port is not connected to any other switches, it will not receive the configuration BPDUs from them.

Related command: **stp edged-port**.

Example

Configure Ethernet2/1/3 as an edge port in system view.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z
[SW8800] stp interface Ethernet 2/1/3 edged-port enable
```

stp interface instance port priority

Syntax

stp interface *interface-list* **instance** *instance-id* **port priority** *priority*

undo stp interface *interface-list* **instance** *instance-id* **port priority**

View

System view

Parameter

interface-list: Ethernet port list, containing multiple Ethernet ports and expressed as *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>. For detail descriptions of *interface-type* and i*nterface-number* parameters, refer to the corresponding descriptions in *Port Command Manual*. &<1-10> means that the preceding parameters can be entered up to 10 times

instance-id: Specifies the spanning tree instance ID, ranging from 0 to 48. The Instance 0 represents CIST.

port priority *priority*: Specifies the port priority, ranging from 0 to 240 with a step length of 16, e.g., 0, 16 and 32. By default, the port has a priority of 128 on every MSTI.

Description

Use the **stp interface instance port priority** command to configure the priority of the specified port on the specified MSTI in system view.

Use the **undo stp interface instance port priority** command to restore the default priority.

You may specify the *instance-id* parameter as 0 to configure CIST priority of the port. The port priority has effect on the port role selection for the specified MSTI. A port can be configured with different priorities on different MSTIs. Thus the traffic from different VLANs can run over different physical links, thereby implementing the VLAN-based load-balancing. MSTP will recalculate the port role and transit its state, upon the port priority changes.

Related command: **stp instance port priority**.

Example

Set the priority of Ethernet 2/1/3 on MSTI 2 to 16 in system view.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] stp interface Ethernet 2/1/3 instance 2 port priority 16
```

stp interface loop-protection

Syntax

stp interface *interface-list* **loop-protection**

undo stp interface *interface-list* **loop-protection**

View

System view

Parameter

interface-list: Ethernet port list, containing multiple Ethernet ports and expressed as *interface-list* = { *interface-type interface-number* [**to** *interface-type*

interface-number] }&<1-10>. For detail descriptions of *interface-type* and i*nterface-number* parameters, refer to the corresponding descriptions in *Port Command Manual*. &<1-10> means that the preceding parameters can be entered up to 10 times

Description

Use the **stp interface loop-protection** command to enable loop protection on the switch in system view.

Use the **undo stp interface loop-protection** command to restore the default loop protection state.

When port roles change, you can use the **stp interface loop-protection** command to change port state from forwarding state to discarding state, thus avoiding port loopback.

Use the **undo stp interface loop-protection** command to restore the default running state of loop protection in system view.

The root port and other blocked ports maintain their state according to the BPDUs sent by uplink switch. Due to link congestion or unidirectional link failure, these ports may be unable to receive BPDUs and the switch will select root port again. In this case, the former root port will turn into the specified port and the former blocked ports will change to the forwarding state, and link loop appears.

The loop protection function can inhibit the generation of loop. After it is enabled, the root port role will change according to the uplink port state. The blocked port will maintain in discarding state and do not forward packets, thus avoiding link loop.

By default, loop protection is disabled.

CAUTION: *If the equipment connected to the port of the switch cannot send STP packets to the switch, do not configure the* ***loop-protection*** *command; otherwise the port will be congested for a long time.*

Related command: **stp loop-protection**.

For a loopback port, if the port participates in STP calculation, it must be specified port regardless of internal loop or external loop. However, the port is always set to be in discarding state on all instances.

Example

Enable loop protection on the Ethernet2/1/1.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] stp interface Ethernet2/1/1 loop-protection
```

stp interface mcheck

Syntax

stp interface *interface-list* **mcheck**

View

System view

Parameter

interface-list: Ethernet port list, containing multiple Ethernet ports and expressed as *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>. For detail descriptions of *interface-type* and i*nterface-number* parameters, refer to the corresponding descriptions in *Port Command Manual*. &<1-10> means that the preceding parameters can be entered up to 10 times

Description

Use the **stp interface mcheck** command to perform mCheck operation on the port in system view.

If a port of an MSTP switch on a switching network has ever been connected to an STP switch, the port will automatically transit to operate in STP-compatible mode. However, when the STP switch is removed, the port stays in STP-compatible mode and cannot automatically transit back to MSTP mode. In this case, you can perform mCheck operation to transit the port to MSTP mode by force.

By default, MSTP runs in MSTP mode, which is compatible with RSTP and STP (This mode can recognize MSTP BPDU, STP config BPDU and RSTP config BPDU). However, the STP switch can only recognize config BPDU (STP BPDU) sent by the STP and RSTP bridges. After the switch running STP-compatible mode switches back to MSTP mode, it will not send MSTP BPDU if you do not execute the ***stp mcheck*** *command. Therefore, the connected device still sends config BPDU (STP BPDU) to it, causing the same configuration exist in different regions and other problems. Remember to perform stp interface mCheck after modifying stp mode.*

Related command: **stp mcheck, stp mode**.

Example

Set the mcheck parameter of Ethernet2/1/3 in system view.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] stp interface Ethernet2/1/3 mcheck
```

stp interface no-agreement-check

Syntax

stp interface *interface-type interface-number* **no-agreement-check**

undo stp interface *interface-type interface-number* **no-agreement-check**

View

System view

Parameter

interface-type: Port type.

interface-number: Port number.

Description

Use the **stp interface no-agreement-check** command to enable port fast transition.

Use the **undo stp interface no-agreement-check** command to disable port fast transition.

By default, port fast transition is disabled.

Related command: **stp no-agreement-check**.

You can configure fast transition only on a root port or an alternate port.

Example

Enable fast transition on GigabitEthernet1/1/1.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800]stp interface GigabitEthernet1/1/1 no-agreement-check
```

stp interface point-to-point

Syntax

stp interface *interface-list* **point-to-point** { **force-true** | **force-false** | **auto** }

undo stp interface *interface-list* **point-to-point**

View

System view

Parameter

interface-list: Ethernet port list, containing multiple Ethernet ports and expressed as *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>. For detail descriptions of *interface-type* and i*nterface-number* parameters, refer to the corresponding descriptions in *Port Command Manual*. &<1-10> means that the preceding parameters can be entered up to 10 times.

force-true: Indicates the Ethernet port connected to a point-to-point link.

force-false: Indicates the Ethernet port not connected to a point-to-point link.

auto: Configures to automatically check if the link to the Ethernet port is a point-to-point link.

Description

Use the **stp interface point-to-point** command to configure a port (not) to be connected to a point-to-point link in system view.

Use the **undo stp interface point-to-point** command to restore the default state of the link to the Ethernet port.

By default, the parameter defaults to auto, that is, MSTP checks if the link to the Ethernet port is a point-to-point link.

The port not connected with the point-to-point link cannot transit fast.

The master ports of the link aggregation and the ports operating in full-duplex mode are connected to the point-to-point link. You are recommended to keep the default settings and let MSTP detect the link state automatically.

This configuration takes effect on the CIST and all the MSTIs. The settings of a port whether to connect the point-to-point link will be applied to all the MSTIs where the port belongs. Note that a temporary loop may be redistributed if you configure a port not physically connected with the point-to-point link as connected to such a link by force.

Related command: **stp point-to-point**.

Example

Configure Ethernet2/1/3 to be connected to the point-to-point link.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] stp interface Ethernet2/1/3 point-to-point force-true
```

stp interface root-protection

Syntax

stp interface *interface-list* **root-protection**

undo stp interface *interface-list* **root-protection**

View

System view

Parameter

interface-list: Ethernet port list, containing multiple Ethernet ports and expressed as *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>. For detail descriptions of *interface-type* and i*nterface-number* parameters, refer to the corresponding descriptions in *Port Command Manual*. &<1-10> means that the preceding parameters can be entered up to 10 times.

Description

Use the **stp interface root-protection** command to enable Root protection on the switch in system view.

Use the **undo stp interface root-protection** command to restore the default Root protection state.

By default, Root protection is disabled.

In case of configuration error or malicious attack, the legal primary root may receive the BPDU with a higher priority and then loose its place, which causes network topology change errors. Due to the illegal change, the traffic supposed to travel over the high-speed link may be pulled to the low-speed link and congestion will occur on the network.

Root protection function is used against such problem. The port configured with Root protection only plays a role of designated port on every instance. Whenever such port receives a higher-priority BPDU, that is, it is about to turn into non-designated port, it will be set to listening state and not forward packets any more (as if the link to the port is disconnected). So, Root protection takes effect only when it is enabled on a designated port. If the port has not received any

higher-priority BPDU for a certain period of time thereafter, it will resume its original state.

Related command: **stp root-protection**.

Example

Enable Root protection on the Ethernet2/1/1

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] stp interface Ethernet2/1/1root-protection
```

stp interface transmit-limit

Syntax

stp interface *interface-list* **transmit-limit** *packetnum*

undo stp interface *interface-list* **transmit-limit**

View

System view

Parameter

interface-list: Ethernet port list, containing multiple Ethernet ports and expressed as *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>. For detail descriptions of *interface-type* and i*nterface-number* parameters, refer to the corresponding descriptions in *Port Command Manual*. &<1-10> means that the preceding parameters can be entered up to 10 times.

packetnum: Maximum number of configuration BPDUs that can be transmitted via the port per Hello Time, ranging from 1 to 255 (expressed as a counter value without any units). By default, the transmission limit on every port is 3.

Description

Use the **stp interface transmit-limit** command to configure an amount limit to the configuration BPDU transmitted via a specified port during the Hello Time in system view.

Use the **undo stp interface transmit-limit** command to restore the default limit on the specified port in system view.

The larger the value is, the more packets can be transmitted in a time unit, yet the more switch resources will be occupied. With a moderate value, the amount of the BPDUs transmitted during Hello Time via every port can be limited and MSTP will not occupy too many bandwidth resources when the network topology flaps.

Related command: **stp transmit-limit**.

Example

Set a limit of 5 to the packets transmitted via Ethernet2/1/3 in system view.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] stp interface Ethernet2/1/3transmit-limit 5
```

stp loop-protection

Syntax

stp loop-protection

undo stp loop-protection

View

Ethernet port view

Parameter

none

Description

Use the **stp loop-protection** command to enable loop protection function.

Use the **undo stp loop-protection** command to restore the default setting.

By default, the loop protection function is not enabled.

The port configured with loop protection can only turn into discarding state on every instance. When such port receives no configuration message for a long time, only the port role changes, its discarding state remains unchanged, so no packets are forwarded. In this way, if the peer end cannot send BPDU packets due to error operation, and the port enters forwarding state directly for not receiving configuration message for a long time, no loop will be generated by enabling the loop protection.

CAUTION: *If the equipment connected to the port of the switch cannot send STP packets to the switch, do not configure the* ***loop-protection*** *command; otherwise the port will be congested for a long time.*

Example

Enable loop protection function in Ethernet2/1/1.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface Ethernet2/1/1
[3Com-Ethernet2/1/1] stp loop-protection
```

stp max-hops

Syntax

stp max-hops *hop*

undo stp max-hops

View

System view

Parameter

hop: Specifies the max hops, ranging from 1 to 40. By default, MST region Max Hops is 20.

Description

Use the **stp max-hops** command to configure the Max Hops of an MST region.

Use the **undo stp max-hops** command to restore the default Max Hops.

On CIST and MSTIs, the Max Hops configured on the region root determines the max switching network diameter supported by the local MST region. As the BPDU travels from the spanning tree root, each time when it is forwarded by a switch, the max hops will be reduced by 1. The switch discards the configuration BPDU with 0 hops left, thereby limiting the network scale inside the region. If the current switch is a CIST root bridge or MSTI root bridge in an MST region, the Max Hops configured on it will be the network diameter of the spanning tree to limit its scale in the local MST region. The Max Hops configured on the root bridge in an MST region will be adopted by other switches in the same region.

Example

Set the Max Hops of an MST region to 35.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] stp max-hops 35
```

stp mcheck

Syntax

stp mcheck

View

Ethernet port view

Parameter

None

Description

Use the **stp mcheck** command to perform mCheck on the current port.

If a port of an MSTP switch on a switching network has ever been connected to an STP switch, the port will automatically transit to operate in STP-compatible mode. However, when the STP switch is removed, the port stays in STP-compatible mode and cannot automatically transit back to MSTP mode. In this case, you can perform mCheck operation to transit the port to MSTP mode by force.

By default, MSTP runs in MSTP mode, which is compatible with RSTP and STP (This mode can recognize MSTP BPDU, STP config BPDU and RSTP config BPDU). However, the STP switch can only recognize config BPDU (STP BPDU) sent by the STP and RSTP bridges. After the switch running STP-compatible mode switches back to MSTP mode, it will not send MSTP BPDU if you do not execute the ***stp mcheck*** *command. Therefore, the connected device still sends config BPDU (STP BPDU) to it, causing the same configuration exist in different regions and other problems. Remember to perform stp interface mCheck after modifying stp mode.*

Related command: **stp mode, stp interface mcheck**.

Example

Set mcheck parameter for Ethernet2/1/1.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
```

```
[SW8800] interface Ethernet2/1/1
[3Com-Ethernet2/1/1] stp mcheck
```

stp mode

Syntax

stp mode { **stp** | **mstp** }

undo stp mode

View

System view

Parameter

stp: Configures the MSTP operation mode as STP-compatible.

mstp: Configures the MSTP operation mode as MSTP.

Description

Use the **stp mode** command to configure MSTP operation mode of the switch.

Use the **undo stp mode** command to restore the default MSTP operation mode.

By default, switch work in MSTP mode

MSTP and RSTP are compatible and they can recognize the packets of each other. However, STP cannot recognize MSTP packets. To implement the compatibility, MSTP provides two operation modes, STP-compatible mode and MSTP mode. In STP-compatible mode, the switch sends STP BPDU packets via every port. In MSTP mode, the switch ports send MSTP BPDU packets. When detecting it is connected to an STP switch (it receives config BPDU packets from the STP switch), the switch port enters automatically STP-compatible mode and sends config BPDU packets from the STP switch. The port enters MSTP mode only when receiving MSTP BPDU packets again.

Related command: **stp mcheck**, **stp**, **stp interface**, **stp interface mcheck**.

Example

Set MSTP operation mode as STP-compatible.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] stp mode stp
```

stp no-agreement-check

Syntax

stp no-agreement-check

undo stp no-agreement-check

View

Ethernet port view

Parameter

None

Description

Use the **stp no-agreement-check** command to enable port fast transition.

Use the **undo stp interface no-agreement-check** command to disable port fast transition.

By default, port fast transition is disabled.

Related command: **stp interface no-agreement-check**.

You can configure fast transition only on a root port or an alternate port.

Example

Enable fast transition on GigabitEthernet1/1/1.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800]interface GigabitEthernet1/1/1
[3Com-GigabitEthernet1/1/1]stp no-agreement-check
[3Com-GigabitEthernet1/1/1]
```

stp non-flooding

Syntax

stp non-flooding [**slot** *slotnum*]

undo stp non-flooding [**slot** *slotnum*]

View

System view

Parameter

slot *slotnum*: Specifies the slot of the I/O Module (line process unit). The *slotnum* argument is the slot number.

Description

Use the **stp non-flooding** command to discard BPDU packets received by STP-disabled ports.

Use the **undo stp non-flooding** command to forward BPDU packets within the VLAN to which the STP-disabled ports belong.

By default, BPDU non-flooding is disabled.

Related command: **stp enable**.

Example

-Discard BPDU packets received on STP-disabled port.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface GigabitEthernet3/1/1
[3Com-GigabitEthernet3/1/1]stp disable
[SW8800] stp non-flooding
```

Discard BPDU packets received on STP-disabled port on slot 3.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface GigabitEthernet3/1/1
[3Com-GigabitEthernet3/1/1]stp disable
[SW8800] stp non-flooding slot 3
```

Discard BPDU packets received on all ports when STP is not globally enabled.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] stp disable
[SW8800] stp non-flooding
```

stp pathcost-standard

Syntax

stp pathcost-standard { **dot1t** | **dot1d-1998** | **legacy** }

View

System view

Parameter

dot1t, **dot1d-1998**, **legacy** : Three standards of the path cost calculation on STP port.

Description

Use the **stp pathcost-standard** command to set the path cost calculation standard on STP port.

The port rate must be obtained first before you can calculate the path cost of a port as the path cost is associated with the port rate. The three standards use their own way to work out the port rate, based on which each standard calculates the port path cost by a certain algorithm.

By default, the legacy standard is applied for the switch Switch 8800 Family.

Example

Set the DOT1D-1998 as the path cost calculation standard on the STP port.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] stp pathcost-standard dot1d-1998
```

stp point-to-point

Syntax

stp point-to-point { **force-true** | **force-false** | **auto** }

undo stp point-to-point

View

Ethernet port view

Parameter

force-true: Indicates the Ethernet port connected to a point-to-point link.

force-false: Indicates the Ethernet port not connected to a point-to-point link.

auto: Configures to automatically check if the link to the Ethernet port is a point-to-point link.

Description

Use the **stp point-to-point** command to configure the current Ethernet port (not) to connect with point-to-point link.

Use **undo stp point-to-point** command to configure the link state to the default state in which MSTP automatically detects if the link to the Ethernet port is point-to-point link.

By default, switch adopts **auto** mode.

The port not connected with the point-to-point link cannot transit fast.

The master ports of the link aggregation and the ports operating in full-duplex mode are connected to the point-to-point link. You are recommended to keep the default settings and let MSTP detect the link state automatically.

This configuration takes effect on the CIST and all the MSTIs. The settings of a port whether to connect the point-to-point link will be applied to all the MSTIs where the port belongs. Note that a temporary loop may be redistributed if you configure a port not physically connected with the point-to-point link as connected to such a link by force.

Related command: **stp interface point-to-point**.

Example

Configure Ethernet2/1/3 to be connected to the point-to-point link.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface Ethernet2/1/3
[3Com-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 port view

Parameter

instance *instance-id*: Specifies the spanning tree instance ID, ranging from 0 to 48. The Instance 0 represents CIST.

port priority *priority*: Specifies the port priority, ranging from 0 to 240, with a step length of 16, e.g., 0, 16, and 32. By default, the priorities of a port on the MSTIs are 128.

Description

Use the **stp port priority** command to configure the priority of a port on a specified MSTI.

Use the **undo stp port priority** command to restore the default priority of the port on the specified MSTI.

You may specify the *instance-id* parameter as 0 to configure CIST priority of the port. The port priority has effect on the port role selection. A port can be configured with different priorities on different MSTIs. Thus the traffic from different VLANs can run over different physical links, thereby implementing the VLAN-based load-balancing. MSTP will recalculate the port role and transit its state, upon the port priority changes.

If you execute these commands without using the **instance** *instance-id* option, your configuration takes effect only on the CIST instance.

Related command: **stp interface port priority**.

Example

Set the priority of Ethernet2/1/3 on MSTI 2 to 16.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface Ethernet2/1/3
[3Com-Ethernet2/1/3] stp instance 2 port priority 16
```

stp region-configuration

Syntax

stp region-configuration

undo stp region-configuration

View

System view

Parameter

None

Description

Use the **stp region-configuration** command to enter MST region view.

Use the **undo stp region-configuration** command to restore the default MSTP region configurations.

By default, the three MST region parameters take the default values. The MST region name of the switch is the first MAC address, all the VLANs are mapped to CIST, and MSTP revision level takes 0.

You can enter MST region view, using the **stp region-configuration** command. Then you can configure the parameters including region name, revision level, and VLAN mapping table of the region.

Example

Enter MST region view.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] stp region-configuration
[3Com-mst-region]
```

stp reset-arp

Syntax

stp reset-arp { **enable** | **disable** }

undo stp reset-arp

View

System view, Ethernet port view

Parameter

None

Description

Use the **stp reset-arp enable** command to enable the function of clearing dynamic ARP entries on the switch or on the port.

Use the **stp reset-arp enable** command to disable the function of clearing dynamic ARP entries on the switch or on the port.

Use the **undo stp reset-arp** command to restore the default value of a dynamic ARP entry.

If you enable the function of clearing dynamic ARP entries in system view, the ARP entries of all the ports will be deleted. If you enable the function of clearing dynamic ARP entries in port view, only the ARP entries of the specified port will be deleted.

Example

Enable the function of clearing dynamic ARP entries in system view.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] stp reset-arp enable
```

Disable the function of clearing dynamic ARP entries in system view.

```
[SW8800] stp reset-arp disable
```

Enable the function of restoring the default value of a dynamic ARP entry in system view.

```
[SW8800] undo stp reset-arp
```

stp instance root secondary

Syntax

stp [**instance** *instance-id*] **root secondary** [**bridge-diameter** *bridgenum*] [**hello-time** *centi-senconds*]

undo stp [**instance instance-id**] **root**

View

System view

Parameter

instance *instance-id*: Specifies the spanning tree instance ID, ranging from 0 to 48. Specify it as 0 to configure CIST.

root secondary: Configures the current switch as the secondary root of the designated MSTI.

bridge-diameter *bridgenum*: Specifies the network diameter of the spanning tree, ranging from 2 to 7.

hello-time *centi-senconds*: Specifies the Hello Time of the spanning tree, which is in the range from 100 to 1000 and is measured in centiseconds.

Description

Use the **stp root secondary** command to configure the current switch as the secondary root bridge of a specified MSTI.

Use the **undo stp root** command to cancel the current switch for the secondary root bridge of a specified MSTI.

Only when the *instance-id* parameter is set to 0, can its following parameters take effect.

By default, the switch does not server as a secondary root bridge.

You can configure one or more secondary root bridges in an MSTI. If the primary root is down or powered off, the secondary root will take its place. Among several secondary root bridges, the one with the smallest MAC address takes the place of the failed primary root.

When configuring the secondary root bridge, you may also specify the switching network diameter and the Hello Time of the switch, so that the other two parameters, Forward Delay and Max Age, of the switch can be determined. To configure the current switch as the root bridge of CIST, simply specify *instance-id* as 0. You can configure only one root bridge for an MSTI and one or more secondary root bridges for it.

After a switch is configured as a primary root bridge or a secondary root bridge, users cannot modify the bridge priority of the switch.

Example

Configure the current switch as the secondary root bridge of MSTI 0 and specify the diameter of the switching network as 5 and the Hello Time of the switch as 300 centiseconds.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] stp instance 0 root primary bridge-diameter 5 hello-time 30
0
```

stp root-protection

Syntax

stp root-protection

undo stp root-protection

View

Ethernet port view

Parameter

None

Description

Use the **stp root-protection** command to enable on Root protection the switch.

Use the **undo stp root-protection** command to restore the default state of Root protection.

By default, Root protection is disabled.

In case of configuration error or malicious attack, the legal primary root may receive the BPDU with a higher priority and then loose its place, which causes network topology change errors. Due to the illegal change, the traffic supposed to travel over the high-speed link may be pulled to the low-speed link and congestion will occur on the network.

MSTP provides Root protection function to protect the root bridge: The port configured with Root protection only plays a role of designated port on every instance. Whenever such a port receives a higher-priority BPDU, it will be set to listening state and not forward packets any more (as if the link to the port is disconnected). If the port has not received any higher-priority BPDU for a certain period of time thereafter, it will resume the normal state.

Related command: **stp interface root-protection**.

Example

Enable Root protection on the Ethernet2/1/1 port of the switch.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface Ethernet2/1/1
[3Com-Ethernet2/1/1] stp root-protection
```

stp tc-protection

Syntax

stp tc-protection enable

stp tc-protection disable

View

System view

Parameter

None

Description

Use the **stp tc-protection enable** command to enable the protection function so that the switch is protected against attack from TC-BPDU packets.

Use the **stp tc-protection disable** command to disable the protection function.

By default, the protection against TC-BPDU packet attack is enabled.

As a general rule, the switch deletes the corresponding entries in the MAC address table and ARP table upon receiving TC-BPDU packets. Under malicious attacks of TC-BPDU packets, the switch shall receive a great number of TC-BPDU packets in a very short period. Too frequent delete operations shall consume huge switch resources and bring great risk to network stability.

When the protection from TC-BPDU packet attack is enabled, the switch just perform one delete operation in a specified period (generally, 15 seconds) after receiving TC-BPDU packets, as well as monitoring whether it receives TC-BPDU packets during this period. Even if it detects a TC-BPDU packet is received in a period shorter than the specified interval, the switch shall not run the delete operation till the specified interval is reached. This can avoid frequent delete operations to the MAC address table and ARP table.

Example

Enable TC-BPDU protection on the switch.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] stp tc-protection enable
```

stp timer forward-delay

Syntax

stp timer forward-delay *centi-senconds*

undo stp timer forward-delay

View

System view

Parameter

centi-senconds: Specifies Forward Delay, which is in the range from 400 to 3000 and measured in centiseconds. By default, the Forward Delay of the switch is 1500 centiseconds.

Description

Use the **stp timer forward-delay** command to configure Forward Delay for the switch.

Use the **undo stp timer forward-delay** command to restore the default Forward Delay.

To avoid temporary loop, MSTP defines a medium state, Learning, when the port switches from the Discarding state to Forwarding state. There is also a delay before state switchover to guarantee the synchronous switchover with the remote switch.

The Forward Delay configured on the root bridge determines the state transition time.

The root bridge will determine the state transition time according to the configured values, while the other switches will apply the forward delay configured on it.

When configuring Hello time, Forward Delay and Max Age, guarantee the following equations:

2 x (Forward Delay - 1.0 second) >= Max Age

Max Age >= 2 x (Hello Time + 1.0 second)

Only if the above-mentioned formulas are equal can the MSTP normally operate on the entire network. Otherwise, the network may flap frequently. You are recommended to use the **stp bridge-diameter** command to specify the diameter of the switching network, so that MSTP can automatically calculate and give the moderate values for the time parameters.

Hello time, ***Forward Delay*** *and* ***Max Age*** *affect each other. Modifying any of them will affect the value of other two parameters.*

Related command: **stp timer hello**, **stp timer max-age**, **stp bridge-diameter**.

Example

Set the Forward Delay of the device to 2000 centiseconds.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] stp timer forward-delay 2000
```

stp timer hello

Syntax

stp timer hello *centi-senconds*

undo stp timer hello

View

System view

Parameter

centi-senconds: Specifies Hello Time value with an integer in the range of 100 to 1000 in units of centiseconds. By default, the Hello Time of the switch is 200 centiseconds.

Description

Use the **stp timer hello** command to configure Hello Time of the switch.

Use the **undo stp timer hello** command to restore the default Hello Time.

The STP defines to transmit configuration BPDU regularly at an interval specified with **Hello Time** to keep the spanning tree stable. If the switch receives no **BPDU** packets for a period of time, it will recalculate the spanning tree upon the BPDU

timeouts. The root bridge transmits **BPDU** packets at an interval as you configured, while other switches apply the **Hello Time** configured on the root bridge.

When configuring Hello time, Forward Delay and Max Age, remember to guarantee the following equations:

2 x (Forward Delay -1.0 second) >= Max Age

Max Age >= 2 x (Hello Time + 1.0 second)

Only if the earlier-mentioned formulas are equal can the MSTP normally operate on the entire network. Otherwise, the network may flap frequently. You are recommended to use the **stp bridge-diameter** command to specify the diameter of the switching network, so that MSTP can automatically calculate and give the moderate values for the time parameters.

Related command: **stp timer forward-delay**, **stp timer max-age**, **stp bridge-diameter**.

Example

Set Hello Time of the switch to 400 centiseconds.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z
[SW8800] stp timer hello 400
```

stp timer max-age

Syntax

stp timer max-age *centi-senconds*

undo stp timer max-age

View

System view

Parameter

centi-seconds: Specifies the Max Age, which is in the range from 600 to 4000 and measured with centiseconds. By default, the Max Age of the switch is 2000 centiseconds.

Description

Use the **stp timer max-age** command to configure the Max Age of the switch.

Use the **undo stp timer max-age** command to restore the default Max Age.

MSTP can detect the link fault and automatically resume the forwarding state of the redundant link. On the CIST, the switch checks if the configuration BPDU received via the port expires according to the Max Age. If the BPDU expires, the MSTI has to be calculated again.

Max Age takes no effect on MSTIs. If the current switch is CIST root bridge, it will check if the configuration BPDU expires according to the configured Max Age. Otherwise, the switch adopts the Max Age configured on the CIST root bridge.

When you configure **Hello time, Forward Delay** and **Max Age**, remember to guarantee the following equations:

2 x (Forward Delay -1.0 second) >= Max Age

Max Age >= 2 x (Hello Time + 1.0 second)

Only if the earlier-mentioned formulas are equal can the MSTP normally operate on the entire network. Otherwise, the network may flap frequently. You are recommended to use the **stp bridge-diameter** command to specify the diameter of the switching network, so that MSTP can automatically calculate and give the moderate values for the time parameters.

Related command: **stp timer forward-delay**, **stp timer hello**, **stp bridge-diameter**.

Example

Set Max Age of the device to 1000 centiseconds.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] stp timer max-age 1000
```

stp timer-factor

Syntax

stp timer-factor *number*

undo stp timer-factor

View

System view

Parameter

number: Specifies the multiple of hello time, in the range of 1 to 10. The default value is 3.

Description

Use the **stp timer-factor** command to configure the multiple of hello time for the switch.

Use the **undo stp timer-factor** command to restore the default multiple value.

The Ethernet switch transmits STP packets every hello time. Generally, if the switch does not receive the STP packets from the upstream switch for three times of hello time, the switch will decide the upstream switch is dead and will recalculate the topology of the network. Then in steady network, the recalculation may be caused when the upstream is busy. In this case, users can redefine the timeout interval to a longer time (four times the hello time or larger) by define the multiple of hello time. It is recommended to set 5, 6 or 7 as the value of multiple in the steady network.

Example

Set the multiple value of hello time to 7.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] stp timer-factor 7
```

stp transmit-limit

Syntax

stp transmit-limit *packetnum*

undo stp transmit-limit

View

Ethernet port view

Parameter

packetnum: Specifies the amount limit to the transmitted packets, ranging from 1 to 255 (expressed as a counter value without any units). By default, the value is 3.

Description

Use the **stp transmit-limit** command to configure an amount limit to the configuration BPDU transmitted via a port during the Hello Time.

Use the **undo stp transmit-limit** command to restore the default limit.

The larger the value is, the more packets can be transmitted in a time unit, yet the more switch resources will be occupied. With a moderate value, the amount of the BPDUs transmitted during Hello Time via every port can be limited and MSTP will not occupy too many bandwidth resources when the network topology flaps.

Related command: **stp interface transmit-limit**.

Example

Set a limit of 5 to the packets transmitted via Ethernet2/1/1.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface Ethernet2/1/1
[3Com-Ethernet2/1/1] stp transmit-limit 5
```

vlan-mapping modulo

Syntax

vlan-mapping modulo *modulo*

undo vlan-mapping modulo

View

MST region view

Parameter

modulo: Specifies the modulus, ranging from 1 to 48.

Description

Use the **vlan-mapping modulo** command to map fast and symmetrically all VLAN lists to the specified MSTIs according to the modulo operation results.

g modulo command to disable the function.

Use the **undo vlan-mappin**

By default, all the VLANs are mapped to CIST, namely Instance 0.

Related command: **region-name**, **revision-level**, **check region-configuration**, **active region-configuration**

Example

Map VLAN to MSTI based on modulo 16.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800]stp region-configuration
[3Com-mst-region] vlan-mapping modulo 16
```

14 DIGEST SNOOPING CONFIGURATION COMMANDS

Digest Snooping Configuration Commands

stp config-digest-snooping

Syntax

stp config-digest-snooping

undo stp config-digest-snooping

View

System view, Ethernet port view

Parameter

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.

Digest snooping is disabled by default.

According to IEEE 802.1s, two connected switches can communicate with each other through multiple spanning tree instances (MSTIs) in a multiple spanning tree protocol (MSTP) domain only when they are configured with the same domain settings. With MSTP employed, interconnected switches determine whether or not they are in the same domain by checking the configuration IDs of the bridge protocol data units (BPDUs) between them. (A configuration ID comprises information such as domain ID, configuration digest.)

As switches of some manufacturers come with some proprietary protocols concerning spanning trees employed, a switch of this type cannot communicate with other switches in an MSTP domain even if it is configured with the same domain settings as other switches in the MSTP domain.

This kind of problems can be overcome by implementing digest snooping. Digest snooping enables a switch to track and maintain configuration digests of other switches that are in the same domain and come from other manufacturers by examining their BPDUs. It also enables the switch to insert corresponding configuration digests in its BPDUs destined for these switches. In this way, switches of different manufacturers are capable of communicating with each other in an MSTP domain.

- You must enable digest snooping on a port first before enabling it globally.
- Digest snooping is unnecessary if the interconnected switches are from the same manufacturer.
- When implementing digest snooping, make sure that the domain configurations of the switches of different manufacturers are exactly the same to prevent possible broadcast storm caused by otherwise inconsistent mapping relationships between VLANs and VPN instances of each switch.
- If you want to change the configuration of a domain with one or multiple of its switches being digest snooping-enabled, be sure to disable digest snooping on these switches first to prevent possible broadcast storm caused by otherwise inconsistent mapping relationships between VLANs and VPN instances of each switch.
- To enable digest snooping, all ports in an MSTP domain connecting to switches coming from other manufacturers must have digest snooping enabled.
- Do not enable digest snooping on border ports of an MSTP domain.
- A digest snooping-enabled switch always keeps the latest configuration digests it receives. A configuration digest remains valid even if the corresponding port goes down.

Example

Enable digest snooping on the GigabitEthernet3/1/1 port.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface GigabitEthernet3/1/1
[3Com-GigabitEthernet3/1/1] stp config-digest-snooping
[3Com-GigabitEthernet3/1/1] quit
[SW8800]stp config-digest-snooping
```

15 BPDU TUNNEL CONFIGURATION COMMANDS

BPDU Tunnel Configuration Commands

vlan-vpn enable

Syntax

vlan-vpn enable

undo vlan-vpn

View

Ethernet port view

Parameter

None

Description

Use the command **vlan-vpn enable** to enable VLAN VPN (QinQ) on the port.

Use the **undo vlan-vpn** command to disable VLAN VPN (QinQ) on the port.

By default, VLAN VPN is disabled on all the ports.

Example

Enable VLAN VPN on the switch. note2

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface Ethernet3/1/3
[3Com-Ethernet3/1/3]vlan-vpn enable
```

vlan-vpn tunnel

Syntax

vlan-vpn tunnel

undo vlan-vpn tunnel

View

System view

Parameter

None

Description

Use the **vlan-vpn tunnel** command to enable bridge protocol data unit (BPDU) Tunnel on the switch.

Use the **undo vlan-vpn tunnel** command to disable BPDU Tunnel on the switch.

BPDU Tunnel enables geographically segmented user network to transmit BPDU packets transparently over the specified VLAN VPN on the operator's network. This allows the user network to participate in a uniform spanning tree calculation while maintaining a separate spanning tree from the operator network.

By default, BPDU Tunnel is disabled.

CAUTION:

- To enable BPDU Tunnel on a switch, you must first enable STP on it. Otherwise, the client network BPDU will not be processed by the CPU when entering the switch, nor MAC address replacement or transparent transmission will be implemented.
- To enable BPDU Tunnel on a port, you must configure the port as access and the intermediate carrier network as trunk.
- You cannot enable BPDU Tunnel on a port on which DOT1X, GComware, STP or NTDP is enabled.

Example

Enable BPDU Tunnel on the switch.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] vlan-vpn tunnel
```

16 ACL COMMANDS

ACL Commands

acl

Syntax

acl { **number** *acl-number* | **name** *acl-name* [**advanced** | **basic** | **link**] } [**match-order** { **config** | **auto** }]

undo acl { **number** *acl-number* | **name** *acl-name* | **all** }

View

System view

Parameter

number *acl-number*: ACL number, in the range of:

2000 to 2999: Represents basic ACL.

3000 to 3999: Represents advanced ACL.

4000 to 4999: Represents Layer 2 ACL.

name *acl-name*: Character string, which must be started with an English letter (i.e., a-z or A-Z), and there should not be a space in it; case insensitive, key words **all** and **any** are not allowed to use.

advanced: Advanced ACL.

basic: Basic ACL.

link: Layer 2 ACL.

config: In configuration order during matching ACL rules.

auto: In depth-first order during matching ACL rules.

all: Deletes all ACLs (both number- and name-identified ones).

Description

Use the **acl** command to define a number- or name-identified ACL and enter its view.

Use the **undo acl** command to delete all rules of an ACL or all ACLs.

By default, the system matches ACL rules in configuration order.

Using the **acl** command, you can create an ACL named "*acl-name*". And the type of this ACL is decided by keywords: "**advanced**", "**basic**" or "**link**". After entering a corresponding ACL view, no matter the ACL is identified by a number or a name, you can use the **rule** command to create rules of this named ACL (you can exit ACL view by using the **quit** command).

You can select the **match-order** keyword to specify whether to match ACL rules in configuration order or depth-first order (matching the rules with smaller range first). By default, the former mode is selected. You cannot modify the matching order once you specify it. To do so, you have to delete all rules of the ACL and specify a matching order for it again.

The user-defined ACL matching order takes effect only when multiple rules of one ACL are applied at the same time. For example, an ACL has two rules. If the two rules are not applied simultaneously, even if you configure the matching order to be depth first, the switch still matches them according to their application order.

If one rule is a subset of another rule in an ACL, it is recommended to apply the rules according to the range of the specified packets. The rule with the smallest range of the specified data packets is applied first, and then other rules are applied based on this principle.

If one ACL is used, you cannot use the **undo acl all** command to delete any ACL.

Related command: **rule**.

Example

Specify depth first order as the match order of number 2000 ACL.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] acl number 2000 match-order auto
```

display acl config

Syntax

display acl config { **all** | *acl-number* | *acl-name* }

View

Any view

Parameter

all: Displays all ACLs (both number- and name-identified ones).

acl-number: Serial number of the ACL to be displayed, in the range of 2000 to 4999.

acl-name: Name of the ACL to be displayed. String parameter which must start with an English letter ([a-z, A-Z]) and no space is allowed in it.

Description

Use the **display acl config** command to view the configuration details of the ACL, including all the rules, their serial numbers, quantities and number of bytes of matched packets.

The matched times here refer to the software matched times, that is, the matched times of the ACLs that needed to be processed by CPU. You can collect hardware matched times value by using the **traffic-statistic** command.

Example

Display contents of all ACLs.

```
<SW8800> display acl config all
Link ACL  4000, 1 rule,
 rule 0 permit ingress any egress any

Basic ACL   traffic-of-host, 1 rule,
 rule 1 deny source 10.1.1.1 0 time-range 3com-3com(0 times matched) (Active)
```

display acl remaining entry

Syntax

display acl remaining entry slot *slotid*

View

Any view

Parameter

slot *slotid*: the ID of the specified slot.

Description

Use the **display acl running-packet-filter** command to display the total number of ACL rules that are applied on the specified card.

Example

Display the total number of ACL rules that are applied on the slot 5.

```
<SW8800> display acl remaining entry slot 5
Slot: 5
  Resource  Total    Reserved  Configured  Remaining    Start        End
    Type    Number   Number     Number      Number    Port Name   Port Name
------------------------------------------------------------------------------
   METER     256        0          0          256       GE5/1/1   GE5/1/12
   METER     256        0          0          256      GE5/1/13   GE5/1/24
    RULE    1024        0          0         1024       GE5/1/1   GE5/1/12
    RULE    1024        0          0         1024      GE5/1/13   GE5/1/24
  ACTION    1024          0          0         1024       GE5/1/1   GE5/1/12
  ACTION    1024        0          0         1024      GE5/1/13   GE5/1/24
```

Table 28 The description of the information on display

Field	Description
Resource Type	Resource type
	METER**:** the resource is the flow **meter** resource; RULE**:** the resource is the rule resource; ACTION**:** the resource is action **resource**
Total Number	The total number of ACL rules that are supported by the hardware
Reserved Number	The number of the reserved ACL rules
Configured Number	The number of the ACL rules that have been configured
Remaining Number	The number of the remaining ACL rules
Start Port **Name, End** Port Name	The name**s** of the start port and the end port

display acl running-packet-filter

Syntax

display acl running-packet-filter { **all** | **interface** *interface-type interface-number* | **vlan** *vlan-id* }

View

Any view

Parameter

all: Displays all the ACLs that have been applied (including the number-identified ones and name-identified ones)

interface *interface-type interface-number*: The port of the switch. Refer to the description in the *Port Module Command Manual* for details. The ACL application information on the specified port of a normal card displays when the parameter is specified.

vlan: Displays the ACL application information under the VLAN configured through the service process card.

vlan-id: the ID of the VLAN, in the range of 1-4094.

Description

Use the **display acl running-packet-filter** command to display the ACL application information, including the name of the ACL, the name of the sub items and the application state.

Example

Display the ACL application information of port Ethernet3/1/1.

```
<SW8800> display acl running-packet-filter ethernet3/1/1
Ethernet3/1/1
 Inbound:
 Acl 4000 rule 0  running
```

Display the ACL application information of VLAN2

```
<SW8800> display acl running-packet-filter vlan 2
Vlan 2
 Inbound:
 Acl 2000 rule 1 slot 6  running
```

display flow-temlate

Syntax

display flow-template [**default** | **interface** *interface-type interface-number* | **slot** *slotid* | **user-defined**]

View

Any view

Parameter

default: Displays the default flow template of the system.

interface *interface-type interface-number*: Displays the flow template applied on the specified port.

slot *slotid*: Displays the flow template applied on the specified card.

user-defined: Displays the user-defined flow template.

Description

Use the **display flow-template** command to view the detailed configuration of flow template. The configuration includes which parameters the flow template defines and which ports/cards is the flow template applied on.

3Com Switch 8800 Family Series Routing Switches (hereinafter referred to as Switch 8800 Family series) support two flow templates: one is user-defined; the other is the default one. If you do not input any parameter for this command, the detailed configuration of all flow templates will be displayed.

Related command: **flow-template user-defined**.

Example

Display information about the default flow-template.

```
<SW8800> display flow-template default
default flow template :  ip-protocol tcp-flag sport dport icmp-type
icmp-code sip 0.0.0.0 dip 0.0.0.0 vlanid
```

display time-range

Syntax

display time-range { **all** | *name* }

View

Any view

Parameter

all: Displays all time ranges.

name: Time range name, string starting with an English letter ([a-z, A-Z]) and in the range of 1 to 32 characters.

Description

Use the **display time-range** command to view the configuration and status of current time range. For active time range, the system shows "active" and "inactive" for inactive time range.

A delay, about one minute, exists in system's updating ACLs, but the result of the **display time-range** command is based on the current time. Then there may the case where a time range have been shown active using the **display time-range** command, while it is still inactive in importing the ACL. You just take it as a normal case.

Related command: **time-range**.

Example

Display all time ranges.

```
<SW8800> display time-range all
Current time is 14:36:36 4-3-2003 Thursday
```

```
Time-range : hhy ( Inactive )
 from 08:30 2-5-2005 to 18:00 2-19-2005

Time-range : hhy1 ( Inactive )
 from 08:30 2-5-2003 to 18:00 2-19-2003
```

Table 29 Description of displayed information

Field	Description
Current time is 14:36:36 4-3-2003 Thursday	The current time of the system
Time-range : hhy (Inactive)	Time range testhhy**. "**Inactive**"** means that the time range is inactive currently ("active" means the time range is active), and the time range is from 08:30 2-5-2005 to 18:00 2-19-2005
from 08:30 2-5-2005 to 18:00 2-19-2005	The displayed information below is similar.

Display time range tm1.

```
<SW8800> display time-range tm1
Current time is 14:37:31 4-3-2003 Thursday

Time-range : tm1 ( Inactive )
from 08:30 2-5-2005 to 18:00 2-19-2005
```

Table 30 Description of displayed information

Filed	Description
Current time is 14:36:36 4-3-2003 Thursday	The current time of the system.
Time-range : tm1 (Inactive)	Time range tml**. "**Inactive**"** means **that** the time range is inactive currently (active means the time range is active), and the time range is from 08:30 2-5-2005 to 18:00 2-19-2005
from 08:30 2-5-2005 to 18:00 2-19-2005	The **displayed** information **below** is similar.

flow-template user-defined

Syntax

flow-template user-defined

undo flow-template user-defined

View

Ethernet port view/port group view

Parameter

None.

Description

Use the **flow-template user-defined** command to apply the user-defined flow template to the current port or port group.

Use the **undo flow-template user-defined** command to cancel the applied flow template on the current port or port group.

Related command: **display flow-template**, **flow-template user-defined slot** *slotid template-info*.

Example

Apply the user-defined flow template to current port Ethernet4/1/1.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface Ethernet2/1/1
[3Com-Ethernet4/1/1] flow-template user-defined
```

flow-template user-defined template-info

Syntax

flow-template user-defined slot *slotid template-info*

undo flow-template user-defined slot *slotid*

View

System view

Parameter

template-info: Information available in defining a traffic template, its value can be:

- bt-flag: BT flag bit, in the length of 6 bytes.
- c-tag-cos: 802.1p priority in the internal 802.1QTag carried by the packet, in the length of 2 bytes together with c-tag-vlanid in the flow template.
- c-tag-vlan: the VLAN ID in the internal 802.1QTag carried by the packet, in the length of 2 bytes together with c-tag-cos in the flow template.
- cos: 802.1p priority in the most external 802.1QTag carried by the packet, in the length of 2 bytes together with s-tag-vlan in the flow template.
- dip *wildcard*: Destination IP domain in the IP packet header, in the length of 4 bytes.
- dmac *wildcard*: Destination MAC domain in the Ethernet packet header, in the length of 6 bytes.
- dport: Destination port domain, in the length of 2 bytes.
- dscp: DSCP domain in the IP packet header. *dscp, exp, ip-precedence and tos* altogether occupy 1 byte.
- ethernet-protocol: Protocol type domain in the Ethernet packet header, in the length of 6 bytes.
- exp: EXP field in MPLS packet. *dscp, exp, ip-precedence and tos* altogether occupy 1 byte.
- fragment-flags: Flag field of fragment in IP packed header, no bytes in flow template.
- icmp-code: ICMP code domain, in the length of 1 byte.
- icmp-type: ICMP type domain, in the length of 1 byte.
- ip-precedence: IP priority domain in the IP packet header. *dscp, exp, ip-precedence and tos* altogether occupy 1 byte.
- ip-protocol: Protocol type domain in the IP packet header, in the length of 1 byte.

- Mac-type: MAC-TYPE field of a specified packet, no bytes in the flow template.
- s-tag-vlan: The VLAN ID in the most external 802.1QTag that the packet carries, in the length of 2 bytes together with cos in the flow template.
- sip *wildcard* : Source IP domain in the IP packet header, in the length of 4 bytes.
- smac *wildcard*: Source MAC domain in the Ethernet packet header, in the length of 6 bytes.
- sport: Source port domain, in the length of 2 bytes.
- tcp-flag: Flag domain in the TCP packet header, in the length of 1 byte.
- tos: TOS (type of service) domain in the IP packet header. *dscp, exp, ip-precedence and tos* altogether occupy 1 byte.
- vlanid: VLAN ID which the switch assigns to the packet , in the length of 2 bytes.
- vpn: the flow template which is pre-defined for the MPLS L2VPN, in the length of 2 bytes.

- The above mentioned information about how many bytes a field occupies applies to traffic templates instead of IP packets. For example, DSCP field occupies one byte in flow template, but six bits in IP packets. You can determines whether the total length of template elements exceeds 16 bytes using these numbers.
- The dscp, exp, ip-precedence and tos fields jointly occupy one byte no matter you define any one of these four fields or the ip-precedence and tos field simultaneously.
- The cos and s-tag-vlan fields jointly occupy two bytes no matter you define one or both of these two fields. The c-tag-cos and c-tag-vlanid fields occupy two bytes in the same way.
- The fragment-flags and mac-type fields occupy no byte in the flow template, so just ignore them when you determine whether the total length of template elements exceeds 16 bytes.

slot *slotid*: Specifies the slot on which the flow template applied.

Description

Use the **flow-template user-defined slot** *slotid template-info* command to define a flow template.

Use the **undo flow-template user-defined slot** *slotid* command to delete a flow template.

In defining a flow template, the total length of all elements should not be more than 16 bytes.

Currently, the default flow template is as follows:

ip-protocol tcp-flag sport dport icmp-type icmp-code sip 0.0.0.0 dip 0.0.0.0 vlanid

You cannot modify or delete the default flow template, but those you have defined.

Related command: **display flow-template**, **flow-template user-defined**.

Example

Define a flow template which classifies traffic by source and destination IP addresses, source and destination TCP/UDP ports, DSCP domain in the IP packet header.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] flow-template user-defined slot 3 sip 0.0.0.0 dip 0.0.0.0
sport dport dscp
```

packet-filter

Syntax

Command Format Which Only Applies IP Group ACL

packet-filter inbound ip-group { *acl-number* | *acl-name* } [**rule** *rule* [**system-index** *index*]]

undo packet-filter inbound ip-group { *acl-number* | *acl-name* } [**rule** *rule*]

In VLAN view:

packet-filter inbound ip-group { *acl-number* | *acl-name* } [**rule** *rule*] [**system-index** *index*] **slot** *slotid*

undo packet-filter inbound ip-group { *acl-number* | *acl-name* } [**rule** *rule*] **slot** *slotid*

Command Format Which Applies IP Group and Link Group ACL at Same time

packet-filter inbound ip-group { *acl-number* | *acl-name* } { **rule** *rule* **link-group** { *acl-number* | *acl-name* } [**rule** *rule* [**system-index** *index*]] | **link-group** { *acl-number* | *acl-name* } **rule** *rule* }

undo packet-filter inbound ip-group { *acl-number* | *acl-name* } { **rule** *rule* **link-group** { *acl-number* | *acl-name* } [**rule** *rule*] | **link-group** { *acl-number* | *acl-name* } **rule** *rule* }

Command Format Which Only Applies Link Group ACL

packet-filter inbound link-group { *acl-number* | *acl-name* } [**rule** *rule* [**system-index** *index*]]

undo packet-filter inbound link-group { *acl-number* | *acl-name* } [**rule** *rule*]

View

Ethernet port view, port group view

Parameter

inbound: Performs filtering to the packets received by the interface.

ip-group { *acl-number* | *acl-name* }: Activates IP ACLs, including basic and advanced ACLs. *acl-number* : Sequence number of ACL, ranging from 2000 to

3999. *acl-name*: Name of the ACL, which must be a character string starting with an English letter (a-z or A-Z), and without any space in it.

link-group { *acl-number* | *acl-name* }: Activates Layer 2 ACLs. *acl-number*: Sequence number of ACL, ranging from 4000 to 4999. *acl-name*: Name of ACL, which must be a character string started with an English letter (a-z or A-Z), and without any space in it.

rule *rule*: Specifies the rule of an active ACL, ranging from 0 to 127; if not specified, all rules of ACL will be activated.

system-index *index* here is the system index for an ACL rule. When delivering a rule, the system assigns a globally unique index to it, for convenience of later retrieval. You can also assign a system index for it when delivering an ACL rule with this command, but this value may change in the system operation process. However, you are not recommended to manually assign a system index if not urgently necessary.

slot *slotid*: Slot number of a service processor card.

Description

Use the **packet-filter** command to activate an ACL.

Use the **undo packet-filter** command to deactivate an active ACL.

Example

Activate ACL 2000.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800]interface ethernet5/1/1
[3Com-Ethernet5/1/1] packet-filter inbound ip-group 2000
```

reset acl counter

Syntax

reset acl counter { **all** | *acl-number* | *acl-name* }

View

User view

Parameter

all: Displays all ACLs (both number- and name-identified ones).

acl-number: Serial number of the ACL, in the range of 2000 to 3999.

acl-name: ACL name, string parameter ranging from 1 to 32 bytes. It must start with an English letter ([a-z, A-Z]). No space is allowed in it. It is case insensitive. The keywords **all** is forbidden.

Description

Use the **reset acl counter** command to clear ACL statistics to zero.

Example

Clear the statistics of ACL 2000.

```
<SW8800> reset acl counter 2000
```

rule **Syntax**

Define or delete the subrules of a basic ACL

rule [*rule-id*] { **permit** | **deny** } [**source** { *source-addr wildcard* | **any** } | **fragment** | **time-range** *name* | **vpn-instance** *instance-name*]*

undo rule *rule-id* [**source** | **fragment** | **time-range** | **vpn-instance** *instance-name*]*

Define or delete the subrules of an advanced ACL

rule [*rule-id*] { **permit** | **deny** } *protocol* [**source** { *source-addr wildcard* | **any** }] [**destination** { *dest-addr wildcard* | **any** }] [**source-port** *operator port1* [*port2*]] [**destination-port** *operator port1* [*port2*]] [**icmp-type** *type code*] [**established**] [[**precedence** *precedence* | **tos** *tos*]* | **dscp** *dscp*] [**fragment**] [**bt-flag**] [**time-range** *name*] [**vpn-instance** *instance-name*]

undo rule *rule-id* [**source** | **destination** | **source-port** | **destination-port** | **icmp-type** | **precedence** | **tos** | **dscp** | **fragment** | **bt-flag | time-range** | **vpn-instance**]*

Define or delete the rules of a Layer 2 ACL

rule [*rule-id*] { **permit** | **deny** } [**cos** *cos-value* | **c-tag-cos** *c-cos-value* | **exp** *exp-value* | *protocol-type* | **mac-type** { **any-broadcast-packet** | **arp-broadcast-packet** | **non-arp-broadcast-packet** | { { **unicast-packet** | **multicast-packet** } [**known** | **unknown**] } } | **ingress** { { *source-vlan-id* [**to** *source-vlan-id-end*] | *source-mac-addr source-mac-wildcard* | **c-tag-vlan** *c-tag-vlanid* }* | **any** } | **egress** { *dest-mac-addr dest-mac-wildcard* | **any** } | **s-tag-vlan** *s-tag-vlanid* | **time-range** *name*]*

undo rule *rule-id*

View

Corresponding ACL view

Parameter

rule-id: Specifies a rule number of the ACL, in the range of 0 to 127

permit: Allows qualified packets to pass.

deny: Forbids qualified packets to pass.

CAUTION: *If the* ***rule*** *command includes the* ***deny*** *key word, the rule created can be used for the* ***packet-filter*** *command and the* ***traffic-statistic*** *command only.*

time-range *name*: Time range name, optional parameter. It means the rule takes effect in this time range.

The following parameters are for the attributes of the packet. The ACL generates rules according to these attribute parameters.

- Parameters specific to basic ACLs:

source { *source-addr wildcard* | **any** }: *source-addr wildcard* specifies the source IP address and wildcard digit of source address represented in dotted decimal notation. **any** represents all source addresses.

fragment: It is only effective to fragmented messages and is ignored by non-fragmented messages.

vpn-instance *instance-name:* VPN instance name. The specified MPLS VPN packets will be identified if this parameter is selected.

- Parameters specific to advanced ACLs:

protocol: Specifies the protocol type which is represented by a name or a number. For name format, the options include icmp, igmp, tcp, udp, ip, gre, ospf, ipinip etc. The IP parameter represents all IP protocols. For number format, the value ranges from 1 to 255.

source { *source-addr wildcard* | **any** }: *source-addr wildcard* specifies the source IP address and wildcard digit of source address represented, in dotted decimal notation. **any** represents all source addresses.

destination { *dest-addr wildcard* | **any** }: *dest-addr wildcard* specifies the destination IP address and wildcard digit of destination address represented, in dotted decimal notation. **any** represents all destination addresses.

source-port *operator port1* [*port2*]: Source TCP or UDP port ID of the packet. *operator* means port operator, with options including eq (equal to), gt (greater than), lt (less than), neq (not equal to) and range (in the range of). Note that it appears only when the *protocol* parameter is set as TCP or UDP. *port1* [*port2*] stands for source TCP or UDP port ID of the packet, in characters or digits. Digital value ranges from 0 to 65535. For character options, see the port ID mnemonic symbol list. Only for the range operator, both *port1* and *port2* are active. For the rest operators, only *port1* is required.

destination-port *operator port1* [*port2*]: Destination TCP or UDP port ID of the packet. See **source-port** *operator port1* [*port2*] for detailed description.

icmp-type *type code*: It is active when the protocol is set as icmp. *type code* specifies an ICMP packet. *type* indicates ICMP packet type, in characters or digits. The digital value ranges from 0 to 255. *code* is ICMP code, which is active when ICMP is selected and the ICMP packet type is expressed in the numeral format. It ranges from 0 to 255. This parameter is used to define an EACL.

Table 31 Relationship of type and code

ICMP packet type (TYPE)	ICMP packet type (TYPE)	ICMP code (CODE)
echo	8	0
echo	0	0
fragmentneed-DFset	3	4
host-redirect	5	1
host-tos-redirect	5	3
host-unreachable	3	1
information-reply	16	0

Table 31 Relationship of type and code

ICMP packet type (TYPE)	ICMP packet type (TYPE)	ICMP code (CODE)
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
ttl-exceeded	11	0

established: (Optional) It is effective only to the first SYN packet established by TCP and active when *protocol* is set as *tcp*.

precedence *precedence*: (Optional) IP priority level, in a number (ranging from 0 to 7) or a name.

tos *tos*: (Optional) Indicating packets are classified by TOS value, in a number (ranging 0 to 15) or a name.

dscp *dscp*: (Optional) Indicating packets are classified by DSCP value, in a number (ranging from 0 to 63) or a name.

fragment: It is only effective to fragmented messages and is ignored by non-fragmented messages.

bt-flag: It indicates that the rule is effective to BT data messages only. If you use this key word, the *protocol* in the rule must be **tcp**. The parameter is applicable to defining the advanced ACLs.

vpn-instance *instance-name:* VPN instance name. The specified MPLS VPN packets will be identified if this parameter is selected.

- Parameters specific to Layer 2 ACLs:

cos: Specifies 802.1p priority in the most external 802.1QTag carried by the packet.

cos-value: In number format (ranging 0 to 7) or just entering the priority name. See Table 1-5 for their correspondence.

Table 32 COS priority definition

Number	Priority name
0	best-effort
1	background

Table 32 COS priority definition

Number	Priority name
2	spare
3	excellent-effort
4	controlled-load
5	video
6	voice
7	network-management

c-tag-cos *c-cos-value*: Specified 802.1p priority in the internal 802.1QTag carried by the packet. Specify the same value for the *c-cos-value* and *cos-value* parameters.

protocol-type: This parameter is used to specify the protocol type carried by the Ethernet frame. The protocol type can be expressed by either a name or a hexadecimal number. When the protocol type is expressed by a name, the value can be arp, ip, ipv6, mpls, nbx, pppoe-control, pppoedata and rarp. When the protocol type is expressed by a hexadecimal number, the range is 1-FFFF.

ingress { { *source-vlan-id* [**to** *source-vlan-id-end*] | *source-mac-addr source-mac-wildcard* | **c-tag-vlan** *c-tag-vlanid* | **any** }: Source information of the packet. *source-vlan-id* [**to** *source-vlan-id-end*] shows its source VLAN or source VLAN range (identified by the external VLAN Tag of the packet). *source-mac-addr source-mac-wildcard* shows source MAC address and wildcard of the source address. The two parameters jointly determine the range of the source MAC addresses in which the user is interested. The smaller the wildcard, the smaller the range of the MAC address. For example, 00e0-fc01-0101 0-0-0 specifies a MAC address: 00e0-fc01-0101, but 00e0-fc01-0101-0-0-fff specifies an address range: 00e0-fc01-0000 to 00e0-fc01-ffff.

c-tag-vlan *c-tag-vlanid*: Indicates the system identifies the source VLAN according to the information about VLAN ID in the internal 802.1QTag carried by the packet. **any** represents all packets received from all the ports.

egress { *dest-mac-addr dest-mac-wildcard* | **any** }: Destination information of the packet. *dest-mac-addr dest-mac-wildcard* shows destination MAC address and wildcard of the destination address. The two parameters work together to determine the range of the destination MAC addresses in which the user is interested. The smaller the wildcard, the smaller the range of the MAC address. For example, 00e0-fc01-0101 0-0-0 specifies a MAC address: 00e0-fc01-0101, but 00e0-fc01-0101-0-0-fff specifies an address range: 00e0-fc01-0000 to 00e0-fc01-ffff. **any** represents all packets transferred at all the ports.

s-tag-vlanid *s-tag-vlanid*: VLAN ID in the most exterior 802.1QTag carried by the specified packets.

mac-type { **any-broadcast-packet** | **arp-broadcast-packet** | **non-arp-broadcast-packet** | { { **unicast-packet** | **multicast-packet** } [**known** | **unknown**] } }: Specifies the packet type, such as unicast, multicast, ARP broadcast, and non-ARP broadcast. Unicast and multicast packets can be divided into known and unknown packets.

Description

Use the **rule** command to add a rule to the ACL.

Use the **undo rule** command to delete a rule from the ACL.

You can define multiple rules for an ACL. Only the specified rules will be deleted if you select parameters in the **undo rule** command.

If you redefine an existing rule, the newly configured option automatically overwrites the corresponding option of the original rule, and the option not being redefined remains. For example:

With the original rule 0:

```
[acl number 2000]rule 0 permit source 10.1.1.1 0 time-range 3Com
```

when redefine it as follows:

```
[acl number 2000]rule 0 permit source 10.1.1.2 0 fragment
```

it becomes:

```
rule 0 permit source 10.1.1.2 0 fragment time-range 3Com
```

That is, the source option is replaced with 10.1.1.2, the fragment option which the original rule does not contain is added, and the time-range 3Com option which the original rule contains is reserved.

CAUTION:

- If you want to replace an existing rule, you are recommended to use the undo command to delete the original rule fist, and then reconfigure the rule. This makes sure the unwanted options are completely removed.
- If you configure a rule without providing the rule number, the system will automatically generate a new rule if the rule is not identical to any existing rules.
- The rule with the specified bt-flag cannot be used in the traffic-redirect command.

Related command: **acl**.

Example

Add a rule to the advanced ACL.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800]acl number 3000
[3Com-acl-adv-3000] rule 1 permit tcp established source 1.1.1.1 0
destination 2.2.2.2 0
```

time-range

Syntax

time-range *time-name* { *start-time* **to** *end-time days-of-the-week* [**from** *start-time start-date*] [**to** *end-time end-date*] | **from** *start-time start-date* [**to** *end-time end-date*] | **to** *end-time end-date* }

undo time-range { *time-name* [*start-time* **to** *end-time days-of-the-week* [**from** *start-time start-date*] [**to** *end-time end-date*] | **from** *start-time start-date* [**to** *end-time end-date*] | **to** *end-time end-date*] | **all** }

View

System view

Parameter

time-name: Name of a particular time range, used as an import identifier.

start-time: (Optional) Starting time of the particular time range, in the format of hh:mm.

end-time: (Optional), End time of the particular time range, in the format of hh:mm.

days-of-the-week: (Optional) Indicating the particular time range takes effect on which day in a week. You can type these values:

- Number (ranging from 0 to 6);
- Monday, Tuesday, Wednesday, Thursday, Friday, Saturday or Sunday;
- Working-day: Monday through Friday inclusive;
- Off-day: Saturday and Sunday;
- daily: Every day of a week.

from *start-time start-date*: (Optional) Starting date of the particular time range, in the format of hh:mm YYYY/MM/DD.

to *end-time end-date*: (Optional) End date of the particular time range, in the format of hh:mm YYYY/MM/DD.

all: All time ranges.

Description

Use the **time-range** command to define a time range.

Use the **undo time-range** command to cancel a time range.

The defined time range includes absolute time range and period time range. *start-time* and *end-time days-of-the-week* define period time range together. **from** *start-time start-date* and *end-time end-date* define absolute time range together.

If a time range only defines the period time range, the time range is only active within the period time range.

If a time range only defines the period time range and multiple ranges of this time range are available (if repeating this time range name, you can configure multiple period time ranges of the same name), the time range is active only within these period time ranges.

If a time range only defines the absolute time range, the time range is only active within the absolute time range.

If a time range only defines the absolute time range and multiple ranges of this time range are available (repeating this time range name can configure multiple absolute time ranges of the same name), the time range is active only within these absolute time ranges.

If a time range defines the period time range and the absolute time range, the time range is only active when the period time range and the absolute time range are both matched. For example, a time range defines a period time range which is from 12:00 to 14:00 every Wednesday, and defines an absolute time range which is from 00:00 2004/1/1 to 23:59 2004/12/31. This time range is only active from 12:00 to 14:00 every Wednesday in 2004.

If a time range defines multiple absolute time ranges and multiple period time ranges, the time range is active only when period time ranges and absolute time ranges are both matched, that is, take the union set of multiple absolute time ranges and multiple period time ranges, and then take the intersection set of the union set of multiple absolute time ranges and that of multiple period time ranges.

If the start time and end time are not configured, the time range is one day (00:00-24:00).

If the end time is not configured, the time range is from the day when the configuration takes effect to the biggest time supported by the system. The maximum time range supported by the system currently is from 1970/01/01 to 2100/12/31.

- If you include any argument in the **undo time-range** command, the system will delete only the content defined by the argument from the time range.
- When you configure a time range, avoid naming the time range with "a", "al", or "all" to prevent collision with the **all** key word.

If you input parameters in the **undo time-range** command, only the content corresponding to the specified time range will be canceled.

Example

Define a time range starting from 0:0, Jan. 1, 2000.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] time-range test from 00:00 2000/1/1
```

17 QoS Commands

QoS Commands

CAUTION:

After QACL is configured in port view, the QACL configuration of all the member ports in the port group keeps the same all the time. After a port is added to the port group, the port configuration is overwritten by that of the port group. You cannot apply the ACL rule as per port.

display port-group

Syntax

display port-group

View

Any view

Parameter

None

Description

Use the **display port-group** command to display all the port groups in the current system.

Related command: **port-group**

Example

Display the port groups in the current system.

```
<SW8800> display port-group
Now, the following port group exist(s): 1
```

display port-group index

Syntax

display port-group *index*

View

Any view

Parameter

index: Number of the designated port.

Description

Use the **display port-group** *index* command to display the configuration information of the designated port group, including the description and member information of the port group.

Related command: **port**

Example

Display the configured information of port group 1.

```
<SW8800> display port-group 1
Port-group ID : 1
Description: Port group 01
Port-group is unlocked.
Port(s) description:
         Ethernet3/1/1         Ethernet3/1/2         Ethernet3/1/3
```

display mirroring-group

Syntax

display mirroring-group [*groupid*]

View

Any view

Parameter

groupid: mirroring group ID, in the range of 1 to 24.

Description

Use the **display mirroring-group** command to view the configuration of a port mirroring group. The information displayed includes the monitored ports, direction of monitored packets, monitoring ports, etc.

Related command: **mirroring-group**.

Example

Display the parameter configuration of a port mirroring group.

```
<SW8800> display mirroring-group
mirroring-group 1 inbound Ethernet6/1/1 mirrored-to Ethernet6/1/2
```

display qos conform-level

Syntax

display qos conform-level [*conform-level-value*] { **dscp-policed-service-map** [*dscp-list*] | **exp-policed-service-map** | **local-precedence-cos-map** }

View

Any view

Parameter

conform-level-value: Conform level, in the range of 0 to 2. If you type value(s) for this parameter, then only the specified conform-level DSCP items will be displayed. Otherwise, the system displays the whole mapping connection.

dscp-policed-service-map [*dscp-list*]: Displays "DSCP + Conform-level -> Service-parameter" mapping table. *dscp-list*: DSCP value, which can be a single value or values, for example, you can type single DSCP value "46", or DSCP values "0 8 10 16" (a space is required between two values). If you type value(s) for this parameter, then only the specified DSCP items will be displayed. Otherwise, the system displays the whole mapping connection. DSCP value is in the range of 0 to 63.

exp-policed-service-map: Displays "EXP + Conform-level -> Service-parameter" mapping table. EXP is MPLS priority of MPLS packets.

local-precedence-cos-map: Displays "Local-precedence + Conform-level -> Priority" mapping table

Description

Use the **display qos conform-level** command to view the "DSCP + Conform-level -> Service-parameter" mapping table, "EXP + Conform-level -> Service-parameter" mapping table and "Local-precedence + Conform-level -> Priority" mapping table.

Example

Display the "DSCP + Conform-level -> Service-parameter" mapping table.

```
<SW8800> display qos conform-level 0 dscp-policed-service-map
Conform-level 0 :
 Dscp-policed-service Map :
dscp   :   dscp    exp    cos   local-precedence      drop-precedence
-------------------------------------------------------------------
    0  :      0         0         0                 0                 0
    8  :      8         1         1                 1                 0
   10  :      10        1         1                 1                 0
   16  :      16        2         2                 2                 0
   18  :      18        2         2                 2                 0
   24  :     24        3         3                 3                 0
   26  :     26        3         3                 3                 0
   32  :     32        4         4                 4                 0
   34  :     34        4         4                 4                 0
   40  :     40        5         5                 5                 0
   46  :     46        5         5                 5                 0
   48  :     48        6         6                 6                 0
   56  :     56        7         7                 7                 0
```

Display the "EXP + Conform-level -> Service-parameter" mapping table.

```
<SW8800> display qos conform-level 0 exp-policed-service-map
conform-level 0 :
    exp :    dscp   exp    cos  local-precedence   drop-precedence
-------------------------------------------------------------------
     0 :         2         0         0           0                 0
     1 :        10         1         1           1                 0
     2 :        18         2         2           2                 0
     3 :        26         3         3           3                 0
     4 :        34         4         4           4                 0
     5 :        42         5         5           5                 0
     6 :        50         6         6           6                 0
     7 :        58         7         7           7                 0
```

Display the "Local-precedence + Conform-level -> Priority" mapping table.

```
<SW8800> display qos conform-level 0 local-precedence-cos-map
conform-level 0 :
 local-precedence :     0    1    2    3      4      5      6      7
-------------------------------------------------------------------
              cos :     0    1    2    3      4      5      6      7
```

display qos cos-drop-precedence-map

Syntax

display qos cos-drop-precedence-map

View

Any view

Parameter

None

Description

Use the **display qos cos-drop-precedence-map** command to view the "CoS-> Drop-precedence" mapping table.

Example

Display the "CoS-> Drop-precedence" mapping table.

```
<SW8800> display qos cos-drop-precedence-map
cos-drop-precedence-map:
            cos :   0     1     2     3     4     5     6     7
-------------------------------------------------------------------
drop-precedence :   2     2     1     1     1     1     0     0
```

display qos cos-local-precedence-map

Syntax

display qos cos-local-precedence-map

View

Any view

Parameter

None

Description

Use the **display qos cos-local-precedence-map** command to view the "CoS -> Local -precedence" mapping table.

Example

Display the "CoS -> Local -precedence" mapping table.

```
<SW8800> display qos cos-local-precedence-map
cos-local-precedence-map:
            cos :       0    1    2    3      4      5      6      7
-------------------------------------------------------------------
 local-precedence :     2    0    1    3      4      5      6      7
```

display qos-interface all

Syntax

display qos-interface [*interface- type interface-number*] **all**

View

Any view

Parameter

interface-type interface-number: Port of the switch, for detailed description, please refer to *Command Manual - Port*.

Description

Use the **display qos-interface all** command to view the QoS configuration of all ports, including drop mode, queue scheduling, traffic shaping etc. If you specify port IDs, only their QoS configuration will be displayed, including drop mode, queue scheduling, traffic shaping etc.

Example

Display all the QoS configurations of the port Ethernet2/1/3.

```
<SW8800> display qos-interface Ethernet2/1/3 all
Ethernet2/1/3 Port Shaping: Disable
 0 kbps, 0 burst, 256 queue-depth
 QID:    status    max-rate(kbps)   burst-size(Kbyte)   queue-depth
----------------------------------------------------------------------
  0 :   Disable           0                  0                128
  1 :   Disable           0                  0                128
  2 :   Disable           0                  0                128
  3 :   Disable           0                  0                128
  4 :   Disable           0                  0                128
  5 :   Disable           0                  0                128
  6 :   Disable           0                  0                128
  7 :   Disable           0                  0                128

 Ethernet2/1/3 Drop-mode: tail-drop, params index: 0

 Ethernet2/1/3 Port scheduling:
 QID:   scheduling-group     weight
-----------------------------------
  0 :   sp                      0
  1 :   sp                      0
  2 :   sp                      0
  3 :   sp                      0
  4 :   sp                      0
  5 :   sp                      0
  6 :   sp                      0
  7 :   sp                      0
```

display qos-interface drop-mode

Syntax

display qos-interface [*interface-type interface-number*] **drop-mode**

View

Any view

Parameter

interface-type interface-number: Port of the switch, for detailed description, please refer to *Command Manual - Port*.

Description

Use the **display qos-interface drop-mode** command to view drop mode configuration of outbound queues at a port. If no port is specified, drop mode configuration of all ports will be displayed.

Related command: **drop-mode**.

Example

Display drop mode and parameters of the port Ethernet2/1/2.

```
<SW8800> display qos-interface Ethernet2/1/2 drop-mode
Ethernet2/1/2 Drop-mode: tail-drop, params index: 0
```

display qos-interface mirrored-to

Syntax

display qos-interface [*interface -type interface-number*] **mirrored-to**

View

Any view

Parameter

interface-type interface-number: Port of the switch, for detailed description, please refer to *Command Manual - Port*.

Description

Use the **display qos-interface mirrored-to** command to view traffic mirroring configuration of a port.

Related command: **mirrored-to**.

Example

Display traffic mirroring configuration.

```
<SW8800> display qos-interface mirrored-to
GigabitEthernet2/1/1: mirrored-to
 Inbound:
   Matches: Acl 2020 rule 0  running
     Mirrored to: cpu
```

display qos-interface queue-scheduler

Syntax

display qos-interface [*interface -type interface-number*] **queue-scheduler**

View

Any view

Parameter

interface-type interface-number: Port of the switch, for detailed description, please refer to *Command Manual - Port*.

Description

Use the **display qos-interface queue-scheduler** command to view queue scheduling mode and parameters of a port. If no port is specified, queue scheduling mode and the parameters of all ports will be displayed.

Related command: **queue-scheduler**.

Example

Display queue scheduling mode and parameters.

```
<SW8800> display qos-interface queue-scheduler
Ethernet5/1/1 Port scheduling:
 QID:   scheduling-group     weight
-----------------------------------
  0 :   sp                       0
  1 :   sp                       0
  2 :   sp                       0
  3 :   wrr , group1            25
  4 :   sp                       0
  5 :   wrr , group2            30
  6 :   sp                       0
  7 :   sp                       0

 Ethernet5/1/ Port scheduling:
 QID:   scheduling-group     weight
-----------------------------------
  0 :   sp                       0
  1 :   sp                       0
  2 :   sp                       0
  3 :   sp                       0
  4 :   sp                       0
  5 :   sp                       0
  6 :   sp                       0
...
```

display qos-interface traffic-limit

Syntax

display qos-interface [*interface -type interface-number*] **traffic-limit**

View

Any view

Parameter

interface-type interface-number: Port of the switch, for detailed description, please refer to *Command Manual - Port*.

Description

Use the **display qos-interface traffic-limit** command to view the parameter setting of traffic rate limitation, including the target ACL, committed average rate, committed burst size (CBS), maximum burst size (MBS), peak rate and the related monitoring actions etc.

Related command: **traffic-limit**.

Example

Display parameter configuration of traffic rate limitation,.

```
<SW8800> display qos-interface traffic-limit
GigabitEthernet2/1/1: traffic-limit
 Inbound:
   Matches: Acl 2020 rule 0  running
     Committed Information Rate: 1000 Kbps
     Committed Burst Size: 1000 byte(s)
     Excess Burst Size: 1000 byte(s)
     Peak Information Rate: 0 Kbps
```

display qos-interface traffic-priority

Syntax

display qos-interface [*interface-type interface-number*] **traffic-priority**

View

Any view

Parameter

interface-type interface-number: Port of the switch, for detailed description, please refer to *Command Manual - Port*.

Description

Use the **display qos-interface traffic-priority** command to view traffic priority configuration of a port, including the target ACL, priority type, priority values etc.

Related command: **traffic-priority**.

Example

Display traffic priority marking configuration.

```
<SW8800> display qos-interface traffic-priority
GigabitEthernet2/1/1: traffic-priority
 Inbound:
   Matches: Acl 2021 rule 0  running
     Priority action: remark-policed-service, dscp: 20
```

display qos-interface traffic-redirect

Syntax

display qos-interface [*interface-type interface-number*] **traffic-redirect**

View

Any view

Parameter

interface-type interface-number: Port of the switch, for detailed description, please refer to *Command Manual - Port*.

Description

Use the **display qos-interface traffic-redirect** command to view traffic redirection configuration of a port, including the target ACL, target port etc.

Related command: **traffic-redirect**.

Example

Display traffic redirection configuration.

```
<SW8800> display qos-interface traffic-redirect
GigabitEthernet3/1/1: traffic-redirect
 Inbound:
   Matches: Acl 2020 rule 0  running
     Redirected to: next-hop 1.1.1.1
```

display qos-interface traffic-shape

Syntax

display qos-interface [*interface-type interface-number*] **traffic-shape**

View

Any view

Parameter

interface-type interface-number: Port of the switch, for detailed description, please refer to *Command Manual - Port*.

Description

Use the **display qos-interface traffic-shape** command to view traffic shaping configuration of a port, including the maximum rate, MBS (in units of kbyte), the maximum queue length. If no port is specified, traffic shaping configuration of all ports will be displayed.

Example

Display traffic shaping configuration.

```
<SW8800> display qos-interface Ethernet2/1/3 traffic-shape
Ethernet2/1/3 Port Shaping: Disable
 0 kbps, 0 burst, 256 queue-depth
 QID:    status    max-rate(kbps)   burst-size(Kbyte)   queue-depth
----------------------------------------------------------------------
  0 :   Disable           0                  0                128
  1 :   Disable           0                  0                128
  2 :   Disable           0                  0                128
  3 :   Disable           0                  0                128
  4 :   Disable           0                  0                128
  5 :   Disable           0                  0                128
  6 :   Disable           0                  0                128
  7 :   Disable           0                  0                128
```

display qos-interface traffic-statistic rate

Syntax

display qos-interface [*interface-type interface-number*] **traffic-statistic** [**rate** [*timeinterval*]]

View

Any view

Parameter

interface-type interface-number: Port of the switch, for detailed description, please refer to *Command Manual - Port*.

rate: Port rate. This parameter is available only when you select *interface-type interface-number*.

timeinterval: Interval for making statistics of rates, ranging from 1 to 5 seconds. The default value is one second.

Description

Use the **display qos-interface traffic-statistic** command to view traffic statistics of a port, including the target ACL, number of calculated packets etc.

Use the **display qos-interface traffic-statistic rate** command to display the actual traffic rate on the port. The displayed information includes the ACL corresponding to the traffic flow to be displayed and packet speed.

Related command: **traffic-statistics**.

Example

Display average traffic rate in the latest three seconds on Ethernet7/1/1.

```
<SW8800> display qos-interface Ethernet7/1/1 traffic-statistic rate
3
Ethernet7/1/1: traffic-statistic
 Inbound:
   Matches: Acl 3000 rule 0  running

Last 3 second(s) rate: 12,574 packet(s)/sec, 12,875,776 bit(s)/sec
```

Display traffic statistics information on port GigabitEthernet7/1/1..

```
<SW8800> display qos-interface GigabitEthernet7/1/1 traffic-statisti
c
GigabitEthernet7/1/1: traffic-statistic
Inbound:
   Matches: Acl 2000 rule 0  running
     12002688 bytes  (green 1270244416 byte(s), yellow 1895874880
byte(s), red 704683968 byte(s) )
     3333270 packets  (green 0 byte(s), yellow 0 byte(s), red 0
byte(s) )
```

display qos-vlan all

Syntax

display qos-vlan [*vlan-id*] **all**

View

Any view

Parameter

vlan-id: ID of a VLAN, in the range of 1 to 4094.

Description

Use the **display qos-vlan all** command to display the QoS configuration (including the configuration of priority marking, traffic policing, traffic redirection, and traffic statistics) information about one specific VLAN (with *vlan-id* parameter) or all VLANs (without *vlan-id* parameter) on the switch.

Example

Display all the QoS parameter configurations of all the VLANs.

```
<SW8800> display qos-vlan all
Vlan 1 traffic-limit
 Inbound:
   There is no configuration.
Outbound:
   There is no configuration.
Vlan 1 traffic-priority
 Inbound:
   There is no configuration.
Outbound:
   There is no configuration
Vlan 1 traffic-redirect
 Inbound:
   There is no configuration.
Outbound:
   There is no configuration
Vlan 1 traffic-statistic
 Inbound:
   There is no configuration.
 Outbound:
   There is no configuration.
Vlan 2 traffic-limit
 Inbound:
   Matches: Acl 2000 rule 1  running (Action-type: Eacl, Destination slot: 3)
     Committed Information Rate: 8192 Kbps
     Committed Burst Size: 10000 byte(s)
     Excess Burst Size: 20000 byte(s)
     Peak Information Rate: 0 Kbps
     Exceed action: drop
Outbound:
  There is no configuration
Vlan 2 traffic-priority
 Inbound:
   Matches: Acl 2000 rule 1  running (Action-type: Eacl, Destination slot: 3)
     Priority action: remark-policed-service, untrusted, dscp: 13, cos: 6,
Local
-precedence: 6, drop-priority: 1
Outbound:
   There is no configuration
Vlan 2 traffic-redirect
Inbound:
   Matches: Acl 2000 rule 1  running (Action-type: Eacl, Destination slot: 3)
     Redirected to: next-hop 1.1.1.1
Outbound:
   There is no configuration
Vlan 2 traffic-statistic
Inbound:
   There is no configuration.
Outbound:
   There is no configuration.
---- More ----
```

display qos-vlan traffic-limit

Syntax

display qos-vlan [*vlan-id*] **traffic-limit**

View

Any view

Parameter

vlan-id: ID of a VLAN, in the range of 1 to 4094.

Description

Use the **display qos-vlan traffic-limit** command to display the parameter configuration for traffic limit in VLAN, including the configuration information about related ACL and policing actions.

Related command: **traffic-limit** and **traffic-params**.

Example

Display the parameter configuration of traffic limit in VLAN.

```
<SW8800> display qos-vlan traffic-limit
Vlan 1 traffic-limit
 Inbound:
   There is no configuration.
Outbound:
   There is no configuration
Vlan 2 traffic-limit
 Inbound:
   Matches: Acl 2000 rule 3  running (Action-type: Eacl, Destination slot: 3)
     Committed Information Rate: 8192 Kbps
     Committed Burst Size: 10000 byte(s)
     Excess Burst Size: 20000 byte(s)
     Peak Information Rate: 0 Kbps
     Exceed action: drop
Outbound:
  There is no configuration.
```

display qos-vlan traffic-priority

Syntax

display qos-vlan [*vlan-id*] **traffic-priority**

View

Any view

Parameter

vlan-id: ID of a VLAN, in the range of 1 to 4094.

Description

Use the **display qos-vlan traffic-priority** command to display the priority marking configuration in VLAN, including the ACL associated with the traffic priority marking, the type and value of the priority marking.

Related command: **traffic-priority**.

Example

Display the priority marking configuration in VLAN.

```
<SW8800> display qos-vlan traffic-priority
Vlan 1 traffic-priority
 Inbound:
   There is no configuration.
Outbound:
   There is no configuration
Vlan 2 traffic-priority
 Inbound:
   Matches: Acl 2000 rule 1  running (Action-type: Eacl, Destination slot: 3)
     Priority action: remark-policed-service, untrusted, dscp: 13, cos: 6,
local-precedence: 6, drop-priority: 1
 Outbound:
  There is no configuration.
```

display qos-vlan traffic-redirect

Syntax

display qos-vlan [*vlan-id*] **traffic-redirect**

View

Any view

Parameter

vlan-id: ID of a VLAN, in the range of 1 to 4094.

Description

Use the **display qos-vlan traffic-redirect** command to display the parameter configuration for traffic redirection in VLAN, including the related ACL and the destination port of the traffic redirection.

Related command: **traffic-redirect**.

Example

Display the parameter configuration for a traffic redirection in VLAN.

```
<SW8800> display qos-vlan 2 traffic-redirect
Vlan 2 traffic-redirect
 Inbound:
   Matches: Acl 2000 rule 1  running (Action-type: Eacl, Destination slot: 3)
     Redirected to: next-hop 1.1.1.1
Outbound:
  There is no configuration.
```

display qos-vlan traffic-statistic

Syntax

display qos-vlan [*vlan-id*] **traffic-statistic**

View

Any view

Parameter

vlan-id: VLAN ID, in the range of 1 to 4,094

Description

Use the **display qos-vlan traffic-statistic** command to display the traffic statistics information in VLAN. The displayed information includes the ACL corresponding to the traffic flow to be output, action type, and statistics result.

Related command: **traffic-statistic**.

Example

Display the traffic statistics information of VLAN 2.

```
<SW8800> display qos-vlan 2 traffic-statistic
Vlan 2 traffic-statistic
 Inbound:
   Matches: Acl 3000 rule 0  running (Action-type: Vlan-acl)
     0 byte  (green 0 byte(s), yellow 0 byte(s), red 0 byte(s) )
     0 packet
   Matches: Acl 3000 rule 0  running (Action-type: Eacl, Destination slot: 2)
     0 byte
 Outbound:
```

```
Matches: Acl 3000 rule 0  running (Action-type: Eacl, Destination slot: 2)
  0 byte
```

display traffic-params

Syntax

display traffic-params [*traffic-index*]

View

Any view

Parameter

traffic-index: Traffic parameter index. The default value is 1.

Description

Use the **display traffic-params** command to display the parameter configuration for traffic policing, including cir, cbs, ebs, pir, and so on.

Related command: **traffic-params**.

Example

Display the parameter configuration for traffic policing.

```
<SW8800> display traffic-params 1
traffic parameters configuration list:
   index :     cir     (Kbps) cbs      (byte) ebs      (byte) pir(Kbps)
------------------------------------------------------------------------
       1 :   20000            5000             5000           30000
```

drop-mode

Syntax

drop-mode { **tail-drop** | **wred** } [*wred-index*]

undo drop-mode

View

Ethernet port view/port group view

Parameter

tail-drop: Tail drop mode.

wred: WRED drop mode.

wred-index: WRED index, in the range of 0 to 3. By default, it is 0. If you type nothing for this parameter, the system will use the parameters specified when WRED index is 0.

Description

Use the **drop-mode** command to configure drop mode for a port.

Use the **undo drop-mode** command to restore the default drop mode, i.e. tail drop mode.

By default, tail drop mode is selected.

In the case of network congestion, the switch drops packets to release system resources. And then no packets are put into long-delay queues. The following two drop modes are available:

- Tail drop mode: different queues (red, yellow and green) are allocated with different drop thresholds. When these thresholds are exceeded respectively, excessive packets will be dropped.
- WRED drop mode: Drop precedence is taken into account in drop action. When only min-thresholds of red, yellow and green packets are exceeded, packets between min-thresholds and max-thresholds are dropped randomly at a given slope. But when max-thresholds of red, yellow and green packets are exceeded, all excessive packets will be dropped.

Example

Set the port Ethernet3/1/1 in WRED drop mode; import WRED 0 as the threshold.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800]interface Ethernet3/1/1
[3Com-Ethernet3/1/1] drop-mode wred 0
```

dscp

Syntax

dscp *dscp-list* : *dscp-value exp-value cos-value local-precedence-value drop-precedence*

undo dscp *dscp-list*

View

Conform level view

Parameter

dscp-list: Original DSCP value, which can be a single value or several values, in the range of 0 to 63. For example, you can type single DSCP value "46", or DSCP values "0 8 10 16" (space is required between two values).

dscp-value: Modified DSCP value, in the range of 0 to 63.

exp-value: Modified EXP value, in the range of 0 to 7. EXP is MPLS priority of MPLS packets.

cos-value: Modified 802.1p priority value, in the range of 0 to 7

local-precedence-value: Modified local precedence value, in the range of 0 to 7.

drop-precedence: Modified drop precedence value, in the range of 0 to 2.

Description

Use the **dscp** command to configure the "DSCP + Conform-level -> Service-parameter" mapping table of current conform level.

Use the **undo dscp** command to restore default configuration of the "DSCP + Conform-level -> Service- parameter" mapping table.

After entering conform level view, you can configure the "DSCP + Conform-level -> Service-parameter" mapping table of the corresponding level. For example, you can enter conform level 0 view and configure the "DSCP + Conform-level 0 -> Service-parameter" mapping table.

Example

Configure the " DSCP + Conform-level 0 -> Service-parameter " mapping table.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800]qos conform-level 0
[3Com-conform-level-0] dscp 0: 0 0 0 0 0
[3Com-conform-level-0] dscp 8 10 : 8 0 1 1 0
[3Com-conform-level-0] dscp 16 18: 16 0 2 2 0
[3Com-conform-level-0] dscp 24 26 : 24 0 3 3 0
[3Com-conform-level-0] dscp 32 34 : 32 0 4 4 0
[3Com-conform-level-0] dscp 40 46: 40 0 5 5 0
[3Com-conform-level-0] dscp 48 : 48 0 6 6 0
[3Com-conform-level-0] dscp 56 : 56 0 7 7 0
```

The configured mapping table:

Table 33 " DSCP + Conform-level - Service-parameter " mapping table

DSCP	CL	Policed-DSCP	Policed-exp	Policed-802.1p	Policed-Localprec	Policed-Drop Precedence
0	0	0	0	0	0	0
8	0	8	0	1	1	0
10	0	8	0	1	1	0
16	0	16	0	2	2	0
18	0	16	0	2	2	0
24	0	24	0	3	3	0
26	0	24	0	3	3	0
32	0	32	0	4	4	0
34	0	32	0	4	4	0
40	0	40	0	5	5	0
46	0	40	0	5	5	0
48	0	48	0	6	6	0
56	0	56	0	7	7	0

exp

Syntax

exp *exp-list* : *dscp-value exp-value cos-value local-precedence-value drop-precedence*

undo exp *exp-list*

View

Conform level view

Parameter

exp-list: Original EXP value, which can be a single value or several values, in the range of 0 to 7. For example, you can type single EXP value "2", or EXP values "2 3 4" (space is required between values). EXP is MPLS priority of MPLS packets.

dscp-value: Modified DSCP value, in the range of 0 to 63.

exp-value: Modified EXP value, in the range of 0 to 7. EXP is MPLS priority of MPLS packets.

cos-value: Modified 802.1p priority value, in the range of 0 to 7.

local-precedence-value: Modified local precedence value, in the range of 0 to 7.

drop-precedence: Modified drop precedence value, in the range of 0 to 2.

Description

Use the **exp** command to configure the "EXP + Conform-level -> Service-parameter" mapping table of current conform level.

Use the **undo exp** command to restore default configuration of the "EXP + Conform-level -> Service-parameter" mapping table.

After entering conform level view, you can configure the "EXP + Conform-level -> Service-parameter" mapping table of the corresponding level. For example, you can enter conform level 0 view and configure the "EXP + Conform-level 0 -> Service-parameter" mapping table.

Example

Configure the "EXP + Conform-level 0 -> Service-parameter" mapping table.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800]qos conform-level 0
[3Com-conform-level-0] exp 0: 0 0 0 0 0
```

local-precedence

Syntax

local-precedence *cos-value0 cos-value1 cos-value2 cos-value3 cos-value4 cos-value5 cos-value6 cos-value7*

undo local-precedence

View

Conform level view

Parameter

cos-value0: 802.1p priority value corresponding to Local-precedence 0, in the range of 0 to 7.

cos-value1: 802.1p priority value corresponding to Local-precedence 1, in the range of 0 to 7.

cos-value2: 802.1p priority value corresponding to Local-precedence 2, in the range of 0 to 7.

cos-value3: 802.1p priority value corresponding to Local-precedence 3, in the range of 0 to 7.

cos-value4: 802.1p priority value corresponding to Local-precedence 4, in the range of 0 to 7.

cos-value5: 802.1p priority value corresponding to Local-precedence 5, in the range of 0 to 7.

cos-value6: 802.1p priority value corresponding to Local-precedence 6, in the range of 0 to 7.

cos-value7: 802.1p priority value corresponding to Local-precedence 7, in the range of 0 to 7.

Description

Use the **local-precedence** command to configure the "Local-precedence + Conform-level -> 802.1p priority" mapping table of current conform level.

Use the **undo local-precedence** command to restore default configuration of the "Local-precedence + Conform-level -> 802.1p priority" mapping table.

After entering conform level view, you can configure the " Local-precedence + Conform-level -> 802.1p priority " mapping table of the corresponding level. For example, you can enter conform level 0 view and configure the " Local-precedence + Conform-level 0 -> 802.1p priority " mapping table.

Example

Configure the "Local-precedence + Conform-level 0 -> 802.1p priority" mapping table.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800]qos conform-level 0
[3Com-conform-level-0] local-precedence 0 1 2 3 5 5 6 7
```

The configured mapping table:

Table 34 Local-precedence + Conform-level - 802.1p priority " mapping table

Local-precedence	Conform-level	802.1p
0	0	0
1	0	1
2	0	2
3	0	3
4	0	5
5	0	5
6	0	6
7	0	7

mirrored-to

Syntax

Command Format Which Only Applies IP Group ACL

mirrored-to inbound ip-group { *acl-number* | *acl-name* } [**rule** *rule* [**system-index** *index*]] { **cpu** | **interface** *interface-type interface-number* } **cpu**

undo mirrored-to inbound ip-group { *acl-number* | *acl-name* } [**rule** *rule*]

Command Format Which Applies IP Group and Link Group ACL at Same time

mirrored-to inbound ip-group { *acl-number* | *acl-name* } { **rule** *rule* **link-group** { *acl-number* | *acl-name* } [**rule** *rule* [**system-index** *index*]] | **link-group** { *acl-number* | *acl-name* } **rule** *rule* } **cpu** { **cpu** | **interface** *interface-type interface-number* }

undo mirrored-to inbound ip-group { *acl-number* | *acl-name* } { **rule** *rule* **link-group** { *acl-number* | *acl-name* } [**rule** *rule*] | **link-group** { *acl-number* | *acl-name* } **rule** *rule* }

Command Format Which Only Applies Link Group ACL

mirrored-to inbound link-group { *acl-number* | *acl-name* } [**rule** *rule* [**system-index** *index*]] { **cpu** | **interface** *interface-type interface-number* }

undo mirrored-to inbound link-group { *acl-number* | *acl-name* } [**rule** *rule*]

View

Ethernet port view/port group view

Parameter

inbound: Mirrors inbound packets at the port.

ip-group { *acl-number* | *acl-name* }: Activates IP ACLs, including basic and advanced ACLs. *acl-number*: Sequence number of ACL, ranging from 2000 to 3999. *acl-name*: Name of the ACL, which must be a character string starting with an English letter (a-z or A-Z), and without any space in it.

link-group { *acl-number* | *acl-name* }: Activates Layer 2 ACLs. *acl-number*: Sequence number of ACL, ranging from 4000 to 4999. *acl-name*: Name of ACL, which must be a character string started with an English letter (a-z or A-Z), and without any space in it.

rule *rule*: Specifies the rule of an active ACL, ranging from 0 to 127; if not specified, all rules of ACL will be activated.

system-index *index* here is the system index for an ACL rule. When delivering a rule, the system assigns a globally unique index to it, for convenience of later retrieval. You can also assign a system index for it when delivering an ACL rule with this command, but this value may change while the system is running. Generally you are not recommended to manually assign a system index.

If the specified system-index is 0, the system selects the index automatically.

cpu: Mirrors traffic to the CPU.

Interface: Mirrors traffic to the designated destination port.

Description

Use the **mirrored-to** command to activate an ACL and mirror data streams to the CPU or the designated destination port. Use the **undo mirrored-to** command to remove traffic mirroring setting.

This configuration is only applicable to the packets which match the permitted rules in the ACL.

Related command: **display qos-interface mirrored-to**.

Example

Mirror the packets which match the permitted rules in the ACL 2000 to Ethernet2/1/1.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800]interface Ethernet2/1/1
[3Com-Ethernet2/1/1] mirrored-to inbound ip-group 2000 cpu rule 0
interface Ethernet 2/1/1
```

mirroring-group

Syntax

mirroring-group *groupid* { **inbound** | **outbound** } *mirroring-port-list*
mirrored-to *monitor-port*

undo mirroring-group *groupid*

View

System view

Parameter

groupid: mirroring group ID, in the range of 1 to 24

inbound: Monitors only the inbound packets at the port.

outbound: Monitors only the outbound packets at the port.

mirroring-port-list: Ethernet port list, including multiple Ethernet ports, in the form of *port-list* = { *interface-type interface-number* } &<1-8>. &<1-8> means the parameter can be typed eight times at most.

mirrored-to *monitor-port*: Specifies monitoring port.

Description

Use the **mirroring-group** command to configure a mirroring group for the port.

Use the **undo mirroring-group** command to remove mirroring group setting.

The switch supports multiple-to-one mirroring, that is, copying the packets at several ports to the monitoring port. For Switch 8800 Family series, you can complete port mirroring setting by configuring mirroring groups. Each mirroring

group may contain one monitoring port and several monitored ports. You can also specify the direction of the monitored packets.

Switch 8800 Family series support up to 24 mirroring groups at a port.

Related command: **display mirroring-group**.

Switch 8800 Family series support cross-card mirroring, that is, the monitoring and monitored ports can be at different cards.

Consider these issues when configuring port mirroring:

- For intra-card mirroring, only one monitoring port can be configured for the mirroring groups in the same direction.
- For cross-card mirroring, only one monitoring port (which is on another card) can be configured for the mirroring groups in the same direction.
- You can only configure eight monitored ports for all the mirroring groups in transmit group.
- One port can act as mirroring port and mirrored port at the same time for different mirroring group.

More issues for the GV48 or GP48 card:

- For the mirroring (including inbound port mirroring and outbound port mirroring) on the same GV48 or GP48 card, only one monitoring port is allowed.
- For all mirroring groups configured in the system, only one monitoring port is allowed on the same GV48 or GP48 card.

By default, two port groups of the XP4 card are created. The member ports are port 0-1 and port 2-3 respectively. Consider these issues when configuring port mirroring:

- The XP4 card does not support cross-group port mirroring, that is, the monitoring ports and monitored ports in the same port mirroring group can only be port 0 to 1 or port 2 to 3.
- You can configure an inbound monitoring port and an outbound monitoring port in a port group respectively. There is only one monitoring port in other types of interface cards.

Related command: **display mirroring-group**.

Example

Configure mirroring group 1, the monitored ports are Ethernet3/1/1 to Ethernet3/1/3, and the monitoring port is Ethernet3/1/4, monitoring only inbound packets.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] mirroring-group 1 inbound ethernet 3/1/1 ethernet 3/1/2
ethernet 3/1/3 mirrored-to ethernet 3/1/4
```

If the mirroring-group has been configured, the system will prompt "The mirroring-group has been configured!"

port

Syntax

port *interface-list*

undo port *interface-list*

View

Port group view

Parameter

interface-list: Ethernet port list to be added to a port group or to be deleted from a port group, in the format of *interface-lis t*= { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-n>. *interface-type* indicates a port type and *interface-number* indicates a port number. The port number after the keyword **to** must be greater than or equal to that before the keyword **to**. &<1-n> indicates that you can input the preceding parameters for up to n times. n indicates the maximum number of ports allowed to be added to a port group.

Description

Use the **port** command to add a port to a port group.

Use the **undo port** command to add remove a port from a port group.

For common interface cards except for the XP4 card, confider the following issues:

- Do not add the ports of different cards to the same port group. Do not add the same port to multiple port groups at the same time.
- Do not add aggregated ports in the port group. If a port in the port group needs to be aggregated, the port must quit the port group first. The port configuration is overwritten by that of the primary port in the aggregation group.
- After a port is added to the port group, the port configuration is overwritten by that of the port group. You cannot apply the ACL rule as per port.
- When the port group is null, it is not allowed to configure QACL. After all the members quit the port group, the QACL configuration of the port group is remained. When a new port joins the port group, QACL will be applied to the port automatically.

Example

Add Ethernet3/1/1, Ethernet3/1/2, and Ethernet3/1/3 to port group 1.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800]port-group 1
[3Com-port-group1] port Ethernet3/1/1 Ethernet3/1/2 Ethernet3/1/3
The original rule on the port will be deleted.
Are you sure?[Y/N] y
Add port Ethernet3/1/1...
Add port Ethernet3/1/2...
Add port Ethernet3/1/3...
```

port-group

Syntax

port-group *index*

undo port-group *index*

View

System view

Parameter

index: Port group number.

Description

Use the **port-group** command to create a port group and enter port group view.

Use the **undo port-group** *index* command to delete a port group. The port group number of a common interface card ranges from 1 to 128.

CAUTION: *The special port group corresponding to the XP4 card port cannot be deleted.*

Example

Create port group 1 and enter port group view.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] port-group 1
[3Com-port-group1]
```

priority

Syntax

In Ethernet port view:

priority *priority-level*

undo priority

In Ethernet port view:

priority { *priority-level* | **trust** }

undo priority

View

Ethernet port view, port group view

Parameter

priority-level: Port priority value, in the range of 0 to 7. By default, it is 0.

Trust: Trusts the local priority in the input packet all the time.

Description

Use the **priority** command to set the default local precedence value for a port.

Use the **undo priority** command to restore the default value of local precedence.

After receiving a packet, the switch allocates a set of service parameters to it according to a specific rule. The procedure to obtain local precedence: First obtain it according to the "CoS ->Local-precedence" mapping table. If failed, the system uses the default local precedence of the port as that for the packet.

Example

Set the defaulted local precedence value of the port Ethernet3/1/1 as 7.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800]interface e thernet3/1/1
[3Com-Ethernet3/1/1] priority 7
```

qos conform-level

Syntax

qos conform-level *conform-level-value*

View

System view

Parameter

conform-level *conform-level-value*: Conform level, in the range of 0 to 2 inclusive.

Description

Use the **qos conform-level** command to create a conform level and enter it.

There are three conform levels available, numbered as 0, 1 and 2. Type the conform level value and you can enter the corresponding view. In the conform level view, you can configure the "DSCP + Conform-level -> Service-parameter" mapping table, "EXP + Conform-level -> Service-parameter" mapping table and the "Local-precedence + Conform-level ->802.1p" mapping table.

Example

Create the conform level 0 view and enter it.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] qos conform-level 0
[3Com-conform-level-0]
```

qos cos-drop-precedence-map

Syntax

qos cos-drop-precedence-map *cos0-map-drop-prec cos1-map-drop-prec cos2-map-drop-prec cos3-map-drop-prec cos4-map-drop-prec cos5-map-drop-prec cos6-map-drop-prec cos7-map-drop-prec*

undo qos cos-drop-precedence-map

View

System view

Parameter

cos0-map-drop-prec: Mapping value from CoS 0 to drop precedence, in the range of 0 to 2.

cos1-map-drop-prec: Mapping value from CoS 1 to drop precedence, in the range of 0 to 2.

cos2-map-drop-prec: Mapping value from CoS 2 to drop precedence, in the range of 0 to 2.

cos3-map-drop-prec: Mapping value from CoS 3 to drop precedence, in the range of 0 to 2.

cos4-map-drop-prec: Mapping value from CoS 4 to drop precedence, in the range of 0 to 2.

cos5-map-drop-prec: Mapping value from CoS 5 to drop precedence, in the range of 0 to 2.

cos6-map-drop-prec: Mapping value from CoS 6 to drop precedence, in the range of 0 to 2.

cos7-map-drop-prec: Mapping value from CoS 7 to drop precedence, in the range of 0 to 2.

Description

Use the **qos cos-drop-precedence-map** command to configure the "CoS -> Drop-precedence" mapping table.

Use the **undo qos cos-drop-precedence-map** command to restore the default values of the "CoS -> Drop-precedence" mapping table.

The system provides "CoS -> Drop-precedence" mapping table as the default value.

Table 35 Default "CoS - Drop-precedence" mapping table

CoS Value	Drop-precedence
0	0
1	0
2	0
3	0
4	0
5	0
6	0
7	0

After receiving a packet, the switch allocates a set of service parameters to it according to a specific rule. The service parameters, including CoS value, local precedence and drop level, are determined according to the packet 802.1p priority value. CoS value is the packet 802.1p priority value, while local and drop precedence values are obtained according to the "CoS -> Local-precedence"

mapping table and the "CoS -> Drop-precedence" mapping table. You can modify the CoS -> Drop-precedence mapping table using this command.

Example

Configure the "CoS -> Drop-precedence" mapping table.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] qos cos-drop-precedence-map 2 2 1 1 1 0 0 0
```

Modified "CoS -> Drop-precedence" mapping table is shown as follows.

Table 36 Modified "CoS - Drop-precedence" mapping table

CoS Value	Drop-precedence
0	2
1	2
2	1
3	1
4	1
5	0
6	0
7	0

qos cos-local-precedence-map

Syntax

qos cos-local-precedence-map *cos0-map-local-prec cos1-map-local-prec cos2-map-local-prec cos3-map-local-prec cos4-map-local-prec cos5-map-local-prec cos6-map-local-prec cos7-map-local-prec*

undo qos cos-local-precedence-map

View

System view

Parameter

cos0-map-local-prec: Mapping value from CoS 0 to local precedence, in the range of 0 to 7.

cos1-map-local-prec: Mapping value from CoS 1 to local precedence, in the range of 0 to 7.

cos2-map-local-prec: Mapping value from CoS 2 to local precedence, in the range of 0 to 7.

cos3-map-local-prec: Mapping value from CoS 3 to local precedence, in the range of 0 to 7.

cos4-map-local-prec: Mapping value from CoS 4 to local precedence, in the range of 0 to 7.

cos5-map-local-prec: Mapping value from CoS 5 to local precedence, in the range of 0 to 7.

cos6-map-local-prec: Mapping value from CoS 6 to local precedence, in the range of 0 to 7.

cos7-map-local-prec: Mapping value from CoS 7 to local precedence, in the range of 0 to 7.

Description

Use the **qos cos-local-precedence-map** command to configure the "CoS -> Local-precedence" mapping table.

Use the **undo qos cos-local-precedence-map** command to restore the default values of the "CoS -> Local-precedence" mapping table.

The system provides "CoS -> Local-precedence" mapping table as the default value.

Table 37 Default "CoS - Local-precedence" mapping connection

CoS Value	Local Precedence
0	2
1	0
2	1
3	3
4	4
5	5
6	6
7	7

After receiving a packet, the switch allocates a set of service parameters to it according to a specific rule. The service parameters, including CoS value, local precedence and drop level, are determined according to the packet 802.1p priority value. CoS value is the packet 802.1p priority value, while local and drop precedence values are obtained according to the "CoS -> Local-precedence" mapping table and the "CoS -> Drop-precedence" mapping table. You can modify the "CoS -> Local-precedence" mapping table using this command.

Example

Configure the "CoS -> Local-precedence" mapping table

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] qos cos-local-precedence-map 0 1 2 3 4 5 6 7
```

Configured "CoS -> Local-precedence" mapping table:

Table 38 Configured "CoS - Local-precedence" mapping table

CoS Value	Local Precedence
0	0
1	1
2	2
3	3

Table 38 Configured "CoS - Local-precedence" mapping table

CoS Value	Local Precedence
4	4
5	5
6	6
7	7

queue

Syntax

queue *queue-id green-min-threshhold green-max-threshhold green-max-prob yellow-min-threshhold yellow-max-threshhold yellow-max-prob red-min-threshhold red-max-threshhold red-max-prob exponent*

undo queue *queue-id*

View

WRED index view

Parameter

queue-id: Outbound queue ID, in the range of 0 to 7

green-min-threshhold: Minimum queue length to trigger random green packet dropping, in the range of 0 to 65535. It must be a multiple of 256 bytes.

green-max-threshhold: Queue length to trigger complete green packet dropping, in the range of 0 to 65535. It must be a multiple of 256 bytes.

green-max-prob: Maximum drop probability for green packets, in the range of 1 to 15.

yellow-min-threshhold: Minimum queue length to trigger random yellow packet dropping, in the range of 0 to 65535. It must be a multiple of 256 bytes.

yellow-max-threshhold: Queue length to trigger complete yellow packet dropping, in the range of 0 to 65535. It must be a multiple of 256 bytes.

yellow-max-prob: Maximum drop probability for yellow packets, in the range of 1 to 15.

red-min-threshhold: Minimum queue length to trigger random red packet dropping, in the range of 0 to 65535. It must be a multiple of 256 bytes.

red-max-threshhold: Queue length to trigger complete red packet dropping, in the range of 0 to 65535. It must be a multiple of 256 bytes.

red-max-prob: Maximum drop probability for green packets, in the range of 1 to 15.

exponent: Weight for calculating average queue length, in the range of 1 to 15. By default, it is 9.

Description

Use the **queue** command to configure parameters for a WRED index.

Use the **undo queue** command to restore the default parameters for the WRED index.

The switch provides four sets of default WRED parameters, respectively numbered as 0, 1, 2 and 3. Each set includes 80 parameters, 10 parameters for each of the eight queues. The ten parameters are *green-min-threshhold*, *yellow-min-threshhold*, *red-min-threshhold*, *green-max-threshhold*, *yellow-max-threshhold*, *red-max-threshhold*, *green-max-prob*, *yellow-max-prob*, *red-max-prob* and *exponent*. You can use the command to modify the parameters of a specific WRED index.

Example

Configure parameters for WRED 0: *queue-id* is 7; *green-min-threshold* is 150; *green-max-threshold* is 500; *green-max-prob* is 5; *yellow-min-threshold* is 100; *yellow-max-threshold* is 150; *yellow-max-prob* is 10; *red-min-threshold* is 50; *red-max-threshold* is 100; *red-max-prob* is 15; *exponent* is 10.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800]wred 0
[3Com-wred-0] queue 7 150 500 5 100 150 10 50 100 15 10
```

queue-scheduler

Syntax

queue-scheduler wrr { **group1** { *queue-id queue-weight* } &<1-8> | **group2** { *queue-id queue-weight* } &<1-8> }*

undo queue-scheduler [*queue-id*] &<1-8>

View

Ethernet port view, port group view

Parameter

wrr: Weighted round robin algorithm.

group1: Adds the queue to WRR priority group 1.

group2: Adds the queue to WRR priority group 2.

queue-id: Outbound queue ID, in the range of 0 to 7.

queue-weight: Queue weight, in the range of 1 to 255.

&<1-8>: You can input the *queue-id* and *queue-weight* parameters eight times at most.

Description

Use the **queue-scheduler** command to choose queue scheduling algorithm and parameters.

Use the **undo queue-scheduler** command to restore the default setting, SP algorithm.

By default, SP algorithm is selected for all outbound queues at a port.

The switch supports eight outbound queues at a port, with different scheduling algorithms for them. You can configure these queues into different scheduling groups: SP group, WRR priority group 1 and group 2. For example, you can set queues 6 and 7 into SP group, queues 0, 1 and 2 into WRR priority group 1 and queues 3, 4 and 5 into WRR priority group 2. Then a queue will be selected respectively for theses three groups according to their own scheduling algorithms. Then these three selected queues will scheduled in SP algorithm.

The queue weight is based on bandwidth. For example, if queues 0, 1 and 2 belong to WRR priority group 1 and their weight is respectively as 20, 20 and 30, then in process, the proportion of their respective weight in the whole bandwidth is 20:20:30

Example

Set queues 0 to 5 in WRR algorithm, queues 0, 1 and 2 belong to group 1, with weight respectively as 20, 20 and 30; queues 3, 4 and 5 belong to group 2, with weight respectively as 20, 20 and 40. Set queues 6 and 7 in SP algorithm, the default one.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800]interface e thernet3/1/1
[3Com-Ethernet3/1/1] queue-scheduler wrr group1 0 20 1 20 2 30 group
2 3 20 4 20 5 40
```

reset traffic-statistic

Syntax

reset traffic-statistic inbound { { **ip-group** { *acl-number* | *acl-name* } **rule** *rule* | **link-group** { *acl-number* | *acl-name* } }* | { **ip-group** { *acl-number* | *acl-name* } | **link-group** { *acl-number* | *acl-name* } **rule** *rule* }* | **ip-group** { *acl-number* | *acl-name* } **rule** *rule* **link-group** { *acl-number* | *acl-name* } **rule** *rule* }

View

Ethernet port view, port group view

Parameter

inbound: Clears statistics of the inbound packets at the port.

ip-group { *acl-number* | *acl-name* }: Activates IP ACLs, including basic and advanced ACLs. *acl-number*: Sequence number of ACL, ranging from 2000 to 3999. *acl-name*: Name of the ACL, which must be a character string starting with an English letter (a-z or A-Z), and without any space in it.

link-group { *acl-number* | *acl-name* }: Activates Layer 2 ACLs. *acl-number*: Sequence number of ACL, ranging from 4000 to 4999. *acl-name*: Name of ACL, which must be a character string started with an English letter (a-z or A-Z), and without any space in it.

rule *rule*: Specifies the subitem of an active ACL, ranging from 0 to 127; if not specified, all subitems of ACL will be activated.

Description

Use the **reset traffic-statistic** command to clear statistics of all traffic or traffic of a specific ACL.

Table 39 Comparison between two statistics clearing commands

Command	Description
reset acl counter	Clears ACL statistics. This command is for the ACLs that perform filtering and traffic classification to the packets processed by software. The cases for software to import ACLs include ACL importing for routing policy, ACL importing for registered user control. The ACL ID available here is in the range of 2000 to 3999.
reset traffic-statistic	Clear traffic statistics. This command is for the ACLs sent to hardware for packet filtering and traffic classification. This command usually clears the statistics collected with the **traffic-statistic** command.

Example

Clear traffic statistics of the ACL 4000.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800]interface e thernet3/1/1
[3Com-Ethernet3/1/1] reset traffic-statistic inbound link-group 4000
```

traffic-limit

Syntax

Command format which only applies IP group ACL

traffic-limit inbound ip-group { *acl-number* | *acl-name* } [**rule** *rule* [**system-index** *index*]] [**tc-index** *index*] *cir cbs ebs* [*pir*] [**conform** { { **remark-cos** | **remark-drop-priority** }* | **remark-policed-service** }] [**exceed** { **forward** | **drop** }]

undo traffic-limit inbound ip-group { *acl-number* | *acl-name* } [**rule** *rule*]

In VLAN view:

traffic-limit inbound ip-group { *acl-number* | *acl-name* } [**rule** *rule* [**system-index** *index*]] **traffic-index** *index*] [**conform** { { **remark-cos** | **remark-policed-service** }] [**exceed** { **forward** | **drop** }] **slot** *slotid*

undo traffic-limit inbound ip-group { *acl-number* | *acl-name* } [**rule** *rule*] **slot** *slotid*

Command format which applies IP group and link group ACL at the same time

traffic-limit inbound ip-group { *acl-number* | *acl-name* } { **rule** *rule* **link-group** { *acl-number* | *acl-name* } [**rule** *rule* [**system-index** *index*]] | **link-group** { *acl-number* | *acl-name* } **rule** *rule* } [**tc-index** *index*] *cir cbs ebs* [*pir*] [**conform** { { **remark-cos** | **remark-drop-priority** }* | **remark-policed-service** }] [**exceed** { **forward** | **drop** }]

undo traffic-limit inbound ip-group { *acl-number* | *acl-name* } { **rule** *rule* **link-group** { *acl-number* | *acl-name* } [**rule** *rule*] | **link-group** { *acl-number* | *acl-name* } **rule** *rule* }

Command format which only applies link group ACL

traffic-limit inbound link-group { *acl-number* | *acl-name* } [**rule** *rule* [**system-index** *index*]] [**tc-index** *index*] *cir cbs ebs* [*pir*] [**conform** { { **remark-cos** | **remark-drop-priority** }* | **remark-policed-service** }] [**exceed** { **forward** | **drop** }]

undo traffic-limit inbound link-group { *acl-number* | *acl-name* } [**rule** *rule*]

View

Ethernet port view, port group view

Parameter

inbound: Sets traffic limitation for the inbound packets at the port.

ip-group { *acl-number* | *acl-name* }: Activates IP ACLs, including basic and advanced ACLs. *acl-number* : Sequence number of ACL, ranging from 2000 to 3999. *acl-name*: Name of the ACL, which must be a character string starting with an English letter (a-z or A-Z), and without any space in it.

link-group { *acl-number* | *acl-name* }: Activates Layer 2 ACLs. *acl-number*: Sequence number of ACL, ranging from 4000 to 4999. *acl-name*: Name of ACL, which must be a character string started with an English letter (a-z or A-Z), and without any space in it.

rule *rule*: Specifies the subitem of an active ACL, ranging from 0 to 127; if not specified, all subitems of ACL will be activated.

system-index *index* here is the system index for an ACL rule. When delivering a rule, the system assigns a globally unique index to it, for convenience of later retrieval. You can also assign a system index for it when delivering an ACL rule with this command, but this value may change while the system is running. Generally you are not recommended to manually assign a system index.

tc-index *index*: Index value of traffic conditioner, ranging from 0 to 12288. If you configured the same index value to different traffic rules during traffic policy configuration, then the sum of these traffics is restricted by the configured traffic policy parameter. For example, configure cir of the traffic that matches rule 1 to 10 kbps, and that of the rule 2 to 10 kbps too; and both of the rules have the same index value of traffic conditioner, then the sum of the average rates of rule 1 and rule 2 is restricted to 10 kbps.

- The parameters of traffic policy must be the same if you configure the same tc-index for different traffic; otherwise the system prompts you for the wrong configuration; when the tc-index is 0, it means that the system will select an index value automatically.

- When you configure traffic policing for a port group, all the ports in the port group occupy the same bandwidth, that is, the configured traffic parameter is shared by all the ports.

cir: Committed information rate in Kbps.

cbs: Committed burst size in bytes.

ebs: Excess burst size in bytes.

pir: Peak information rate in Kbps.

conform: Optional parameter used to set the action to be taken when the traffic does not exceed the set value.

remark-cos: Sets new 802.1p priority value for the packet according to its conform level and local precedence.

remark-drop-priority: Sets drop precedence value for the packet according to its conform level.

remark-policed-service: Sets new service parameters for the packet according to its conform level and DSCP value.

exceed: Optional parameter to set action for the case when traffic threshold is exceeded.

- forward: Forwards the packet.
- drop: Drops the packet.

traffic-index *index*: Traffic index.

slot *slotid*: Slot number of a service processor card.

Description

Use the **traffic-limit** command to activate an ACL and set traffic limitation to take different actions for the packets within and beyond the preset traffic threshold.

Use the **undo traffic-limit** command to remove traffic limitation setting.

This command is only applicable to the packets which match the permitted rules in the ACL.

It is required that CIR is less than or equal to PIR and CBS is less than or equal to EBS. You are recommended to configure CBS and EBS to numbers that are 100 to 150 times of CIR.

For the same traffic, you cannot select both the **remark-cos** and **remark-policed-service** keywords, or both the **remark-drop-priority** and **remark-policed-service** keywords.

Before selecting the **remark-policed-service** keyword, you must make sure you have configured the DSCP + Conform-Level -> Service parameter mapping table. Before selecting the **remark-cos** keyword, you must ensure you have configured

the Local-precedence + Conform-level-> 802.1p priority mapping table. For details about the two mapping tables, see the **qos conform-level**, **dscp** and **local-precedence** commands.

Example

Set traffic limitation for the packets match the permitted rules in the ACL 4000: CIR is 200 kbps, CBS is 2000 bytes, EBS is 2500 bytes, drop the excessive packets.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800]interface ethernet2/1/1
[SW8800] traffic-limit inbound link-group 4000 200 2000 2500 conform

remark-policed-service exceed drop
```

traffic-priority

Syntax

Command Format Which Only Applies IP Group ACL

traffic-priority inbound ip-group { *acl-number* | *acl-name* } [**rule** *rule* [**system-index** *index*]] { **auto** | **remark-policed-service** { **trust-dscp** | **dscp** *dscp-value* | **untrusted dscp** *dscp-value* **cos** *cos-value* **local-precedence** *local-precedence* **drop-priority** *drop-level* } }

undo traffic-priority inbound ip-group { *acl-number* | *acl-name* } [**rule** *rule*]

Command Format Which Applies IP Group and Link Group ACL at Same time

traffic-priority inbound ip-group { *acl-number* | *acl-name* } { **rule** *rule* **link-group** { *acl-number* | *acl-name* } [**rule** *rule* [**system-index** *index*]] | **link-group** { *acl-number* | *acl-name* } **rule** *rule* } { **auto** | **remark-policed-service** { **trust-dscp** | **dscp** *dscp-value* | **untrusted dscp** *dscp-value* **cos** *cos-value* **local-precedence** *local-precedence* **drop-priority** *drop-level* } }

undo traffic-priority inbound ip-group { *acl-number* | *acl-name* } { **rule** *rule* **link-group** { *acl-number* | *acl-name* } [**rule** *rule*] | **link-group** { *acl-number* | *acl-name* } **rule** *rule* }

Command Format Which Only Applies Link Group ACL

traffic-priority inbound link-group { *acl-number* | *acl-name* } [**rule** *rule* [**system-index** *index*]] { **auto** | **remark-policed-service** { **trust-dscp** | **dscp** *dscp-value* | **untrusted dscp** *dscp-value* **cos** *cos-value* **local-precedence** *local-precedence* **drop-priority** *drop-level* } }

undo traffic-priority inbound link-group { *acl-number* | *acl-name* } [**rule** *rule*]

View

Ethernet port view, port group view

Parameter

inbound: Sets traffic priority for inbounds packets at the port.

ip-group { *acl-number* | *acl-name* }: Activates IP ACLs, including basic and advanced ACLs. *acl-number*: Sequence number of ACL, ranging from 2000 to

3999. *acl-name*: Name of the ACL, which must be a character string starting with an English letter (a-z or A-Z), and without any space in it.

link-group { *acl-number* | *acl-name* }: Activates Layer 2 ACLs. *acl-number*: Sequence number of ACL, ranging from 4000 to 4999. *acl-name*: Name of ACL, which must be a character string started with an English letter (a-z or A-Z), and without any space in it.

rule *rule*: Specifies the subitem of an active ACL, ranging from 0 to 127; if not specified, all subitems of ACL will be activated.

system-index *index* here is the system index for an ACL rule. When delivering a rule, the system assigns a globally unique index to it, for convenience of later retrieval. You can also assign a system index for it when delivering an ACL rule with this command, but this value may change while the system is running. Generally you are not recommended to manually assign a system index.

auto: Chooses the service parameters allocated automatically by the switch.

remark-policed-service: Reallocates service parameters.

trust-dscp: Reallocates service parameters according to packet DSCP values.

dscp *dscp-value*: Reallocates service parameters according to user's DSCP values or EXP values. For IP packets, *dscp-value* is the specified DSCP priority value (six bits in the packet header) and in the range of 0 to 63; for MPLS packets, other than that the *dscp-value* stands for their DSCP priority value, the three high-order bits of the value represent the EXP flag field. Set the EXP value when defining the *dscp-value*.

untrusted dscp *dscp-value* **cos** *cos-value* **local-precedence** *local-precedence* **drop-priority** *drop-level*: Customizes a set of service parameters. For IP packets, *dscp-value* is the specified DSCP priority value (six bits in the packet header) and in the range of 0 to 63; for MPLS packets, other than that the *dscp-value* stands for their DSCP priority value, the three high-order bits of the value represent the EXP flag field. Set the EXP value when defining the *dscp-value*; *local-precedence* is local precedence, in number (ranging 0 to 7) or name; *cos-value* is 802.1p priority, in number (ranging 0 to 7) or name; *drop-level* is drop level, in number (ranging 0 to 2) or name.

The mapping relationship between dscp-value and EXP is:

- When the Switch 8800 Family switch is used as the ingress PE device, for the IP packets, EXP is matched according to the "DSCP+Conform-Level-service parameters" mapping table; for TCP and UDP packets, the value of EXP is the lower 3 bits of *dscp-value*.
- When the Switch 8800 Family switch is used as the ingress P, the value of EXP is the lower 3 bits of the *dscp-value*.

Description

Use the **traffic-priority** command to activate an ACL and choose a set of service parameters for the matched traffic (only available to permitted ACL rules).

Use the **undo traffic-priority** command to remove service parameter setting.

The system can set service parameters for the matched traffic in one of following modes:

1 Employ the service parameters automatically allocated by the switch. Upon receiving a packet, the switch allocates a set of service parameters for it according to a specific rule. To choose this mode, you should select the **auto** keyword in this command.

2 Choose service parameters from the "DSCP + Conform-Level -> Service-parameter" mapping table according to packet DSCP value and conform level. To choose this mode, you should select the **remark-policed-service trust-dscp** keyword in this command.

3 Choose service parameters from the " DSCP + Conform-Level -> Service-parameter " mapping table or " EXP + Conform-Level -> Service-parameter " mapping table according to user's DSCP priority or EXP value of MPLS packets and packet conform level. To choose this mode, you should select the **remark-policed-service dscp** *dscp-value* parameter in this command.

4 Customize a set of service parameters. To choose this mode, you should select the **remark-policed-service untrusted dscp** *dscp-value* **cos** *cos-value* **local-precedence** *local-precedence* **drop-priority** *drop-level* parameter in this command.

- The "DSCP + Conform-Level -> Service-parameter" mapping table and " EXP + Conform-Level -> Service-parameter " mapping table here is that for the conform level 0.
- Before selecting the second or third mode, you should make sure that you have configured the "DSCP + Conform-Level -> Service-parameter" mapping table and " EXP + Conform-Level -> Service-parameter " mapping table. For more information about this mapping table, see the **qos conform-level**, **dscp** and **exp** commands.

Related command: **display qos-interface traffic-priority**.

Example

Choose auto service parameters for the packets which match the permitted rules in the ACL 4000.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800]interface e thernet5/1/2
[3Com-Ethernet5/1/2] traffic-priority inbound link-group 4000 auto
```

traffic-redirect

Syntax

Command Format Which Only Applies IP Group ACL

traffic-redirect inbound ip-group { *acl-number* | *acl-name* } [**rule** *rule* [**system-index** *index*]] { **cpu** | **interface** *interface-type interface-number destination-vlan* { **l2-vpn** | **l3-vpn** } | **next-hop** *ip-addr1* [*ip-addr2*] [**invalid** { **forward** | **drop** }] | **slot** *slotid* { *vlanid* | **designated-vlan** *vlanid* } [**join-vlan**] }

undo traffic-redirect inbound ip-group { *acl-number* | *acl-name* } [**rule** *rule*]

Command Format Which Applies IP Group and Link Group ACL at Same time

traffic-redirect inbound ip-group { *acl-number* | *acl-name* } [**rule** *rule*] **link-group** { *acl-number* | *acl-name* } [**rule** *rule*] { **cpu** | **interface** *interface-type interface-number destination-vlan* { **l2-vpn** | **l3-vpn** } | **next-hop** *ip-addr1* [*ip-addr2*] [**invalid** { **forward** | **drop** }] | **slot** *slotid* **designated-vlan** *vlanid* [**join-vlan**] }

undo traffic-redirect inbound ip-group { *acl-number* | *acl-name* } { **rule** *rule* **link-group** { *acl-number* | *acl-name* } [**rule** *rule*] | **link-group** { *acl-number* | *acl-name* } **rule** *rule* [**join-vlan**] }

or **undo traffic-redirect inbound link-group** { *acl-number* | *acl-name* } { **rule** *rule* **ip-group** { *acl-number* | *acl-name* } | **ip-group** { *acl-number* | *acl-name* } **rule** *rule* }

Command Format Which Only Applies Link Group ACL

traffic-redirect inbound link-group { *acl-number* | *acl-name* } [**rule** *rule* [**system-index** *index*]] { **cpu** | **interface** *interface-type interface-number destination-vlan* { **l2-vpn** | **l3-vpn** } | **next-hop** *ip-addr1* [*ip-addr2*] [**invalid** { **forward** | **drop** }] | **slot** *slotid* **designated-vlan** *vlanid* [**join-vlan**] }

undo traffic-redirect inbound link-group { *acl-number* | *acl-name* } [**rule** *rule*]

View

Ethernet port view, port group view

Parameter

ip-group { *acl-number* | *acl-name* }: Activates IP ACLs, including basic and advanced ACLs. *acl-number* : Sequence number of ACL, ranging from 2000 to 3999. *acl-name*: Name of the ACL, which must be a character string starting (1 to 32 characters) with an English letter (a-z or A-Z), and without any space in it.

link-group { *acl-number* | *acl-name* }: Activates Layer 2 ACLs. *acl-number*: Sequence number of ACL, ranging from 4000 to 4999. *acl-name*: Name of ACL, which must be a character string (1 to 32 characters) started with an English letter (a-z or A-Z), and without any space in it.

rule *rule*: Specifies the rule of an active ACL, ranging from 0 to 127; if not specified, all rules of ACL will be activated.

system-index *index* here is the system index for an ACL rule. When delivering a rule, the system assigns a globally unique index to it, for convenience of later retrieval. You can also assign a system index for it when delivering an ACL rule with this command, but this value may change while the system is running. Generally you are not recommended to manually assign a system index.

cpu: Redirects packets to the CPU.

interface *interface-type interface-number destination-vlan* { **l2-vpn** | **l3-vpn** : Redirects packets to the specified Ethernet port. *interface-number* and *interface-type* together can define a port. *destination-vlan* { **l2-vpn** | **l3-vpn** } is used to redirect MPLS packets. **l2-vpn** means that MPLS l2-vpn packets are

allowed to pass, and **l3-vpn** means that MPLS l3-vpn packets are allowed to pass. *destination-vlan* must be the VLAN where the destination port belongs to.

next-hop *ip-addr1* [*ip-addr2*]: Redirects packets to the specified IP address. You can define two IP addresses at a stoke, but the first one is with higher priority. That is, the system redirects packets to the second IP address only if the first one is unreachable.

invalid { **forward** | **drop** }: Sets the method of processing packets (forward or drop) when the IP address of the next hop is invalid. The packet will be dropped by default.

slot *slotid*: Redirects packets to the specified service processor card.

vlanid: Specifies the VLAN of the packets to be redirected.

designated-vlan *vlanid*: VLAN where a designated port resides.

join-vlan: if this key word is specified, and if redirection is enabled, the system will add the port into the *destination-vlan* automatically; if redirection is disabled, the system will remove the port from VLAN, if the last **join-vlan** enabled redirection in VLAN is deleted. This field should be specified in the redirection applications related to MPLS (such as VPLS, L3VPN and interchangeably plugged cards). Only the Ethernet and GigabitEthernet port views support **join-vlan** currently.

Description

Use the **traffic-redirect** command to activate an ACL and configure traffic redirection. Use the **undo traffic-redirect** command to remove traffic redirection setting.

You can redirect packets to the CPU, a specified Ethernet port, a specified IP address or a specified slot.

- Traffic redirection setting is only available for the permitted rules in the ACL.
- The packet redirected to the CPU cannot be forwarded normally.
- You can achieve policy route by selecting the **next-hop** keyword in this command.
- Multicast packets are not allowed to be redirected to the service processor cards.

Related command: **display qos-interface traffic-redirect**. Refer to the "VLAN&QinQ" section in the manual for the information on the **traffic-redirect** { **nested-vlan** | **modified-vlan** } command.

Example

Configure traffic redirection on the interface cards for packets that match the permit rules in ACL 4000: packets are redirected to the port Ethernet5/1/1.the destination-vlan ID is 4094, L3 VPN packet is permitted..

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800]interface e thernet5/1/2
```

```
[3Com-Ethernet5/1/2] traffic-redirect inbound link-group 4000
interface ethernet5/1/1 4094 l3-vpn
```

Configure traffic redirection on a service processor card for packets that match the permit rules in ACL 3000.

1 Redirect the packets of VLAN4 that match the permit rules in ACL 3000 to a service processor card in Ethernet port view.

```
<SW8800> system-view
```

System View: return to User View with Ctrl+Z.

```
[SW8800]interface e thernet5/1/2
[3Com-Ethernet5/1/2] traffic-redirect inbound ip-group 3000 slot 2 4
```

2 Redirect the packets that are distributed to the service processor card to the next hop 202.119.85.1 and 202.119.95.1 in VLAN view.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] vlan 4
[3Com-vlan4] traffic-redirect inbound ip-group 3000 next-hop 202.119
.85.1 202.119.95.1 slot 2
```

traffic-shape

Syntax

traffic-shape [**queue** *queue-id*] *max-rate burst-size*

undo traffic-shape [**queue** *queue-id*]

View

Ethernet port view, port group view

Parameter

queue *queue-id*: Specifies queue ID, in the range of 0 to 7.

max-rate: Maximum traffic rate in Kbps of the port.

burst-size: Burst size in KB. Its value should be the integer of 4.

Description

Use the **traffic-shape** command to enable traffic shaping.

Use the **undo traffic-shape** command to cancel traffic shaping.

The switch supports both shaping traffic based on port (shaping all traffic at the port) and shaping the traffic in a specified queue at the port. You can achieve the former mode by specifying no queue ID or the latter mode by specifying queue ID.

Example

Shape the traffic in the outbound queue 2 at the port: maximum rate 500 Kbps, burst size 12 Kbytes.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
```

```
[SW8800]interface e thernet3/1/1
[3Com-Ethernet3/1/1] traffic-shape queue 2 500 12
```

traffic-statistic

Syntax

Command Format Which Only Applies IP Group ACL

traffic-statistic inbound ip-group { *acl-number* | *acl-name* } [**rule** *rule* [**system-index** *index*]] [**tc-index** *index*]

undo traffic-statistic inbound ip-group { *acl-number* | *acl-name* } [**rule** *rule*]

Command Format Which Apply IP Group ACL and Link Group ACL at the Same Time

traffic-statistic inbound ip-group { *acl-number* | *acl-name* } { **rule** *rule* **link-group** { *acl-number* | *acl-name* }{ **rule** *rule* [**system-index** *index*] | **link-group** { *acl-number* | *acl-name* } **rule** *rule* } [**tc-index** *index*]

undo traffic-statistic inbound ip-group { *acl-number* | *acl-name* } { **rule** *rule* **link-group** { *acl-number* | *acl-name* } [**rule** *rule*] | **link-group** { *acl-number* | *acl-name* } **rule** *rule* }

Command Format Which Only Applies Link Group ACL

traffic-statistic inbound link-group { *acl-number* | *acl-name* } [**rule** *rule* [**system-index** *index*]] [**tc-index** *index*]

undo traffic-statistic inbound link-group { *acl-number* | *acl-name* } [**rule** *rule*]

View

Ethernet port view, port group view

Parameter

inbound: Sets traffic statistics for inbound packets at the port.

ip-group { *acl-number* | *acl-name* }: Activates IP ACLs, including basic and advanced ACLs. *acl-number*: Sequence number of ACL, ranging from 2000 to 3999. *acl-name*: Name of the ACL, which must be a character string starting with an English letter (a-z or A-Z), and without any space in it.

link-group { *acl-number* | *acl-name* }: Activates Layer 2 ACLs. *acl-number*: Sequence number of ACL, ranging from 4000 to 4999. *acl-name*: Name of ACL, which must be a character string started with an English letter (a-z or A-Z), and without any space in it.

rule *rule*: Specifies the rules of an active ACL, ranging from 0 to 127; if not specified, all rules of ACL will be activated.

system-index *index* here is the system index for an ACL rule. When delivering a rule, the system assigns a globally unique index to it, for convenience of later retrieval. You can also assign a system index for it when delivering an ACL rule with this command, but this value may change while the system is running. Generally you are not recommended to manually assign a system index.

tc-index *index*: Index value of traffic conditioner, ranging from 0 to 12288. If you configured the same index value to different traffic rules during traffic statistic configuration, then the statistic of these traffics is performed.

Description

Use the **traffic-statistic** command to activate an ACL and run traffic statistics (only available for the permitted rules in the ACL).

Use the **undo traffic-statistic** command to cancel traffic statistics.

The **traffic-statistic** command only counts the hardware matching times in packet forwarding. You can view the statistics using the **display qos-interface traffic-statistic** commands.

*Use the **traffic-statistic** command in port group view to make statistics of traffic information of all the ports in the port group.*

Related command: **display qos-interface traffic-statistic**.

Example

Run traffic statistics for the packets which match the permitted rules in the ACL 2000.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800]interface e thernet3/1/1
[3Com-Ethernet3/1/1] traffic-statistic inbound ip-group 2000
```

share descriptors

Syntax

share descriptors *slotid*

undoshare descriptors *slotid*

View

System view

Parameter

slotid: Slot ID of a card.

Description

Use the **share descriptors** command to enable the descriptor share function.

Use the **undo share descriptors** command to disable the descriptor share function.

The descriptor share function is disabled by default.

Example

Enable descriptor share on No.3 card.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z. [SW8800] share descriptors 3
```

wred

Syntax

wred *wred-index*

undo wred *wred-index*

View

System view

Parameter

wred-index: WRED index, in the range of 0 to 3.

Description

Use the **wred** command to create a WRED index view and enter it.

Use the **undo wred** command to restore the default WRED parameters.

The switch provides four sets of default WRED parameters, respectively numbered as 0, 1, 2 and 3. The ten parameters for a port are *green-min-threshhold*, *yellow-min-threshhold*, *red-min-threshhold*, *green-max-threshhold*, *yellow-max-threshhold*, *red-max-threshhold*, *green-max-prob*, *yellow-max-prob*, *red-max-prob* and *exponent*. Red, yellow and green packets respectively refer to those with drop precedent levels 2, 1 and 0.

Example

Create WRED 0 view and enter it.

```
[SW8800] wred 0
[3Com-wred-0]
```

18 ACL CONTROL COMMANDS TO CONTROL LOGIN USERS

The ACL Control Commands to Control Login Users

acl

Syntax

acl *acl-number1* { **inbound** | **outbound** }

undo acl *acl-number1* { **inbound** | **outbound** }

acl *acl-number2* **inbound**

undo acl *acl-number2* **inbound**

View

User interface view

Parameter

acl-number1: Numbers of basic number-based ACLs and advanced ACLs, ranging from 2,000 to 3,999.

acl-number2: Number of number-based Layer 2 ACL, ranging from. from 4,000 to 4,999.

inbound: Performs ACL control to the users who access the local switch using Telnet or SSH.

outbound: Performs ACL control to the users who access other switches from the local switch using Telnet or SSH.

Description

Use the **acl** command to apply an ACL to implement the ACL control to the users accessing through Telnet or SSH.

Use the **undo acl** command to remove the ACL control configured for users accessing through Telnet or SSH.

- You can only apply number-based ACLs to implement the ACL control to users accessing through Telnet or SSH.
- When you use a basic or advanced ACL to implement the ACL control to the users accessing through Telnet or SSH, incoming/outgoing connecting requests are restricted based on the source or destination IP addresses. Therefore, when

you use the rules of a basic or advanced ACL, only the source IP address and its mask, the destination IP address and its mask, and the **time-range** parameter in them are valid. Similarly, when you use Layer 2 ACLs to implement the ACL control to the users accessing through Telnet or SSH, incoming/outgoing requests are restricted based on the source MAC addresses. Therefore, when you use the rules of a Layer 2 ACL, only the source MAC address and its mask and the **time-range** parameter are valid.

- When you use a Layer 2 ACL to implement ACL control to the users accessing through Telnet or SSH, only incoming requests are restricted.
- If a user fails to log in due to ACL restriction, the system logs the failure, including the IP address, login method, user interface index value and the cause.

By default, the system does not restrict incoming/outgoing requests.

Example

Perform ACL control to the users who access the local switch through Telnet (assuming that ACL 2000 is previously created).

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] user-interface vty 0 4
[3Com-user-interface-vty0-4] acl 2000 inbound
```

snmp-agent community

Syntax

snmp-agent community { **read** | **write** } *community-name* [**mib-view** *view-name*] [**acl** *acl-number*]

undo snmp-agent community *community-name*

View

System view

Parameter

read: Indicates that this community name has the read-only right within the specified view.

write: Indicates that this community name has the read-write right within the specified view.

community-name: Community name, consisting of 1 to 32 characters.

mib-view: Set the MIB view name which can be accessed by the community name.

view-name: MIB view name, consisting of 1 to 32 characters.

acl *acl-number*: The number identifier of basic number-based ACLs, ranging from 2000 to 2999.

Description

Use the **snmp-agent community** command to set the community access name, permit the access to the switch using SNMP, and reference the ACL to perform ACL control to the network management users by *acl-number*.

Use the **undo snmp-agent community** command to remove the setting of community access name.

By default, SNMPV1 and SNMPV2C use community name to perform access.

Example

Set the community name as "3Com", permit the user to perform read-only access by using this community name, and reference the ACL 2000 to perform ACL control to the network management users (basic ACL 2000 has already been defined).

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] snmp-agent community read 3com acl 2000
```

snmp-agent group

Syntax

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*

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: V 1 security mode.

v2c: V 2 security mode.

v3: V 3 security mode.

group-name: Group name, ranging from 1 to 32 bytes.

authentication: With this parameter, the system will authenticate SNMP data without encrypting it.

privacy: Authenticates and encrypts packets.

read-view: Sets read-only view.

read-view: Name of read-only view, ranging from 1 to 32 bytes.

write-view: Permits to set read-write view.

write-view: Name of read-write view, ranging from 1 to 32 bytes.

notify-view: Sets notify view.

notify-view: Name of notify view, ranging from 1 to 32 bytes.

acl *acl-number*: Number identifier of basic number-based ACLs, ranging from 2000 to 2999.

Description

Use the **snmp-agent group** command to configure a new SNMP group and reference the ACL to perform ACL control to the network management users by **acl** *acl-number*. Use the **undo snmp-agent group** command to remove a specified SNMP group.

Example

Create a SNMP group "3com", and reference the ACL 2001 to perform ACL control to the network management users (basic ACL 2001 has already been defined).

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] snmp-agent group v1 3com acl 2001
```

snmp-agent usm-user

Syntax

snmp-agent usm-user { **v1** | **v2c** } *user-name group-name* [**acl** *acl-number*]

undo snmp-agent usm-user { **v1** | **v2c** } *user-name group-name*

snmp-agent usm-user v3 *user-name group-name* [**authentication-mode** { **md5** | **sha** } *auth-password*] [**privacy des56** *priv-password*] [**acl** *acl-number*]

undo snmp-agent usm-user v3 *user-name group-name* { **local** | **engineid** *engineid-string* }

View

System view

Parameter

v1: V 1 security mode.

v2c: V 2 security mode.

v3: V 3 security mode.

user-name: User name, ranging from 1 to 32 bytes.

group-name: Corresponding group name of the user, ranging from 1 to 32 bytes.

authentication-mode: Specifies the security level to "to be authenticated"

md5: Specifies the authentication protocol as HMAC-MD5-96.

sha: Specifies the authentication protocol as HMAC-SHA-96.

auth-password: Authentication password, character string, ranging from 1 to 64 bytes.

privacy: Specifies the security level as encryption.

des56: Specifies the DES encryption protocol.

priv-password: Encryption password, character string, ranging from 1 to 64 bytes.

acl *acl-number*: Number identifier of basic number-based ACLs, ranging from 2000 to 2999.

local: Local entity user.

engineid: Specifies the engine ID related to the user.

engineid-string: Engine ID character string.

Description

Use the **snmp-agent usm-user** command to add a new user to an SNMP group, and reference the ACL to perform ACL control to the network management users by **acl** *acl-number*.

Use the **undo snmp-agent usm-user** command to remove the user from the related SNMP group as well as the configuration of the ACL control of the user.

Example

Add a user "3com" to the SNMP group "3comgroup". Specify the security level to "to be authenticated", the authentication protocol to HMAC-MD5-96 and the authentication password to "sw8800", and reference the ACL 2002 to perform ACL control to the network management users (basic ACL 2002 has already been defined).

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] snmp-agent usm-user v3 3com 3comgroup authentication-mode m
d5 sw8800 acl 2002
```

19 VLAN-ACL CONFIGURATION COMMANDS

VLAN-ACL Configuration Commands

The VLAN-ACL configuration is subject to the following limitations:

1. Limitations on flow templates:
   - The system only applies VLAN-ACL to ports with the default flow template applied. The applied ACL rule field must be specified by the default flow template.
   - If no port in a VLAN has ACL rules applied to, the system checks all ports in the VLAN when applying an ACL rule in VLAN view and prohibits the ACL rule from being applied if a port in the VLAN has a customized flow template applied to.
   - If a VLAN-ACL is applied to some of the ports in a VLAN, a port with a customized flow template applied to can be added to the VLAN. But the system will fail to apply the VLAN-ACL to the newly added port. That is, you can apply the VLAN-ACL in VLAN view to all the ports in the VLAN except the newly added one. However, when the self-defined flow template is deleted under the port, the system will apply QACL rules in the VLAN to the new port automatically.
   - You will fail to apply the self-defined flow template of a port with a VLAN-ACL already applied to a customized flow template.
2. If both a VLAN and one of its ports have QACL rules applied, only those applied to the port work. In this case, the VLAN-ACL takes effect only after the QACL rules applied to the port are removed and the flow template applied to the port changes to the default flow template.
3. When the VLAN contains no ports, the system is prohibited from applying VLAN-ACL (including adding and deleting rules).
4. Two ports differing in VLAN-ACL configuration cannot be aggregated dynamically.
5. A VLAN-ACL is prohibited from being applied to a VLAN containing MPLS intermixing ports. Similarly, a VLAN with a VLAN-ACL applied to is prohibited from being used for MPLS intermixing.

mirrored-to

Syntax

mirrored-to inbound ip-group { *acl-number* | *acl-name* } [**rule** *rule* [**system-index** *index*]] **cpu**

undo mirrored-to inbound ip-group { *acl-number* | *acl-name* } [**rule** *rule*]

View

VLAN view

Parameter

inbound: Mirrors inbound packets at the port.

ip-group { *acl-number* | *acl-name* }: Activates IP ACLs, including basic and advanced ACLs. *acl-number*: Sequence number of ACL, ranging from 2000 to 3999. *acl-name*: Name of the ACL, which must be a character string starting with an English letter (a-z or A-Z), and without any space in it.

rule *rule*: Specifies the subitem of an active ACL, ranging from 0 to 127; if not specified, all subitems of ACL will be activated.

system-index *index*: Specifies the system index value of the rule which will be indexed during operation. After delivering a rule, the system automatically assigns a globally unique index value to the rule. When using the **mirrored-to** command to deliver a rule, you can also specify a system index value for the rule, but this value may change while the system is running. In general, you are not recommended to specify this parameter manually.

cpu: Mirrors traffic to the CPU.

Description

Use the **mirrored-to** command to activate an ACL and mirror matching data streams in VLAN to the CPU.

Use the **undo mirrored-to** command to remove traffic mirroring setting.

This configuration is only applicable to the packets which match the permit rules in the ACL.

Example

Mirror to the CPU the packets which are received by a port in VLAN2 and match the permit rules in the ACL 2000.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] vlan 2
[3Com-vlan2] mirrored-to inbound ip-group 2000 cpu
```

packet-filter

Syntax

packet-filter inbound ip-group { *acl-number* | *acl-name* } [**rule** *rule* [**system-index** *index*]]

undo packet-filter inbound ip-group { *acl-number* | *acl-name* } [**rule** *rule*]

View

VLAN view

Parameter

inbound: Mirrors inbound packets at the port.

ip-group { *acl-number* | *acl-name* }: Activates IP ACLs, including basic and advanced ACLs. *acl-number*: Sequence number of ACL, ranging from 2000 to 3999. *acl-name*: Name of the ACL, which must be a character string starting with an English letter (a-z or A-Z), and without any space in it.

rule *rule*: Specifies the subitem of an active ACL, ranging from 0 to 127; if not specified, all subitems of ACL will be activated.

system-index *index*: Specifies the system index value of the rule which will be indexed during operation. After delivering a rule, the system automatically assigns a globally unique index value to the rule. When using this command to deliver a rule, you can also specify a system index value for the rule, but this value may change while the system is running. In general, you are not recommended to specify this parameter manually.

Description

Use the **packet-filter** command to activate the ACLs in VLAN.

Use the **undo packet-filter** command to deactivate an active ACL.

Example

Activate ACL 2000 of each port in VLAN 2.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] vlan 2
[3Com-vlan2] packet-filter inbound ip-group 2000
```

traffic-limit

Syntax

traffic-limit inbound ip-group { *acl-number* | *acl-name* } [**rule** *rule* [**system-index** *index*]] [**tc-index** *index*] { **traffic-index** *traffic-index* | *cir cbs ebs* [*pir*] } { **conform** { **remark-cos** | **remark-policed-service** } | **exceed** { **forward** | **drop** } }*

undo traffic-limit inbound ip-group { *acl-number* | *acl-name* } [**rule** *rule*]

View

VLAN view

Parameter

inbound: Implements traffic policing for data packets received on the port.

ip-group { *acl-number* | *acl-name* }: Activates the ACL identified by the *acl-number* or *acl-name* argument. The ACL here can be a basic ACL or an advanced ACL. *acl-number*: Sequence number of the ACL, ranging from 2000 to 3999. *acl-name*: Name of the ACL, a string beginning with character a-z or A-Z. Note that this argument cannot contain spaces.

rule *rule*: Specifies the rule identified by the *rule* argument of the ACL. The *rule* argument ranges from 0 to 127. Without this keyword, this command applies to all rules of the ACL.

system-index *index*: Specifies the system index value of the rule. Normally, an applied rule is assigned a globally unique index value automatically for being indexed. You can also specify the index value for the rule, but this value may change while the system is running. In general, you are not recommended to specify this parameter manually.

tc-index *index*: The traffic control index. If the same index is configured under different flow rules when you configure the traffic policing, the total traffic of all these flows will be limited by the configured flow policing parameters. For example, the cir value of the flow of match rule 1 is configured to be 10kbps, and that of match rule 2 is configured to be 10kbps. The **tc-index** values of the two rules are the same at the same time. Then the sum of the average rate of the flow matching rule 1 and the flow matching rule 2 will be limited to 10kbps.

traffic-index *traffic index*: Traffic index value. Quote the traffic parameters through *traffic-index*. These traffic parameters are configured with the **traffic-params** command.

When you specifies the same tc-index value for different flows, the parameter settings of the traffic policing action must be consistent completely; otherwise the system will prompt errors; when the tc-index is set to 0, it means that the system will select the index automatically.

cir: Committed information rate in Kbps.

cbs: Committed burst size in bytes.

ebs: Excess burst size in bytes.

pir: Peak information rate in Kbps.

remark-cos: Sets new 802.1p priority value for the packet according to its conform-level and local precedence.

remark-drop-priority: Sets drop precedence value for the packet according to its conform-level.

remark-policed-service: Sets new service parameters for the packet according to its conform-level and DSCP priority value.

exceed: Optional parameter, used to set the action to be taken when traffic threshold is exceeded.

forward: Forwards the packet.

drop: Drops the packet.

Description

Use the **traffic-limit** command to activate ACL flow identification to perform flow limit for the matching data flow in the VLAN and perform different actions on the packets within the flow limit and those beyond the flow limit.

Use the **undo traffic-limit** command to undo the flow limit.

Use the command to perform flow limit on the packets matching the specified ACL (only available to the rules whose action is **permit** in the ACL).

When the parameter is set, it is required that *cir<=pir,cbs<=ebs.* It is recommended to set the values of *cbs* and *ebs* 100-150 times of the value of *cir.*

The setting of **tc-index** is subject to the following limitations:

- **remark-cos** and **remark-policed-service** cannot be set at the same time for the same data flow, neither can **remark-drop-priority** and **remark-policed-service**.
- You need to configure the "DSCP+Conform-level Ð† Service parameter" mapping table before configuring the **remark-policed-service** action; you need to configure the "Local-precedence + Conform-level Ð† 802.1p priority" mapping table before configuring the **remark-cos** action. Refer to the **qos control-level, dscp, local-precedence** command for the descriptions of the two mapping tables.

Example

Perform flow limit on packets received on the ports in VLAN 2 if they match the permit rule in ACL3000. Set the CIR to 2000 kbps, the CBS to 2000 bytes and the EBS to 2500 bytes. Drop packets when this threshold is exceeded.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] vlan 2
[3Com-vlan2] traffic-limit inbound ip-group 3000 200 2000 2500
conform remark-policed-service exceed drop
```

traffic-priority

Syntax

traffic-priority inbound ip-group { *acl-number* | *acl-name* } [**rule** *rule* [**system-index** *index*]] { **auto** | **remark-policed-service** { **trust-dscp | dscp** *dscp-value* | **untrusted dscp** *dscp-value* **cos** *cos-value* **local-precedence** *local-precedence* **drop-priority** *drop-level* } }

undo traffic-priority inbound ip-group { *acl-number* | *acl-name* } [**rule** *rule*]

View

VLAN view

Parameter

inbound: Sets priority for packets received on the port.

ip-group { *acl-number* | *acl-name* }: Activates the ACL identified by the *acl-number* or *acl-name* argument. The ACL here can be a basic ACL or an advanced ACL. *acl-number*: Sequence number of the ACL, ranging from 2000 to 3999. *acl-name*: Name of the ACL, a string beginning with character a-z or A-Z. Note that this argument cannot contain spaces.

rule *rule*: Specifies the rule identified by the *rule* argument of the ACL. The *rule* argument ranges from 0 to 127. Without this keyword, this command applies to all rules of the ACL.

system-index *index*: Specifies the system index value of the rule. Normally, a applied rule is assigned a globally unique index value automatically for being indexed. You can also specify the index value for the rule, but this value may change while the system is running. In general, you are not recommended to specify this parameter manually.

auto: Chooses the service parameters allocated automatically by the switch.

remark-policed-service: Reallocates service parameters.

trust-dscp: Reallocates service parameters according to the DSCP values carried by packets.

dscp *dscp-value*: Reallocates service parameters according to customized DSCP values or EXP values. For IP packets, *dscp-value* is the DSCP priority (six bits in length in the packet header) ranging from 0 to 63 and is set by users. For MPLS packets, the *dscp-value* argument indicates the DSCP priority. In addition, the least three bits of the value also act as the EXP flag field, which is set simultaneously when the user specifies the *dscp-value* argument.

untrusted dscp *dscp-value* **cos** *cos-value* **local-precedence** *local-precedence* **drop-priority** *drop-level*: Customizes a set of service parameters. For IP packets, *dscp-value* is the DSCP priority (six bits in length in the packet header) ranging from 0 to 63 and is set by users. For MPLS packets, the *dscp-value* indicates the DSCP priority value. In additional, the least three bits of the value also acts as the EXP flag field, which is set simultaneously when the user specifies the *dscp-value* argument. The *local-precedence* argument is local precedence, in the range of 0 to 7. The *cos-value* argument is 802.1p priority, in the range of 0 to 7. The *drop-level* argument is drop level, in the range of 0 to 2.

Description

Use the **traffic-priority** command to activate an ACL for flow classification and choose a set of service parameters for the matched flow in VLAN (only available to ACL rules that permit packets).

Use the **undo traffic-priority** command to remove service parameters for the specified flow.

The system can perform the following operations to the service parameters of the matched flow:

1. Employ the service parameters automatically allocated by the switch. Upon receiving a packet, the switch allocates a set of service parameters for it according to a specific rule. To choose this mode, specify the **auto** keyword when executing this command.
2. Choose service parameters from the "DSCP + Conform-Level -> Service-parameter" mapping table according to the DSCP priority and conform level of the packet. To choose this mode, specify the **remark-policed-service trust-dscp** keyword when executing this command.
3. Choose service parameters from the " DSCP + Conform-Level -> Service-parameter " mapping table and "EXP + Conform-Level -> Service-parameter " mapping table according to Conform-Level and customized

DSCP priorities and EXP values of MPLS packets. To choose this mode, specify the **remark-policed-service dscp** *dscp-value* when executing this command.

4 Specify a set of service parameters. To choose this mode, specify **remark-policed-service untrusted dscp** *dscp-value* **cos** *cos-value* **local-precedence** *local-precedence* **drop-priority** *drop-level* parameter when executing this command.

- The "DSCP + Conform-Level -> Service-parameter" mapping table and "EXP + Conform-Level -> Service-parameter" mapping table here are mapping tables with the Conform-Level of 0.
- Before selecting the second or third mode listed above, make sure the "DSCP + Conform-Level -> Service-parameter" mapping table and "EXP + Conform-Level -> Service-parameter" mapping table already exist. For more information about these mapping tables, refer to the **qos conform-level**, **dscp**, and **exp** commands.

Example

Choose automatically-allocated service parameters for the packets matching the rules that permit packets in the ACL 3000 in the data flow that the ports in VLAN receives.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] vlan 2
[3Com-vlan2] traffic-priority inbound ip-group 3000 auto
```

traffic-redirect

Syntax

traffic-redirect inbound ip-group { *acl-number* | *acl-name* } [**rule** *rule* [**system-index** *index*]] { **cpu** | **next-hop** *ip-addr1* [*ip-addr2*] [**invalid** { **forward** | **drop** }] }

undo traffic-redirect inbound ip-group { *acl-number* | *acl-name* } [**rule** *rule*]

View

VLAN view

Parameter

inbound: Redirects data packets received by a port.

ip-group { *acl-number* | *acl-name* }: Activates IP ACLs, including basic and advanced ACLs. *acl-number*: Sequence number of ACL, ranging from 2000 to 3999. *acl-name*: Name of the ACL, which must be a character string starting with an English letter (a-z or A-Z), and without any space in it.

rule *rule*: Specifies the subitem of an active ACL, ranging from 0 to 127; if not specified, all subitems of ACL will be activated.

system-index *index*: Specifies the system index value of the rule which will be indexed during operation. After delivering a rule, the system automatically assigns a globally unique index value to the rule. When using this command to deliver a rule, you can also specify a system index value for the rule, but the value may

change while the system is running. In general, you are not recommended to specify this parameter manually.

cpu: Redirects packets to the CPU.

next-hop *ip-addr1* [*ip-addr2*]: Redirects packets to the specified IP address. You can define two IP addresses at a stoke. The system redirects packets to the first IP address if the fist IP address has higher priority. However, if the first one is unreachable, the system automatically redirects packets to the second IP address.

invalid { **forward** | **drop** }: Sets the method of processing packets (forward or drop) when the IP address of the next hop is invlaid. The packet will be dropped by default.

Description

Use the **traffic-redirect** command to activate an ACL and configure traffic redirection for the matching data flow in VLAN (only available to permit ACL rules).

Use the **undo traffic-redirect** command to remove traffic redirection setting.

You can redirect packets to the CPU or a specified IP address.

- Traffic redirection setting is only available for the permit rules in the ACL.
- The packet redirected to the CPU cannot be forwarded normally.
- You can achieve policy route by selecting the **next-hop** keyword in this command.

Example

Redirect to the CPU the packets of VLAN2 that match the permit rules in ACL 3000.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] vlan 2
[3Com-vlan2] traffic-redirect inbound ip-group 3000 cpu
```

traffic-statistic

Syntax

traffic-statistic inbound ip-group { *acl-number* | *acl-name* } [**rule** *rule* [**system-index** *index*]] [**tc-index** *index*]

undo traffic-statistic inbound ip-group { *acl-number* | *acl-name* } [**rule** *rule*]

View

VLAN view

Parameter

inbound: Makes statistics of traffics of data packets received by a port.

ip-group { *acl-number* | *acl-name* }: Activates IP ACLs, including basic and advanced ACLs. *acl-number*: Sequence number of ACL, ranging from 2000 to

3999. *acl-name*: Name of the ACL, which must be a character string starting with an English letter (a-z or A-Z), and without any space in it.

rule *rule*: Specifies the subitem of an active ACL, ranging from 0 to 127; if not specified, all subitems of ACL will be activated.

system-index *index*: Specifies the system index value of the rule which will be indexed during operation. After delivering a rule, the system automatically assigns a globally unique index value to the rule. When using this command to deliver a rule, you can also specify a system index value for the rule, but the value may change while the system is running. In general, you are not recommended to specify this parameter manually.

tc-index *index*: Traffic adjustment index value. If you configure the same index value for different ACL rules when configuring traffic statistics, the switch will make statistics of these traffics.

Description

Use the **traffic-statistic** command to activate an ACL and run traffic statistics for the matching data flow in VLAN (only available for the permit rules in the ACL).

Use the **undo traffic-statistic** command to cancel traffic statistics.

The statistics information contains the hardware matching times in packet forwarding.

Example

In VLAN 2, run traffic statistics for the packets which match the permit rules in ACL 2000.

```
[3Com-vlan2] traffic-statistic inbound ip-group 2000
```

port can-access vlan-acl

Syntax

port can-access vlan-acl vlan *vlan-id*

View

Ethernet port view

Parameter

vlan-id: VLAN ID, in the range of 1 to 4,094.

Description

Use the **port can-access vlan-acl** command to synchronize VLAN-ACL configuration of the specified VLAN to the port.

When being added to a VLAN, a port automatically synchronizes VLAN-ACL configuration of the VLAN. The synchronization fails if system resources are not enough. In this case, you can delete part of configuration of the card and then use this command to manually synchronize the ACL rules applied to the VLAN to the specified port.

Example

Synchronize ACL configuration of VLAN 5 to Ethernet3/1/1 port manually.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface Ethernet3/1/1
[3Com-Ethernet3/1/1]port can-access vlan-acl vlan 5
```

display vlan-acl-member-ports

Syntax

display vlan-acl-member-ports vlan *vlan-id*

View

Any view

Parameter

vlan-id: VLAN ID, in the range of 1 to 4,094.

Description

Use the **display vlan-acl-member-ports** command to view in this VLAN the ports with the ACL configuration of the VLAN synchronized to.

When a port is added to a VLAN, you may fail to synchronize the VLAN-ACL configuration of the VLAN because the resources are not enough or user-defined flow templates are applied to ports. You can use this command to view the ports to which the ACL rule configured on the specified VLAN is applied.

Example

View the ports to which the ACL rule configured on VLAN 5 is applied.

```
<SW8800>display vlan-acl-member-ports vlan 5
Vlan-acl member port(s):
      Ethernet2/1/11          Ethernet2/1/20          Ethernet2/1/21
      Ethernet2/1/22          Ethernet2/1/23          Ethernet2/1/24
      Ethernet2/1/25          Ethernet2/1/40
```

20 802.1X CONFIGURATION COMMANDS

802.1x Configuration Commands

anti-attack

Syntax

anti-attack { **arp | dot1x | ip** }{ **disable | enable** }

View

System view

Parameter

arp: ARP packet.

dot1x :dot1 packet.

ip: IP packet.

Description

Use the **anti-attack** { **arp | dot1x | ip** } **enable** command to enable packet attack prevention.

Use the **anti-attack** { **arp | dot1x | ip** } **disable** command to disable packet attack prevention.

By default, IP packet attack prevention is enabled, and ARP packet attack prevention and dot1x packet attack prevention are disabled.

Example

Enable ARP packet attack prevention.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] anti-attack arp enable
```

Disable IP packet attack prevention.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] anti-attack ip disable
```

display dot1x

Syntax

display dot1x [**enabled-interface** | **guest vlan** | **interface** *interface-list* | **sessions** | **statistics**]

View

Any view

Parameter

enabled-interface: Configures to display the Ethernet port that starts 802.1x.

guest vlan: Displays Guest VLAN IDs and specifies the port that enables Guest VLAN.

interface: Configures to display the 802.1x information on the specified interface.

interface-list: Ethernet interface list expressed in the format *interface-list =interface-type interface-number* [**to** *interface-type interface-number*] *&<1-10>*. *interface-type* means the interface type, *interface-number* is the interface number. Refer to command parameters in the "Port" section in the manual for the respective meanings and value ranges of them. The interface number after the key word **to** should be no smaller than the interface number before **to**. *&<1-10>* in the command means that the preceding parameter can be entered up to 10 times.

sessions: Configures to display the session connection information of 802.1x.

statistics: Configures to display the relevant statistics information of 802.1x.

Description

Use **display dot1x** command to view the relevant information of 802.1x, including configuration information, running state (session connection information) and relevant statistics information.

By default, all the relevant 802.1x information about each interface will be displayed.

This command can be used to display the following information on the specified interface: 802.1x configuration, state or statistics. If no port is specified when executing this command, the system will display all 802.1x related information. For example, 802.1x configuration of all ports, 802.1x session connection information, and 802.1x data statistical information. The output information of this command can help the user to verify the current 802.1x configurations so as to troubleshoot 802.1x.

Related command: **reset dot1x statistics**, **dot1x**, **dot1x retry**, **dot1x max-user**, **dot1x port-control**, **dot1x port-method**, **dot1x timer**.

Example

Display the configuration information of 802.1x.

```
<SW8800> display dot1x
Equipment 802.1X protocol is enabled
 CHAP authentication is enabled
 DHCP-launch is disabled
 Proxy trap checker is disabled
 Proxy logoff checker is disabled

 Configuration: Transmit Period     30 s,  Handshake Period       30 s
                Quiet Period        60 s,  Quiet Period Timer is disabled
                Supp Timeout        30 s,  Server Timeout         100 s
                The maximal retransmitting times          2
```

```
 Total maximum 802.1x user resource number is 2048
 Total current used 802.1x resource number is 0

 Ethernet3/1/1  is link-down
   802.1X protocol is disabled
   Proxy trap checker is disabled
   Proxy logoff checker is disabled
   The port is a(n) authenticator
   Authenticate Mode is auto
   Port Control Type is Mac-based
   Max on-line user number is 1024
... (Omitted)
```

Table 40 Description of 802.1x configuration information

Field	Description
Equipment 802.1X protocol is enabled	802.1X protocol is enabled on the switch.
CHAP authentication is enabled	CHAP authentication is enabled
DHCP-launch is disabled	If any user configures a static IP without authorization in DHCP environment, the switch will trigger authentication on the user.
Proxy trap checker is disabled Proxy logoff checker is disabled	The system does not check the access of users who log on through a proxy.
Transmit Period	Transmit interval timer
Handshake Period	The interval of sending handshake packets of 802.1x
Quiet Period	Quiet period set by Quiet timer
Quiet Period Timer is disable	Quiet Period Timer is disable
Supp Timeout	Timeout timer for Supplicant authentication
Server Timeout	Timeout timer for Authentication Server
The maximal retransmitting times	The maximal times for the Ethernet switch to retransmit authentication request frames to access user
Total maximum 802.1x user resource number	The maximum number of access users allowed
Total current used 802.1x resource number	Number of access users currently on line
Ethernet3/1/1 is link-up	The state of Ethernet 2/1/1 is Up.
802.1X protocol is disabled	802.1X protocol is disabled on the port
Proxy trap checker is disabled Proxy logoff checker is disabled	The port prohibits the access of users who log on through a proxy
The port is a(n) authenticator	The port acts as authenticator
Authenticate Mode is auto	The authentication mode of the port is Auto
Port Control Type is Mac-based	The port control type is Mac-based, namely, authentication of access users is implemented based on the MAC address.
Max on-line user number	The maximum number of on-line users
...	Omitted

dot1x

Syntax

dot1x [**interface** *interface-list*]

undo dot1x [**interface** *interface-list*]

View

System view, Ethernet port view

Parameter

interface-list: Ethernet interface list expressed in the format *interface-list =interface-type interface-number* [**to** *interface-type interface-number*] *&<1-10>*. *interface-type* means the interface type, *interface-number* is the interface number. Refer to command parameters in the "Port" section in the manual for the respective meanings and value ranges of them. The interface number after the key word **to** should be no smaller than the interface number before **to**. *&<1-10>* in the command means that the preceding parameter can be entered up to 10 times.

Description

Use the **dot1x** command to enable 802.1x on the specified port or globally (i.e., on the current device).

Use the **undo dot1x** command to disable the 802.1x on the specified port or globally.

By default, 802.1x is disabled on all the ports and globally on the device.

When the **dot1x** command is used in system view, if the parameter *interface-list* is not specified, 802.1x will be globally enabled. If the parameter *interface-list* is specified, 802.1x will be enabled on the specified port. When this command is used in Ethernet port view, the parameter *interface-list* cannot be input and 802.1x can only be enabled on the current port.

The configuration command can be used to configure the global or port 802.1x performance parameters before or after 802.1x is enabled. Before 802.1x is enabled globally, if the parameters are not configured globally or for a specified port, they will maintain the default values.

After the global 802.1x performance is enabled, only when port 802.1x performance is enabled will the configuration of 802.1x become effective on the port.

If 802.1x is enabled on a port, you cannot configure the maximum number of learned MAC addresses (by using the **mac-address max-mac-count** command). and vice versa.

Related command: **display dot1x**.

Example

Enable 802.1x on Ethernet 3/1/1.

```
[SW8800] dot1x interface Ethernet 3/1/1
```

Enable the 802.1x globally.

```
[SW8800] dot1x
```

dot1x authentication-method

Syntax

dot1x authentication-method { **chap** | **pap** | **eap** { **md5-challenge** | **peap** | **tls** }

undo dot1x authentication-method

View

System view

Parameter

chap: Uses CHAP authentication method.

pap: Uses PAP authentication method.

eap: Uses EAP authentication method. By now, only MD5 encryption method is available.

md5-challenge: EAP MD5-Challenge authentication method

peap: EAP PEAP authentication method

tls: EAP TLS authentication method

Description

Use the **dot1x authentication-method** command to configure the authentication method for 802.1x user.

Use the **undo dot1x authentication-method** command to restore the default authentication method of 802.1x user.

By default, CHAP authentication is used for 802.1x user authentication.

Password Authentication Protocol (PAP) is a kind of authentication protocol with two handshakes. It sends password in the form of simple text.

Challenge Handshake Authentication Protocol (CHAP) is a kind of authentication protocol with three handshakes. It only transmits username but not password. CHAP is more secure and reliable.

In the process of EAP authentication, switch directly sends authentication information of 802.1x user to RADIUS server in the form of EAP packet. It is not necessary to transfer the EAP packet to standard RADIUS packet first and then send it to RADIUS server.

Please note: To realize PAP, CHAP or EAP authentication, RADIUS server should support PAP, CHAP or EAP authentication respectively.

Related command: **display dot1x**.

Example

Configure 802.1x user to use PAP authentication

```
[SW8800] dot1x authentication-method pap
```

dot1x dhcp-launch

Syntax

dot1x dhcp-launch

undo dot1x dhcp-launch

View

System view

Parameter

None

Description

Use the **dot1x dhcp-launch** command to set 802.1x to disable the switch to trigger the user ID authentication over the users who configure static IP addresses in DHCP environment.

Use the **undo dot1x dhcp-launch** command to set 802.1x to enable the switch to trigger the authentication over them.

By default, the switch can trigger the user ID authentication over the users who configure static IP addresses in DHCP environment.

Related command: **dot1x**.

Example

Disable the switch to trigger the authentication over the users who configure static IP addresses in DHCP environment.

```
[SW8800] dot1x dhcp-launch
```

dot1x guest-vlan

Syntax

dot1x guest-vlan *vlan-id* [**interface** *interface-list*]

undo dot1x guest-vlan *vlan-id* [**interface** *interface-list*]

View

System view, Ethernet interface view

Parameter

vlan-id: ID of the VLAN specified as the Guest VLAN. It ranges from 1 to 4094.

interface-list: List of Guest VLAN-enabled ports expressed in the format *interface-list =interface-type interface-number* [**to** *interface-type interface-number*] *&<1-10>*. *interface-type* means the interface type, *interface-number* is the interface number. Refer to command parameters in the "Port" section in the manual for the respective meanings and value ranges of them. The interface number after the key word **to** should be no smaller than the interface number before **to**. *&<1-10>* in the command means that the preceding parameter can be entered up to 10 times.

Description

Use the **dot1x guest-vlan** command to enable Guest VLAN on a specific port.

Use the **undo dot1x guest-vlan** command to disable Guest VLAN.

If you execute the **dot1x guest-vlan** command in system view and do not provide the *interface-list* argument, Guest VLAN is enabled on all ports. However, if you

provide the *interface-list* argument, Guest VLAN is enabled on the ports specified by this argument.

If you execute the **dot1x guest-vlan** command in Ethernet interface view, this command does not accept the *interface-list* argument and Guest VLAN is enabled only on the current port.

Example

Specify to perform port-based authentications.

```
[SW8800] dot1x port-method portbased
```

Enable Guest VLAN on all ports.

```
[SW8800] dot1x guest-vlan 1
```

dot1x max-user

Syntax

dot1x max-user *user-number* [**interface** *interface-list*]

undo dot1x max-user [**interface** *interface-list*]

View

System view, Ethernet port view

Parameter

user-number: Specifies the limit to the amount of supplicants on the port, ranging from 1 to 1024.

By default, the maximum user number is 1024. And a switch can accommodate a total of 2048 users.

interface *interface-list*: Ethernet interface list expressed in the format *interface-list =interface-type interface-number* [**to** *interface-type interface-number*] *&<1-10>*. *interface-type* means the interface type, *interface-number* is the interface number. Refer to command parameters in the "Port" section in the manual for the respective meanings and value ranges of them. The interface number after the key word **to** should be no smaller than the interface number before **to**. *&<1-10>* in the command means that the preceding parameter can be entered up to 10 times.

Description

Use the **dot1x max-user** command to configure a limit to the amount of supplicants on the specified interface of 802.1x.

Use the **undo dot1x max-user** command to restore the default value.

This command is used for setting a limit to the amount of supplicants that 802.1x can hold on the specified interface. This command has effect on the interface specified by the parameter *interface-list* when executed in system view. It has effect on all the interfaces when no interface is specified. The parameter *interface-list* cannot be input when the command is executed in Ethernet interface view and it has effect only on the current interface.

Related command: **display dot1x**.

Example

Configure the interface Ethernet 3/1/1 to hold no more than 32 users.

```
[SW8800] dot1x max-user 32 interface Ethernet 3/1/1
```

dot1x port-control

Syntax

dot1x port-control { **auto** | **authorized-force** | **unauthorized-force** } [**interface** *interface-list*]

undo dot1x port-control [**interface** *interface-list*]

View

System view, Ethernet interface view

Parameter

auto: Automatic identification mode, showing that the initial state of the interface is unauthorized. The user is only allowed to receive or transmit EAPoL packets but not to access the network resources. If the user passes the authentication flow, the interface will switch over to the authorized state and then the user is allowed to access the network resources. This is the most common case.

authorized-force: Forced authorized mode, showing that the interface to always stay in authorized state and the user is allowed to access the network resources without authentication/authorization.

unauthorized-force: Forced unauthorized mode, showing that the interface to always stay in non-authorized mode, the switch does not respond to authentication requests and the user is not allowed to access the network resources.

interface *interface-list*: Ethernet interface list expressed in the format *interface-list =interface-type interface-number* [**to** *interface-type interface-number*] *&<1-10>*. *interface-type* means the interface type, *interface-number* is the interface number. Refer to command parameters in the "Port" section in the manual for the respective meanings and value ranges of them. The interface number after the key word **to** should be no smaller than the interface number before **to**. *&<1-10>* in the command means that the preceding parameter can be entered up to 10 times.

Description

Use the **dot1x port-control** command to configure the mode for 802.1x to perform access control on the specified interface.

Use the **undo dot1x port-control** command to restore the default access control mode.

By default, the access control mode is **auto**.

This command is used to set the mode, or the interface state, for 802.1x to perform access control on the specified interface. This command has effect on the interface specified by the parameter *interface-list* when executed in system view. It has effect on all the interfaces when no interface is specified. The parameter

interface-list cannot be input when the command is executed in Ethernet port view and it has effect only on the current interface.

Related command: **display dot1x**.

Example

Configure the interface Ethernet 3/1/1 to be in **unauthorized-force** state.

```
[SW8800] dot1x port-control unauthorized-force interface ethernet 3/1/1
```

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

Parameter

macbased: Configures the 802.1x authentication system to perform authentication on the supplicant based on MAC address.

portbased: Configures the 802.1x authentication system to perform authentication on the supplicant based on interface number.

interface *interface-list*: Ethernet interface list expressed in the format *interface-list =interface-type interface-number* [**to** *interface-type interface-number*] *&<1-10>*. *interface-type* means the interface type, *interface-number* is the interface number. Refer to command parameters in the "Port" section in the manual for the respective meanings and value ranges of them. The interface number after the key word **to** should be no smaller than the interface number before **to**. *&<1-10>* in the command means that the preceding parameter can be entered up to 10 times.

Description

Use the **dot1x port-method** command to configure the base for 802.1x to perform access control on the specified interface.

Use the **undo dot1x port-method** command to restore the default access control base.

By default, the value is **macbased**.

This command is used to set the base for 802.1x to perform access control, namely authenticate the users, on the specified interface. When **macbased** is adopted, the user access this interface must be authenticated independently, and if one successful authentication user is to finish network service, the other accessed users can still use network service. When **portbased** is adopted, if only the first access user by this interface can be authenticated successfully, the other access users followed can be considered authenticated successfully automatically, but if the first one finish the network service, the other accessed users' network service will be rejected.

This command has effect on the interface specified by the parameter *interface-list* when executed in system view. It has effect on all the interfaces when no interface is specified. The parameter *interface-list* cannot be input when the command is executed in Ethernet interface view and it has effect only on the current interface.

Related command: **display dot1x**.

Example

Authenticate the supplicant based on the interface number on Ethernet 3/1/1.

```
[SW8800] dot1x port-method portbased interface ethernet 3/1/1
```

dot1x quiet-period

Command

dot1x quiet-period

undo dot1x quiet-period

View

System view

Parameter

None

Description

Use the **dot1x quiet-period** command to enable the Quiet-period timer.

Use the **undo dot1x quiet-period** command to disable this timer.

If an 802.1x user has not passed the authentication, the Authenticator will keep quiet for a while (which is specified by quiet-period timer) before launching the authentication again. During the quiet period, the Authenticator does not do anything related to 802.1x authentication.

By default, Quiet-period timer is disabled.

Related command: **display dot1x** , **dot1x timer quiet-period**.

Example

Enable quiet-period timer.

```
[SW8800] dot1x quiet-period
```

dot1x retry

Syntax

dot1x retry max-*retry-value*

undo dot1x retry

View

System view

Parameter

max-retry-value: Specifies the maximum times an Ethernet switch can retransmit the authentication request frame to the supplicant, ranging from 1 to 10.

By default, the value is 2, that is, the switch can retransmit the authentication request frame to the supplicant for 2 times.

Description

Use the **dot1x retry** command to configure the maximum times an Ethernet switch can retransmit the authentication request frame to the supplicant.

Use the **undo dot1x retry** command to restore the default maximum retransmission time.

After the switch has transmitted authentication request frame to the user for the first time, if no user response is received during the specified time-range, the switch will re-transmit authentication request to the user. This command is used for specifying how many times the switch can re-transmit the authentication request frame to the supplicant. When the time is 1, the switch is configured to transmit authentication request frame only once. 2 indicates that the switch is configured to transmit authentication request frame once again when no response is received for the first time and so on. This command has effect on all the port after configuration.

Related command: **display dot1x**.

Example

Configure the current device to transmit authentication request frame to the user for no more than 9 times.

```
[SW8800] 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

Parameter

logoff: Cuts network connection to a user upon detecting the use of proxy.

trap: Sends trap message upon detecting a user using proxy to access the switch.

interface *interface-list*: Ethernet interface list expressed in the format *interface-list =interface-type interface-number* [**to** *interface-type interface-number*] *&<1-10>*. *interface-type* means the interface type, *interface-number* is the interface number. Refer to command parameters in the "Port" section in the manual for the respective meanings and value ranges of them. The interface number after the key word **to** should be no smaller than the interface number before **to**. *&<1-10>* in the command means that the preceding parameter can be entered up to 10 times.

Description

Use the **dot1x supp-proxy-check** command to configure the control method for 802.1x access users via proxy logon the specified interface.

Use the **undo dot1x supp-proxy-check** command to cancel the control method set for the 802.1x access users via proxy.

Note that when performing this function, the user logging on via proxy need to run 3Com 802.1x client program,(3Com 802.1x client program version V1.29 or above is needed).

This command is used to set on the specified interface when executed in system view. The parameter *interface-list* cannot be input when the command is executed in Ethernet Port view and it has effect only on the current interface. After globally enabling proxy user detection and control in system view, only if you enable this feature on a specific port can this configuration take effects on the port.

Related command: **display dot1x**.

Example

Configure the switch cut network connection to a user upon detecting the use of proxy on Ethernet 2/1/1 through Ethernet 2/1/8.

```
[SW8800] dot1x supp-proxy-check logoff
[SW8800] dot1x supp-proxy-check logoff interface Ethernet 2/1/1 to
Ethernet 2/1/8
```

Configure the switch to send trap message upon detecting the use of proxy on Ethernet 2/1/9.

```
[SW8800] dot1x supp-proxy-check trap
[SW8800] dot1x supp-proxy-check trap interface Ethernet 2/1/9
```

or

```
[SW8800] dot1x supp-proxy-check trap
[SW8800] interface Ethernet 2/1/9
[3Com-GigabitEthernet2/1/9] dot1x supp-proxy-check trap
```

dot1x timer

Syntax

dot1x timer { **handshake-period** *handshake-period-value* | **quiet-period** *quiet-period-value* | **tx-period** *tx-period-value* | **supp-timeout** *supp-timeout-value* | **server-timeout** *server-timeout-value* }

undo dot1x timer { **handshake-period** | **quiet-period** | **tx-period** | **supp-timeout** | **server-timeout** }

View

System view

Parameter

handshake-period: This timer begins after the user has passed the authentication. After setting handshake-period, system will send the handshake packet by the period. Suppose the dot1x retry time is configured as N, the system

will consider the user having logged off and set the user as logoff state if system doesn't receive the response from user for consecutive N times.

handshake-period-value: Handshake period. The value ranges from 1 to 1024 in units of second and defaults to 30.

quiet-period: Specifies the quiet timer. If an 802.1x user has not passed the authentication, the Authenticator will keep quiet for a while (which is specified by quiet-period timer) before launching the authentication again. During the quiet period, the Authenticator does not do anything related to 802.1x authentication.

quiet-period-value: Specifies how long the quiet period is. The value ranges from 10 to 120 in units of second and defaults to 60.

server-timeout: Specifies the timeout timer of an Authentication Server. If an Authentication Server has not responded before the specified period expires, the Authenticator will resend the authentication request.

server-timeout-value: Specifies how long the duration of a timeout timer of an Authentication Server is. The value ranges from 100 to 300 in units of second and defaults to 100 seconds.

supp-timeout: Specifies the authentication timeout timer of a Supplicant. After the Authenticator sends Request/Challenge request packet which requests the MD5 encrypted text, the supp-timeout timer of the Authenticator begins to run. If the Supplicant does not respond back successfully within the time range set by this timer, the Authenticator will resend the above packet.

supp-timeout-value: Specifies how long the duration of an authentication timeout timer of a Supplicant is. The value ranges from 10 to 120 in units of second and defaults to 30.

tx-period: Has two major effects, which are described in detail in the following section.

- Specifies the transmission timeout timer. After the Authenticator sends the Request/Identity request packet which requests the user name or user name and password together, the tx-period timer of the Authenticator begins to run. If the Supplicant does not respond back with authentication reply packet successfully, then the Authenticator will resend the authentication request packet.
- Specifies the interval of multicasting 802.1x request packets periodically. In order to be compatible with clients who do not send EAPoL-Start frames actively, Switch 8800 Family switches will multicast 802.1x request packets periodically. The client will respond after receiving these packets. tx-period specifies the period of multicasting 802.1x request packets.

tx-period-value: Specifies how long the duration of the transmission timeout timer is. The value ranges from 10 to 120 in units of second and defaults to 30.

It is recommended to configure different handshake period value and handshake timeout times according to the number of users:

- When the number of users is 2048, the handshake period value should be no smaller than 2 minutes, and the handshake timeout times should be no less than 3 times;
- When the number of users is 1024, the handshake period value should be no smaller than 1 minutes, and the handshake timeout times should be no less than 3 times
- When the number of users is 512, the handshake period value should be no smaller than 30 seconds, and the handshake timeout times should be no less than 2 times.

Description

Use the **dot1x timer** command to configure the 802.1x timers.

Use the **undo dot1x timer** command to restore the default values.

When it is run, 802.1x enables many timers to control the rational and orderly interacting of the Supplicant, the Authenticator and the Authenticator Server. This command can set some of the timers (while other timers cannot be set) to adapt the interaction process. It could be necessary for some special and hard network environment. Generally, the user should keep the default values of the timers.

Related command: **display dot1x**.

Example

Set the Authentication Server timeout timer is 150s.

```
[SW8800] dot1x timer server-timeout 150
```

reset dot1x statistics

Syntax

reset dot1x statistics [**interface** *interface-list*]

View

User view

Parameter

interface *interface-list*: Ethernet interface list expressed in the format *interface-list =interface-type interface-number* [**to** *interface-type interface-number*] *&<1-10>*. *interface-type* means the interface type; *interface-number* is the interface number. Refer to command parameters in the "Port" section in the manual for the respective meanings and value ranges of them. The interface number after the key word **to** should be no smaller than the interface number before **to**. *&<1-10>* in the command means that the preceding parameter can be entered up to 10 times.

Description

Use the **reset dot1x statistics** command to reset the statistics of 802.1x.

This command can be used to re-perform information statistics if the user wants to delete the former statistics of 802.1x.

When the original statistics is cleared, if no port type or port number is specified, the global 802.1x statistics of the switch and 802.1x statistics on all the ports will

be cleared. If the port type and port number are specified, the 802.1x statistics on the specified port will be cleared.

Related command: **display dot1x**.

Example

Clear the 802.1x statistics on Ethernet 3/1/2.

```
<SW8800> reset dot1x statistics interface Ethernet 3/1/2
```

21 AAA AND RADIUS/HWTACACS PROTOCOL CONFIGURATION COMMANDS

AAA Configuration Commands

access-limit

Syntax

access-limit { **disable** | **enable** *max-user-number* }

undo access-limit

View

ISP domain view

Parameter

disable: No limit to the supplicant number in the current ISP domain.

enable *max-user-number*: Specifies the maximum supplicant number in the current ISP domain, ranging from 1 to 2312.

Description

Use the **access-limit** command to configure a limit to the amount of supplicants in the current ISP domain.

Use the **undo access-limit** command to restore the limit to the default setting.

By default, there is no limit to the amount of supplicants in the current ISP domain.

This command limits the amount of supplicants contained in the current ISP domain. The supplicants may contend with each other for the network resources. So setting a suitable limit to the amount will guarantee the reliable performance for the existing supplicants.

Example

Set a limit of 500 supplicants for the ISP domain, 3com163.net.

```
[3Com-isp-3com163.net] access-limit enable 500
```

accounting optional

Syntax

accounting optional

undo accounting optional

View

ISP domain view

Parameter

None

Description

Use the **accounting optional** command to enable accounting to be optional.

Use the **undo accounting optional** command to disable accounting to be optional.

By default, accounting is not optional. By executing the **accounting optional** command, you can enable users to utilize the network resources even when no accounting server is available or the switch fails to communicate with the accounting server. Users are denied if you do not execute this command under the same circumstance. This command is used when you want the server to authenticate without charging.

Example

Enable accounting option for domain user named 3com163.net.

```
[SW8800] domain 3com163.net
[3Com-isp-3com163.net] accounting optional
```

attribute

Syntax

attribute { **ip** *ip-address* | **mac** *mac-address* | **idle-cut** *second* | **access-limit** *max-user-number* | **vlan** *vlanid* | **location** { **nas-ip** *ip-address* **port** *portnum* | **port** *portnum* }*

undo attribute { **ip** | **mac** | **idle-cut** | **access-limit** | **vlan** | **location** }*

View

Local user view

Parameter

ip: Specifies the IP address of a user.

mac *mac-address*: Specifies the MAC address of a user. Where, *mac-address* takes on the hexadecimal format of *X-X-X*.

idle-cut *second*: Allows/Disallows the local users to enable the idle-cut function. (The specific data for this function depends on the configuration of the ISP domain where the users locate.) The argument minute defines the idle-cut time, which is in the range of 60 to 7200 seconds.

access-limit *max-user-number*: Specifies the maximum number who access the device by using the current user name. The argument *max-user-number* is in the range of 1 to 2048.

vlan *vlanid*: Sets the VLAN attribute of user, in other words, the VLAN to which a user belong. The argument *vlanid* is an integer in the range of 1 to 4094.

location: Sets the port binding attribute of user.

nas-ip *ip-address*: IP address of the access server in the event of binding a remote port with a user. The argument *ip-address* is an IP address in dotted decimal format and defaults to 127.0.0.1 (which represents the local machine).

port *portnum*: Sets the port with which a user is bound. The argument *portnum* is represented by "SlotNumber SubSlotNumber PortNumber". If the bound port has no SubSlotNumber, the value 0 can be used as the SubSlotNumber.

When you are setting a port with which you are bound, this setting takes effect only when the slot number, the subslot number and the port number exist.

Description

Use the **attribute** command to configure some attributes for specified local user.

Use the **undo attribute** command to cancel the attributes that have been defined for this local user.

As for attributes of the users that are of local LAN service type, user IP address and MAC address attribute are valid only when the ISP domain authentication scheme is a local authentication scheme, or the ISP domain authentication scheme is a RADIUS authentication scheme and the type of the RADIUS scheme is 3COM.

It should be noted that the argument **nas-ip** must be defined for a user bound with a remote port, which is unnecessary, however, in the event of a user bound with a local port.

Related command: **display local-user**.

Example

Configure the IP address 10.110.50.1 to the user 3com1.

```
[3Com-luser-3com1] attribute ip 10.110.50.1
```

cut connection

Syntax

cut connection { **all** | **access-type** { **dot1x** | **gcm** | **mac-authentication** } | **domain** *domain-name* | **interface** *interface-type interface-num* | **ip** *ip-address* | **mac** *mac-address* | **radius-scheme** *radius-scheme-name* | **vlan** *vlanid* | **ucibindex** *ucib-index* | **user-name** *user-name* }

View

System view

Parameter

all : Configures to disconnect all connection.

access-type dot1x: Configures to disconnect the user connections that are of specified access category.

dot1x: Specifies 802.1x users.

gcm: Specifies GCM users.

mac-authentication: Specifies users authenticated by MAC addresses.

domain *domain-name*: Configures to cut the connection according to ISP domain. *domain-name* specifies the ISP domain name with a character string not exceeding 24 characters. The specified ISP domain shall have been created.

mac *mac-address*: Configures to cut the connection of the supplicant whose MAC address is *mac-address*. The argument *mac-address* is in the hexadecimal format (x-x-x).

radius-scheme *radius-server-name*: Configures to cut the connection according to RADIUS scheme name. *radius-server-name* specifies the RADIUS server name with a character string not exceeding 32 characters.

interface *interface-type interface-num*: Configures to cut the connection according to the port.

ip *ip-address*: Configures to cut the connection according to IP address.

vlan *vlanid*: Configures to cut the connection according to VLAN ID. Here, *vlanid* ranges from 1 to 4094.

ucibindex *ucib-index*: Configures to cut the connection according to *ucib-index*. Here, *ucib-index* ranges from 0 to 2311.

user-name *user-name*: Configures to cut the connection according to user name . *user-name* is the argument specifying the username. It is a character string not exceeding 32 characters, excluding "/", ":", "*", "?", "<" and ">". The @ character can only be used once in one username. The pure username (the part before @, namely the user ID) cannot exceed 55 characters.

Description

Use the **cut connection** command to disconnect a user or a category of users by force.

Related command: **display connection**.

Example

Cut all the connections in the ISP domain, 3com163.net.

```
[SW8800] cut connection domain 3com163.net
```

display connection

Syntax

display connection [**access-type** { **dot1x** | **gcm** } | **domain** *domain-name* | **hwtacacs-scheme** hwtacacs-*scheme-name* | **interface** *interface-type interface-number* | **ip** *ip-address* | **mac** *mac-address* | **radius-scheme** *radius-scheme-name* | **vlan** *vlanid* | **ucibindex** *ucib-index* | **user-name** *user-name*]

View

Any view

Parameter

access-type dot1x: Configures to display the user connections that are of the specified access category.

dot1x: Specifies 802.1x access mode.

gcm: Specifies GCM access mode.

domain *domain-name*: Configures to display all the users in an ISP domain. *domain-name* specifies the ISP domain name with a character string not exceeding 24 characters. The specified ISP domain shall have been created.

hwtacacs-scheme hwtacacs-*scheme-name*: Displays all the user connections of the **hwtacacs** scheme named hwtacacs *-scheme-name*. hwtacacs *-scheme-name* is a string of no more than 32 characters.

mac *mac-address*: Configures to display the supplicant whose MAC address is *mac-address*. The argument *mac-address* is in the hexadecimal format (*x-x-x*).

radius-scheme *radius-server-name*: Configures to display the supplicant according to RADIUS server name. *radius-server-name* specifies the RADIUS server name with a character string not exceeding 32 characters.

interface *interface-type interface-number*: Configures to display the supplicant according the port.

ip *ip-address*: Configures to display the user specified with IP address.

vlan *vlanid*: Configures to display the user specified with VLAN ID. Here, *vlanid* ranges from 1 to 4094.

ucibindex *ucib-index*: Configures to display the user specified with *ucib-index*. Here, *ucib-index* ranges from 0 to 2311.

user-name *user-name*: Configures to display a user specifies with *user-name*. *user-name* is the argument specifying the username. It is a character string not exceeding 32 characters, excluding "/", ":", "*", "?", "<" and ">". The @ character can only be used once in one username. The pure username (the part before @, namely the user ID) cannot exceed 24 characters.

Description

Use the **display connection** command to view the relevant information of all the supplicants or the specified one(s). The output can help you with the user connection diagnosis and troubleshooting.

If no parameter is specified, this command displays the related information about all connected users.

Related command: **cut connection**.

Example

Display the relevant information of all the users.

```
<SW8800>display connection
Total 0 connections matched ,0 listed.
```

display domain

Syntax

display domain [*isp-name*]

View

Any view

Parameter

isp-name: Specifies the ISP domain name, with a character string not exceeding 24 characters. The specified ISP domain shall have been created.

Description

Use the **display domain** command to view the configuration of a specified ISP domain or display the summary information of all ISP domains.

By default, this command displays the summary information about all the ISP domains in the system.

This command is used to output the configuration of a specified ISP domain or display the summary information of all ISP domains. If an ISP domain is specified, the configuration information will be displayed exactly the same, concerning the content and format, as the displayed information of the **display domain** command. The output information can help with ISP domain diagnosis and troubleshooting.

Related command: **access-limit**, **domain**, **radius scheme**, **user-template**, **state**, **display domain**.

Example

Display the summary information of all ISP domains of the system.

```
<SW8800> display domain
0  Domain = system
   State = Active
   Scheme = LOCAL   Access-limit = Disable
   Vlan-assignment-mode = Integer
   Domain User Template:
   Idle-cut = Disable
   Self-service = Disable
Default Domain Name: system
Total 1 domain(s).1 listed.
```

display local-user

Syntax

display local-user [**domain** *isp-name* | **idle-cut** { **enable** | **disable** } | **service-type** { **ftp** | **lan-access** | **ppp** | **ssh** | **telnet** | **terminal** } | **state** { **active** | **block** } | **user-name** *user-name* | **vlan** *vlanid*]

View

Any view

Parameter

domain *isp-name*: Configures to display all the local users in the specified ISP domain. *isp-name* specifies the ISP domain name with a character string not exceeding 24 characters. The specified ISP domain shall have been created.

idle-cut: Configures to display the local users according to the state of idle-cut function. **disable** means that the user disables the idle-cut function and **enable**

means the user enables the function. This parameter only takes effect on the users configured as Lan-access type. For other types of users, the **display local-user idle-cut enable** and **display local-user idle-cut disable** commands will not display any information.

service-type: Configures to display local user of a specified type.

ftp means that the specified user type is FTP.

lan-access means that the specified user type is Lan-access which mainly refers to Ethernet accessing users, 802.1x supplicants for example.

ppp: Specifies PPP users.

ssh: Specifies SSH users.

telnet: Specifies Telnet users.

terminal: Specifies terminal users.

state { **active** | **block** }: Configures to display the local users in the specified state. **active** means that the system allows the user requesting network service and **block** means the system does not allow the user requesting network service.

user-name *user-name*: Configures to display a local user specified with *user-name* . *user-name* is the argument specifying the username. It is a character string not exceeding 32 characters, excluding "/", ":", "*", "?", "<" and ">". The @ character can only be used once in one username. The pure username (the part before @, namely the user ID) cannot exceed 55 characters.

vlan *vlanid*: Configures to display the local users belonged to specified VLAN. *vlanid* is the integer, ranging from 1 to 4094.

Description

Use the **display local-user** command to view the relevant information about all the local users or the specified one(s).

The output can help you with the fault diagnosis and troubleshooting related to local user.

By default, this command displays the relevant information about all the local users.

Related command: **local-user**.

Example

Display the relevant information of all the local users.

```
<SW8800> display local-user
The contents of local user user1:
 State:          Active            ServiceType Mask: None
 Idle Cut:       Disable
 AccessLimit:    Disable           Current AccessNum: 0
 Bind location:  Disable
 Vlan ID:        Disable
```

```
 IP address:     Disable
 MAC address:    Disable

Total 1 local user(s) Matched,1 listed.
```

Table 41 Description of output information of the display local-user command

Field	Description
State	State
Service Type Mask	Service type mask
Idle Cut	Idle cut switch
AccessLimit	Limit on the number of access connections
Current AccessNum	Number of current accesses
Bind location	Whether to be bound with port
VLAN ID	VLAN that the user belongs to
IP address	IP address of the user
MAC address	MAC address of the user

domain

Syntax

domain { *isp-name* | **default** { **disable** | **enable** *isp-name* } }

undo domain *isp-name*

View

System view

Parameter

isp-name: Specifies an ISP domain name. The name is expressed with a character string not exceeding 24 characters, excluding "/", ": ", "*", "? ", "<", and ">".

default enable *isp-name*: Enables the default ISP domain specified by *isp-name*.

default disable: Disables the configuration of the default ISP. Restores the default ISP domain to "system".

Description

Use the **domain** command to configure an ISP domain or enter the view of an existing ISP domain.

Use the **undo domain** command to cancel a specified ISP domain.

By default, a domain named as system has been created in the system. The attributes of system are all default values.

ISP domain is a group of users belonging to the same ISP. Generally, for a username in the userid@isp-name format, taking gw20010608@3com163.net as an example, the isp-name (i.e.3com163.net) following the @ is the ISP domain name. When 3Com Series Switches control user access, as for an ISP user whose username is in userid@isp-name format, the system will take userid part as username for identification and take isp-name part as domain name.

The purpose of introducing ISP domain settings is to support the application environment with several ISP domains. In this case, an access device may have supplicants from different ISP domains. Because the attributes of ISP users, such as username and password structures, service types, may be different, it is necessary to separate them by setting ISP domains. In ISP domain view, you can configure a complete set of exclusive ISP domain attributes for each ISP domain, which includes AAA schemes (RADIUS scheme group applied and so forth.)

For a switch, each supplicant belongs to an ISP domain. The system supports to configure up to 16 ISP domains.

When this command is used, 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 command: **access-limit**, **radius scheme**, **state**, **display domain**.

Example

Create a new ISP domain, 3com163.net, and enters its view.

```
[SW8800] domain 3com163.net
New Domain added.
[3Com-isp-3com163.net]
```

idle-cut

Syntax

idle-cut { **disable** | **enable** *minute flow* }

View

ISP domain view

Parameter

disable: means disabling the user to use idle-cut function.

enable: means enabling the user to use idle-cut function.

minute: Specifies the maximum idle time, ranging from 1 to 120 and measured in minutes.

flow: Minimum data traffic, ranging from 1 to 10,240,000 and measured in bytes.

Description

Use the **idle-cut** command to configure the user template in the current ISP domain.

By default, after an ISP domain is created, this attribute in user template is **disable**, that is, the user Idle-cut is disabled.

The user template is a set of default user attributes. If a user requesting for the network service does not have some required attributes, the corresponding attributes in the template will be endeavored to him as default ones. The user template of the switch you are using may only provide user Idle-cut settings. After a user is authenticated, if the Idle-cut is configured to enable or disable by neither

the user nor the RADIUS server, the user will adopt the Idle-cut state in the template.

Because a user template only works in one ISP domain, it is necessary to configure user template attributes for users from different ISP domain respectively.

Related command: **domain**.

Example

Enable the user in the current ISP domain, 3com163.net, to use the Idle-cut attribute specified in the user template (that is, enabling the user to use the Idle-cut function). The maximum idle time is 50 minutes and the minimum data traffic is 500 bytes.

```
[3Com-isp-3com163.net] idle-cut enable 50 500
```

ip pool

Syntax

ip pool *pool-number low-ip-address* [*high-ip-address*]

undo ip pool *pool-number*

View

System view, ISP domain view

Parameter

pool-number: Address pool number ranging from 0 to 99.

low-ip-address and *high-ip-address*: Two ends of the IP address pool. The number of IP addresses in an address pool cannot exceed 1024. If you do not provide the *high-ip-address* argument, then the address pool only contains the one specified by the *low-ip-address* argument.

Description

Use the **ip pool** command to create a local IP address pool for PPP users.

Use the **undo ip pool** command to remove a specified local address pool.

By default, no local IP address pool is created.

After creating an IP address pool in system view, you can use the **remote address** command to assign IP addresses in it to PPP users.

The IP addresses in an IP address pool created in ISP domain view are mainly for PPP users of the ISP domain. This kind of IP address pools is suitable for ports with many PPP users connected to them and the available IP address these ports provide are not sufficient. For example, a PPPoE-enabled Ethernet port can accommodate up to 4095 users, but its Virtual Template can have only one IP address pool configured, which contains up to only 1024 IP address. By configuring an ISP domain address pool for the Ethernet port, PPP users of the ISP can obtain their IP addresses from the IP address pool, through which the tension of the port address pool can be eased.

Related command: **remote address**.

Example

Create a local IP address pool ranging from 129.102.0.1 to 129.102.0.10.

```
[SW8800] domain 3com163.net
[3Com-isp-3com163.net] ip pool 0 129.102.0.1 129.102.0.10
```

level

Syntax

level *level*

undo level

View

Local user view

Parameter

level: User priority, an integer ranging from 0 to 3.

Description

Use the **level** command to set user priority.

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

By default, the user priority is 0.

Related command: **local user**.

If you specify not to authenticate or to authenticate by passwords, the levels of the commands available to an authenticated user are determined by the priority of the user interface. If a user needs to provide user name and password to pass the authentication, the levels of the commands available to an authenticated user are determined by the priority of the user.

Example

Set the user priority to 3.

```
[3Com-luser-3com1] level 3
```

local-user

Syntax

local-user { *username* | **multicast** [**domain** *domain-name*] *ipaddress* | **password-display-mode** { **auto** | **cipher-force** } }

undo local-user { *username* | **all** [**service-type** { **ftp** | **lan-access** | **telnet** | **ppp** | **ssh** | **terminal** }] | **multicast** [**domain** *domain-name*] *ipaddress* | **password-display-mode** }

View

System view

Parameter

username : Name of the user.

all: All users.

multicast [**domain** *domain-name*]: Add or delete multicast addresses according to the domain.

ipaddress: IP address of multicast.

password-display-mode { **auto | cipher-force** }: Specifies the password display mode. **auto** means displaying the password in user-specified mode; **cipher-force** means displaying password in cipher text by force.

all [**service-type** { **ftp** | **lan-access** | **telnet | ppp | ssh | terminal** }]: Deletes all local users. **ftp** means deleting all local FTP users, **lan-access** means deleting all local Lan-access users, **telnet** means deleting all local Telnet users, **ppp** means deleting all local PPP views, **ssh** means deleting all local SSH views, and **terminal** means deleting all the terminals.

Description

Use the **local-user** command to configure a local user and enter the local user view.

Use the **undo local-user** command to cancel a specified local user.

By default, the user database of the system is empty. If the client user wants to access FTP Server (Switch 8800 Family devices) through FTP, this configuration is required.

Related commands: **display local-user**, **service-type**.

Example

Add a local user named 3com1.

```
<SW8800> system-view
[SW8800] local-user 3com1
[3Com-luser-3com1]
```

local-user password-display-mode

Syntax

local-user password-display-mode { **cipher-force** | **auto** }

undo local-user password-display-mode

View

System view

Parameter

cipher-force: Forced Cipher mode specifies that the passwords of all the accessed users must be displayed in cipher text.

auto: The auto mode specifies that a user is allowed to use the **password** command to set a password display mode.

Description

Use the **local-user password-display-mode** command to configure the password display mode of all the accessing users.

Use the **undo local-user password-display-mode** command to cancel the password display mode that has been set for all the accessing users.

If **cipher-force** has been adopted, the user efforts of specifying to display passwords in simple text will render useless.

The default password display mode for all the access users is **auto**.

Related command: **display local-user** , **password**.

Example

Force all the accessing users to display passwords in cipher text.

```
[SW8800] local-user password-display-mode cipher-force
```

name **Syntax**

name *string*

undo name

View

VLAN view

Parameter

string: Name of the delivered VLAN. The name can contain up to 32 characters.

Description

Use the **name** command to configure the name of a delivered VLAN.

Use the **undo name** command to remove the name configured for a delivered VLAN.

By default, a delivered VLAN has no name.

The **name** command works with the function of dynamic VLAN delivering. For information about dynamic VLAN delivering, refer to the **vlan-assignment-mode** command.

Related command: **dot1x guest-vlan**, **vlan-assignment-mode**.

Example

Set the name of VLAN 100 to test.

```
[SW8800] vlan 100
[3Com-vlan100] name test
```

password **Syntax**

password { **simple** | **cipher** } *password*

undo password

View

Local user view

Parameter

simple: Specifies to display passwords in simple text.

cipher: Specifies to display passwords in cipher text.

password: Defines a password, which is a character string of up to 16 characters if it is in simple text and of up to 24 characters if it is in cipher text.

Description

Use the **password** command to configure a password display mode for local users.

Use the **undo password** command to cancel the specified password display mode.

If **local-user password-display-mode cipher-force** has been adopted, the user efforts of using the **password** command to set the password display mode to simple text (**simple**) will render useless.

Related command: **display local-user**.

Example

Set the user 3com1 to display the password in simple text, given the password is 20030422.

```
[3Com-luser-3com1] password simple 20030422
```

scheme

Syntax

scheme { **radius-scheme** *radius-scheme-name* [**local**] | **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** | **none** }

undo scheme { **radius-scheme** | **hwtacacs-scheme** | **none** }

View

ISP domain view

Parameter

radius-scheme-name: RADIUS scheme name, a string no longer than 32 characters in length.

hwtacacs-scheme-name: HWTACACS scheme name, a string no longer than 32 characters in length.

local: Specifies to perform local authentications.

none: Specifies not to perform authentications.

Description

Use the **scheme** command to configure the AAA scheme used in the current ISP domain.

Use the **undo scheme** command to restore the default domain AAA scheme.

By default, an AAA scheme specifies to perform local authentications.

The **scheme** command specifies a RADIUS/HWTACACS scheme for the current ISP domain. The specified scheme must be an existing scheme.

You can use the **radius-scheme** *radius-scheme-name* **local** or **hwtacacs-scheme** *hwtacacs-scheme-name* **local** command to specify to perform local authentications in case the Radius Server or the Tacacs Server fails to respond properly. That is, local authentications are performed only when the Radius Server or the Tacas Server fails.

If you specify local authentications to be the primary scheme, then only local authentications are performed and you cannot adopt RADIUS and HWTACACS scheme simultaneously. In this case, the **none** and **local** keywords act the same.

Related command: **radius scheme**, **hwtacacs scheme**.

Example

With 3com163.net as the current ISP domain, specify to adopt the RADIUS scheme named 3com.

```
[3Com-isp-3com163.net] scheme radius-scheme 3com
```

Specify the ISP domain named 3com to adopt the Scheme named rd, with Local authentication as the secondary authentication Scheme.

```
[3Com-isp-3com] scheme radius-scheme rd local
```

Specify the ISP domain named 3com to adopt **hwtacacs-scheme** hwtac Scheme, with Local authentication as the secondary authentication Scheme.

```
[3Com-isp-3com] scheme hwtacacs-scheme hwtac local
```

private-group-id mode standard

Syntax

private-group-id mode standard

undo private-group-id mode standard

View

System view

Parameter

private-group-id: Specifies the way to represent the RADIUS attribute **private-group-id**.

mode: Specifies the way to represent the RADIUS attribute **private-group-id**.

standard: Specify to code the RADIUS attribute **private-group-id** according to RFC 2868.

Description

Use the **private-group-id mode standard** command to configure VLAN delivering mode. A VLAN ID can be a string.

By default, a switch does not support a VLAN ID delivered by a RADIUS server to be of string type.

Dynamic VLAN delivering enables an Ethernet switch to monitor network resources available to users by adding the ports to which the authenticated users connect to different VLANS according to the attributes delivered by RADIUS servers. To work with Guest VLAN, ports are usually configured to perform port-based authentications. (If you configure a port to perform MAC address-based authentications, it can have only one user connected.)

Example

Configure the VLAN delivering mode to be of string type.

```
[SW8800] private_group_id mode standard
```

self-service-url

Syntax

self-service-url enable *url-string*

self-service-url disable

View

ISP domain view

Parameter

url-string: The URL (uniform resource locator) of the Web page on a self-service server. The Web page is used to modify passwords. This argument is a string that is of 1 to 64 characters in length. Do not provide character of "?" in this argument. If an URL contains "?", replace it with "|" when inputting the URL in the command line.

Description

Use the **self-service-url enable** command to configure self-service server uniform resource locator (URL).

Use the **self-service-url disable** command to remove the configuration of self-service server URL.

By default, self-service server URL is not configured on a switch.

This command must be incorporated with a RADIUS server (such as a CAMS server) that supports self-service. Self-service means that users can manage their accounts and card numbers by themselves. And a server with the self-service software installed is called a self-service server.

Once this function is enabled on a switch, users can locate the self-service server through the following operations:

- Select "Change user password" on the 802.1x client.
- After the client opens the default explorer (IE or NetScape), it locates the specified URL page used to change the user password on the self-service server.
- Change user password on this page.

The "Change user password" option is available only when the user passes the authentication; otherwise, this option is in grey and unavailable.

Example

Specify the URL of the Web page used to change password on the self-service server to be http://10.153.89.94/selfservice/modPasswd1x.jsp|userName.

```
[SW8800] domain system
[3Com-isp-system] self-service-url enable
http://10.153.89.94/selfservice/modP
asswd1x.jsp|userName
```

service-type

Syntax

service-type { **ftp** [**ftp-directory** *directory*] | **lan-access** | **ppp** [**call-number** *call-number* | **callback-nocheck** | **callback-number** *callback-number*] | **ssh** [**level** *level* | **telnet** | **terminal**] | **telnet** [**level** *level* | **ssh** | **terminal**] | **terminal** [**level** *level* | **ssh** | **telnet**] }

undo service-type { **ftp** [**ftp-directory** *directory*] | **lan-access** | **ppp** [**call-number** *call-number* | **callback-nocheck** | **callback-number** *callback-number*] | **ssh** [**level** *level* | **telnet** | **terminal**] | **telnet** [**level** *level* | **ssh** | **terminal**] | **terminal** [**level** *level* | **ssh** | **telnet**] }

View

Local user view

Parameter

ftp: Specifies user types as FTP.

ftp-directory *directory*: Specifies the directory of FTP users, *directory* is a character string of up to 64 characters.

lan-access: Specifies user type to Lan-access, which mainly refers to Ethernet accessing users, 802.1x supplicants for example.

ppp: Specifies PPP users.

call-number: Sets the phone number of the caller.

callback-nocheck: Specifies nocheck when the Modem calls back.

callback-number: Sets the callback number for callback user.

ssh: Specifies SSH users.

telnet: Specifies user type as Telnet.

level *level*: Specifies the level of Telnet or SSH users. The argument *level* is an integer in the range of 0 to 3 and defaults to 0.

terminal: Specifies user type as Terminal.

Description

Use the **service-type** command to configure a service type for a particular user.

Use the **undo service-type** command to cancel the specified service type for the user.

Example

Set to provide the Lan-access service for the user 3com1.

```
[3Com-luser-3com1] service-type lan-access
```

state

Syntax

state { **active** | **block** }

View

ISP domain view, Local user view

Parameter

active: Configures the current ISP domain (ISP domain view)/current user (local user view) as being in active state, that is, the system allows the users in the domain (ISP domain view) or the current user (local user view) to request network service.

block: Configures the current ISP domain (ISP domain view)/current user (local user view) as being in block state, that is, the system does not allow the users in the domain (ISP domain view) or the current user (local user view) to request network service.

Description

Use the **state** command to configure the state of the current ISP domain/ current user.

By default, after an ISP domain is created, it is in the **active** state (in ISP domain view).

A local user will be **active** (in local user view) upon its creation.

In ISP domain view, every ISP can either be in Active or Block state. If an ISP domain is configured to be Active, the users in it can request for network service, while in Block state, its users cannot request for any network service, which will not affect the users currently online.

Related command: **domain**.

Example

Set the current ISP domain 3com163.net to be in the block state. The supplicants in this domain cannot request for the network service.

```
[3Com-isp-3com163.net] state block
```

Set the user 3com1 to be in the block state.

```
[3Com-luser-3com1] state block
```

vlan-assignment-mode

Syntax

vlan-assignment-mode { **integer** | **string** }

View

ISP domain view

Parameter

integer: Specify the VLAN delivery mode to be integer.

string: Specify the VLAN delivery mode to be string.

Description

Use the **vlan-assignment-mode** command to specify the VLAN delivery mode (integer or string).

By default, the **integer** mode is used, that is, the switch supports the RADIUS server delivering VLAN IDs in integer form.

Dynamic VLAN delivering aims to control the network resources available to a user. With this function enabled, a switch adds the ports connecting to authenticated users to specified VLANs according to the attribute values delivered by the RADIUS server. In actual use, ports are usually set to operate in port-based mode in order to work together with Guest VLAN. A port operating in MAC address-based mode can only have one host connected to it. Currently, the VLAN IDs delivered by RADIUS servers can be of integer or string type.

- As for a VLAN ID that is of integer type, a switch adds the port to the corresponding VLAN according to the VLAN ID delivered by the RADIUS authentication server. If the VLAN does not exist, the switch creates the VLAN first and then adds the port to the VLAN.
- As for a VLAN ID that is of string type, a switch compares the VLAN ID delivered by the RADIUS authentication server with the names of the VLANs existing on the switch. If a matching entry is found, the switch adds the port into the corresponding VLAN. Otherwise, the delivery fails and the user fails to pass the authentication.

- When configuring a VLAN delivering mode, keep the mode configured on the switch consistent with the mode configured on the Radius Server.
- For the string delivery mode, the value range of the VLAN name supported by the switch is 1-32 characters. If the name configured on the Radius Server exceeds 32 characters, the delivery will fail.
- For the string delivery mode, a string that contains numerals only is first interpreted as a number. That is, if the VLAN name delivered by the RADIUS server contains only numerals (such as "1024"), and the equivalent integer is within the range 1 to 4,094, the switch takes the VLAN name as an integer and add the authenticated port to the VLAN identified by the integer (In this case, the switch will add the port to VLAN 1024). If the equivalent integer is not within the range 1 to 4,094 (such as string "12345"), the RADIUS server fails to deliver the VALN name; if the all-numeral string contains space, such as " 12 345", the first block of non-spaced numbers in the string will be converted into its equivalent integer, namely, integer 12 in this example.
- Hybrid ports and Trunk ports do not support VLAN delivering; only Access ports support VLAN delivering.

Related command: **name**, **dot1x guest-vlan**.

Example

Specify the dynamic VLAN delivery mode to be string.

```
[3Com-isp-3com163.net] vlan-assignment-mode string
```

RADIUS Protocol Configuration Commands

accounting optional

Syntax

accounting optional

undo accounting optional

View

RADIUS scheme view

Parameter

None

Description

Use the **accounting optional** command to enable the RADIUS accounting option.

Use the **undo accounting optional** command to disable the RADIUS accounting option.

By default, selection of RADIUS accounting option is disabled.

If no RADIUS server is available or if RADIUS accounting server fails when the **accounting optional** is configured, the user can still use the network resource, otherwise, the user will be disconnected.

The user configured with **accounting optional** command in RADIUS scheme will no longer send real-time accounting update packet or stop accounting packet.

The **accounting optional** command in RADIUS scheme view is only effective on the accounting that uses this RADIUS scheme.

Example

Enable the selection of RADIUS accounting of the RADIUS scheme named as CAMS.

```
[3Com-radius-cams] accounting optional
```

data-flow-format

Syntax

data-flow-format data { **byte** | **giga-byte** | **kilo-byte** | **mega-byte** } **packet** { **giga-byte** | **kilo-byte** | **mega-byte** | **one-packet** }

undo data-flow-format

View

RADIUS scheme view

Parameter

data: Sets data unit.

byte: Sets 'byte' as the unit of data flow.

giga-byte: Sets 'giga-byte' as the unit of data flow.

kilo-byte: Sets 'kilo-byte' as the unit of data flow.

mega-byte: Sets 'mega-byte' as the unit of data flow.

packet: Sets data packet unit.

giga-packet: Sets 'giga-packet' as the unit of packet flow.

kilo-packet: Sets 'kilo-packet' as the unit of packet flow.

mega-packet: Sets 'mega-packet' as the unit of packet flow.

one-packet: Sets 'one-packet' as the unit of packet flow.

Description

Use the **data-flow-format** command to configure the unit of data flow that send to RADIUS Server.

Use the **undo data-flow-format** command to restore the unit to the default setting.

By default, the data unit is byte and the data packet unit is one-packet.

Related command, see **display radius**.

Example

Set the unit of data flow that send to RADIUS Server 3Com is kilo-byte and the data packet unit is kilo-packet.

```
[3Com-radius-3com] data-flow-format data kilo-byte packet kilo-packet
```

debugging radius

Syntax

debugging radius packet

undo debugging radius packet

View

User view

Parameter

packet: Enable packet debugging

Description

Use the **debugging radius** command to enable RADIUS packet debugging.

Use the **undo debugging radius** command to disable RADIUS packet debugging.

By default, RADIUS packet debugging is disabled.

Example:

Enable RADIUS packet debugging.

```
<SW8800> debugging radius packet
```

display local-server

Syntax

display local-server { **statistics** | **nas-ip** }

View

Any view

Parameter

None

Description

Use the **display local-server statistics** command to view the statistics of local RADIUS scheme.

Use the **display local-server nas-ip** command to view the Nas-ip that is allowed to access the Local-server.

Related command: **local-server**.

Example

Display the statistics of local RADIUS scheme.

```
<SW8800> display local-server statistics
The localserver packet statistics:
Receive:                0          Send:                    0
Discard:                0          Receive Packet Error:    0
Auth Reveive:           0          Auth Send:               0
Acct Receive:           0          Acct Send:               0
```

display radius

Syntax

display radius [*radius-server-name*]

View

Any view

Parameter

radius-server-name: Specifies the RADIUS scheme name with a character string not exceeding 32 characters. Display all RADIUS scheme when the parameter is not set.

Description

Use the **display radius** command to view the configuration information of all RADIUS scheme or a specified one.

By default, This command outputs the configuration information about the specified or all the RADIUS scheme.

Related command: **radius scheme**.

Example

Display the configuration information of all the RADIUS scheme.

```
<SW8800> display radius
------------------------------------------------------------------
SchemeName  =system                              Index=0    Type=3com
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= 3com
Acct Server Encryption Key= 3com
TimeOutValue(in second)=3 RetryTimes=3 RealtimeACCT(in minute)=12
Permitted send realtime PKT failed counts       =5
Retry sending times of noresponse acct-stop-PKT =500
Username format                                 =without-domain
Data flow unit                                  =Byte
Packet unit                                     =1
------------------------------------------------------------------
Total 1 RADIUS scheme(s). 1 listed
```

Table 42 Description of output information of the display radius command

Field	Description
SchemeName	The name of Radius Scheme
Index	The index of Radius Scheme
Type	The type of Radius Scheme
Primary Auth IP/ Port/ State	The IP address of the primary authentication server/the number of the access port/the current state of the server
Primary Acct IP/ Port/ State	The IP address of the primary accounting server/the number of the access port/the current state of the server
Second Auth IP/ Port/ State	The IP address of the secondary authentication server/the number of the access port/the current state of the server
Second Acct IP/ Port/ State	The IP address of the secondary accounting server/the number of the access port/the current state of the server
Auth Server Encryption Key	The login password of the authentication server
Acct Server Encryption Key	The login password of the accounting server
TimeOutValue (seconds)	Response timeout value of the RADIUS server
Retry Times	The maximum transmitting times of RADIUS request packet.
Permitted send realtime PKT failed counts	The maximum times of sending real-time no-response accounting packet
Retry sending times of noresponse acct-stop-PKT	The maximum retry times of buffered no-response accounting stop packet
Username format	The format of the username
Data flow unit	The unit of data flow

Table 42 Description of output information of the display radius command

Field	Description
Packet unit	The unit of packets

display radius nas-ip

Syntax

display radius nas-ip

View

Any view

Parameter

None

Description

Use the **display radius nas-ip** command to display all the global NAS-IP information configured in system view, including the global NAS-IP information of public network and private network. When the NAS-IP information of global private network is displayed, the name of the VPN that the NAS-IP belongs to is also displayed.

Related command: **radius nas-ip**.

Example

Display all NAS-IP information.

```
<SW8800> display radius nas-ip
Radius VPN nas-ip:    192.168.1.1   vpn-instance:vpn1
Radius VPN nas-ip:    192.168.2.1   vpn-instance:vpn2
Radius global nas-ip: 192.168.3.1
```

display radius statistics

Syntax

display radius statistics

View

Any view

Parameter

None

Description

Use the **display radius statistics** command to view the statistics information of RADIUS packet.

The displayed packet information can help with RADIUS diagnosis and troubleshooting.

Related command: **radius scheme**.

Example

Display the statistics information of RADIUS packets.

```
<SW8800> display radius statistics
state statistic(total=4120):
DEAD=4120     AuthProc=0        AuthSucc=0
AcctStart=0         RLTSend=0         RLTWait=0
 AcctStop=0          OnLine=0            Stop=0
 StateErr=0

Receive and Send packets statistic:
Send PKT total  :0        Receive 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
Code=22,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
Leaving 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                ,Num=2317    ,Err=0       ,Succ=2317
PKT response                    ,Num=0       ,Err=0       ,Succ=0
EAP reauth_request              ,Num=0       ,Err=0       ,Succ=0
PORTAL access                   ,Num=0       ,Err=0       ,Succ=0
Update ack                      ,Num=0       ,Err=0       ,Succ=0
PORTAL access ack               ,Num=0       ,Err=0       ,Succ=0
Session ctrl pkt                ,Num=0       ,Err=0       ,Succ=0
RADIUS send messages statistic:
Normal auth accept              ,Num=0
Normal auth reject              ,Num=0
EAP auth accept                 ,Num=0
EAP auth reject                 ,Num=0
EAP auth replying               ,Num=0
EAP reauth accept               ,Num=0
EAP_reauth_reject               ,Num=0
Account success                 ,Num=0
Account failure                 ,Num=0
Account off ack                 ,Num=0
Update request                  ,Num=0
Leaving ack                     ,Num=0
Cut 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=0
```

Table 43 Description on the fields of the display radius statistics command

Field	Description
state statistic(total=4120)	State statistics (total=2312)

Table 43 Description on the fields of the display radius statistics command

Field	Description
DEAD	Dead state
AuthProc	Processing authentication
AuthSucc	Authentication successful
AcctStart	Starting accounting
RLTSend	Sending real time accounting
RLTWait	Waiting for real time accounting
AcctStop	Stop waiting for accounting
OnLine	Online
Stop	Stop
StateErr	State error

display stop-accounting-buffer

Syntax

display stop-accounting-buffer { **radius-scheme** *radius-scheme-name* | **session-id** *session-id* | **time-range** *start-time stop-time* | **user-name** *user-name* }

View

Any view

Parameter

radius-scheme *radius-server-name*: Configures to display the saved stopping accounting requests according to RADIUS scheme name. *radius-server-name* specifies the RADIUS scheme name with a character string not exceeding 32 characters.

session-id *session-id*: Configures to display the saved stopping accounting requests according to the Session ID. *session-id* specifies the Session ID with a character string not exceeding 50 characters.

time-range *start-time stop-time*: Configures to display the saved stopping accounting requests according to the saving time. *start-time* specifies the start time of the saving time range and *stop-time* specifies the stop time of the saving time range. The time is expressed in the format hh:mm:ss-yyyy/mm/dd. When this parameter is specified, all the stopping accounting requests saved in the time range since *start-time* to *stop-time* will be displayed.

user-name *user-name*: Configures to display the saved stopping accounting requests according to the username. *User-name* specifies the username, a character string not exceeding 32 characters, excluding "/", ":", "*", "?", "<" and ">". The @ character can only be used once in one username. The pure username (the part before @, namely the user ID) cannot exceed 24 characters.

Description

Use the **display stop-accounting-buffer** command to view the stopping accounting requests, which have not been responded and saved in the buffer. You can select to display the packets sent to a certain RADIUS scheme, or display the packets according to user Session ID or username. You may also display the

request packets saved during a specified time range. The displayed packet information can help with diagnosis and troubleshooting.

After transmitting the stopping accounting requests, if there is no response from the RADIUS scheme, the switch will save the packet in the buffer and retransmit it for several times, which is set through the **retry stop-accounting** command.

Related command: **reset stop-accounting-buffer**, **stop-accounting-buffer enable**, **retry stop-accounting**.

Example

Display the stopping accounting requests saved in the system buffer since 0:0:0 to 23:59:59 on August 31, 2002.

```
<SW8800> display stop-accounting-buffer time-range 0:0:0-2002/08/31
23:59:59-2002/08/31
Total find    0 record
```

key

Syntax

key { **accounting** | **authentication** } *string*

undo key { **accounting** | **authentication** }

View

RADIUS scheme view

Parameter

accounting: Configures to set the encryption key for RADIUS accounting packet.

authentication: Configures to set the encryption key for RADIUS authentication/authorization packet.

string: Specifies the key with a character string not exceeding 16 characters. By default, the key is 3com.

Description

Use the **key** command to configure encryption key for RADIUS authentication/authorization or accounting packet.

Use the **undo key** command, you can restore the default key.

RADIUS client (switch system) and RADIUS scheme use MD5 algorithm to encrypt the exchanged packets. The two ends verify the packet through setting the encryption key. Only when the keys are identical can both ends accept the packets from each other and give responses. So it is necessary to ensure that the keys set on the switch and the RADIUS scheme are identical. If the authentication/authorization and accounting are performed on two different servers with different encryption keys, you are supposed to set two encryption keys respectively.

Related command: **primary accounting**, **primary authentication**, **radius scheme**.

Example

Set the authentication/authorization key of the RADIUS scheme, 3com, to hello.

```
[3Com-radius-3com] key authentication hello
```

Set the accounting packet key of the RADIUS scheme, 3com, to ok.

```
[3Com-radius-3com] key accounting ok
```

local-server

Syntax

local-server enable

undo local-server

View

System view

Parameter

None

Description

Use the **local-server enable** command to enable the local RADIUS server and enable port 1645 and 1646. You must use this command to enable ports before using local RADIUS servers.

Use the **undo local-server** command to disable the local RADIUS server. Port 1645 and port 1646 are disabled, and RADIUS servers are unavailable in this case.

By default, local RADIUS servers are enabled, and port 1645 and port 1646 are enabled too.

Example

Enable the local RADIUS server.

```
<SW8800>system-view
[SW8800]local-server enable
```

local-server nas-ip

Syntax

local-server nas-ip *ip-address* **key** *password*

undo local-server nas-ip *ip-address*

View

System view

Parameter

nas-ip *ip-address*: Sets Nas-IP address of access server. *ip-address* is expressed in the format of dotted decimal. By default, there is a local server with the NAS-IP address of 127.0.0.1.

key *password*: Sets password of logon user. *password* is a character string containing up to 16 characters.

Description

Use the **local-server** command to configure the parameters of local RADIUS server. Using **undo local-server** command, you can cancel a local RADIUS server.

RADIUS service, which adopts authentication/authorization/accounting servers to manage users, is widely used in 3Com series switches. Besides, local authentication/authorization service is also used in these products and it is called local RADIUS function, i.e. realize basic RADIUS function on the switch.

CAUTION:

- When using local RADIUS server function of 3Com, remember the number of UDP port used for authentication is 1645 and that for accounting is 1646.
- The password configured by this command must be the same as that of the RADIUS authentication/authorization packet configured by the command **key authentication** in RADIUS scheme view.
- When operating as a local RADIUS server, a 3Com Switch 8800 Family Series Routing Switch supports CHAP and PAP authentications but not EAP MD5-challenge authentication.

3Com series switches support up to 16 local RADIUS scheme.

Related command: **radius scheme**, **state**.

Example

Set the IP address of local RADIUS scheme to 10.110.1.2 and the password to 3com.

```
[SW8800] local-server nas-ip 10.110.1.2 key 3Com
```

nas-ip

Syntax

nas-ip *ip-address*

undo nas-ip

View

RADIUS scheme view

Parameter

ip-address: Source IP address which is expressed in the format of dotted decimal notation.

Description

Use the **nas-ip** command to configure the source IP address which NAS switch uses to send RADIUS packets. In this case, all the packets sent to Radius server carry the same source IP address.

Use the **undo nas-ip** command to undo the configuration.

By specifying the source IP address used in sending Radius packets, you can avoid unreachability of packets back from the server when the physical interface fails. It is recommended to use the Loopback interface address.

By default, the source IP address of packets is the IP address of the VLAN interface to which the port connecting with the server belongs.

Related commands: **display radius, radius nas-ip**

Example

Configure the IP address that NAS (switch) uses to send RADIUS packets as 10.1.1.1.

```
[SW8800] radius scheme test1
[3Com-radius-test1] nas-ip 10.1.1.1
```

primary accounting

Syntax

primary accounting *ip-address* [*port-number*]

undo primary accounting

View

RADIUS scheme view

Parameter

ip-address: IP address, in dotted decimal format.

port-number: Specifies UDP port number. ranging from 1 to 65535.

Description

Use the **primary accounting** command to configure the IP address and port number for the primary accounting server.

Use the **undo primary accounting** command to restore the default IP address and port number of the primary RADIUS accounting server. By default, the primary accounting server of the RADIUS scheme created by the system, whose name is "system", uses IP address of 127.0.0.1 and UDP port of 1646. The primary accounting server of a newly created RADIUS scheme uses IP address of 0.0.0.0 and UDP port of 1813.

After creating a new RADIUS scheme, you need to set the IP address and the UDP port for the RADIUS servers the scheme contains, such as authentication/authorization server and accounting server. Besides, you can set primary and secondary server for each kind of server. Although, in actual use, these settings depend on specific demands, at least one authentication/authorization server and one accounting server is required. Make sure the port settings on the switch about RADIUS service are identical to those on the RADIUS servers.

Related command: **key**, **radius scheme**, **state**.

Example

Set the IP address of the primary accounting server of RADIUS scheme, "3com", to 10.110.1.2 and the UDP port 1813 to provide RADIUS accounting service.

```
[3Com-radius-3com] primary accounting 10.110.1.2 1813
```

primary authentication

Syntax

primary authentication *ip-address* [*port-number*]

undo primary authentication

View

RADIUS scheme view

Parameter

ip-address: IP address, in dotted decimal format.

port-number: Specifies UDP port number. ranging from 1 to 65535.

Description

Use the **primary authentication** command to configure the IP address and port number for the primary RADIUS authentication/authorization.

Use the **undo primary authentication** command to restore the default IP address and port number of the primary RADIUS authentication/authorization.

By default, the primary authentication server of the RADIUS scheme created by the system, whose name is "system", uses IP address of 127.0.0.1 and UDP port of 1645. The secondary authentication server uses IP address of 0.0.0.0 and UDP port of 1812. The primary and secondary authentication server of a newly created RADIUS scheme uses IP address of 0.0.0.0 and UDP port of 1812.

After creating a RADIUS scheme, you are supposed to set IP addresses and UDP port numbers for the RADIUS servers, including primary/secondary authentication/authorization servers and accounting servers. In real networking environments, the above parameters shall be set according to the specific requirements. However, at least you have to set one authentication/authorization server and an accounting server. Besides, ensure that the RADIUS service port settings on the switch is consistent with the port settings on the RADIUS server.

Related command: **key**, **radius scheme** , **state**.

Example

Set the IP address of the primary authentication/authorization server of RADIUS scheme, "3com", to 10.110.1.1 and the UDP port 1812 to provide RADIUS authentication/authorization service.

```
[3Com-radius-3com] primary authentication auth 10.110.1.1 1812
```

radius client

Syntax

radius client enable

undo radius client

View

System view

Parameter

None

Description

Use the **radius client enable** command to enable the port 1812. You must use this command to enable ports before using RADIUS authentication.

Use the **undo radius client** to disable the port 1812. You can use this command to disable ports when you do not use RADIUS authentication. The system does not receive (or respond to) UDP packets whose destination port is the port 1812 after the port 1812 is disabled.

The port 1812 is disabled by default.

Currently the RADIUS service of the system adopts the port 1812 as the source port in authentication and accounting packets, so the system cannot receive RADIUS response packets any more if the port 1812 is disabled. Thus, RADIUS service is disabled.

Example

Enable the port 1812.

```
<SW8800> system-view
[SW8800] radius client enable
```

radius nas-ip

Syntax

radius nas-ip *ip-address* [**vpn-instance** *vpn-instance-name*]

undo radius nas-ip [**vpn-instance** *vpn-instance-name*]

View

System view

Parameter

ip-address: Source IP address expressed in the format of dotted decimal notation. It must be a legal unicast address.

vpn-instance-name: The name of VPN instances, which is a string ranging of 1 to 19 characters.

Description

Use the **radius nas-ip** command to configure the nas-ip of the global public network. Only one public network nas-ip can be configured globally. Use the **radius nas-ip** *ip-address* **vpn-instance** command to configure the nas-ip of the global private network. Only one nas-ip can be configured for each private network and a maximum of 16 private networks can be configured.

Use the **undo radius** nas-ip command to cancel the nas-ip configuration for global public network. Use the **undo radius nas-ip vpn-instance** command to cancel the nas-ip configuration for a private network.

Related command: **display radius nas-ip.**

Example

Configure the source IP address that the switch uses to send RADIUS packets as 129.10.10.1.

```
<SW8800>system-view
[SW8800] radius nas-ip 129.10.10.1
```

radius scheme

Syntax

radius scheme *radius-server-name*

undo radius scheme *radius-server-name*

View

System view

Parameter

radius-server-name: Specifies the RADIUS scheme name with a character string not exceeding 32 characters.

Description

Use the **radius scheme** command to configure a RADIUS scheme and enter its view.

Use the **undo radius scheme** command to delete the specified RADIUS scheme.

By default, RADIUS scheme named as system has been created in the system. The attributes of system are all default values.

RADIUS protocol configuration is performed on a per-RADIUS-scheme basis. Every RADIUS scheme shall at least have the specified IP address and UDP port number of the RADIUS authentication/authorization/accounting server and some necessary parameters exchanged with the RADIUS client end (switch system). So it is necessary to create the RADIUS scheme and enter its view before performing other RADIUS protocol configurations.

A RADIUS scheme can be used by several ISP domains at the same time. You can configure up to 16 RADIUS schemes, including the default scheme named as system.

Although **undo radius scheme** can remove a specified RADIUS scheme. However, the default one cannot be removed. Note that a scheme currently in use by the online user cannot be removed.

Related command: **key**, **retry realtime-accounting**, **radius-scheme**, **timer realtime-accounting**, **stop-accounting-buffer enable**, **retry stop-accounting**, **server-type**, **state**, **user-name-format**, **retry**, **display radius**, **display radius statistics**.

Example

Create a RADIUS scheme named "3com" and enters its view.

```
[SW8800] radius scheme 3com
[3Com-radius-3com]
```

reset radius statistics

Syntax

reset radius statistics

View

User view

Parameter

None

Description

Use the **reset radius statistics** command to clear the statistic information related to the RADIUS protocol.

Related command: **display radius**.

Example

Clear the RADIUS protocol statistics.

```
<SW8800> reset radius statistics
```

reset stop-accounting-buffer

Syntax

reset stop-accounting-buffer { **radius-scheme** *radius-scheme-name* | **session-id** *session-id* | **time-range** *start-time stop-time* | **user-name** *user-name* }

View

User view

Parameter

radius-scheme *radius-server-name*: Configures to delete the stopping accounting requests from the buffer according to the specified RADIUS scheme. *radius-server-name* specifies the RADIUS scheme name with a character string not exceeding 32 characters.

session-id *session-id*: Configures to delete the stopping accounting requests from the buffer according to the specified session ID. *session-id* specifies the Session ID with a character string not exceeding 50 characters.

time-range *start-time stop-time*: Configures to delete the stopping accounting requests from the buffer according to the saving time. S*tart-time* specifies the start time of the saving time range and *stop-time* specifies the stop time of the saving time range. The time is expressed in the format hh:mm:ss-yyyy/mm/dd. When this parameter is set, all the stopping accounting requests saved since *start-time* to *stop-time* will be deleted.

user-name *user-name*: Configures to delete the stopping accounting requests from the buffer according to the username. *User-name* specifies the username, a character string not exceeding 32 characters, excluding "/", ":", "*", "?", "<" and ">". The @ character can only be used once in one username. The pure username (the part before @, namely the user ID) cannot exceed 24 characters.

Description

Use the **reset stop-accounting-buffer** command to reset the stopping accounting requests, which are saved in the buffer and have not been responded.

After transmitting the stopping accounting requests, if there is no response from the RADIUS scheme, the switch will save the packet in the buffer and retransmit it for several times, which is set through the **retry stop-accounting** command.

This command is used to delete the stopping accounting requests from the switch buffer. You can select to delete the packets transmitted to a specified RADIUS scheme, or according to the Session-id or username, or delete the packets transmitted during the specified time-range.

Related command: **stop-accounting-buffer enable**, **retry stop-accounting**, **display stop-accounting-buffer**.

Example

Delete the stopping accounting requests saved in the system buffer by the user, user0001@3com163.net.

```
<SW8800> reset stop-accounting-buffer user-name user0001@3com163.net
```

Delete the stopping accounting requests saved in the system buffer since 0:0:0 to 23:59:59 on August 31, 2002.

```
<SW8800> reset stop-accounting-buffer time-range 0:0:0-2002/08/31 23
:59:59-2002/08/31
```

retry

Syntax

retry *retry-times*

undo retry

View

RADIUS scheme view

Parameter

retry-times: Specifies the maximum times of retransmission, ranging from 1 to 20. By default, the value is 3.

Description

Use the **retry** command to configure retransmission times of RADIUS request packet.

Use the **undo retry** command to restore the retransmission times to default value.

Because RADIUS protocol uses UDP packets to carry the data, its communication process is not reliable. If the RADIUS server has not responded NAS until timeout, NAS has to retransmit RADIUS request packet. Suppose the maximum retransmission times is N. If the accumulative transmission times is more than N-[N/2] but the primary RADIUS server still gives no answer, the NAS will consider that it has lost the communication with the current RADIUS server and then turn to transmit the request to another RADIUS server.

Setting a suitable retry-time according to the network situation can speed up the system response.

Related command: **radius scheme**.

Example

Set to retransmit the RADIUS request packet no more than 5 times in the RADIUS scheme "3Com".

```
[3Com-radius-3com] retry 5
```

retry realtime-accounting

Syntax

retry realtime-accounting *retry-times*

undo retry realtime-accounting

View

RADIUS scheme view

Parameter

retry-times: Specifies the maximum times of real-time accounting request failing to be responded, ranging from 1 to 255. By default, the accounting request can fail to be responded up to 5 times.

Description

Use the **retry realtime-accounting** command to configure the maximum times of real-time accounting request failing to be responded.

Use the **undo retry realtime-accounting** command to restore the maximum times of real-time accounting request failing to be responded to the default value.

RADIUS server usually checks if a user is online with timeout timer. If the RADIUS server has not received the real-time accounting packet from NAS, it will consider that there is line or device failure and stop accounting. Accordingly, it is necessary to disconnect the user at NAS end and on RADIUS server synchronously when some unexpected failure occurs. 3Com Series Switches support to set maximum times of real-time accounting request failing to be responded. NAS will disconnect the user if it has not received real-time accounting response from RADIUS server for some specified times.

How to calculate the value of *count*? Suppose RADIUS server connection will timeout in T and the real-time accounting interval of NAS is t, then the integer part of the result from dividing T by t is the value of *count*. Therefore, when applied, T is suggested the numbers which can be divided exactly by t.

Related command: **radius scheme**, **timer realtime-accounting**.

Example

Allow the real-time accounting request failing to be responded for up to 10 times.

```
[3Com-radius-3com] retry realtime-accounting 10
```

retry stop-accounting

Syntax

retry stop-accounting *retry-times*

undo retry stop-accounting

View

RADIUS scheme view

Parameter

retry-times: Maximal retransmission times of a buffered stop-accounting request, ranging from 10 to 65535. By default, the value is 500.

Description

Use the **retry stop-accounting** command to configure the maximal retransmission times after a stop-accounting request is saved into the buffer due to getting no response.

Use the **undo retry stop-accounting** command to restore the retransmission times to the default value.

Because the stopping accounting request concerns account balance and will affect the amount of charge, which is very important for both the user and ISP, NAS shall make its best effort to send the message to RADIUS accounting server. Accordingly, if the message from the switch to RADIUS accounting server has not been responded, the switch shall save it in the local buffer and retransmit it until the server responds or discard the messages after transmitting for specified times.

Related command: **reset stop-accounting-buffer**, **radius scheme**, **display stop-accounting-buffer**.

Example

#Perform the following configuration such that the switch can retransmit a buffered stop-accounting request to the server configured for the RADIUS scheme "3Com" for up to 1000 times

```
[3Com-radius-3com] retry stop-accounting 1000
```

secondary accounting

Syntax

secondary accounting *ip-address* [*port-number*]

undo secondary accounting

View

RADIUS scheme view

Parameter

ip-address: IP address, in dotted decimal format. By default, the IP addresses of secondary accounting server is at 0.0.0.0.

port-number: Specifies the UDP port number, ranging from 1 to 65535. By default, the accounting service is provided via UDP 1813.

Description

Use the **secondary accounting** command to configure the IP address and port number for the secondary RADIUS accounting server.

Use the **undo secondary accounting** command to restore the IP address and port number to default values.

For detailed information, read the description of the **primary accounting** command.

Related command: **key**, **radius scheme**, **state**.

Example

Set the IP address of the secondary accounting server of RADIUS scheme, 3com, to 10.110.1.1 and the UDP port 1813 to provide RADIUS accounting service.

```
[3Com-radius-3com] secondary accounting 10.110.1.1 1813
```

secondary authentication

Syntax

secondary authentication *ip-address* [*port-number*]

undo secondary authentication

View

RADIUS scheme view

Parameter

ip-address: IP address, in dotted decimal format. By default, the IP address of secondary authentication/authorization server is 0.0.0.0.

port-number: Specifies the UDP port number, ranging from 1 to 65535. By default, the authentication/authorization service is provided via UDP 1812.

Description

Use the **secondary authentication** command to configure the IP address and port number for the secondary RADIUS authentication/authorization server.

Use the **undo secondary authentication** command to restore the IP address and port number to default values.

For detailed information, read the description of the **primary authentication** command.

Related command: **key**, **radius scheme**, **state**.

Example

Set the IP address of the secondary authentication/authorization server of RADIUS scheme, "3com", to 10.110.1.2 and the UDP port 1812 to provide RADIUS authentication/authorization service.

```
[3Com-radius-3com] secondary authentication 10.110.1.2 1812
```

server-type

Syntax

server-type { **3com** | **portal**| **standard** }

undo server-type

View

RADIUS scheme view

Parameter

3com: Configures the switch system to support the RADIUS scheme of 3Com type, which requires the RADIUS client end (switch system) and RADIUS server to interact according to the private RADIUS protocol regulation and packet format of 3Com Corporation Co., Ltd.

portal: RADIUS server cooperating with iTellin Portal system.

standard: Configures the switch system to support the RADIUS server of Standard type, which requires the RADIUS client end (switch system) and RADIUS server to interact according to the regulation and packet format of standard RADIUS protocol (RFC 2138/2139 or newer).

Description

Use the **server-type** command to configure the RADIUS scheme type supported by the switch.

Use the **undo server-type** command to restore the RADIUS scheme type to the default value.

The default RADIUS server type of a newly created RADIUS scheme is **standard**. The RADIUS server type of the default RADIUS scheme (with a name of "system"), which is created by the system, is **3com**.

3Com Switch 8800 Family Series Routing Switches support standard RADIUS protocol and the extended RADIUS service platform IP Hotel, 201+ and Portal etc independently developed by 3Com Corporation. This command is used to select the supported RADIUS scheme type.

Related command: **radius scheme**.

Example

Set RADIUS scheme type of RADIUS scheme "3com", to 3com**.**

```
[3Com-radius-3com] server-type 3com
```

state

Syntax

state { **primary** | **secondary** } { **accounting** | **authentication** } { **block** | **active** }

View

RADIUS scheme view

Parameter

primary: Configures to set the state of the primary RADIUS server.

secondary: Configures to set the state of the secondary RADIUS server.

accounting: Configures to set the state of RADIUS accounting server.

authentication: Configures to set the state of RADIUS authentication/authorization.

block: Configures the RADIUS server to be in the state of **block**.

active: Configures the RADIUS server to be **active**, namely the normal operation state.

Description

Use the **state** command to configure the state of RADIUS server.

By default, for the RADIUS scheme named "system", which the system creates by default, the primary RADIUS server is in the state of **active**, and the secondary RADIUS server is in the state of **block**. For a new RADIUS scheme, the RADIUS server is in the state of **block** if an IP address is not configured for the server; the RADIUS server is in the state of **active** if an IP address is configured for the server.

For the primary and secondary servers (no matter an authentication/authorization or an accounting server), if the primary server is disconnected to NAS for some fault, NAS will automatically turn to exchange packets with the secondary server. However, after the primary one recovers, NAS will not resume the communication with it at once, instead, it continues communicating with the secondary one. When the secondary one fails to communicate, NAS will turn to the primary one again. This command is used to set the primary server to be **active** manually, in order that NAS can communicate with it right after the troubleshooting.

When the primary and secondary servers are all **active** or **block**, NAS first sends the packets to the primary server. If NAS fails to connect the primary servers, it sends the packets to the secondary server.

Related command: **radius scheme**, **primary authentication**, **secondary authentication**, **primary accounting**, **secondary accounting**.

Example

Set the secondary authentication server of RADIUS scheme, "3com", to be Active.

```
[3Com-radius-3com] state secondary authentication active
```

stop-accounting-buffer enable

Syntax

stop-accounting-buffer enable

undo stop-accounting-buffer enable

View

RADIUS scheme view

Parameter

None

Description

Use the **stop-accounting-buffer enable** command to configure to save the stopping accounting requests without response in the switch system buffer.

Use the **undo stop-accounting-buffer enable** command to cancel the function of saving the stopping accounting requests without response in the switch system buffer.

By default, enable to save the stopping accounting requests in the buffer.

Because the stopping accounting request concerns account balance and will affect the amount of charge, which is very important for both the user and ISP, NAS shall make its best effort to send the message to RADIUS accounting server. Accordingly, if the message from the switch to RADIUS accounting server has not been responded, the switch shall save it in the local buffer and retransmit it until the server responds or discard the messages after transmitting for specified times.

Related command: **reset stop-accounting-buffer**, **radius scheme**, **display stop-accounting-buffer**.

Example

Enable the switch to buffer the stop-accounting requests that get no answer from the server configured for the RADIUS scheme "3com".

```
[3Com-radius-3com] stop-accounting-buffer enable
```

timer quiet

Syntax

timer quiet *minutes*

undo timer quiet

View

RADIUS scheme view

Parameter

minutes: The parameter ranges from 1 to 255 in minutes. By default, the primary server waits for 5 minutes before it resumes the Active state.

Description

Use the **timer quiet** command to configure the time that the primary server takes to resume the Active state.

Use the **undo timer quiet** command to restore the default configuration.

This command is designed to inhibit the switch from processing user request packets for a period of time when the communication between the switch and the server is interrupted. After the switch has waited for a period of time that is equal to or greater than the time set by this command, it restarts sending user request packets to the server.

Related command: **display radius**

Example

Set the quiet timer of the primary server to 10 minutes.

```
[SW8800] radius scheme test1
[3Com-radius-test1] timer quiet 10
```

timer realtime-accounting

Syntax

timer realtime-accounting *minute*

undo timer realtime-accounting

View

RADIUS scheme view

Parameter

minute: Real-time accounting interval, ranging from 3 to 60 and measured in minutes. It must be a multiple of 3.By default, the value is 12.

Description

Use the **timer realtime-accounting** command to configure the real-time accounting interval.

Use the **undo timer realtime-accounting** command to restore the default interval.

To implement real-time accounting, it is necessary to set a real-time accounting interval. After the attribute is set, NAS will transmit the accounting information of online users to the RADIUS server regularly.

The value of *minute* is related to the performance of NAS and RADIUS server. The smaller the value is, the higher the requirement for NAS and RADIUS server is. When there are a large amount of users (more than 1000, inclusive), we suggest a larger value. The following table recommends the ratio of *minute* value to number of users.

Table 44 Recommended ratio of minute to number of users

Number of users	Real-time accounting interval (in minutes)
1 to 99	3
100 to 499	6
500 to 999	12
‚â•1000	‚â•15

Related command: **retry realtime-accounting** , **radius scheme**.

Example

Set the real-time accounting interval of RADIUS scheme, "3com", to 15 minutes.

```
[3Com-radius-3com] timer realtime-accounting 15
```

timer response-timeout

Syntax

timer response-timeout *seconds*

undo timer response-timeout

View

RADIUS scheme view

Parameter

seconds: The value range is 1 to 10 in seconds. The default response timeout value of the RADIUS server is 3 seconds.

Description

Use the **timer response-timeout** command to set the response-timeout value of RADIUS server.

Use the **undo timer response-timeout** command to restore the default configuration.

Related command: **display radius.**

Example

Set the response timeout value of the RADIUS server to 5 seconds.

```
[SW8800] radius scheme test1
[3Com-radius-test1] timer response-timeout 5
```

user-name-format

Syntax

user-name-format { **with-domain** | **without-domain** }

View

RADIUS scheme view

Parameter

with-domain: Specifies to send the username with domain name to RADIUS server.

without-domain: Specifies to send the username without domain name to RADIUS server.

Description

Use the **user-name-format** command to configure the username format sent to RADIUS server.

By default, as for the newly created RADIUS scheme, the username sent to RADIUS servers includes an ISP domain name; as for the "system" RADIUS scheme created by the system, the username sent to RADIUS servers excludes the ISP domain name.

The supplicants are generally named in userid@isp-name format. The part following "@" is the ISP domain name. The switch will put the users into certain ISP domains according to the domain names. However, some earlier RADIUS

servers reject the username including ISP domain name. In this case, the username will be sent to the RADIUS server after its domain name is removed. Accordingly, the switch provides this command to decide whether the username to be sent to RADIUS server carries ISP domain name or not.

If a RADIUS scheme is configured to reject usernames including ISP domain names, the RADIUS scheme shall not be simultaneously used in more than one ISP domains. Otherwise, the RADIUS server will regard two users in different ISP domains as the same user by mistake, if they have the same username (excluding their respective domain names.)

Related command: **radius scheme**.

Example

Specify to send the username without domain name to RADIUS scheme.

```
[3Com-radius-3com] user-name-format without-domain
```

vpn-instance

Syntax

vpn-instance *vpn-name*

View

RADIUS scheme view

Parameter

vpn-name: The name of the VPN instance, which is a string of 1 to 19 characters.

Description

Use the **vpn-instance** command to configure the VPN that the RADIUS scheme belongs to.

Use the **undo vpn-instance** command to cancel the configuration for VPN.

The VPN in this command must exist and must be assigned with an route distinguisher (RD). One RADIUS scheme can only be bound to one VPN.

The nas-ip configured must belong to the VLAN bound to the specified VPN after a VPN is specified by the RADIUS scheme; otherwise the packets cannot be sent. Also pay attention to this point when configuring global RADIUS nas-ip.

Related command: **radius scheme.**

Example

Specify the VPN to which the RADIUS server belongs in the RADIUS scheme "3com" as vpn1.

```
[3Com-radius-3com] vpn-instance vpn1
```

HWTACACS Configuration Commands

data-flow-format

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 view

Parameter

data: Sets data unit.

byte: Sets 'byte' as the unit of data flow.

giga-byte: Sets 'giga-byte' as the unit of data flow.

kilo-byte: Sets 'kilo-byte' as the unit of data flow.

mega-byte: Sets 'mega-byte' as the unit of data flow.

packet: Sets data packet unit.

giga-packet: Sets 'giga-packet' as the unit of packet flow.

kilo-packet: Sets 'kilo-packet' as the unit of packet flow.

mega-packet: Sets 'mega-packet' as the unit of packet flow.

one-packet: Sets 'one-packet' as the unit of packet flow.

Description

Use the **data-flow-format** command to configure the unit of data flow sent to TACACS Server.

Use the **undo data-flow-format** command to restore the unit to the default setting.

By default, the data unit is byte and the data packet unit is one-packet.

Related command: **display hwtacacs**.

Example

Set the unit of data flow sent to TACACS Server 3Com to kilo-byte and the data packet unit to kilo-packet.

```
[3Com-hwtacacs-3com] data-flow-format data kilo-byte packet kilo-packet
```

debugging hwtacacs

Syntax

debugging hwtacacs { **all** | **error** | **event** | **message** | **receive-packet** | **send-packet** }

undo debugging hwtacacs { **all** | **error** | **event** | **message** | **receive-packet** | **send-packet** }

View

User view

Parameter

all: Enables all HWTACACS debugging.

error: Enables error debugging.

event: Enables event debugging.

message: Enables message debugging.

receive-packet: Enables incoming packet debugging.

send-packet: Enables outgoing packet debugging.

Description

Use the **debugging hwtacacs** command to enable HWTACACS debugging.

Use the **undo debugging hwtacacs** command to disable HWTACACS debugging.

By default, HWTACACS debugging is disabled.

Example

Enable the event debugging of HWTACACS.

```
<SW8800> debugging hwtacacs event
```

display hwtacacs

Syntax

display hwtacacs [*hwtacacs-scheme-name*]

View

Any view

Parameter

hwtacacs-scheme-name: Scheme name of the HWTACACS server, a string of 1 to 32 case-insensitive characters, excluding "?". If this argument is null, configuration information of all HWTACACS schemes are displayed.

Description

Use the **display hwtacacs** command to view configuration information of one or all HWTACACS schemes.

By default, configuration information of all HWTACACS schemes is displayed.

Related command: **hwtacacs scheme**.

Example

Display the configuration information of the HWTACACS scheme gy.

```
<SW8800> display hwtacacs gy
-------------------------------------------------------------------
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
  Source-IP-address               : 0.0.0.0
  key authentication              : 790131
  key authorization               : 790131
  key accounting                  : 790131
  Quiet-interval(min)             : 5
  Response-timeout-Interval(sec)  : 5
  Domain-included                 : No
  Traffic-unit                    : B
  Packet traffic-unit             : one-packet
```

display stop-accounting-buffer hwtacacs-scheme

Syntax

display stop-accounting-buffer hwtacacs-scheme *hwtacacs-scheme-name*

View

Any view

Parameter

hwtacacs-scheme *hwtacacs-scheme-name*: Displays information on buffered stop-accounting requests related to the HWTACACS scheme specified by *hwtacacs-scheme-name*, a character string not exceeding 32 characters, excluding "?".

Description

Use the **display stop-accounting-buffer** command to view information on the stop-accounting requests buffered in the switch.

Related command: **reset stop-accounting-buffer**, **stop-accounting-buffer enable**, **retry stop-accounting**.

Example

Display information on the buffered stop-accounting requests related to the HWTACACS scheme "3com".

```
<SW8800> display stop-accounting-buffer hwtacacs-scheme 3com
%No accounting stop packet exists.
```

hwtacacs nas-ip

Syntax

hwtacacs nas-ip *ip-address*

undo hwtacacs nas-ip

View

System view

Parameter

ip-address: IP address of a specified source, which is that of the local host and cannot be a broadcast address of class A, B or C, a class D address, an all-zero address, or an address begins with 127.

Description

Use the **hwtacacs nas-ip** command to specify the source address of the HWTACACS packet sent from NAS.

Use the **undo hwtacacs nas-ip** command to restore the default setting.

By specifying the source address of the HWTACACS packet, you can avoid unreachable packets as returned from the server upon interface failure. The source address is normally recommended to be a loopback interface address.

For the **hwtacacs nas-ip** command, the HWTACACS view takes precedence over the system view.

By default, the source address is not specified, that is, the address of the interface sending the packet serves as the source address.

This command specifies only one source address; therefore, the newly configured source address may overwrite the original one.

Example

Configure the switch to send hwtacacs packets from 129.10.10.1.

```
[SW8800] hwtacacs nas-ip 129.10.10.1
```

hwtacacs scheme

Syntax

hwtacacs scheme *hwtacacs-scheme-name*

undo hwtacacs scheme *hwtacacs-scheme-name*

View

System view

Parameter

hwtacacs-scheme-name: Name of a HWTACACS scheme, a character string not exceeding 32 characters.

Description

Use the **hwtacacs scheme** command to enter the HWTACACS view. If you specified a nonexistent scheme, a new HWTACACS scheme will be created.

Use the **undo hwtacacs scheme** command to delete a HWTACACS scheme.

Example

Create a HWTACACS scheme named test1 and enter the HWTACACS view.

```
[SW8800] hwtacacs scheme test1
[3Com-hwtacacs-test1]
```

key

Syntax

key { **accounting** | **authentication** | **authorization** } *string*

undo key { **accounting** | **authentication** | **authorization** } *string*

View

HWTACACS view

Parameter

accounting: Shared key of the accounting server.

authentication: Shared key of the authentication server.

authorization: Shared key of the authorization server.

string: Shared key, a string up to 16 characters excluding the characters "?".

Description

Use the **key** command to configure a shared key for HWTACACS authentication, authorization or accounting.

Use the **undo key** command to delete the configuration.

By default, no key is set.

The HWTACACS client (the switch system) and HWTACACS server use MD5 algorithm to encrypt the exchanged packets. The two ends verify packets using a shared key. Only when the same key is used can both ends accept the packets from each other and give responses. So it is necessary to ensure that the same key is set on the switch and the HWTACACS server. If the authentication/authorization and accounting are performed on two server devices with different shared keys, you must set one shared key for each.

Related command: **display hwtacacs**.

Example

Use "hello" as the shared key for HWTACACS accounting.

```
[SW8800] hwtacacs scheme test1
[3Com-hwtacacs-test1] key accounting hello
```

nas-ip

Syntax

nas-ip *ip-address*

undo nas-ip

View

HWTACACS view

Parameter

ip-address: Source IP address, in dotted decimal format.

Description

Use the **nas-ip** command to set the source IP address for HWTACACS packets sent from the NAS (switch), such that all the packets sent to the TACACS server carry the same source IP address.

Use the **undo nas-ip** command to delete the configuration.

Specifying the source address for sending HWTACACS packet avoids the unreachability of packet returned from the server when the physical interface fails. Generally, the Loopback interface address is recommended.

By default, the source IP address of the packets is the IP address of the interface of the VLAN to which the port connecting the server belongs.

Related command: **display hwtacacs** and **hwtacacs nas-ip**.

Example

Configure the source IP address for HWTACACS packets sent from the NAS (switch) to 10.1.1.1.

```
[SW8800] hwtacacs scheme test1
[3Com-hwtacacs-test1] nas-ip 10.1.1.1
```

primary accounting

Syntax

primary accounting *ip-address* [*port-number*]

undo primary accounting

View

HWTACACS view

Parameter

ip-address: IP address of the server, a valid unicast address in dotted decimal format.

port-number: Port number of the server, which is in the range 1 to 65535 and defaults to 49.

Description

Use the **primary accounting** command to configure a primary TACACS accounting server.

Use the **undo primary accounting** command to delete the configured primary TACACS accounting server.

By default, the IP address of the TACACS accounting server is all zeros.

You are not allowed to assign the same IP address to both primary and secondary accounting servers.

If you repeatedly use this command, the latest configuration overwrites the previous one.

You can remove a TACACS scheme accounting server only when no Active TCP connection used to send accounting packets is now using the server, and the removal impacts only packets forwarded afterwards.

Example

Configure a primary accounting server.

```
[SW8800] hwtacacs scheme test1
[3Com-hwtacacs-test1] primary accounting 10.163.155.12 49
```

primary authentication

Syntax

primary authentication *ip-address* [*port-number*]

undo primary authentication

View

HWTACACS view

Parameter

ip-address: IP address of the server, a valid unicast address in dotted decimal format.

port-number: Port number of the server, which is in the range 1 to 65535 and defaults to 49.

Description

Use the **primary authentication** command to configure a primary TACACS authentication server.

Use the **undo primary authentication** command to delete the configured authentication server.

By default, the IP address of the TACACS authentication server is all zeros.

You are not allowed to assign the same IP address to both primary and secondary authentication servers.

If you repeatedly use this command, the latest configuration overwrites the previous one.

You can remove a TACACS scheme authentication server only when no Active TCP connection used to send authentication packets uses the server., and the removal impacts only packets forwarded afterwards.

Related command: **display hwtacacs**.

Example

Configure a primary authentication server.

```
[SW8800] hwtacacs scheme test1
[3Com-hwtacacs-test1] primary authentication 10.163.155.13 49
```

primary authorization

Syntax

primary authorization *ip-address* [*port-number*]

undo primary authorization

View

HWTACACS view

Parameter

ip-address: IP address of the server, a valid unicast address in dotted decimal format.

port-number: Port number of the server, which is in the range 1 to 65535 and defaults to 49.

Description

Use the **primary authorization** command to configure a primary TACACS authorization server.

Use the **undo primary authorization** command to delete the configured primary authorization server.

By default, the IP address of the TACACS authorization server is all zeros.

You are not allowed to assign the same IP address to both primary and secondary authorization servers.

If you repeatedly use this command, the latest configuration overwrites the previous one.

You can remove a TACACS scheme authorization server only when no Active TCP connection used to send authorization packets is now using the server, and the removal impacts only packets forwarded afterwards.

Related command: **display hwtacacs**.

Example

Configure a primary authorization server.

```
[SW8800] hwtacacs scheme test1
[3Com-hwtacacs-test1] primary authorization 10.163.155.13 49
```

reset hwtacacs statistics

Syntax

reset hwtacacs statistics { **accounting** | **authentication** | **authorization** | **all** }

View

User view

Parameter

accounting: Clears all the HWTACACS accounting statistics.

authentication: Clears all the HWTACACS authentication statistics.

authorization: Clears all the HWTACACS authorization statistics.

all: Clears all statistics.

Description

Use the **reset hwtacacs statistics** command to clear HWTACACS protocol statistics.

Related command: **display hwtacacs**.

Example

Clear all HWTACACS protocol statistics.

```
<SW8800> reset hwtacacs statistics
```

reset stop-accounting-buffer

Syntax

reset stop-accounting-buffer hwtacacs-scheme *hwtacacs-scheme-name*

View

User view

Parameter

hwtacacs-scheme *hwtacacs-scheme-name*: Configures to delete the stop-accounting requests from the buffer according to the specified HWTACACS scheme name. The *hwtacacs-scheme-name* specifies the HWTACACS scheme name with a character string not exceeding 32 characters, excluding"?".

Description

Use the **reset stop-accounting-buffer** command to clear the stop-accounting requests that have no response and are buffered on the switch.

Related command: **stop-accounting-buffer enable**, **retry stop-accounting**, **display stop-accounting-buffer**.

Example

Delete the buffered stop-accounting requests that are related to the HWTACACS scheme "3com".

```
<SW8800> reset stop-accounting-buffer hwtacacs-scheme 3Com
```

retry stop-accounting

Syntax

retry stop-accounting *retry-times*

undo retry stop-accounting

View

HWTACACS view

Parameter

retry-times: The maximum number of stop-accounting request attempts. It is in the range 1 to 300 and defaults to 100.

Description

Use the **retry stop-accounting** command to enable stop-accounting packet retransmission and configure the maximum number of stop-accounting request attempts.

Use the **undo retry stop-accounting** command to restore the default setting.

By default, stop-accounting packet retransmission is enabled and up to 100 packets are allowed to be transmitted for each request.

Related command: **reset stop-accounting-buffer**, **hwtacacs scheme**, and **display stop-accounting-buffer**.

Example

Enable stop-accounting packet retransmission and allow up to 50 packets to be transmitted for each request.

```
[SW8800] retry stop-accounting 50
```

secondary accounting

Syntax

secondary accounting *ip-address* [*port-number*]

undo secondary accounting

View

HWTACACS view

Parameter

ip-address: IP address of the server, a valid unicast address in dotted decimal format.

port-number: Port number of the server, which is in the range 1 to 65535 and defaults to 49.

Description

Use the **secondary accounting** command to configure a secondary TACACS accounting server.

Use the **undo secondary accounting** command to delete the configured secondary TACACS accounting server.

By default, IP address of TACACS accounting server is all zeros.

You are not allowed to assign the same IP address to both primary and secondary accounting servers.

If you repeatedly use this command, the latest configuration overwrites the previous one.

You can remove a TACACS scheme accounting server only when no Active TCP connection used to send accounting packets is now using the server, and the removal impacts only packets forwarded afterwards.

Example

Configure a secondary accounting server.

```
[SW8800] hwtacacs scheme test1
[3Com-hwtacacs-test1] secondary accounting 10.163.155.12 49
```

secondary authentication

Syntax

secondary authentication *ip-address* [*port-number*]

undo secondary authentication

View

HWTACACS view

Parameter

ip-address: IP address of the server, a valid unicast address in dotted decimal format.

port-number: Port number of the server, which is in the range 1 to 65535 and defaults to 49.

Description

Use the **secondary authentication** command to configure a secondary TACACS authentication server.

Use the **undo secondary authentication** command to delete the configured secondary authentication server.

By default, IP address of TACACS authentication server is all zeros.

You are not allowed to assign the same IP address to both primary and secondary authentication servers.

If you repeatedly use this command, the latest configuration overwrites the previous one.

You can remove a TACACS scheme authentication server only when no Active TCP connection used to send authentication packets is now using the server, and the removal impacts only packets forwarded afterwards.

Related command: **display hwtacacs**.

Example

Configure a secondary authentication server.

```
[SW8800] hwtacacs scheme test1
[3Com-hwtacacs-test1] secondary authentication 10.163.155.13 49
```

secondary authorization

Syntax

secondary authorization *ip-address* [*port-number*]

undo secondary authorization

View

HWTACACS view

Parameter

ip-address: IP address of the server, a legal unicast address in dotted decimal format.

port-number: Port number of the server, ranging from 1 to 65535. By default, it is 49.

Description

Use the **secondary authorization** command to configure a secondary TACACS authorization server.

Use the .**undo secondary authorization** command to delete the configured secondary authorization server.

By default, IP address of TACACS authorization server is all zeros.

You are not allowed to assign the same IP address to both primary and secondary authorization servers.

If you repeatedly use this command, the latest configuration overwrites the previous one.

You can remove a TACACS scheme authorization server only when no Active TCP connection used to send authorization packets is now using the server, and the removal impacts only packets forwarded afterwards.

Related command: **display hwtacacs**.

Example

Configure the secondary authorization server.

```
[SW8800] hwtacacs scheme test1
[3Com-hwtacacs-test1] secondary authorization 10.163.155.13 49
```

timer quiet

Syntax

timer quiet *minutes*

undo timer quiet

View

HWTACACS view

Parameter

minutes: Ranges from 1 to 255 minutes. By default, the primary server must wait five minutes before it resumes the active state.

Description

Use the **timer quiet** command to set the waiting time before the primary server resumes the active state.

Use the **undo timer quiet** command to restore the default configuration.

This command is designed to inhibit the switch from processing user request packets for a time when the communication between the switch and the server is interrupted. After the switch waits for a time that is equal or greater than the time set by this command, it re-attempts to send packets to the server.

Related command: **display hwtacac**.

Example

Set the quiet timer for the primary server to ten minutes.

```
[SW8800] hwtacacs scheme test1
[3Com-hwtacacs-test1] timer quiet  10
```

timer realtime-accounting

Syntax

timer realtime-accounting *minutes*

undo timer realtime-accounting

View

HWTACACS view

Parameter

minutes: Real-time accounting interval, which is in the range of 3 to 60 minutes and must be a multiple of 3. By defaults, it is 12 minutes.

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 interval.

The setting of real-time accounting interval is necessary for real-time accounting. After an interval is set, the NAS transmits the accounting information of online users to the TACACS accounting server periodically.

The setting of real-time accounting interval somewhat depends on the performance of the NAS and the TACACS server: a shorter interval requires higher device 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 numbers of users and the recommended intervals.

Table 45 Number of users and recommended interval

Number of users	Real-time accounting interval (in minutes)
1 - 99	3
100 - 499	6
500 - 999	12
≥1000	≥15

Example

Set the real-time accounting interval of the HWTACACS scheme 3com to 51 minutes.

```
[3Com-hwtacacs-3com] timer realtime-accounting 51
```

timer response-timeout

Syntax

timer response-timeout *seconds*

undo timer response-timeout

View

HWTACACS view

Parameter

seconds: TACACS server response timeout time, which is in the range of 1 to 300 seconds and defaults to 5 seconds.

Description

Use the **timer response-timeout** command to set the TACACS server response timeout time.

Use the **undo timer response-timeout** command to restore the default setting.

Since HWTACACS is implemented based on TCP, so server response timeout or TCP timeout may terminate the connection to the TACACS server.

Related command: **display hwtacacs**.

Example

Set the TACACS server response timeout time to 30 seconds.

```
[SW8800] hwtacacs scheme test1
[3Com-hwtacacs-test1] timer response-timeout 30
```

user-name-format

Syntax

user-name-format { **with-domain** | **without-domain** }

View

HWTACACS view

Parameter

with-domain: Specifies that the domain name is taken along with the username that will be sent to the TACACS server.

without-domain: Specifies that no domain name is taken along with the username that will be sent to the TACACS server.

Description

Use the **user-name-format** command to set the username format acceptable to the TACACS server.

For a HWTACACS scheme, each username sent to a TACACS server contains a domain name by default.

Username is usually in the "userid@isp-name" format, with the ISP domain name following "@". The switch uses domain names to group users to different ISP domains. While some earlier TACACS servers do not accept the username with domain name. In this case, you must remove the domain name before sending a username to the server.

When you specify that no ISP domain name is contained in usernames for a HWTACACS scheme, this scheme cannot be used in two or more ISP domains at the same time; otherwise, errors may occur because the TACACS server considers users in different ISP domains but with the same name as one user.

Related command: **hwtacacs scheme**.

Example

Specify that no domain name is taken along with the username that will be sent out with the HWTACACS scheme 3com.

```
[3Com-hwtacacs-3com] user-name-format without-domain
```

22 PORTAL CONFIGURATION COMMANDS

Portal Configuration Commands

debugging portal

Syntax

debugging portal { **acm** | **all** | **arp-handshake** | **server** | **tcp-cheat** }

undo debugging portal { **acm** | **all** | **arp-handshake** | **server** | **tcp-cheat** }

View

User view

Parameter

acm: Enables the debugging for authentication connection management (ACM), that is to say, enables the debugging for state machines related with authentication, connection and management.

all: Enables all the debugging for Portal.

arp-handshake: Enables the debugging for ARP-handshake.

server: Enables the debugging for Portal server.

tcp-cheat: Enables the debugging for TCP cheat.

Description

Use the **debugging portal** command to enable the debugging for Portal.

Use the **undo debugging portal** command to disable the debugging output.

Example

Enable all the debugging for Portal.

```
<SW8800> debugging portal all
```

display portal

Syntax

1. display portal { **acm** | **server | tcp-cheat** } **statistics**

2. display portal [**auth-network** [*auth-vlan-id*] | **free-ip** | **free-user** | **server** [*server-name*] | **vlan** [vlan-id]]

3. display portal user [**ip** *ipaddress* | **interface** *interface-type interface-number* | **vlan** *vlan-id*]

View

Any View

Parameter

acm statistics: Displays the statistics about ACM, that is to say, displays the statistics about the state machines related with authentication, connection and management.

auth-network *auth-vlan-id*: Displays the authentication network section. *auth-vlan-id* is the ID of the VLAN where the access port (where the authentication users access into the switch across the network) lies in.

free-ip: Displays the configured authentication-free IP addresses.

free-user: Displays the configured authentication-free users.

server *server-name*: Displays the information about the Portal server with the specified name.

server statistics: Displays the statistics about the Portal server.

tcp-cheat statistics: Displays the statistics about TCP cheats.

ipaddress: Information about users using the specified IP address.

interface-type: Port type, whose value is Ethernet or GigabitEthernet.

interface-number: Port number, expressed in the form of slot number/card number/port number.

vlan *vlan-id*: Displays the information about all the users in a VLAN.

Description

Use the **display portal** command to display the information about Portal.

Example

Display the information about Portal.

```
[SW8800] display portal
This operation may take few minutes ,please wait
Run Method:
 Direct
Free IP:
  1)IP = 192.168.0.200        Net Mask = 255.255.255.255
Authenticate network:
     1)IP = 1.1.1.1        Net Mask = 255.255.0.0        VLAN = 3
Free User:
 No Free User
Portal Server:
  1)pt2:
    IP   = 192.168.0.200
    Key  = 3com
    Port = 2000
    URL  = "http://192.168.0.200/portal/index_default.jsp"
ARP-HandShake:
```

```
 Interval: 60s    Retry Times: 5
VLAN Portal Configuration:
 VLAN 3    : Portal Started    Portal Server: pt2
 Index  State             MAC              IP                VLAN  P
ort
```

Table 46 Description on the fields of the display portal command

Field	Description
Run Method	Portal servers run in one of the three methods: direct, ReDHCP and Layer3
Free IP	Free IP addresses. A Portal server will use one free IP address automatically
Free User	Authentication-free users
Portal Server	The basic information about the configuration of a Portal server, including its IP address, key, port and URL that HTTP redirects
ARP-HandShake	The information about the ARP handshake, including the interval of handshake and retry times.
VLAN Portal Configuration	Information about the Portal-enabled VLANs, including whether Portal is enabled, the name of the enabled Portal server, and the information about the connecting users (including the users' state, MAC address, IP address, connecting port and so on).

Display the statistics about Portal ACM.

```
[SW8800] display portal acm statistics
ACM Statistics            Running State Statistics
 WAIT_MAC_ACK              0
 DISCOVERED                0
 WAIT_AUTH_ACK             0
 WAIT_LOGIN_ACK            0
 WAIT_ACL_ACK              0
 WAIT_NEW_IP               0
 ONLINE                    0
 WAIT_LOGOUT_ACK           0
 Message Statistics :
 MSG NAME                  RCV MSG NUM
 PT_MSG_AUTH_ACK           0
 PT_MSG_LOGIN_ACK          0
 PT_MSG_LOGOUT_ACK         0
 PT_MSG_LEAVING_ACK        0
 PT_MSG_CUT_REQ            0
 PT_MSG_MAC_ACK            0
 PT_MSG_ACL_ACK            0
 PT_MSG_ARPPKT             77
 PT_MSG_TMR_AUT            0
 PT_MSG_TMR_LGN            0
 PT_MSG_TMR_LGT            0
 PT_MSG_TMR_LEV            0
 PT_MSG_TMR_HDS            85249
 PT_MSG_ARP_FAIL           0
 PT_MSG_TMR_ACL            0
 PT_MSG_TMR_MAC            0
 PT_MSG_TMR_NIP            0
 ERROR Statistics:
 MEM Error: 0           RCV MSG ERR: 0           SND MSG ERR: 0
```

Table 47 Description on the fields of the display portal acm statistics command

Field	Description
ACM Statistics	Statistics about state machines
WAIT_MAC_ACK	Time of waiting for MAC address acknowledgements. This value is 0 for the Layer 3 method
DISCOVERED	Number of users discovered
WAIT_AUTH_ACK	Time of waiting for authentication acknowledgements
WAIT_LOGIN_ACK	Time of waiting for login acknowledgements
WAIT_ACL_ACK	Time of waiting for ACL acknowledgements. This value is 0 for ReDHCP method
WAIT_NEW_IP	Time of waiting for NEW IP. This value is 0 for both Direct and Layer 3 methods.
ONLINE	Number of users online
WAIT_LOGOUT_ACK	Time of waiting for logout acknowledgements
PT_MSG_AUTH_ACK	Authentication acknowledgement message
PT_MSG_LOGIN_ACK	Login acknowledgement message
PT_MSG_LOGOUT_ACK	Logout acknowledgement message
PT_MSG_LEAVING_ACK	Leaving acknowledgement message
PT_MSG_CUT_REQ	Cut request message to force the users to log out
PT_MSG_MAC_ACK	MAC acknowledgement message. This value is 0 for Layer 3 method
PT_MSG_ACL_ACK	ACL acknowledgement message. This value is 0 for ReDHCP method
PT_MSG_ARPPKT	ARP packet message. This value is 0 for Layer 3 method
PT_MSG_TMR_AUT	Statistics about authentication timers
PT_MSG_TMR_LGN	Statistics about login timers
PT_MSG_TMR_LGT	Statistics about logout timers
PT_MSG_TMR_LEV	Statistics about leaving timers
PT_MSG_TMR_HDS	Statistics about handshake timers. This value is 0 for Layer 3 method
PT_MSG_ARP_FAIL	Statistics about ARP failures. This value is 0 for Layer 3 method
PT_MSG_TMR_ACL	Statistics about ACL timers. This value is 0 for ReDHCP method
PT_MSG_TMR_MAC	Statistics about MAC timers. This value is 0 for Layer 3 method
PT_MSG_TMR_NIP	Statistics about New IP timers. This value is 0 for Direct and Layer 3 methods
MEM Error/RCV MSG ERR/SND MSG ERR	Statistics about error messages, including memory errors, received message errors and sent message errors

portal

Example

portal *server-name*

undo portal

View

VLAN interface view.

Parameter

server-name: Name of a Portal server. It is a string in the range of 1 to 32 characters.

Description

Use the **portal** command to enable the Portal authentication function on a VLAN interface.

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

If the Portal runs in the Layer 3 Portal authentication method, you must configure an authentication section before enabling the Portal authentication function on a VLAN interface.

When you enable the Portal authentication function on a VLAN interface, you must first make sure that VLAN IDs are in the range of 2 to 4094, and the make sure that a valid IP address is configured for this VALN interface and that the specified Portal server exists.

Example

Enable the Portal authentication function on VLAN-interface 10. Specify 3Com as the Portal server.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800]interface Vlan-interface 10
[3Com-Vlan-interface10] portal 3Com
```

portal arp-handshake

Syntax

portal arp-handshake { **interval** *interval* | **retry-times** *retry-times* }*

undo portal arp-handshake { **interval** | **retry-times** }

View

System view

Parameter

interval: Interval of ARP handshakes in seconds, in the range of 10 to 180. Its step is 10. It is 60 seconds by default.

retry-times: Maximum retry times of ARP packets, that is to say, the maximum times of permitted handshake failures. This value is in the range of three times to 10 times. It is five times by default.

Description

Use the **portal arp-handshake** command to configure the interval of handshakes between the portal server and the host and the maximum retry times.

Use the **undo portal arp-handshake** command to restore the default value.

When authentications are performed in the Direct method or ReDHCP method, the switch handshakes with the host through ARP packets after the host (user PC) has passed the Portal authentication. The switch sends ARP packets at the interval.

If the user PC still does not respond after the sending times exceed the retry times, the switch will regard the handshakes as abnormal, cut the connection with this user actively and notify the Portal server about this case.

This command is ineffective for the Layer 3 Portal authentication method.

Example

Set the interval of handshakes between the switch and the host to 120 seconds, and set the maximum retry times to six times.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] portal arp-handshake interval 120 retry-times 6
```

portal auth-network

Syntax

portal auth-network *network-address net-mask* **vlan** *vlan-id*

undo portal auth-network { *network-address net-mask* | **vlan** *vlan-id* | **all** }

View

System view

Parameter

network-address net-mask: Address and subnet mask of the authentication network section.

vlan-id: ID of the VLAN where the access port (where the authentication users access into the switch across the network) lies in.

all: Disables all the configured authentication network sections.

Description

Use the **portal auth-network** command to configure the authentication network section of a Portal client.

Use the **undo portal auth-network** command to disable the authentication network section for a Portal client.

No authentications network section is configured by default.

This command is effective only for the Layer 3 Portal authentication method.

Example

Configure the authentication network section for a Portal client: 192.168.0.200/16.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] portal auth-network 192.168.0.200 255.255.0.0 vlan 1
```

portal delete-user

Syntax

portal delete-user *ip-address*

View

System view

Parameter

ip-address: Deletes the Portal users using the specified IP address.

Description

Use the **portal delete-user** command to delete the Portal users using the specified IP address.

Example

Delete users using the IP address 10.153.94.8.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] portal delete-user 10.153.94.8
```

portal free-ip

Syntax

portal free-ip *ip-address* [*mask* | *mask-length*]

undo portal free-ip *ip-address* [*mask* | *mask-length*]

View

System view

Parameter

ip-address: Free IP address of the host.

mask: Mask.

mask-length: Length of a mask.

Description

Use the **portal free-ip** command to set the free IP addressees for a Portal client.

Use the **undo portal free-ip** command to delete the specified free IP address.

No free IP address is configured by default. .

Free IP addresses can be the IP addresses of DNS servers or the IP addresses that ISP provides to access free websites. All users can access these free IP addresses unrestrictedly.

Up to 8 free IP addresses can be configured in one system. .A Portal server will use one free IP address automatically.

Example

Set the IP address 10.1.1.0 as a free IP address

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] portal free-ip 10.1.1.0
```

portal free-user

Syntax

In system view:

portal free-user mac *mac-address* **ip** *ip-address* **vlan** *vlan-id* **interface** *interface-type interface-number*

undo portal free-user { **mac** *mac-address* | **all** }

In Ethernet port view:

portal free-user mac *mac-address* **ip** *ip-address* **vlan** *vlan-id*

undo portal free-user { **mac** *mac-address* | **all** }

View

System view, Ethernet port view

Parameter

mac *mac-address*: Sets the Mac addresses of authentication-free users.

ip *ip-address*: Sets the IP addresses of authentication-free users. These addresses cannot be full-zero addresses, loopback addresses, multicast addresses or broadcast addresses.

vlan *vlan-id*: ID of the VLAN that the authentication-free users belongs to, in the range of 1 to 4094.

interface: Port of the switch that the authentication-free users lie in. This port must belong to the VLAN that this command specifies.

interface-type: Port type, whose value is Ethernet or GigabitEthernet.

interface-number: Port number, expressed in the form of slot number/card number/port number.

all: Deletes all authentication-free users.

Description

Use the **portal free-user** command to configure the Portal authentication-free users.

Use the **undo portal free-user** command to delete the specified or all authentication-free users.

In the network practice, you can configure network devices attached to the switch or several servers as authentication-free users, so that they can access all networks without authentication.

The information about authentication-free users includes IP addresses, MAC addresses, and the connected switch ports and VLANs. Only the users who match all the information can access networks without authentication.

CAUTION:

- The ReDHCP authentication method requires that the IP address of an authentication-free user and the master IP address of the interface belong to the same network section. The Direct authentication method requires that the IP address of an authentication-free user and that of the VLAN interface belong to the same network section.
- This configuration takes effect after Portal is enabled in the VLAN that the authentication-free users belongs to.
- The Layer 3 Portal authentication method does not support the authentication-free user configuration.

Example

Configure authentication-free users for the Portal authentication.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] portal free-user mac 00e0-fc01-0101 ip 10.110.1.1 vlan 10 i
nterface ethernet 2/1/1
```

portal method

Syntax

portal method { **direct** | **layer3** | **redhcp** }

undo portal method

View

System view

Parameter

direct: Adopts the direct authentication method in Portal authentication.

layer3: Adopts the layer 3 Portal authentication method, namely, accoss-layer-3 Portal authentication method in authentication.

redhcp: Adopts the ReDHCP authentication method in Portal authentication.

Description

Use the **portal method** command to set the running method of Portal authentication.

Use the **undo portal method** command to restore the default running method of Portal authentication.

The direct authentication method is adopted in Portal authentication by default.

Example

Set to adopt the ReDHCP method in Portal authentication.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] portal method redhcp
```

portal server

Syntax

portal server *server-name* { **ip** *ip-address* | **key** *key-string* | **port** *port* | **url** *url-string* } *

undo portal server *server-name* [**key** | **port** | **url**]

View

System view

Parameter

server-name: Name of a Portal server. It is a string in the range of 1 to 32 characters.

ip-address: IP address of a Portal server. This address cannot be full-zero addresses, loopback addresses, multicast addresses or broadcast addresses.

key-string: Shared keys that the Portal server needs when it communicates with the switch. It is a string in the range of 1 to 16 characters. It is "3com" by default.

port: Port that a switch uses to send packets to a Portal server. It is in the range of 1 to 65534. It is 50100 by default.

url-string: URL that HTTP redirects to, which is the string form of the *ip-address* by default. For example, if the *ip-address* is 10.1100.100.100, the default URL is http://10.11.100.100. The string need not be bracketed when entered.

Description

Use the **portal server** command to create a Portal server or modify the configuration of a Portal server.

Use the **undo portal server** command to delete the specified server, or restore the default parameter configuration of the specified server.

CAUTION:

- When configuring a Portal server, you must also configure the IP address for that server.
- If the Portal server has been configured on a VLAN virtual interface, you must disable this Portal server on the virtual VLAN interface before modifying its parameters. Enable the Portal server again after parameters are modified.
- A Portal server will use a free IP address automatically. If the number of free IP addresses has reached the maximum when a Portal server is configured, this configuration will fail.

Example

Set the IP address of the Portal server named 3Com to 10.10.100.100, communication key to lanswitch, port to 50101, and the URL that HTTP redirects to http://www.3com.com.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] portal server 3Com ip 10.10.100.100 key lanswitch port 5010
1 url http://www.3com.com
```

portal upload-interface

Example

portal upload-interface

undo portal upload-interface

View

Ethernet port view

Parameter

None

Description

Use the **portal upload-interface** command to enable the Portal rate limit function on the upload interface.

Use the **undo portal upload-interface** command to disable the Portal rate limit function.

By default, the Portal rate limit function is disabled.

The Portal rate limit function is used together with the bandwidth limit service that the CAMS server provides. The bandwidth limit service is that you can specify the bandwidth for each user when you are configuring the service for each user on the CAMS server.

The principle of Portal rate limit is as follows: when the switch receives the bandwidth limit rules for Portal users from the CAMS server, the switch will limit the traffic on the upload interface where the **portal upload-interface** command is executed, that is to say, the switch will perform bandwidth control for the upload rates of Portal users. An upload interface is the interface to connect the switch with the upstream network devices.

CAUTION: *Only one upload interface for rate limit can be configured in one system.*

Example

Configure Ethernet2/1/43 as the upload interface for Portal rate limit.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800]interface Ethernet 2/1/48
[3Com-Ethernet2/1/43]portal upload-interface
```

reset portal

Syntax

reset portal { **acm** | **server** | **tcp-cheat** } **statistics**

View

User view

Parameter

acm: Clears the statistics about ACM, that is to say, clears the statistics about the state machines related with authentication, connection and management.

server: Clears the statistics about the Portal server.

tcp-cheat: Clears the statistics about TCP cheats.

Description

Use the **reset portal** command to clear the related statistics about Portal.

Example

Clear the statistics about ACM of the Portal client.

```
<SW8800> reset portal acm statistics
```

23 STATIC ROUTE CONFIGURATION COMMANDS

When a switch runs a routing protocol, it can perform the router functions. A router that is referred to in the following or its icon represents a generalized router or an Switch 8800 Family series routing switch running routing protocols. To improve readability, this will not be described in the other parts of the manual.

For the configuration of VPN instance, refer to the MPLS module in *3Com Switch 8800 Family Series Routing Switches Operation Manual*.

Display Commands of the Routing Table

display ip routing-table

Syntax

display ip routing-table

View

Any view

Parameter

None

Description

Use **display ip routing-table** command to view the routing table summary.

This command displays routing table information in summary form. Each line represents one route. The contents include destination address/mask length, protocol, preference, metric, next hop and output interface.

Only current used route, namely, best route, is displayed using **display ip routing-table** command.

Example

View the summary of the routing table.

```
<SW8800> display ip routing-table
Routing Table: public net
Destination/Mask   Protocol   Pre Cost        Nexthop    Interface
1.1.1.0/24         DIRECT       0   0       1.1.1.1  Vlan-interface1
1.1.1.1/32         DIRECT       0   0       127.0.0.1    InLoopBack0
2.2.2.0/24         DIRECT       0   0       2.2.2.1  Vlan-interface2
2.2.2.1/32         DIRECT       0   0       127.0.0.1    InLoopBack0
3.3.3.0/24         DIRECT       0   0       3.3.3.1  Vlan-interface3
3.3.3.1/32         DIRECT       0   0       127.0.0.1    InLoopBack0
4.4.4.0/24         DIRECT       0   0       4.4.4.1  Vlan-interface4
```

```
4.4.4.1/32          DIRECT       0    0        127.0.0.1     InLoopBack0
127.0.0.0/8         DIRECT       0    0        127.0.0.1     InLoopBack0
127.0.0.1/32        DIRECT       0    0        127.0.0.1     InLoopBack0
```

Table 48 Description of the fields of the display ip routing-table command

Field	Description
Destination/Mask	Destination address/Mask length
Protocol	Routing protocol
Pre	Routing preference
Cost	Cost
Nexthop	Next hop address
Interface	Output interface, through which the data packet destined for the destination network segment is sent

display ip routing-table acl

Syntax

display ip routing-table acl { *acl-number* | *acl-name* } [**verbose**]

View

Any view

Parameter

acl-number: The number of basic ACL, ranging from 2000 to 2999.

acl-name: The basic ACL name introduced via names.

verbose: With the parameter, this command displays the verbose information of both the Active and Inactive routes that passed filtering rules. Without the parameter, this command only displays the summary of the Active routes that passed filtering rules.

Description

Use the **display ip routing-table acl** command to view the route filtered through specified basic access control list (ACL).

This command is used in track display of route policy to display the route that passed the filtering rule according the input basic ACL number or name.

The command is only applicable to display the route that passed basic ACL filtering rules.

Example

Display the summary of Active routes that are filtered through basic acl 2000.

```
[SW8800] acl number 2000
[3Com-acl-basic-2000] rule permit source 10.1.1.1 0.0.0.255
[3Com-acl-basic-2000] rule deny source any
[3Com-acl-basic-2000] display ip routing-table acl 2000
Routes matched by access-list 2000:
Summary count: 4
Destination/Mask   Protocol Pre  Cost        Nexthop       Interface
10.1.1.0/24 DIRECT  0   0   10.1.1.2        Vlan-interface1
10.1.1.2/32 DIRECT  0   0   127.0.0.1      InLoopBack0
```

For detailed description of the output information, see Table 48.

Display the verbose information of the Active and Inactive routes that are filtered through basic acl 2000.

```
<SW8800> display ip routing-table acl 2000 verbose
Routes matched by access-list 2000:
  + = Active Route, - = Last Active, # = Both   * = Next hop in use

  Summary count: 2

**Destination: 10.1.1.0         Mask: 255.255.255.0
        Protocol: #DIRECT       Preference: 0
        *NextHop: 10.1.1.2         Interface: 10.1.1.2(Vlan-interface1)
        Vlinkindex: 0
        State: <Int ActiveU Retain Unicast>
        Age: 7:24       Cost: 0/0       Tag: 0

**Destination: 10.1.1.2         Mask: 255.255.255.255
        Protocol: #DIRECT       Preference: 0
        *NextHop: 127.0.0.1        Interface: 127.0.0.1(InLoopBack0)
        Vlinkindex: 0
        State: <NoAdvise Int ActiveU Retain Gateway Unicast>
        Age: 7:24       Cost: 0/0       Tag: 0
```

Table 49 Description of the fields of the display ip routing-table acl verbose command

Field	Description
Destination	Destination address
Mask	Mask
Protocol	Routing protocol
Preference	Routing preference
Nexthop	Next hop address
Interface	Output interface, through which the data packet destined for the destination network segment is sent
Vlinkindex	Virtual link index

Table 49 Description of the fields of the display ip routing-table acl verbose command

Field	Description	
State	Route state description:	
	ActiveU	Valid unicast route. U stands for unicast.
	Blackhole	Blackhole route is similar to Reject route, but it will not send the ICMP unreachable message to the source end
	Delete	The route is deleted
	Gateway	Indicates that the route is not directly reachable
	Hidden	The route exists, but it is unavailable temporarily for some reasons (e.g., configured policy or interface is Down). Moreover, you do not wish to delete it. Therefore, you need to hide it, so as to restore it again later
	Holddown	Holddown is one kind of route redistribution policy adopted by some distance-vector (D-V) routing protocols (e.g., RIP), through which these routing protocols can avoid the flooding of error routes and deliver the routing unreachable message accurately. For example, the RIP imports a certain route every a period of time regardless of whether the actually found routes destined for the same destination change. For more details, refer to the specific routing protocols.
	Int	The route is discovered by interior gateway protocol (IGP).
	NoAdvise	The routing protocol does not import NoAdvise route when it imports routes based on the policy.
	NotInstall	The routing protocol generally selects the route with the highest precedence from its routing table, then places it in its core routing table and imports it. Although the NotInstall route cannot be placed in the core routing table, it is possibly that it is selected and imported.
	Reject	Unlike the normal routes, the Reject route will discard the packets that select it as their route, and the router will send ICMP unreachable message to the source end. Reject route is usually used for the network test
	Retain	When the routes from the core routing table are deleted, the routes with the Retain flag will not be deleted. Using this function you can set the Retain flag for some static routes, so that they can exist in the core routing table.
	Static	The route with Static flag will not be cleared from the routing table after you save it and reboot the router. Generally, the static route configured manually in the router belongs to a Static route.

Table 49 Description of the fields of the display ip routing-table acl verbose command

Field	Description
Age	Lifetime of a route entry, in *hh* : *mm* : *ss*, where hh is hours, mm is minutes, and ss is seconds. The displayed time should be read from right to left. For example, 7:24 indicates that the lifetime of a route is seven hours and 24 minutes.
Cost	Value of the cost
Tag	Route tag

display ip routing-table ip-address

Syntax

display ip routing-table *ip-address* [*mask*] [**longer-match**] [**verbose**]

View

Any view

Parameter

ip-address: Destination IP address, in dotted decimal format.

mask: IP address mask, length in dotted decimal notation or integer. It ranges from 0 to 32 when it is expressed with integer.

longer-match: Address route matching the destination address in natural mask range.

verbose: With the **verbose** argument, this command displays the verbose information of both the Active and Inactive routes. Without the parameter, this command only displays the summary of Active routes.

Description

Use the **display ip routing-table** *ip-address* command to view the routing information of the specified destination address.

With different parameters, the output of command is different. The following is the output description for different forms of this command:

- **display ip routing-table** *ip-address*

If destination address, *ip-address,* has corresponding route in natural mask range, this command will display all subnet routes or only the route best matching the destination address, *ip-address,* is displayed. And only the Active matching route is displayed.

- **display ip routing-table** *ip-address mask*,

This command only displays the route fully matching with specified destination address and mask.

- **display ip routing-table** *ip-address* **longer-match**

This command displays all destination address route matching with destination address in natural mask range.

Example

There is a corresponding route in natural mask range. Display the summary.

```
<SW8800>display ip routing-table 169.0.0.0
Destination/Mask    Protocol Pre  Cost        Nexthop         Interface
169.0.0.0/16        STATIC   60   0           192.168.1.2     Vlan-interface10
169.0.0.0/8         STATIC   60   0           192.168.1.2     Vlan-interface10
```

For detailed description of the output information, see Table 48.

There is no corresponding route (only the longest matching route is displayed) in natural mask range and summary is displayed.

```
<SW8800>display ip routing-table 192.168.1.2
Destination/Mask    Protocol Pre  Cost        Nexthop         Interface
192.168.1.0/24      DIRECT   0    0           192.168.1.1     Vlan-interface10
```

There are corresponding routes in the natural mask range. Display the detailed information.

```
<SW8800> display ip routing-table 169.0.0.0 verbose
Routing tables:
  Generate Default: no
  + = Active Route, - = Last Active, # = Both    * = Next hop in use

  Summary count: 3

**Destination: 169.0.0.0         Mask: 255.255.0.0
         Protocol: #STATIC       Preference: 60
         *NextHop: 192.168.1.2      Interface: 192.168.1.1(Vlan-interface10)
         Vlinkindex: 0
         State: <Int ActiveU Gateway Static Unicast>
         Age: 10:20      Cost: 0/0       Tag: 0

**Destination: 169.0.0.0         Mask: 255.0.0.0
         Protocol: #STATIC       Preference: 60
         *NextHop: 192.168.1.2      Interface: 192.168.1.1(Vlan-interface10)
         Vlinkindex: 0
         State: <Int ActiveU Gateway Static Unicast>
         Age: 4:39       Cost: 0/0       Tag: 0
```

There are no corresponding routes in the natural mask range (only displaying the longest matched route). Display the detailed information.

```
<SW8800> display ip routing-table 169.168.1.2 verbose
Routing tables:
  Generate Default: no
  + = Active Route, - = Last Active, # = Both    * = Next hop in use

  Summary count: 1

**Destination: 192.168.1.0       Mask: 255.255.255.0
         Protocol: #DIRECT       Preference: 0
         *NextHop: 192.168.1.1      Interface: 192.168.1.1(Vlan-interface10)
         Vlinkindex: 0
         State: <Int ActiveU Retain Unicast>
         Age: 12:51      Cost: 0/0       Tag: 0
```

For detailed description of the output information, see Table 49.

display ip routing-table ip-address1 ip-address2

Syntax

display ip routing-table *ip-address1 mask1 ip-address2 mask2* [**verbose**]

View

Any view

Parameter

ip-address1, ip-address2: Destination IP address in dotted decimal notation. *ip-address1, mask1, mask2* and *ip-address2* determine one address range together. Anding *ip-address1* with *mask1* specifies the start of the range while anding *ip-address2* with *mask2* specifies the end. This command is used to display the routes in this address range.

mask1, mask2: IP address mask, length in dotted decimal notation or integer form. It ranges from 0 to 32 when it is presented in integer.

verbose: With the **verbose** keyword, this command displays the verbose information of both the active and inactive routes. Without the parameter, this command only displays the summary of Active routes.

Description

Use the **display ip routing-table ip-address1 ip-address2** command to view the route information in the specified address range.

Example

Display the routing information of destination addresses ranging from 1.1.1.0 to 2.2.2.0.

```
<SW8800>display ip routing-table 1.1.1.0 24 2.2.2.0 24
Routing tables:
  Summary count: 3
Destination/Mask   Protocol   Pre Cost        Nexthop      Interface
1.1.1.0/24         DIRECT   0   0            1.1.1.1         Vlan-interface1
1.1.1.1/32         DIRECT   0   0            127.0.0.1    InLoopBack0
2.2.2.0/24         DIRECT   0   0            2.2.2.1         Vlan-interface2
```

For detailed description of the output information, see Table 48.

display ip routing-table ip-prefix

Syntax

display ip routing-table ip-prefix *ip-prefix-name* [**verbose**]

View

Any view

Parameter

ip-prefix-name: ip prefix list name.

verbose: With the parameter, this command displays the verbose information of both the active and inactive routes that passed filtering rules. Without the parameter, this command displays the summary of the active routes that passed filtering rules.

Description

Use the **display ip routing-table ip-prefix** command to view the route information that passed the filtering rule according the input ip prefix list name.

This command is mainly used to trace the route-policy and display the corresponding route information.

If there is no specified address prefix list, this command will display the verbose information of all Active and Inactive routes with the **verbose** keyword and it will display the summary of all Active routes without the **verbose** keyword.

Example

Configure the ip prefix list abc2, allowing the routes with the prefix as 10.1.1.0 and a mask length in the range 24 to 32 to pass.

```
[SW8800] ip ip-prefix abc2 permit 10.1.1.0 24 less-equal 32
<SW8800> dis ip routing-table protocol static
STATIC Routing tables:
  Summary count: 3
STATIC Routing table status:<active>:
  Summary count: 3
Destination/Mask   Protocol Pre  Cost        Nexthop         Interface
10.1.0.0/16        STATIC   60   0           48.48.48.2      Vlan-interface48
10.1.1.0/24        STATIC   60   0           48.48.48.2      Vlan-interface48
10.1.1.2/32        STATIC   60   0           48.48.48.2      Vlan-interface48
STATIC Routing table status:<inactive>:
  Summary count: 0
<SW8800> display ip routing-table ip-prefix abc2
Routes matched by ip-prefix abc2:
  Summary count: 2
Destination/Mask   Protocol Pre  Cost        Nexthop         Interface
10.1.1.0/24        STATIC   60   0           48.48.48.2      Vlan-interface48
10.1.1.2/32        STATIC   60   0           48.48.48.2      Vlan-interface48
```

For detailed description of the output information, see Table 48.

Display the details of the active and inactive routes filtered by the prefix list abc2.

```
<SW8800> display ip routing-table ip-prefix abc2 verbose
Routes matched by ip-prefix abc2:
  Generate Default: no
  + = Active Route, - = Last Active, # = Both    * = Next hop in use

  Summary count: 2

**Destination: 10.1.1.0          Mask: 255.255.255.0
         Protocol: #STATIC       Preference: 60
         *NextHop: 48.48.48.2       Interface: 48.48.48.1(Vlan-interface48)
         Vlinkindex: 0
         State: <Int ActiveU Gateway Static Unicast>
         Age: 12:42      Cost: 0/0       Tag: 0

**Destination: 10.1.1.2          Mask: 255.255.255.255
         Protocol: #STATIC       Preference: 60
         *NextHop: 48.48.48.2       Interface: 48.48.48.1(Vlan-interface48)
         Vlinkindex: 0
         State: <Int ActiveU Gateway Static Unicast>
         Age: 12:48      Cost: 0/0       Tag: 0
```

For explanations of the above information, see Table 49.

display ip routing-table protocol

Syntax

display ip routing-table protocol *protocol* [**inactive** | **verbose**] [**vpn-instance** *vpn-instance-name*]

View

Any view

Parameter

inactive: With the parameter, this command displays the inactive route information. Without the parameter, this command displays the active and inactive route information.

verbose: With the **verbose** keyword, this command displays the verbose route information. Without the parameter, this command displays the route summary.

protocol: The parameter has multiple selectable values:

- **direct**: Displays direct connection route information
- **static**: Displays the static route information.
- **bgp**: Displays BGP route information.
- **isis**: Displays IS-IS route information.
- **ospf**: Displays OSPF route information.
- **ospf-ase**: Displays OSPF ASE route information.
- **ospf-nssa**: Displays OSPF NSSA route information.
- **rip**: Displays RIP route information.

vpn-instance-name: Indicates a VPN instance name.

Description

Use the **display ip routing-table protocol** command to view the route information of specified protocol.

Example

Display all direct connection routes summary.

```
<SW8800> display ip routing-table protocol direct
DIRECT Routing tables:
Summary count: 4
DIRECT Routing tables status:<active>:
Summary count: 3
Destination/Mask        Protocol    Pre Cost    Nexthop     Interface
20.1.1.1/32         DIRECT          0   0       127.0.0.1   InLoopBack0
127.0.0.0/8         DIRECT          0   0       127.0.0.1   InLoopBack0
127.0.0.1/32            DIRECT          0   0       127.0.0.1   InLoopBack0
DIRECT Routing tables status:<inactive>:
Summary count: 1
Destination/Mask        Protocol   Pre  Cost    Nexthop     Interface
210.0.0.1/32            DIRECT      0       0       127.0.0.1   InLoopBack0
```

View the static routing table.

```
<SW8800> display ip routing-table protocol static
STATIC Routing tables:
  Summary count: 1
STATIC Routing tables status:<active>:
  Summary count: 0
STATIC Routing tables status:<inactive>:
  Summary count: 1
Destination/Mask   Protocol   Pre Cost       Nexthop      Interface
1.2.3.0/24          STATIC     60  0          1.2.4.5      Vlan-interface10
```

```
STATIC Routing tables status:<inactive>:
  Summary count: 1
```

For detailed description of the output information, see Table 48.

display ip routing-table radix

Syntax

display ip routing-table radix

View

Any view

Parameter

None

Description

Use the **display ip routing-table radix** command to view route information in tree format.

Example

Display route information in tree format.

```
<SW8800> display ip routing-table radix
Radix tree for INET (2) inodes 7 routes 5:
                +-32+--{210.0.0.1
            +--0+
              | | +--8+--{127.0.0.0
              | | | +-32+--{127.0.0.1
              | +--1+
              |  +--8+--{20.0.0.0
              |  +-32+--{20.1.1.1
```

Table 50 Description of the fields of the display ip routing-table radix command

Field	Description
INET	Address suite
inodes	Number of nodes
routes	Number of routes

display ip routing-table statistics

Syntax

display ip routing-table statistics

View

Any view

Parameter

None

Description

Use the **display ip routing-table statistics** command to view the integrated routing information.

The integrated routing information includes total route amount, the route amount added or deleted by protocol, amount of the routes that are labeled "Deleted" but not deleted, and the Active route amount.

Example

Display the integrated route information.

```
<SW8800> display ip routing-table statistics
Routing tables:
Proto       route        active       added        deleted
DIRECT      24           4            25           1
STATIC      4            1            4            0
BGP         0            0            0            0
RIP         0            0            0            0
IS-IS       0            0            0            0
OSPF        0            0            0            0
O_ASE       0            0            0            0
O_NSSA      0            0            0            0
AGGRE       0            0            0            0
Total       28           5            29           1
```

Table 51 Description of the fields of the display ip routing-table statistics command

Field	Description
Proto	Routing protocol. O_ASE indicates OSPF_ASE routes, O_NSSA indicates OSPF_NSSA routes and AGGRE indicates aggregated routes.
Route	Number of routes
Active	Number of active routes
Added	Number of added routes after the router is rebooted or the routing table is cleared last time
Deleted	Number of deleted routes (such routes will be freed in a period of time)
Total	Total number of the different kinds of routes

display ip routing-table vpn-instance

Syntax

display ip routing-table vpn-instance *vpn-instance-name*

View

Any view

Parameter

vpn-instance: Specifies VPN instance parameter.

vpn-instance-name: VPN instance name.

Description

Use the **display ip routing-table vpn-instance** command to view the routing information about the VPN instance.

Example

View the routing information about the VPN instance.

```
<SW8800> dis ip routing-table vpn-instance vpn49-1
  vpn49-1   Route Information
 Routing Table:  vpn49-1   Route-Distinguisher:   49:1
Destination/Mask   Protocol Pre  Cost        Nexthop         Interface
```

```
77.77.77.77/32      STATIC   60   0           195.195.1.10    Vlan-interface1016
195.168.130.0/24    DIRECT   0    0           195.168.130.1   Vlan-interface1013
195.168.130.1/32    DIRECT   0    0           127.0.0.1       InLoopBack0
195.195.0.0/16      DIRECT   0    0           195.195.1.1     Vlan-interface1016
195.195.1.1/32      DIRECT   0    0           127.0.0.1       InLoopBack0
```

display ip routing-table verbose

Syntax

display ip routing-table verbose

View

Any view

Parameter

None

Description

Use the **display ip routing-table verbose** command to view the verbose routing table information.

With the **verbose** keyword, this command displays the verbose routing table information. The descriptor describing the route state will be displayed first, then the statistics of the entire routing table will be output and finally the verbose description of each route will be output.

All current routes, including inactive route and invalid route, can be displayed using the **display ip routing-table verbose** command.

Example

Display the verbose routing table information.

```
<SW8800> display ip routing-table verbose
Routing Tables:
  Generate Default: no
  + = Active Route, - = Last Active, # = Both    * = Next hop in use
  Destinations: 3       Routes: 3
  Holddown: 0    Delete: 62      Hidden: 0
**Destination: 1.1.1.0           Mask: 255.255.255.0
         Protocol: #DIRECT       Preference: 0
         *NextHop: 1.1.1.1          Interface: 1.1.1.1(Vlan-interface1)
         State: <Int ActiveU Retain Unicast>
         Age: 20:17:41   Cost: 0/0
**Destination: 1.1.1.1           Mask: 255.255.255.255
         Protocol: #DIRECT       Preference: 0
         *NextHop: 127.0.0.1        Interface: 127.0.0.1(InLoopBack0)
         State: <NoAdvise Int ActiveU Retain Gateway Unicast>
         Age: 20:17:42   Cost: 0/0
**Destination: 2.2.2.0           Mask: 255.255.255.0
         Protocol: #DIRECT       Preference: 0
         *NextHop: 2.2.2.1          Interface: 2.2.2.1(Vlan-interface2)
         State: <Int ActiveU Retain Unicast>
         Age: 20:08:05   Cost: 0/0
```

First, display statistics of the whole routing table and then output detailed information of every route entry in turn. The meaning of route status is shown in Table 49, and the statistics of routing table is shown in the following table.

Table 52 Description of the fields of the display ip routing-table verbose command

Field	Description
Holddown	Number of held-down routes
Delete	Number of deleted routes
Hidden	Number of hidden routes

Static Route Configuration Commands

delete static-routes all

Syntax

delete static-routes all

View

System view

Parameter

None

Description

Use the **delete static-routes all** command to delete all the static routes.

The system will request your confirmation before it deletes all the configured static routes.

Related commands: **ip route-static**, **display ip routing-table**.

Example

Delete all the static routes in the router.

```
[SW8800] delete static-routes all
Are you sure to delete all the unicast static routes?[Y/N]
```

delete vpn-instance

Syntax

delete vpn-instance *vpn-instance-name* **static-routes all**

View

System view

Parameter

vpn-instance: Specifies VPN instance parameter.

vpn-instance-name: VPN instance name.

static-routes: VPN static route.

all: All static routes.

Description

Use the **delete vpn-instance** command to remove all the static routes of the VPN. When you use this command to remove the static routes, the system will prompt your acknowledgement. The system removes all configured static routes after the acknowledgement.

Related commands: **ip route-static, display ip routing-table vpn-instance**.

Example

Remove all static routes of the VPN.

```
[SW8800] delete vpn-instance vp1 static-routes all
Are you sure to delete all the VPN static routes?[Y/N]
```

ip route-static

Syntax

ip route-static [**vpn-instance** *vpn-instance-name*-list] *ip-address* { *mask* | *mask-length* } { *interface-type interface-number* | [**vpn-instance** *vpn-instance-name*] *gateway-address* } [**preference** *preference-value*] [**reject** | **blackhole**]

undo ip route-static [**vpn-instance** *vpn-instance-name-list*] *ip-address* { *mask* | *mask-length* } [*interface-type interface-number* | [**vpn-instance** *vpn-instance-name*] *gateway-address*] [**preference** *preference-value*]

View

System view

Parameter

vpn-instance: Specifies VPN instance parameter.

vpn-instance-name-list: VPN instance name list. *vpn-instance-name-list*= *vpn-instance-name & <1-6*>. &<1-6> in the command represents that the preceding parameter can be input repeatedly up to 6 times.

ip-address: Destination IP address in dotted decimal notation.

mask: Mask.

mask-length: Mask length. Since "1" s in the 32-bit mask are required to be consecutive, the mask in dotted decimal format can be replaced by *mask-length*, which is the number of the consecutive "1" s in the mask.

vpn-instance-name: Name of a VPN instance.

interface-type interface-number: Specifies the outgoing interface for the next hop. The null interface is a kind of virtual interface, where data packets are discarded directly to decrease the system load. *gateway-address*: Specifies the next hop IP address of the route, in dotted decimal format.

preference-value: Preference level of the route in the range from 1 to 255.

reject: Indicates an unreachable route. When a static route to a destination has the "**reject**" attribute, all the IP packets to this destination will be discarded, and the source host will be informed that the destination is unreachable.

blackhole: Indicates a blackhole route. If a static route to a destination has the "**blackhole**" attribute, the outgoing interface of this route is the Null 0 interface regardless of the next hop address, and any IP packets addressed to this destination are dropped without notifying the source host.

Description

Use the **ip route-static** command to configure a static route.

Use the **undo ip route-static** command to delete the configured static route.

By default, the system can obtain the sub-net route directly connected with the router. If it is not specified as **reject** or **blackhole**, the route will be reachable by default.

Precautions for static route configuration:

- When the destination IP address and the mask are both 0.0.0.0, it is the configured default route. If it is failed to detect the routing table, a packet will be forwarded along the default route.
- For different configuration of preference level, flexible routing management policy can be adopted.

Related commands: **display ip routing-table**, and **delete static-routes all**.

Note that if you configure static routes for the specified interface, you must specify the right next hop at the same time.

Example

Configure the next hop of the default route as 129.102.0.2.

```
[SW8800] ip route-static 0.0.0.0 0.0.0.0 129.102.0.2
```

Configure static route 129.102.0.2 255.255.255.0 in multiple VPNs.

```
[SW8800] ip route-static vpn-instance vpn1 vpn2 vpn3 129.102.0.2 255
.255.255.0 null 0
```

24 RIP CONFIGURATION COMMANDS

When a switch runs a routing protocol, it can perform the router functions. A router that is referred to in the following or its icon represents a generalized router or an Switch 8800 Family series routing switch running routing protocols. To improve readability, this will not be described in the other parts of the manual.

For the configuration of VPN instance, refer to the MPLS module in *3Com Switch 8800 Family Series Routing Switches Operation Manual*.

RIP Configuration Commands

checkzero

Syntax

checkzero

undo checkzero

View

RIP view

Parameter

None

Description

Use the **checkzero** command to check the zero field of RIP-1 packet.

Use the **undo checkzero** command to disable the checking of the zero fields.

By default, RIP-1 performs zero field check.

According to the protocol (RFC1058) specifications, some fields in RIP-1 packets must be zero, called zero fields. You can use the **checkzero** command to enable the zero field check operation on RIP-1 packet. During the zero field check operation, if the RIP-1 packet in which the zero fields are not zeros is received, it will be rejected.

This command is ineffective to RIP-2 since RIP-2 packets have no zero fields.

Example

Configure not to perform zero check for RIP-1 packet.

```
[3Com-rip] undo checkzero
```

default cost

Syntax

default cost *value*

undo default cost

View

RIP view

Parameter

value: The default routing cost to be set, ranging from 1 to 16. The default value is 1.

Description

Use **default cost** command to set the default routing cost of an imported route.

Use the **undo default cost** command to restore the default value.

If no specific routing cost is specified when importing the route of another routing protocol with the **import-route** command, the redistribution will be performed with the default routing cost specified with the **default cost** command.

Related command: **import-route**.

Example

Set the default routing cost of the imported route of another routing protocol to 3.

```
[3Com-rip] default cost 3
```

display rip

Syntax

display rip [**routing** | **vpn-instance**]

View

Any view

Parameter

routing: Displays RIP routing information.

vpn-instance: Displays VPN instance information.

Description

Use the **display rip** command to view the current RIP running state and its configuration information.

Example

Display the current running state and configuration information of the RIP.

```
<SW8800> display rip
RIP is running
  public net VPN-Instance
    Checkzero is on         Default cost : 1
    Summary is on          Preference : 100
    Traffic-share is off
```

```
Period update timer : 30
Timeout timer : 180
Garbage-collection timer : 120
No peer router
Network :
202.38.168.0
```

Table 53 Description of the fields of the display rip command

Field	Description
RIP is running	RIP is active
public net VPN-Instance	Public network in the VPN
Checkzero is on	Enable zero field checking
Default cost : 1	The default route cost is 1
Summary is on	Routes are summarized automatically
Preference : 100	The preference of RIP is 100
Traffic-share is off	Load balancing state for the interface
Period update timer : 30	Three timers of RIP
Timeout timer : 180	
Garbage-collection timer : 120	
No peer router	No destination address of a transmission is specified
Network :202.38.168.0	Enable RIP on network segment 202.38.168.0

filter-policy export

Syntax

filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [*routing-protocol*]

undo filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [*routing-protocol*]

View

RIP view

Parameter

acl-number: Access control list number used for filtering the destination addresses of the routing information.

ip-prefix-name: Name of address prefix list used for filtering the destination addresses of the routing information.

routing-protocol: Routing protocol whose routing information is to be filtered, including **direct**, **isis**, **bgp**, **ospf**, **ospf-ase**, **ospf-nssa** and **static** at present.

Description

Use the **filter-policy export** command to configure to filter the advertised routing information by RIP.

Use the **undo filter-policy export** command to configure not to filter the advertised routing information.

By default, RIP does not filter the advertised routing information.

Related commands: **acl**, **filter-policy import**, **ip ip-prefix**.

Example

Filter the advertised route information according to ACL 2000.

```
[3Com-rip] filter-policy 2000 export
```

filter-policy import

Syntax

filter-policy gateway *ip-prefix-name* **import**

undo filter-policy gateway *ip-prefix-name* **import**

filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name* [**gateway** *ip-prefix-name*] } **import**

undo filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name* [**gateway** *ip-prefix-name*] } **import**

View

RIP view

Parameter

acl-number: Access control list number used for filtering the destination addresses of the routing information.

ip-prefix-name: Name of address prefix list used for filtering the destination addresses of the routing information.

gateway *ip-prefix-name:* Name of address prefix list used for filtering the addresses of the neighboring routers advertising the routing information.

Description

Use the **filter-policy gateway import** command to configure to filter the received routing information distributed from the specified address.

Use the **undo filter-policy gateway import** command to configure not to filter the received routing information distributed from the specified address.

Use the **filter-policy import** command to configure the filtering to the received global routing information.

Use the **undo filter-policy import** command to disable filtering to the received global routing information

By default, RIP does not filter the received routing information.

Related commands: **acl**, **filter-policy export**, **ip ip-prefix**.

Example

Configure the filtering of the received global routing information according to ACL 2000.

```
[3Com-rip] filter-policy 2000 import
```

host-route

Syntax

host-route

undo host-route

View

RIP view

Parameter

None

Description

Use the **host-route** command to control the RIP to accept the host route.

Use the **undo host-route** command to reject the host route.

By default, RIP accepts the host route.

In some special cases, RIP receives a great number of host routes in the same network segment. These routes cannot help the path searching much but occupy a lot of resources. In this case, the **undo host-route** command can be used to reject a host route.

Example

Configure RIP to reject a host route.

```
[3Com-rip] undo host-route
```

import-route

Syntax

import-route *protocol* [**cost** *value* | **route-policy** *route-policy-name*]*

undo **import-route** *protocol*

View

RIP view

Parameter

protocol: Specifies the source routing protocol to be imported by RIP. At present, RIP can import the following routes: **direct**, **bgp**, **ospf**, **ospf-ase**, **ospf-nssa**, **isis** and **static**.

value: Cost value of the route to be imported.

route-policy *route-policy-name*: Configures to import the route matching the condition of the specified Route-policy only.

Description

Use the **import-route** command to import the routes of other protocols into RIP.

Use the **undo import-route** command to cancel the routes imported from other protocols.

By default, RIP does not import any other route.

The **import-route** command is used to import the route of another protocol by using a certain **cost** *value*. RIP regards the imported route as its own route and transmits it with the specified **cost** *value*. This command can greatly enhance the RIP capability of obtaining routes, thus increasing the RIP performance.

If the **cost** *value* is not specified, routes will be imported according to the **default cost** ranging from 1 to 16. If the cost value of the imported route is 16, then RIP continues to advertise this cost to other routers running RIP, and marks this route "Hold Down". However, this router can still forward packets until the Garbage Collection timer times out (defaults to 120 seconds).

Related command: **default cost**.

Example

Import a static route with the cost value of 4.

```
[3Com-rip] import-route static cost 4
```

Set the default cost and import an OSPF route with the default cost.

```
[3Com-rip] default cost 3
[3Com-rip] import-route ospf
```

network

Syntax

network *network-address*

undo network *network-address*

View

RIP view

Parameter

network-address: IP address of the RIP interface. It can be the IP network address of any interface.

Description

Use the **network** command to enable Routing Information Protocol (RIP) for the specified network connected to the router.

Use the **undo network** command to disable the RIP on the interface.

By default, all RIP interfaces are disabled.

RIP route processes are disabled on all interfaces by default. To enable a RIP route process on an interface, use the **network** command.

The **undo network** command is similar to the **undo rip work** command in terms of function. But they are not identical. Their similarity is that the interface using either command will not receive/transmit RIP routes. The difference between them is that, in the case of **undo rip work**, other interfaces will still forward the routes of the interface using the **undo rip work** command. In the case of **undo**

network, other interfaces will not forward the routes of the interface using this command and it seems that the interface disappeared.

When the **network** command is used on an address, the effect is that the interface on the network segment at this address is enabled. For example, the results of viewing the **network** 129.102.1.1 with both the **display current-configuration** command and the **display rip** command are shown as the network 129.102.0.0.

Related command: **rip work**.

Example

Enable the RIP on the interface with the network address as 129.102.0.0.

```
[3Com-rip] network 129.102.0.0
```

peer

Syntax

peer *ip-address*

undo peer *ip-address*

View

RIP view

Parameter

ip-address: The interface IP address of the peer router, in dotted decimal format.

Description

Use the **peer** command to configure the sending destination address of the peer device. Use the **undo peer** command to cancel the set destination address.

By default, do not send RIP packet to any destination.

RIP exchanges routing information with non-broadcasting networks in unicast view. This command specifies the sending destination address to fit some non-broadcast networks. Usually, it is not recommended to use this command.

Example

Specify the sending destination address 202.38.165.1.

```
[3Com-rip] peer 202.38.165.1
```

preference

Syntax

preference *value*

undo preference

View

RIP view

Parameter

value: Preference level, ranging from 1 to 255. By default, the value is 100.

Description

Use the **preference** command to configure the route preference of RIP.

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

Every routing protocol has its own preference. Its default value is determined by the specific routing policy. The preference will finally determine the routing algorithm to obtain the optimal route in the IP routing table. This command can be used to modify the RIP preference manually.

Example

Specify the RIP preference as 20.

```
[3Com-rip] preference 20
```

reset

Syntax

reset

View

RIP view

Parameter

None

Description

Use the **reset** command to reset the system configuration parameters of RIP.

When you need to re-configure parameters of RIP, this command can be used to restore to the default setting.

Example

Reset the RIP system.

```
[3Com-rip] reset
```

rip

Syntax

rip

undo rip

View

system view

Parameter

None

Description

Use the **rip** command to enable the RIP and enter the RIP view.

Use the **undo rip** command to disable RIP.

By default, the system does not run RIP.

To enter the RIP view to configure various RIP global parameters, RIP should be enabled first. Whereas the configuration of parameters related to the interfaces is not restricted by enabling/disabling RIP.

Note that the interface parameters configured previously would be invalid when RIP is disabled or reset.

Example

Enable the RIP and enter the RIP view.

```
[SW8800] rip
[3Com-rip]
```

rip authentication-mode

Syntax

rip authentication-mode { **simple** *password* | **md5** { **usual** *key-string* | **nonstandard** *key-string key-id* } }

undo rip authentication-mode

View

Interface view

Parameter

simple: Simple text authentication mode.

password: Simple text authentication key. It is a character string of 1 to 16 characters.

md5: MD5 cipher text authentication mode.

usual: Specifies the MD5 cipher text authentication packet to use the general packet format (RFC1723 standard format).

key-string: MD5 cipher text authentication key. If it is input in a plain text form, MD5 *key* is a character string not exceeding 16 characters. And it will be displayed in a cipher text form in a length of 24 characters when the **display current-configuration** command is executed. Inputting the MD5 *key* in a cipher text form with 24 characters long is also supported.

nonstandard: Specifies the MD5 cipher text authentication packet to use a nonstandard packet format described in RFC2082.

key-id: MD5 cipher text authentication identifier, ranging from 1 to 255.

Description

Use the **rip authentication-mode** command to configure RIP-2 authentication mode and its parameters.

Use the **undo rip authentication-mode** command to cancel the RIP-2 authentication.

RIP-1 does not support authentication. There are two RIP authentication modes: simple authentication and MD5 cipher text authentication for RIP-2. When MD5

cipher text authentication mode is used, there are two types of packet formats. One of them is that described in RFC 1723, which was brought forward earlier. The other format is the one described specially in RFC 2082. The router supports both of the packet formats and the user can select either of them on demands.

Related command: **rip version**.

Example

Specify Interface Vlan-interface 10 to use the **simple** authentication with the key as aaa.

```
[SW8800] interface Vlan-interface 10
[3Com-Vlan-interface10] rip version 2
[3Com-Vlan-interface10] rip authentication-mode simple aaa
```

Set MD5 authentication at Vlan-interface 10 with the key string as aaa and the packet type as usual.

```
[SW8800] interface Vlan-interface 10
[3Com-Vlan-interface10] rip version 2
[3Com-Vlan-interface10] rip authentication-mode md5 usual aaa
```

rip input

Syntax

rip input

undo rip input

View

Interface view

Parameter

None

Description

Use the **rip input** command to allow an interface to receive RIP packets.

Use the **undo rip input** command to disable an interface to receive RIP packets.

By default, all interfaces except loopback interfaces are enabled to receive RIP packets.

This command is used in cooperation with the other two commands: **rip output** and **rip work**. Functionally, **rip work** is equivalent to **rip input** & **rip output**. The latter two control the receipt and the transmission of RIP packets respectively on an interface. The former command equals the functional combination of the latter two commands.

Related command: **rip output**, **rip work**.

Example

Specify Vlan-interface 10 not to receive RIP packets.

```
[3Com-Vlan-interface10] undo rip input
```

rip metricin

Syntax

rip metricin *value*

undo rip metricin

View

Interface view

Parameter

value: Additional route metric added when an interface receives a packet, ranging from 0 to 16. By default, the value is 0.

Description

Use the **rip metricin** command to configure the additional route metric added to the route when an interface receives RIP packets.

Use the **undo rip metricin** command to restore the default value of this additional route metric.

Related command: **rip metricout**.

Example

Specify the additional route metric to 2 when the interface Vlan-interface 10 receives RIP packets.

```
[SW8800] interface Vlan-interface 10
[3Com-Vlan-interface10] rip metricin 2
```

rip metricout

Syntax

rip metricout *value*

undo rip metricout

View

Interface view

Parameter

value: Additional route metric added when an interface transmits a packet, ranging from 1 to 16. By default, the value is 1.

Description

Use the **rip metricout** command to configure the additional route metric to the route when an interface transmits RIP packets.

Use the **undo rip metricout** command to restore the default value of this additional route metric.

Related command: **rip metricin**.

Example

Set the additional route metric to 2 when the interface Vlan-interface 10 transmits RIP packets.

```
[SW8800] interface Vlan-interface 10
[3Com-Vlan-interface10] rip metricout 2
```

rip output

Syntax

rip output

undo rip output

View

Interface view

Parameter

None

Description

Use the **rip output** command to allow an interface to transmit RIP packets to the external.

Use the **undo rip output** command to disable an interface to transmit RIP packets to the external.

By default, all interfaces except loopback interfaces are enabled to transmit RIP packets to the external.

This command is used in cooperation with the other two commands: **rip input** and **rip work**. Functionally, **rip work** is equivalent to **rip input** & **rip output**. The latter two control the receipt and the transmission of RIP packets respectively on an interface. The former command equals the functional combination of the latter two commands.

Related command: **rip input**, **rip work**.

Example

Disable the interface Vlan-interface 10 to transmit RIP packets.

```
[SW8800] interface Vlan-interface 10
[3Com-Vlan-interface10] undo rip output
```

rip split-horizon

Syntax

rip split-horizon

undo rip split-horizon

View

Interface view

Parameter

None

Description

Use the **rip split-horizon** command to configure an interface to use split horizon when transmitting RIP packets.

Use **undo rip split-horizon** command to configure an interface not to use split horizon when transmitting RIP packets.

By default, an interface is enabled to use split horizon when transmitting RIP packets.

Normally, split horizon is necessary for reducing route loop. Only in some special cases, you need to disable split horizon to ensure the correct execution of protocols. When doing that, make sure that it is necessary.

Example

Specify the interface Vlan-interface 10 not to use split horizon when processing RIP packets.

```
[SW8800] interface Vlan-interface 10
[3Com-Vlan-interface10] undo rip split-horizon
```

rip version

Syntax

rip version 1

rip version 2 [**broadcast** | **multicast**]

undo rip version

View

Interface view

Parameter

1: Version of RIP packets on an interface is RIP-1.

2: Version of RIP packets on an interface is RIP-2.

broadcast: Transmission mode of RIP-2 packet is broadcast.

multicast: Transmission mode of RIP-2 packet is multicast.

Description

Use the **rip version** command to configure the version of RIP packets on an interface. Use the **undo rip version** command to restore the default value of RIP packet version on the interface.

By default, the interface RIP version is RIP-1. RIP-1 transmits packets in broadcast mode, while RIP-2 transmits packets in multicast mode by default.

When running RIP-1, the interface only receives and transmits RIP-1 broadcast packets, and receives RIP-2 broadcast packets, but does not receive RIP-2 multicast packets. When running RIP-2 in broadcast mode, the interface only receives and transmits RIP-2 broadcast packets, receives RIP-1 packets and RIP-2 multicast packets. When running RIP-2 in multicast mode, the interface only receives and transmits RIP-2 multicast packets, receives RIP-2 broadcast packets, but does not receive RIP-1 packets.

Example

Configure the interface Vlan-interface 10 as RIP-2 broadcast mode.

```
[SW8800] interface Vlan-interface 10
[3Com-Vlan-interface10] rip version 2 broadcast
```

rip work

Syntax

rip work

undo rip work

View

Interface view

Parameter

None

Description

Use the **rip work** command to enable the running of RIP on an interface.

Use the **undo rip work** command to disable the running of RIP on an interface.

By default, RIP is running on an interface.

This command is used in cooperation with **rip input**, **rip output** and **network** commands. Refer to the usage guideline of the related commands.

Related command: **network**, **rip input**, **rip output**.

Example

Disable the interface Vlan-interface 10 to run the RIP.

```
[SW8800] interface Vlan-interface 10
[3Com-Vlan-interface10] undo rip work
```

summary

Syntax

summary

undo summary

View

RIP view

Parameter

None

Description

Use the **summary** command to configure to activate RIP-2 automatic route summarization.

Use the **undo summary** command to disable RIP-2 automatic route summarization.

By default, RIP-2 route summarization is used.

Automatic route summarization can be performed to reduce the routing traffic on the network as well as to reduce the size of the routing table. If RIP-2 is used, route summarization function can be disabled with the **undo summary** command, when it is necessary to broadcast the subnet route.

RIP-1 does not support subnet mask. Forwarding subnet route may cause ambiguity. Therefore, RIP-1 uses route summarization all the time. Thus, the **undo summary** command does not take effect on RIP-1.

Related command: **rip version**.

Example

Set RIP version on the interface Vlan-interface 10 to RIP-2 and disable the route summarization function.

```
[SW8800] interface Vlan-interface 10
[3Com-Vlan-interface10] rip version 2
[3Com-Vlan-interface10] quit
[SW8800] rip
[3Com-rip] undo summary
```

timers

Syntax

timers { **update** *update-timer-length* | **timeout** *timeout-timer-length* } *

undo timers { **update** | **timeout** } *

View

RIP view

Parameter

update-timer-length: Value of the Period Update timer, ranging from 1 to 3600 seconds. By default, it is 30 seconds.

timeout-timer-length: Value of the Timeout timer, ranging from 1 to 3600 seconds. By default, it is 180 seconds.

Description

Use the **timers** command to modify the values of the three RIP timers: Period Update, Timeout, and Garbage-collection.

Use the **undo timers** command to restore the default settings.

By default, the values of Period Update, Timeout, and Garbage-collection timers are 30 seconds, 180 seconds, and 120 seconds respectively.

Generally, it is regarded that the value of Garbage-collection timer is fixed to four times of that of Period Update timer. Adjusting Period Update timer will affect Garbage-collection timer.

The modification of RIP timers is validated immediately.

Related command: **display rip**.

Example

Set the values of Period Update timer and Timeout timer of RIP to 10 seconds and 30 seconds respectively.

```
[SW8800] rip
[3Com-rip] timers update 10 timeout 30
```

25 OSPF CONFIGURATION COMMANDS

When a switch runs a routing protocol, it can perform the router functions. A router that is referred to in the following or its icon represents a generalized router or an Switch 8800 Family series routing switch running routing protocols. To improve readability, this will not be described in the other parts of the manual.

OSPF Configuration Commands

abr-summary

Syntax

abr-summary *ip-address mask* [**advertise** | **not-advertise**]

undo abr-summary *ip-address mask*

View

OSPF Area view

Parameter

ip-address: Network segment address.

mask: Network mask.

advertise: Advertises only the summarized route that matches the specified IP address and mask.

not-advertise : Not advertises routes matching the specified IP address and mask.

Description

Use the **abr-summary** command to configure automatic route summarization on the area border router.

Use the **undo abr-summary** command to disable the function of route summarization on the area border router.

By default, the area border router does not summarize routes.

This command is applicable only to the area border router (ABR) and is used for the route summarization in an area. The ABR only transmits a summarized route to other areas. Route summarization refers to that the routing information is processed in the ABR and for each network segment configured with route summarization, there is only one route transmitted to other areas.

You can summarize multiple network segments in one OSPF area.

Example

Summarize two network segments, 36.42.10.0 and 36.42.110.0, in OSPF area 1 into one summarized route 36.42.0.0 and transmit it to other areas.

```
[3Com-ospf-1] area 1
[3Com-ospf-1-area-0.0.0.1] network 36.42.10.0 0.0.0.255
[3Com-ospf-1-area-0.0.0.1] network 36.42.110.0 0.0.0.255
[3Com-ospf-1-area-0.0.0.1] abr-summary 36.42.0.0 255.255.0.0
```

area

Syntax

area *area-id*

undo area *area-id*

View

OSPF view

Parameter

area-id: ID of the OSPF area, which can be a decimal integer (ranging from 0 to 4,294,967,295) or in IP address format.

Description

Use the **area** command to enter OSPF Area view.

Use the **undo area** command to remove the specified area.

Example

Enter OSPF Area 0 view.

```
[3Com-ospf-1] area 0
[3Com-ospf-1-area-0.0.0.0]
```

asbr-summary

Syntax

asbr-summary *ip-address mask* [**not-advertise** | **tag** *value*]

undo asbr-summary *ip-address mask*

View

OSPF view

Parameter

ip-address: Matched IP address in dotted decimal format.

mask: IP address mask in dotted decimal format.

not-advertise: Do not advertise routes matching the specified IP address and mask. **tag** *value*: Tag value, which is mainly used to control advertisement of routes via route-policy. It is in the range from 0 to 4,294,967,295. The default tag value is 1.

Description

Use the **asbr-summary** command to configure summarization of imported routes by OSPF.

Use the **undo asbr-summary** command to cancel the summarization.

By default, summarization of imported routes is disabled.

After the summarization of imported routes is configured, if the local router is an autonomous system border router (ASBR), this command summarizes the imported Type-5 LSAs in the summary address range. When NSSA is configured, this command will also summarize the imported Type-7 LSAs in the summary address range.

If the local router acts as both an ABR and a router in the NSSA, this command summarizes Type-5 LSAs transformed from Type-7 LSAs. If the router is not the router in the NSSA, the summarization is disabled.

Related command: **display ospf asbr-summary**.

Example

Set summarization of 3Com imported routes.

```
[SW8800] ospf
[3Com-ospf-1] asbr-summary 10.2.0.0 255.255.0.0 not-advertise
```

authentication-mode

Syntax

authentication-mode { **simple** | **md5** }

undo authentication-mode

View

OSPF area view

Parameter

simple: Uses simple text authentication mode.

md5: Uses MD5 cipher text authentication mode.

Description

Use the **authentication-mode** command to configure one area of OSPF to support the authentication attribute.

Use the **undo authentication-mode** command to cancel the authentication attribute of this area.

By default, an area does not support authentication attribute.

All the routers in one area must use the same authentication mode (no authentication, simple text authentication or MD5 cipher text authentication). If the mode of supporting authentication is configured, all routers on the same segment must use the same authentication key. To configure a simple text authentication key, use the **ospf authentication-mode simple** command. Use

the **ospf authentication-mode md5** command to configure the MD5 cipher text authentication key if the area is configured to support MD5 cipher text authentication mode.

Related command: **ospf authentication-mode**.

Example

Enter area 0 view.

```
[3Com-ospf-1] area 0
```

Specify the OSPF area 0 to support MD5 cipher text authentication:

```
[3Com-ospf-1-area-0.0.0.0] authentication-mode md5
```

debugging ospf

Syntax

debugging ospf [*process-id*] { **event** | **packet** [**ack** | **dd** | **hello** | **interface** *interface-type interface-number* | **request** | **update**] | **lsa-originate** | **spf** | **graceful-restart** }

undo debugging ospf [*process-id*] { **event** | **packet** [**ack** | **dd** | **hello** | **interface** *interface-type interface-number* | **request** | **update**] | **lsa-originate** | **spf** | **graceful-restart** }

View

User view

Parameter

process-id: Process ID of OSPF. The command enables/disables all process debugging if you do not specify a process ID.

event: Enables/Disables OSPF event debugging.

packet: Enables/Disables OSPF packet debugging. OSPF packets include:

ack: LSAck packet.

dd: Database Description packet.

hello: Hello packet.

request: Link State Request packet.

update: Link State Update packet.

interface *interface-type interface-number*: Interface type and number, which indicates to enable/disable debugging for the OSPF packets obtained on the specified interface.

lsa-originate: Enables/Disables OSPF LSA packet debugging.

spf: Enables/Disables OSPF minimum tree calculation debugging.

graceful-restart: Enables the debugging for OSPF GR.

Description

Use the **debugging ospf** command to enable OSPF process debugging.

Use the **undo debugging ospf** command to disable OSPF process debugging.

In OSPF multiple processes, the **debugging** command can enable a certain debugging for all the processes, or enable the debugging of one of them.

If you do not specify a process ID, the command is applied to all processes. While the router is operating, the debugging state always remains regardless of the existing OSPF process. If you specify a process ID, the command is only applied to the specified process.

Related command: **display debugging ospf**.

Example

Enable OSPF packet debugging.

```
<SW8800> debugging ospf packet
```

Enable the debugging for OSPF GR.

```
<SW8800> debugging ospf graceful-restart
```

default cost

Syntax

default cost *value*

undo default cost

View

OSPF view

Parameter

value: Default routing cost of an external route imported by OSPF, ranging from 0 to 16,777,214. By default, its value is 1.

Description

Use the **default cost** command to configure the default cost for OSPF to import external routes.

Use the **undo default cost** command to restore the default value of the default routing cost configured for OSPF to import external routes.

Since OSPF can import external routing information, whose routing cost can influence routing selection and calculation, and propagate it to the entire autonomous system, it is necessary to specify the default routing cost for the protocol to import external routes.

Example

Specify the default routing cost for OSPF to import external routes as 10.

```
[3Com-ospf-1] default cost 10
```

default interval

Syntax

default interval *seconds*

undo default interval

View

OSPF view

Parameter

seconds: Default interval in seconds for importing external routes. It ranges from 1 to 2,147,483,647 and defaults to 1.

Description

Use the **default interval** command to configure the default interval for OSPF to import external routes.

Use the **undo default interval** command to restore the default value of the default interval for importing external routes.

Because OSPF can import the external routing information and broadcast it to the entire autonomous system, and importing routes too often will greatly affect the performances of the device, it is necessary to specify the default interval for the protocol to import external routes.

Example

Specify the default interval for OSPF to import external routes as 10 seconds.

```
[3Com-ospf-1] default interval 10
```

default limit

Syntax

default limit *routes*

undo default limit

View

OSPF view

Parameter

routes: Default value to the imported external routes in a unit time, ranging from 200 to 2,147,483,647. By default, the value is 1000.

Description

Use the **default limit** command to configure the default value of maximum number of imported routes.

Use the **undo default limit** command to restore the default value.

OSPF can import external routing information and advertise them to the whole AS. Importing too much external routes once will greatly affect the performances of the device.

Related command: **default interval**.

Example

Specify the default value of OSPF imported external routes as 200.

```
[3Com-ospf-1] default limit 200
```

default tag

Syntax

default tag *tag*

undo default tag

View

OSPF view

Parameter

tag: Default tag, ranging from 0 to 4,294,967,295. The default value is 1.

Description

Use the **default tag** command to configure the default tag that OSPF assigns to imported routes.

Use the **undo default tag** command to restore the default of the default tag that OSPF assigns to imported routes.

When OSPF imports a route found by other routing protocols in the router and uses it as the external routing information of its own autonomous system, some additional parameters are required, including the default cost and the default tag of the route.

Related command: **default type**.

Example

Set the default tag that OSPF assigns to imported routes to 10.

```
[3Com-ospf-1] default tag 10
```

default type

Syntax

default type { **1** | **2** }

undo default type

View

OSPF view

Parameter

type 1: External routes of type 1.

type 2: External routes of type 2.

Description

Use the **default type** command to configure the default type when OSPF imports external routes.

Use the **undo default type** command to restore the default type when OSPF imports external routes.

By default, the external routes of type 2 are imported.

OSPF specifies the two types of external routing information. The command described in this section can be used to specify the default type when external routes are imported.

Related command: **default tag**.

Example

Specify the default type as type 1 when OSPF imports an external route.

```
[3Com-ospf-1] default type 1
```

default-cost

Syntax

default-cost *value*

undo default-cost

View

OSPF Area view

Parameter

value: Specifies the cost value of the default route transmitted by OSPF to the Stub or NSSA area, ranging from 0 to 16,777,214. The default value is 1.

Description

Use the **default-cost** command to configure the cost of the default route transmitted by OSPF to the Stub or NSSA area.

Use the **undo default-cost** command to restore the cost of the default route transmitted by OSPF to the Stub or NSSA area to the default value.

This command only applies to the border routers connected to the Stub or NSSA areas.

To configure a Stub area, you need to use two commands: **stub** and **default-cost**. The **stub** command is used to configure the Stub attribute for this area.

Related command: **stub**, **nssa**.

Example

Set the area 1 as the Stub area and the cost of the default route transmitted to this Stub area to 60.

```
[3Com-ospf-1] area 1
[3Com-ospf-1-area-0.0.0.1] network 20.0.0.0 0.255.255.255
[3Com-ospf-1-area-0.0.0.1] stub
[3Com-ospf-1-area-0.0.0.1] default-cost 60
```

default-route-advertise

Syntax

default-route-advertise [**always** | **cost** *value* | **type** *type-value* | **route-policy** *route-policy-name*]*

undo default-route-advertise [**always** | **cost** | **type** | **route-policy**]*

View

OSPF view

Parameter

always: The parameter will generate an ASE LSA which describes the default route and will advertise it if the local router is not configured with the default route. If this parameter is not set, the local router cannot import the ASE LSA, which generates the default route only when it is configured with the default route.

cost *value*: The cost value of this ASE LSA. The metric-value ranges from 0 to 16,777,214. If the parameter is not configured, the default value is 1.

type *type-value:* Cost type of this ASE LSA. It ranges from 1 to 2. If the parameter is not configured, the default value is 2.

route-policy *route-policy-name:* If the default route match the route-policy specified by *route-policy-name*, route-policy will affect the value in ASE LSA. The length of *route-policy-name* argument is a character string of 1 to 19 characters.

Description

Use the **default-route-advertise** command to import default route to OSPF route area. Use the **undo default-route-advertise** command to cancel the redistribution of default route.

By default, OSPF does not import default route.

The **import-route** command cannot import the default route. To import the default route to the route area, this command must be used. When local router is not configured with default route, the keyword **always** should be used by ASE LSA to generate default route.

Related command: **import-route**.

Example

If local route has no default route, the ASE LSA of default route will be generated. Otherwise, it will not be generated.

```
[3Com-ospf-1] default-route-advertise
```

The ASE LSA of default route will be generated and advertised to OSPF route area even the local router has no default route.

```
[3Com-ospf-1] default-route-advertise always
```

display debugging ospf

Syntax

display debugging ospf

View

Any view

Description

Use the **display debugging ospf** command to view the debugging states of global OSPF and all processes.

Related command: **debugging ospf**.

Example

Display the debugging states of global OSPF and all processes.

```
<SW8800> display debugging ospf
OSPF global debugging state:
OSPF SPF debugging is on
OSPF LSA debugging is on
OSPF process 100 debugging state:
OSPF SPF debugging is on

OSPF process 200 debugging state:
OSPF SPF debugging is on
OSPF LSA debugging is on
```

display ospf abr-asbr

Syntax

display ospf [*process-id*] **abr-asbr**

View

Any view

Parameter

process-id: Process ID of OSPF. The command is applied to all current OSPF processes if you do not specify a process ID.

Description

Use the **display ospf abr-asbr** command to view the information about the ABR and ASBR of OSPF.

Example

Display the information of the OSPF area border routers and autonomous system border routers.

```
<SW8800> display ospf abr-asbr
OSPF Process 1 with Router ID 10.110.98.138
Routing Table to ABR and ASBR
 I = Intra i = Inter A = ASBR B = ABR S = SumASBR
Destination        Area            Cost   Nexthop         Interface
IA 2.2.2.2         0.0.0.0         10     10.153.17.89    Vlan-interface1
```

Table 54 Description of the fields of the display ospf abr-asbr command

Field	Description
Destination	Router ID of the ABR or ASBR
Area	Area where the router is connected with ASBR
Cost	The routing overhead value of the route

Table 54 Description of the fields of the display ospf abr-asbr command

Field	Description
Nexthop	Nexthop address
Interface	The local output interface

display ospf asbr-summary

Syntax

display ospf [*process-id*] **asbr-summary** [*ip-address mask*]

View

Any view

Parameter

process-id: Process ID of OSPF. The command is applied to all current OSPF processes if you do not specify a process ID.

ip-address: Matched IP address in dotted decimal format.

mask: IP address mask in dotted decimal format.

Description

Use the **display ospf asbr-summary** command to view the summary information of OSPF imported route.

If the parameters are not set, the summary information of all OSPF imported routes will be displayed.

Related command: **asbr-summary**.

Example

Display the summary information of all OSPF imported routes.

```
<SW8800> display ospf asbr-summary
OSPF Process 1 with Router ID 1.1.1.1
Summary Addresses
Total summary address count:   2

                 Summary Address
net      : 168.10.0.0
mask     : 255.254.0.0
tag      : 1
status   : Advertise
The Count of Route is 0

                 Summary Address
net      : 1.1.0.0
mask     : 255.255.0.0
tag      : 100
status   : DoNotAdvertise
The Count of Route is 0
```

Table 55 Description of the fields of the display ospf asbr-summary command

Field	Description
net	Destination network segment

Table 55 Description of the fields of the display ospf asbr-summary command

Field	Description	
mask	Mask	
tag	Tag	
status	Status information, including two values:	
	DoNotAdvertise	The summary routing information to the network segment will not be advertised
	Advertise	The summary routing information to the network segment will be advertised

display ospf brief

Syntax

display ospf [*process-id*] **brief**

View

Any view

Parameter

process-id: Process ID of OSPF. The command is applied to all current OSPF processes if you do not specify a process ID.

Description

Use the **display ospf brief** command to view the main summary of OSPF.

Example

Display the OSPF summary.

```
<SW8800> display ospf brief
OSPF Process 1 with Router ID 10.110.95.189
OSPF Protocol Information
RouterID: 10.110.95.189  Border Router: Area AS
spf-schedule-interval: 5
Routing preference: Inter/Intra: 10 External: 150
Default ASE parameters: Metric: 1 Tag: 0.0.0.1 Type: 2
SPF computation count: 16
Area Count: 1    Nssa Area Count: 0

 Area 0.0.0.0:
   Authtype: none   Flags: <>
   SPF scheduled: <>
   Interface: 201.1.1.4 (Vlan-interface1)
     Cost: 1 State: DR    Type: Broadcast
     Priority: 1
     Designated Router: 201.1.1.4
     Backup Designated Router: 201.1.1.3
     Timers: Hello 10, Dead 40, Poll 0, Retransmit 5, Transmit Delay 1
```

Table 56 Description of the fields of the display ospf brief command

Field	Description
RouterID	Router ID of the router
Border Router	Border routers for connection to the area, including autonomous system border router (ASBR) and area border router (ABR)
spf-schedule-interval	Interval of SPF schedule in seconds
Authtype	Authentication type of OSPF

Table 56 Description of the fields of the display ospf brief command

Field	Description	
Routing preference	Routing preference of OSPF. The internal route of OSPF includes intra/inter area route, and its default routing preference is 10. While that of the external route of OSPF is 150 by default	
Default ASE parameters	Default ASE parameters of OSPF, including metric, type and tag	
SPF computation count	SPF computation count since OSPF is enabled	
Area Count	Areas for connection to this router	
Nssa Area Count	Number of NSSA areas	
SPF scheduled	SPF scheduled (flag)	
Interface	Interface name belonging to this area	
Cost	Cost of routes	
State	State information	
Type	Network type of OSPF interface	
Priority	Priority	
Designated Router	IP address of designated router (DR)	
Backup Designated Router	IP address of backup designated router (BDR)	
Timers	OSPF timers, defining as follows:	
	Hello	Interval of hello packet
	Dead	Interval of dead neighbors
	Poll	Interval of poll
	Retransmit	Interval of retransmitting LSA
Transmit Delay	Delay time of transmitting LSA	

display ospf cumulative

Syntax

display ospf [*process-id*] **cumulative**

View

Any view

Parameter

process-id: Process ID of OSPF. The command is applied to all current OSPF processes if you do not specify a process ID.

Description

Use the **display ospf cumulative** command to view the OSPF cumulative information.

Example

Display the OSPF cumulative information.

```
<SW8800> display ospf cumulative
OSPF Process 1 with Router ID 1.1.1.1
Cumulations
IO Statistics
Type                    Input       Output
Hello                   225         437
DB Description      78          86
```

```
Link-State Req      18          18
Link-State Update   48          53
Link-State Ack      25          21
ASE: 1 Checksum Sum:  FCAF
LSAs originated by this router
    Router: 50  SumNet: 40  SumASB: 2
LSAs Originated: 92  LSAs Received: 33
Area 0.0.0.0:
    Neighbors: 1  Interfaces: 1
    Spf: 54     Checksum Sum F020
    rtr: 2 net: 0 sumasb: 0 sumnet: 1
Area 0.0.0.1:
    Neighbors: 0  Interfaces: 1
    Spf: 19  Checksum Sum 14EAD
    rtr: 1 net: 0   sumasb: 1   sumnet: 1
Routing Table:
Intra Area: 2   Inter Area: 0   ASE: 1
```

Table 57 Description of the fields of the display ospf cumulative command

Field		Description
IO Statistics	Type	Type of input/output OSPF packet
	Input	Number of received packets
	Output	Number of transmitted packets
ASE		Number of all ASE LSAs
checksum sum		Checksum of ASE LSA
LSAs	originated	Number of originated LSAs
	received	Number of received LSAs generated by other routers
Router		Number of all Router LSAs
SumNet		Number of all Sumnet LSAs
SumASB		Number of all SumASB LSAs
Area	Neighbors	Number of neighbors in this area
	Interfaces	Number of interfaces in this area
	Spf	Number of SPF computation count in this area
	rtr, net, sumasb, sumnet	Number of all LSAs in this area
Routing Table	Intra Area	Number of intra-area routes
	Inter Area	Number of inter-area routes
	ASE	Number of external routes

display ospf error

Syntax

display ospf [*process-id*] **error**

View

Any view

Parameter

process-id: Process ID of OSPF. The command is applied to all current OSPF processes if you do not specify a process ID.

Description

Use the **display ospf error** command to view the OSPF error information.

Example

Display the OSPF error information.

```
<SW8800> display ospf error
OSPF Process 1 with Router ID 1.1.1.1
OSPF packet error statistics:
   0: IP: received my own packet       0: OSPF: wrong packet type
   0: OSPF: wrong version              0: OSPF: wrong checksum
   0: OSPF: wrong area id              0: OSPF: area mismatch
   0: OSPF: wrong virtual link         0: OSPF: wrong authentication type
   0: OSPF: wrong authentication key   0: OSPF: too small packet
   0: OSPF: packet size > ip length    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: router id confusion       0: HELLO: virtual neighbor unknown
   0: DD: router id confusion          0: DD: extern option mismatch
   0: DD: unknown LSA type             0: LS ACK: neighbor state low
   0: LS ACK: wrong ack                0: LS ACK: duplicate ack
   0: LS ACK: unknown LSA type         0: LS REQ: neighbor state low
   0: LS REQ: empty request            0: LS REQ: wrong request
   0: LS UPD: neighbor state low       0: LS UPD: newer self-generate LSA
   0: LS UPD: LSA checksum wrong       0: LS UPD: received less recent LSA
   0: LS UPD: unknown LSA type         0: OSPF routing: next hop not exist
   0: DD: MTU option mismatch          0: ROUTETYPE: wrong type value
```

Table 58 Description of the fields of the display ospf error command

Field	Description
IP: received my own packet	Received my own packet
OSPF: wrong packet type	OSPF packet type error
OSPF: wrong version	OSPF version error
OSPF: wrong checksum	OSPF checksum error
OSPF: wrong area id	OSPF area ID error
OSPF: area mismatch	OSPF area mismatch
OSPF: wrong virtual link	OSPF virtual link error
OSPF: wrong authentication type	OSPF authentication type error
OSPF: wrong authentication key	OSPF authentication key error
OSPF: too small packet	OSPF packet too small
OSPF: packet size > ip length	OSPF packet size exceeds IP packet length
OSPF: transmit error	OSPF transmission error
OSPF: interface down	OSPF interface is down, unavailable
OSPF: unknown neighbor	OSPF neighbors are unknown
HELLO: netmask mismatch	Network mask mismatch
HELLO: hello timer mismatch	Interval of HELLO packet is mismatched
HELLO: dead timer mismatch	Interval of dead neighbor packet is mismatched
HELLO: extern option mismatch	Extern option of Hello packet is mismatched

Table 58 Description of the fields of the display ospf error command

Field	Description
HELLO: router id confusion	Hello packet: Router ID confusion
HELLO: virtual neighbor unknown	Hello packet: unknown virtual neighbor
DD: neighbor state low	Database description (DD) packet: asynchronous neighbor state
DD: unknown LSA type	DD packet: unknown LSA type
LS ACK: neighbor state low	Link state acknowledgment (LS ACK) packet: states of neighbors are not synchronized.
LS ACK: wrong ack	Link state acknowledgment packet: ack error
LS ACK: duplicate ack	Link state acknowledgment packet: ack duplication
LS ACK: unknown LSA type	Link state acknowledgment packet: unknown LSA type
LS REQ: neighbor state low	Link state request (LS REQ) packet: The states of neighbors are not synchronized
LS REQ: empty request	Link state request packet: empty request
LS REQ: wrong request	Link state request packet: erroneous request
LS UPD: neighbor state low	Link state update packet: The states of neighbors are synchronized.
LS UPD: newer self-generate LSA	Link state update packet: newer LSA generated by itself
LS UPD: LSA checksum wrong	Link state update packet: LSA checksum error
LS UPD: received less recent LSA	Link state update packet: received less recent LSA
LS UPD: unknown LSA type	Link state update packet: unknown LSA type
OSPF routing: next hop not exist	Next hop of OSPF routing does not exist
DD: MTU option mismatch	MTU option of DD packet is mismatched
ROUTETYPE: wrong type value	Route type: the value of the type is wrong

display ospf interface

Syntax

display ospf [*process-id*] **interface** [*interface-type interface-number*]

View

Any view

Parameter

process-id: Process ID of OSPF. The command is applied to all current OSPF processes if you do not specify a process ID.

interface-type interface-number: Specifies an interface.

Description

Use the **display ospf interface** command to view the OSPF interface information.

Example

Display the OSPF interface information of Vlan-interface1.

```
<SW8800> display ospf interface vlan-interface 1
OSPF Process 1 with Router ID 1.1.1.1
Interfaces
Interface: 10.110.10.2 (Vlan-interface1)
 Cost: 1 State: BackupDR    Type: Broadcast
```

```
Priority: 1
Designated Router: 10.110.10.1
Backup Designated Router: 10.110.10.2
Timers: Hello 10, Dead 40, Poll 0, Retransmit 5, Transmit Delay 1
```

Table 59 Description of the fields of the display ospf interface command

Field	Description	
Cost	Cost of the interface	
State	State of the interface state machine	
Type	Network type of OSPF on the interface	
Priority	Priority of the interface for DR election in its network	
Designated Router	DR on the network in which the interface resides	
Backup Designated Router	BDR on the network in which the interface resides	
Timers	OSPF timers, defining as follows:	
	Hello	Interval of Hello packet
	Dead	Interval of dead neighbors
	Poll	Interval of poll
	Retransmit	Interval of retransmitting LSA
Transmit Delay	Delay time of transmitting LSA	

display ospf lsdb

Syntax

display ospf [*process-id*] [*area-id*] **lsdb** [**brief** | [**asbr** | **ase** | **network** | **nssa** | **router** | **summary** [**verbose**]] [*ip-address*] [**originate-router** *ip-address* | **self-originate**] [**verbose**]]

View

Any view

Parameter

process-id: Process ID of OSPF. The command is applied to all current OSPF processes if you do not specify a process ID.

area-id: ID of the OSPF area, which can be a decimal integer in the range 0 to 4,294,967,295 or in IP address format.

brief: Views brief database information.

asbr: Views the database information of Type-4 LSA (summary-Asbr-LSA).

ase: Views the database information of Type-5 LSA (AS-external-LSA).

network: Views the database information of Type-2 LSA (Network-LSA).

nssa: Views the database information of Type-7 LSA (NSSA-external-LSA).

router: Views the database information of Type-1 LSA (Router-LSA).

summary: Views the database information of Type-3 LSA (Summary-Net-LSA).

ip-address: Link state ID in IP address format.

originate-router *ip-address*: Views the IP address of the LSA generator.

self-originate: Views the database information of self-originated LSA.

Description

Use the **display ospf lsdb** command to view the link-state database (LSDB) of OSPF.

Example

Display the LSDB of OSPF.

```
<SW8800> display ospf lsdb verbose
OSPF Process 1 with Router ID 1.1.1.1
Link State Database
Area: 0.0.0.0
Type LinkState ID    AdvRouter      Age Len  Sequence   Metric Where
Rtr  2.2.2.2            2.2.2.2       465 36   8000000c        0 SpfTree
Rtr  1.1.1.1            1.1.1.1       449 36   80000004        0 SpfTree
Net  10.153.17.89       2.2.2.2       465 32   80000004        0 SpfTree
SNet 10.153.18.0        1.1.1.1     355 28   80000003        10 Inter List
Area: 0.0.0.1
Type LinkState ID    AdvRouter    Age Len  Sequence   Metric Where
Rtr  1.1.1.1         1.1.1.1      449 36   80000004   0     SpfTree
Rtr  3.3.3.3         3.3.3.3      429 36   8000000a   0       Clist
Net  10.153.18.89    3.3.3.3      429 32   80000003   0     SpfTree
SNet 10.153.17.0     1.1.1.1      355 28   80000003   10  Inter List
ASB  2.2.2.2    1.1.1.1 355 28   80000003    10 SumAsb List
AS External Database:
Type LinkState ID    AdvRouter    Age Len  Sequence   Metric Where
ASE  10.153.18.0     1.1.1.1      1006 36   80000002  1      Ase List
ASE  10.153.16.0     2.2.2.2      798 36    80000002  1 Uninitialized
ASE  10.153.17.0     2.2.2.2      623 36    80000003  1 Uninitialized
ASE  10.153.17.0     1.1.1.1      1188 36   80000002  1      Ase List
```

Table 60 Description of the fields of the display ospf lsdb command

Field	Description
Type	Type of the LSA
LinkStateID	Link state ID of the LSA
AdvRouter	Router ID of the router originating the LSA
Age	Age of the LSA, in seconds
Len	Length of the LSA
Sequence	Sequence number of the LSA
Metric	Cost from the router originating the LSA to the LSA destination
Where	Location of the LSA

```
<SW8800> display ospf lsdb ase
OSPF Process 1 with Router ID 1.1.1.1
Link State Data Base
    type : ASE
    ls id :  2.2.0.0
    adv rtr: 1.1.1.1
    ls age:  349
    len:    36
    seq#:   80000001
    chksum:  0xfcaf
    Options: (DC)
    Net mask:255.255.0.0
```

```
Tos 0 metric: 1
E type :    2
Forwarding Address: 0.0.0.0
Tag: 1
```

Table 61 Description of the fields of the display ospf lsdb ase command

Field	Description
type	Type of the LSA
ls id	Link state ID of the LSA
adv rtr	Router ID of the router originating the LSA
ls age	Age of the LSA in seconds
len	Length of the LSA
seq#	Sequence number of the LSA
chksum	Checksum of the LSA
Options	Options of the LSA
Net mask	Network mask
E type	Type of external route
Forwarding Address	Forwarding address
Tag	Tag

display ospf nexthop

Syntax

display ospf [*process-id*] **nexthop**

View

Any view

Parameter

process-id: Process ID of OSPF. The command is applied to all current OSPF processes if you do not specify a process ID.

Description

Use the **display ospf nexthop** command to view the information about the next-hop.

Example

Display the OSPF next-hop information.

```
<SW8800> display ospf nexthop
OSPF Process 1 with Router ID 1.1.1.1
Address        Type   Refcount     Intf Addr         Intf Name
------------------------------------------------------------------------
202.38.160.1    Direct   3          202.38.160.1          Vlan-interface2
202.38.160.2    Neighbor     1          202.38.160.1         Vlan-interface2
```

Table 62 Description of the fields of the display ospf nexthop command

Field	Description
Address	Address of next hop
Type	Type of next hop
Refcount	Reference count of the next hop, i.e., number of routes using this address as the next hop
Intf Addr	IP address of the outgoing interface to the next hop

Table 62 Description of the fields of the display ospf nexthop command

Field	Description
Intf Name	The outgoing interface to the next hop

display ospf peer

Syntax

display ospf [*process-id*] **peer** [**brief**]

View

Any view

Parameter

process-id: Process ID of OSPF. The command is applied to all current OSPF processes if you do not specify a process ID.

Description

Use the **display ospf peer** command to view information about OSPF peers.

Use the **display ospf peer brief** command to view the brief information of every peer in OSPF, mainly the numbers of peers at all states in every area.

Example

View the neighbor brief information of OSPF.

```
<SW8800> display ospf peer brief
OSPF Process 1 with Router ID 85.1.1.1
                        Neighbor Brief Information

  Virtual Link:
  Router ID       Address         Pri    Interface           State
  85.1.1.2        63.56.1.1       0      Vlan-interface561   Down
```

Table 63 Description of the fields of the display ospf peer brief command

Field	Description
Router ID	Router ID of neighbor router
Address	Address of the interface through which the neighbor router communicates with the local router
Pri	Priority
Interface	Interface address of the network segment
State	State information

display ospf request-queue

Syntax

display ospf [*process-id*] **request-queue**

View

Any view

Parameter

process-id: ID of an OSPF process. The command is applied to all current OSPF processes if you do not specify a process ID.

Description

Use the **display ospf request-queue** command to view the information about the OSPF request-queue.

Example

Display the information of OSPF request-queue.

```
<SW8800> display ospf request-queue
The Router's Neighbors is
  RouterID:  1.1.1.1          Address: 1.1.1.1
  Interface: 1.1.1.3          Area: 0.0.0.0
  LSID:1.1.1.3          AdvRouter:1.1.1.3  Sequence:80000017  Age:35
```

Table 64 Description of the fields of the display ospf request-queue command

Field	Description
RouterID	Router ID of neighbor router
Address	Address of the interface, through which neighbor routers communicate with the router
Interface	Address of the interface on the network segment
Area	Number of an OSPF area
LSID:1.1.1.3	Link State ID of the LSA
AdvRouter	Router ID of the router originating the LSA
Sequence	Sequence number of the LSA, used to discover old and repeated LSAs
Age	Age in seconds of the LSA

display ospf retrans-queue

Syntax

display ospf [*process-id*] **retrans-queue**

View

Any view

Parameter

process-id: ID of an OSPF process. The command is applied to all current OSPF processes if you do not specify a process ID.

Description

Use the **display ospf retrans-queue** command to view information about the OSPF retransmission queue.

Example

Display information about the OSPF retransmission queue.

```
<SW8800> display ospf retrans-queue
OSPF Process 200 with Router ID 103.160.1.1
Retransmit List
      The Router's Neighbors is
  RouterID: 162.162.162.162 Address: 103.169.2.2
  Interface: 103.169.2.5     Area: 0.0.0.1
          Retrans list:
          Type: ASE  LSID:129.11.77.0  AdvRouter:103.160.1.1
          Type: ASE  LSID:129.11.108.0  AdvRouter:103.160.1.1
```

Table 65 Description of the fields of the display ospf retrans-queue command

Field	Description
RouterID	Router ID of neighbor router
Address	Address of the interface, through which neighbor routers communicate with the router
Interface	Address of the interface on the network segment
Area	Number of an OSPF area
Type	Type of the LSA
LSID	Link State ID of the LSA
AdvRouter	Router ID of the router originating the LSA

display ospf routing

Syntax

display ospf [*process-id*] **routing**

View

Any view

Parameter

process-id: ID of an OSPF process. The command is applied to all current OSPF processes if you do not specify a process ID.

Description

Use the **display ospf routing** command to view information about the OSPF routing table.

Example

View the OSPF routing table.

```
<SW8800> display ospf routing
OSPF Process 1 with Router ID 1.1.1.1
Routing Tables
Routing for Network
Destination             Cost Type NextHop         AdvRouter        Area
10.110.0.0/16              1 Net  10.110.10.1     1.1.1.1          0
10.10.0.0/16               1 Stub 10.10.0.1       3.3.3.3          0
Total Nets: 2
  Intra Area: 2  Inter Area: 0  ASE: 0  NSSA: 0
```

Table 66 Description of the fields of the display ospf routing command

Field	Description
Destination	Destination network segment
Cost	Cost of route
Type	Type of route
NextHop	Next hop of route
AdvRouter	Router ID of the router advertising the route
Area	Area ID
Intra Area	Number of intra-area routes
Inter Area	Number of inter-area routes
ASE	Number of external routes

Table 66 Description of the fields of the display ospf routing command

Field	Description
NSSA	Number of NSSA routes

display ospf abr-summary

Syntax

display ospf [*process-id*] **abr-summary**

View

Any view

Parameter

process-id: OSPF process number. If no process number is specified, the command functions on all the currently active OSPF processes.

Description

Use the **display ospf abr-summary** command to view the inter-area route summarization information of OSPF.

Related command: **abr-summary**.

Example

View all the imported route summarization information of OSPF.

```
<SW8800> display ospf abr-summary
 OSPF Process 1 with Router ID 1.1.1.1

ABR summary in area 0.0.0.1, total 2:
Network        Mask        Cost         Status         Used
-------------    ---------------   --------       -------------   --------
1.2.0.0         255.255.0.0    1          advertise      Yes
2.3.0.0         255.255.0.0    16777215   advertise      No
```

Table 67 Description of the fields of the display ospf abr-summary command

Fields	Description	
Network	Destination network segment	
Mask	Mask	
Cost	Cost of summary route	
Status	Status information. Which can be:	
	not-Advertise	Summary route information to this network segment will not be advertised
	advertise	Summary route information to this network segment will be advertised
Used	Status information. Which can be:	
	Yes	The configuration of summary route to this network segment includes match route
	No	The configuration of summary route to this network segment does not include match route

display ospf graceful-restart status

Syntax

display ospf [*process-id*] **graceful-restart status**

View

Any View

Parameter

process-id: ID of an OSPF process. If the process ID is not specified, the major information about all the OSPF processes will be displayed in the order in which IDs are configured.

Description

Use the **display ospf graceful-restart status** command to display the information about OSPF Graceful Restart. .

Example

Display the information about OSPF Graceful Restart.

```
<SW8800> display ospf graceful-restart status
                 OSPF Process 1 with Router ID 30.1.1.1
                              Restart Status
Restart Mode          : Compatible
Restart Status       : Help Restart
Help NBR Number      : 1
     NBR ID           : 91.1.1.1
OOB NBR Number       : 1
     NBR ID           : 91.1.1.1

                 OSPF Process 2 with Router ID 10.1.1.1
                              Restart Status
Restart Mode          : Standard
Restart Interval     : 120
Restart Status        : Help Restart
Help NBR Number      : 1
     NBR ID            : 10.1.1.2
```

Display the information about Graceful Restart of OSPF 1.

```
<SW8800> display ospf 1 graceful-restart status
                 OSPF Process 1 with Router ID 30.1.1.1
                              Restart Status
Restart Mode          : Compatible
Restart Status       : Help Restart
Help NBR Number      : 1
     NBR ID           : 91.1.1.1
OOB NBR Number       : 1
     NBR ID           : 91.1.1.1
```

display ospf vlink

Syntax

display ospf [*process-id*] **vlink**

View

Any view

Parameter

process-id: ID of an OSPF process. The command is applied to all current OSPF processes if you do not specify a process ID.

Description

Use the **display ospf vlink** command to view the information about OSPF virtual links.

Example

View OSPF virtual links information.

```
<SW8800> display ospf vlink
OSPF Process 1 with Router ID 1.1.1.1
Virtual Links
 Virtual-link Neighbor-id  -> 2.2.2.2, State: Full
   Cost: 0 State: Full    Type: Virtual
   Transit Area: 0.0.0.2
   Timers: Hello 10, Dead 40, Poll 0, Retransmit 5, Transmit Delay 1
```

Table 68 Description of the fields of the display ospf vlink command

Field	Description	
Virtual-link Neighbor-id	Router ID of virtual-link neighbor router	
State	State	
Interface	IP address the interface on the virtual link	
Cost	Route cost of the interface	
Type	Type: virtual link	
Transit Area	ID of transit area that the virtual link passes, and it cannot be backbone area, Stub area and NSSA area	
Timers	OSPF timers, defining as follows:	
	Hello	Interval of Hello packet
	Dead	Interval of dead neighbors
	Poll	Interval of poll
	Retransmit	Interval for retransmitting LSA on the interface
Transmit Delay	Delay time of transmitting LSA on the interface	

filter-policy export

Syntax

filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [*routing-protocol*]

undo filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name*} **export** [*routing-protocol*]

View

OSPF view

Parameter

acl-number: Number of a basic or advanced access control list.

ip-prefix-name: Name of the address prefix list used for filtering the destination addresses in routing information.

routing-protocol: Protocol advertising the routing information, including **direct**, **isis**, **bgp**, **rip** and **static** at present.

Description

Use the **filter-policy export** command to configure the rule used by OSPF to filter advertised routing information.

Use the **undo filter-policy export** command to cancel the filtering rules that have been set.

By default, no filtering of the advertised routing information is performed.

In some cases, it may be required that only the routing information meeting some conditions can be advertised. Then, the **filter-policy** command can be used to set the filtering conditions for the routing information to be advertised. Only the routing information passing the filtration can be advertised.

This command takes effect on the routes imported by OSPF using the **import-route** command. If the *routing-protocol* argument is specified, only the routes imported from this specified protocol are filtered. If the *routing-protocol* argument is not specified, all imported routes are filtered.

Related command: **acl**, **ip ip-prefix**.

Example

Configure OSPF to advertise only the routing information permitted by acl 2000.

```
[SW8800] acl number 2000
[3Com-acl-basic-2000] rule permit source 11.0.0.0  0.255.255.255
[3Com-acl-basic-2000] rule deny source any
[3Com-ospf-1] filter-policy 2000 export
```

filter-policy export

Syntax

filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name* } **export**

undo filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name*} **export**

View

OSPF area view

Parameter

acl-number: Specifies the number of the basic or advanced ACL used for filtering Type-3 LSAs.

ip-prefix-name: Specifies the name of the address prefix list used for filtering Type-3 LSAs.

Description

Use the **filter-policy export** command to set the filter condition for the Type-3 LSAs advertised from an OSPF area.

Use the **undo filter-policy export** command to cancel the set filter condition.

By default, no advertised Type-3 LSA is filtered.

In some situations, it may be required that only some Type-3 LSAs meeting a certain condition be advertised. In this case, you can define a Filter-policy to set the filter condition for advertised Type-3 LSAs so that only the Type-3 LSAs having passed the filtration can be advertised.

Use the **filter-policy export** command to filter the Type-3 LSAs generated locally in an OSPF area so that only those Type-3 LSAs having passed the filtration can be added into the link state database of the other areas. The filtration is implemented according to the link state ID of the Type-3 LSAs.

Related command: **acl**, **ip ip-prefix**.

Example

Configure the filter condition so that the OSPF backbone area advertises only those Type-3 LSAs having passed ACL 2000.

```
[SW8800] acl number 2000
[3Com-acl-basic-2000] rule permit source 11.0.0.0  0.255.255.255
[3Com-acl-basic-2000] rule deny source any
[3Com-ospf-1-area-0.0.0.1] filter-policy 2000 export
```

filter-policy import

Syntax

filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name* | **gateway** *ip-prefix-name* } **import**

undo filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name* | **gateway** *ip-prefix-name* } **import**

View

OSPF view

Parameter

acl-number: Number of a basic or advanced access control list used for filtering the destination addresses of the routing information.

ip-prefix-name: Name of the address prefix list used for filtering the destination addresses of the routing information.

gateway *ip-prefix-name:* Name of the address prefix list used for filtering the addresses of the neighboring routers advertising the routing information.

Description

Use the **filter-policy import** command to configure the OSPF rules of filtering the routing information received.

Use the **undo filter-policy import** command to cancel the filtering of the routing information received.

By default, no filtering of the received routing information is performed.

In some cases, it may be required that only the routing information meeting some conditions can be received. Then, the **filter-policy** command can be used to set

the filtering conditions for the routing information to be received. Only the routing information passing the filtration can be received.

The **filter-policy import** command is used to filter the routes calculated by OSPF. Only the routes that pass the filter are added into the routing table. The command can filter the routes by next hop or by destination address.

Because OSPF is a link state-based dynamic routing protocol, its routing information is hidden in LSAs. OSPF, however, cannot filter advertised and received LSAs. Compared with the case with vector-based routing protocols, the use of this command is rather limited with OSPF.

Example

Filter the received routing information according to the rule defined by the access control list 2000.

```
[SW8800] acl number 2000
[3Com-acl-basic-2000] rule permit source 20.0.0.0 0.255.255.255
[3Com-acl-basic-2000] rule deny source any
[3Com-ospf-1] filter-policy 2000 import
```

filter-policy import

Syntax

filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name* } **import**

undo filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name* } **import**

View

OSPF area view

Parameter

acl-number: Specifies the number of the basic or advanced ACL used for filtering Type-3 LSAs.

ip-prefix-name: Specifies the name of the address prefix list used for filtering Type-3 LSAs.

Description

Use the **filter-policy import** command to set the filter condition for the Type-3 LSAs received by an OSPF area.

Use the **undo filter-policy import** command to cancel the set filter condition.

By default, no received Type-3 LSA is filtered.

In some situations, it may be required that only some Type-3 LSAs meeting a certain condition be received. In this case, you can define a Filter-policy to set the filter condition for received Type-3 LSAs so that only the Type-3 LSAs having passed the filtration can be received.

Use the **filter-policy import** command to filter the Type-3 LSAs generated locally in an OSPF area so that only those Type-3 LSAs having passed the filtration can be added into the link state database of the other areas. The filtration is implemented according to the link state ID of the Type-3 LSAs.

Related command: **acl**, **ip ip-prefix**.

Example

Filter the received routing information as per the condition defined in ACL 2000.

```
[SW8800] acl number 2000
[3Com-acl-basic-2000] rule permit source 20.0.0.0  0.255.255.255
[3Com-acl-basic-2000] rule deny source any
[3Com-acl-basic-2000] quit
[SW8800] ospf 1
[3Com-ospf-1]area 1
[3Com-ospf-1-area-0.0.0.1] filter-policy 2000 import
```

graceful-restart

Syntax

graceful-restart [*value* | **compatible**]

undo graceful-restart

View

OSPF view

Parameter

value: GR period in the way defined in the RFC3623 standard. It is 120 seconds by default.

compatible: Performs GR in compatible way.

Description

Use the **graceful-restart** [*value*] command to configure the OSPF protocol for the switch to perform GR in the way defined in the RFC3623 standard. The *value* argument specifies the period of GR and it is 40 seconds by default. Use the **graceful-restart compatible** command to configure the OSPF protocol for the switch to perform GR in the compatible way.

Use the **undo graceful-start** command to disable the OSPF GR function.

GR is not supported by default.

The OSPF GR function solves the problem of route oscillation and forwarding break caused by protocol-software-reset on the distributed system where control and forward are separate. This function is an enhanced OSPF function. GR can be implemented in one of the following two ways: the way defined in the RFC3623 standard and the compatible way to interconnect with other vendors.

Example

Specify the OSPF process 2 to perform GR in the way defined in the RFC3623 standard at the period of 300 seconds.

```
<SW8800>system-view
[SW8800] ospf 2
[3Com-ospf-2] graceful-restart 300
```

import-route

Syntax

import-route *protocol* [**cost** *value* | **type** *value* | **tag** *value* | **route-policy** *route-policy-name*]*

undo import-route *protocol*

View

OSPF view

Parameter

protocol: Specifies the source routing protocol that can be imported. At present, it includes **direct**, **rip**, **isis**, **bgp**, **ospf-ase**, **ospf-nssa** and **static**.

cost *value*: Specifies the cost of imported route.

type *value*: Specifies the cost type of imported external routes. The value ranges from 1 to 2.

tag *value*: Specifies the value of tag for imported external routes.

route-policy *route-policy-name*: Configures only to import the routes matching the specified Route-policy.

Description

Use the **import-route** command to import routes from another routing protocol. Use the **undo import-route** command to disable OSPF to import routes from the specified routing protocol.

By default, the routing information of other protocols is not imported.

You are recommended to configure the route type, cost and tag together in one command. Otherwise, the new configuration overwrites the old one.

Example

Specify an imported RIP route as the route of type 2, with the route tag as 33 and the route cost as 50.

```
[3Com-ospf-1] import-route rip type 2 tag 33 cost 50
```

import-route-limit

Syntax

import-route-limit *num*

undo import-route-limit

View

OSPF view

Parameter

num: Specifies the maximum number of exterior routes allowed to be imported.

Description

Use the **import-route-limit** command to set the maximum number of exterior routes allowed to be imported.

Use the **undo import-route** command to restore the default value of the maximum of exterior routes allowed to be imported.

By default, a maximum of 20K exterior routes are allowed to be imported.

Example

Set the maximum number of exterior routes allowed to be imported to 50K.

```
[3Com-ospf-1] import-route-limit 50000
```

log-peer-change

Syntax

log-peer-change

undo log-peer-change

View

OSPF view

Parameter

None

Description

Use the **log-peer-change** command to enable the switch for reporting the OSPF peer changes.

Use the **undo log-peer-change** command to disable the switch for reporting the OSPF peer changes.

The switch for reporting the OSPF peer changes is disabled by default.

Example

Enable the switch for reporting the OSPF peer changes.

```
<SW8800> system-view
[SW8800] ospf
[3Com-ospf-1] log-peer-change
```

network

Syntax

network *ip-address ip-mask*

undo network *ip-address ip-mask*

View

OSPF Area view

Parameter

ip-address: Address of the network segment where the interface resides.

ip-mask: IP address wildcard (similar to the complement of the IP address mask), which also supports IP address mask input.

Description

Use the **network** command to configure the interfaces running OSPF.

Use the **undo network** command to cancel the interfaces running OSPF.

By default, interfaces do not belong to any OSPF area.

With the two parameters, *ip-address* and *ip-mask*, one or more interfaces can be configured as an area. To run the OSPF protocol on one interface, the main IP address of this interface must belong to the network segment specified by this command. If only the secondary IP address of the interface is in the range of the network segment specified by this command, this interface will not run OSPF.

Related command: **ospf**.

Example

Specify the interfaces whose main IP addresses are in the segment range of 10.110.36.0 to run OSPF and specify the number of the OSPF area (where these interfaces are located) as 6.

```
[3Com-ospf-1] area 6
[3Com-ospf-1-area-0.0.0.6] network 10.110.36.0.0 0.0.0.255
```

nssa

Syntax

nssa [**default-route-advertise**] [**no-import-route**] [**no-summary**]*

undo nssa

View

OSPF area view

Parameter

default-route-advertise: Imports default route to NSSA area.

no-import-route: Configures not to import route to NSSA area.

no-summary: ABR is disabled to transmit Summary_net LSAs to the NSSA area.

Description

Use the **nssa** command to configure the type of an OSPF area as a NSSA area.

Use the **undo nssa** command to cancel the function.

By default, NSSA area is not configured.

For all the routers connected to the NSSA area, the command **nssa** must be used to configure the area as the NSSA attribute.

The **default-route-advertise** keyword is used to generate default type-7 LSA. No matter whether there is route 0.0.0.0 in routing table on ABR, type-7 LSA default

route will be generated always. Only when there is route 0.0.0.0 in routing table on ASBR, will type-7 LSA default route be generated.

On ASBR, the **no-import-route** keyword enables the external route imported by OSPF through **import-route** command not to be advertised to NSSA area.

Example

Configure area 1 as a NSSA area.

```
[3Com-ospf-1] area 1
[3Com-ospf-1-area-0.0.0.1] network 36.0.0.0 0.255.255.255
[3Com-ospf-1-area-0.0.0.1] nssa
```

ospf

Syntax

ospf [*process-id* [**router-id** *router-id* | **vpn-instance** *vpn-instance-name*]]

undo ospf [*process-id*]

View

System view

Parameter

process-id: ID of an OSPF process, in the range 1 to 65,535. By default, the process ID is 1. *process-id* is locally significant.

router-id: Router ID in dotted decimal format for the specified OSPF process.

vpn-instance: Specifies VPN instance parameter.

vpn-instance-name: VPN instance name.

Description

Use the **ospf** command to enable the OSPF protocol.

Use the **undo ospf** command to disable the OSPF protocol.

After starting OSPF protocol, the user can make the corresponding configuration in the OSPF protocol view.

By default, the system does not run the OSPF protocol.

Related command: **network**.

Example

Enable the running of the OSPF protocol.

```
[SW8800] router id 10.110.1.8
[SW8800] ospf
[3Com-ospf-1]
```

Enable the running of the OSPF protocol with process ID specified as 120.

```
[SW8800] router id 10.110.1.8
[SW8800] ospf 120
[3Com-ospf-120]
```

Enable the OSPF process 120, bind the VPN instance and run the OSPF protocol.

```
[SW8800] ospf 120 router id 9.9.9.9 vpn-instance vpn9
[3Com-ospf-120]
```

ospf authentication-mode

Syntax

ospf authentication-mode { **simple** *password* | **md5** *key-id key* }

undo ospf authentication-mode { **simple** | **md5** }

View

Interface view

Parameter

simple *password:* Enables plain text authentication and specifies a password not exceeding 8 characters.

key-id: ID of the authentication key in MD5 authentication mode in the range from 1 to 255.

key: MD5 authentication key. If it is input in a plain text form, MD5 *key* is a character string in the range 1 to 16 characters. It will be displayed in a cipher text form in a length of 24 characters when the **display current-configuration** command is executed. Inputting the MD5 *key* in a cipher text form with 24 characters is also supported.

Description

Use the **ospf authentication-mode** command to configure the authentication mode and key between adjacent routers.

Use the **undo ospf authentication-mode** command to cancel the authentication key that has been set.

By default, the interface does not authenticate OSPF packets.

The passwords for authentication keys of the routers on the same network segment must be identical. In addition, using the **authentication-mode** command, you can set the authentication type of the area so as to validate the configuration.

Related command: **authentication-mode**.

Example

Set the area 1 where the network segment 131.119.0.0 of Interface Vlan-interface 1 is located to support MD5 cipher text authentication. The authentication key identifier is set to 15 and the authentication key is 3Com.

```
[3Com-ospf-1] area 1
[3Com-ospf-1-area-0.0.0.1] network 131.119.0.0 0.0.255.255
[3Com-ospf-1-area-0.0.0.1] authentication-mode md5
[3Com-Vlan-interface1] ospf authentication-mode md5 15 3Com
```

ospf cost

Syntax

ospf cost *value*

undo ospf cost

View

Interface view

Parameter

value: Cost for running OSPF protocol, ranging from 1 to 65,535.

Description

Use the **ospf cost** command to configure different message sending costs so as to send messages from different interfaces.

Use the **undo ospf cost** command to restore the default cost.

For 3Com Switch 8800 Family Series Routing Switches, the default cost for running OSPF protocol on the VLAN interface is 10.

Example

Specify the cost spent when an interface runs OSPF as 33.

```
[SW8800] interface Vlan-interface 10
[3Com-Vlan-interface10] ospf cost 33
```

ospf dr-priority

Syntax

ospf dr-priority *value*

undo ospf dr-priority

View

Interface view

Parameter

value: Interface priority for electing the "designated router", ranging from 0 to 255. The default value is 1.

Description

Use the **ospf dr-priority** command to configure the priority for electing the "designated router" on an interface.

Use the **undo ospf dr-priority** command to restore the default value.

The priority of the interface determines the qualification of the interface when the "designated router" is elected. The interface with higher priority will be considered first when vote collision occurs.

Example

Set the priority of the interface Vlan-interface 10 to 8, when electing the DR.

```
[SW8800] interface Vlan-interface 10
[3Com-Vlan-interface10] ospf dr-priority 8
```

ospf mib-binding

Syntax

ospf mib-binding *process-id*

undo ospf mib-binding

View

System view

Parameter

process-id: ID of an OSPF process, in the range 1 to 65,535. If no OSPF process is specified, the default process ID 1 applies.

Description

Use the **ospf mib-binding** command to bind the MIB operation to the specified OSPF process.

Use the **undo ospf mib-binding** command to restore the default.

When OSPF protocol enables the first process, it always binds MIB operation to this process. You can use this command to bind MIB operation to another OSPF process. Execute the **undo ospf mib-binding** command if you want to cancel the setting. OSPF will automatically re-bind MIB operation to the first process that it enables.

By default, MIB operation is bound to the first enabled OSPF process.

Example

Bind MIB operation to OSPF process 100.

```
[SW8800] ospf mib-binding 100
```

Restore the default MIB binding.

```
[SW8800] undo ospf mib-binding
```

ospf mtu-enable

Syntax

ospf mtu-enable

undo ospf mtu-enable

View

Interface view

Parameter

None

Description

Use the **ospf mtu-enable** command to enable the interface to write MTU value when sending DD packets.

Use the **undo ospf mtu-enable** command to restore the default settings.

By default, The MTU value is 0 when the interface sends DD packets, i.e. the actual MTU value of the interface is not written.

Database Description (DD) packets are used to describe its own LSDB when the router running OSPF protocol is synchronizing the database.

The default MTU value of DD packet is 0. With this command, the specified interface can be set manually to write the MTU value area in DD packets when sending DD packets, namely, the actual MTU value of the interface is written in.

Example

Set interface Vlan-interface 3 to write MTU value field when sending DD packets.

```
[SW8800] interface Vlan-interface 3
[3Com-Vlan-interface3] ospf mtu-enable
```

ospf network-type

Syntax

ospf network-type { **broadcast** | **nbma** | **p2mp** | **p2p** }

undo ospf network-type

View

Interface view

Parameter

broadcast: Changes the interface network type to broadcast.

nbma: Changes the interface network type to NBMA.

p2mp: Changes the interface network type to **p2mp**.

p2p: Changes the interface network type to point-to-point.

Note: Due to the media type used on the Switch 8800, Broadcast is the only valid option.

Description

Use the **ospf network-type** command to configure the network type of OSPF interface. Use the **undo ospf network-type** command to restore the default network type of the OSPF interface.

- Broadcast: If Ethernet or FDDI is adopted, OSPF defaults the network type to broadcast.

Related command: **ospf dr-priority**.

ospf timer dead

Syntax

ospf timer dead { *seconds* | **minimal multi-hello** *packets* }

undo ospf timer dead [**minimal multi-hello**]

View

Interface view

Parameter

seconds: Dead interval of the OSPF neighbor. It is in seconds and ranges from 1 to 65,535.

minimal: Specifies the port to run Fast Hello function.

multi-hello: Sends multiple hello packets.

packets: Number of Hello packets sent within one second.

Description

Use the **ospf timer dead** command to configure the dead interval of the OSPF peer. Use the **undo ospf timer dead** command to restore the default value of the dead interval of the peer.

By default, the dead interval for the OSPF peers of **broadcast** interfaces are 40 seconds.

The dead of OSPF peers means that within this interval, if no Hello packet is received from the peer, the peer will be considered to be invalid. The value of **dead** *seconds* should be at least four times that of the **Hello** *seconds*. The **dead** *seconds* for the routers on the same network segment must be identical.

Related command: **ospf timer hello**.

Use the **ospf timer dead minimal multi-hello** *packets* command to set Fast Hello function on the port. The fixed dead interval is 1. The *packets* argument is the specified number of sent Hello packets.

Example

Set the peer dead timer on the interface Vlan-interface 10 to 80 seconds.

```
[SW8800] interface Vlan-interface 10
[3Com-Vlan-interface10] ospf timer dead 80
```

Configure the number of Hello packets sent on the port Vlan-interface 10 within three seconds.

```
[SW8800] interface Vlan-interface 10
[3Com-Vlan-interface10] ospf timer dead minimal multi-hello 3
```

ospf timer hello

Syntax

ospf timer hello *seconds*

undo ospf timer hello

View

Interface view

Parameter

seconds: Interval in seconds for an interface to transmit hello packet. It ranges from 1 to 255.

Description

Use the **ospf timer hello** command to configure the interval for transmitting Hello packets on an interface.

Use the **undo ospf timer hello** command to restore the interval to the default value.

By default, the interval is 10 seconds for an interface of **broadcast** type to transmit Hello packets.

Related command: **ospf timer dead**.

Example

Configure the interval for transmitting Hello packets on the interface Vlan-interface 10 to 20 seconds.

```
[SW8800] interface Vlan-interface 10
[3Com-Vlan-interface10] ospf timer hello 20
```

ospf timer retransmit

Syntax

ospf timer retransmit *interval*

undo ospf timer retransmit

View

Interface view

Parameter

interval: Interval in seconds for re-transmitting LSA on an interface. It ranges from 1 to 65,535. The default value is 5 seconds.

Description

Use the **ospf timer retransmit** command to configure the interval for LSA re-transmitting on an interface.

Use the **undo ospf timer retransmit** command to restore the default interval value for LSA re-transmitting on the interface.

If a router running OSPF transmits a "link state advertisement" (LSA) to the peer, it needs to wait for the acknowledgement packet from the peer. If no acknowledgement is received from the peer within the LSA retransmit, this LSA will be re-transmitted. This command can change the interval of re-transmitting LSA. However, according to RFC2328, the LSA retransmit between adjacent routers should not be set too short. Otherwise, unexpected re-transmission will be caused.

Example

Specify the retransmit for LSA transmitting between the interface Vlan-interface 10 and the adjacent routers to 12 seconds.

```
[SW8800] interface Vlan-interface 10
[3Com-Vlan-interface10] ospf timer retransmit 12
```

ospf trans-delay

Syntax

ospf trans-delay *seconds*

undo ospf trans-delay

View

Interface view

Parameter

seconds: Transmitting delay of LSA on an interface. It ranges from 1 to 3600. By default, the value is 1 second.

Description

Use the **ospf trans-delay** command to configure the LSA transmitting delay on an interface.

Use the **undo ospf trans-delay** command to restore the default value of the LSA transmitting delay on an interface.

LSA will age in the "link state database" (LSDB) of the router as time goes by (add 1 for every second), but it will not age during network transmission. Therefore, it is necessary to add a period of time set by this command to the aging time of LSA before transmitting it.

Example

Specify the trans-delay of transmitting LSA on the interface Vlan-interface 10 as 3 seconds.

```
[SW8800] interface Vlan-interface 10
[3Com-Vlan-interface10] ospf trans-delay 3
```

preference

Syntax

preference [**ase**] *value*

undo preference [**ase**]

View

OSPF view

Parameter

value: OSPF protocol route preference, ranging from 1 to 255.

ase: Indicates the preference of an imported external route of the AS.

Description

Use the **preference** command to configure the preference of an OSPF protocol route. Use the **undo preference** command to restore the default value of the OSPF protocol route.

By default, the preference of an OSPF protocol internal route is 10 and the preference of an external route is 150.

Because multiple dynamic routing protocols could be running on a router, there is the problem of routing information sharing among routing protocols and selection. Therefore, a default preference is specified for each routing protocol. When a route is identified by different protocols, the protocol with a high preference will play a decisive role.

Example

Specify the preference of an imported external route of the AS as 160.

```
[3Com-ospf-1] preference ase 160
```

reset ospf

Syntax

reset ospf [**statistics**] { **all** | *process-id* }

View

User view

Parameter

statistics: Resets OSPF statistics.

all: Resets all OSPF processes.

process-id: ID of an OSPF process. If no OSPF process is specified, all OSPF processes are reset.

Description

Use the **reset ospf all** command to reset all OSPF processes.

Use the **reset ospf** *process-id* command to reset the corresponding OSPF process.

The following are the benefits of the **reset ospf all** command:

- Clear invalid LSA immediately without waiting for LSA timeout.
- If the Router ID changes, a new Router ID will take effect by executing the command.
- Re-elect DR and BDR conveniently.
- OSPF configuration before the restart will not lose.

The system will require the user to confirm whether to re-enable the OSPF protocol after execution of the command.

Example

Reset all the OSPF processes.

```
<SW8800> reset ospf all
```

Reset OSPF process 200.

```
<SW8800> reset ospf 200
```

router id

Syntax

router id *router-id*

undo router id

View

System view

Parameter

router-id: Router ID that is a 32-bit unsigned integer.

Description

Use the **router id** command to configure the ID of a router running the OSPF protocol. Use the **undo router id** command to cancel the router ID that has been set.

By default, if LoopBack interface addresses exist, the system chooses the LoopBack address with the greatest IP address value as the router ID; if no LoopBack interface is configured, then the address of the physical interface with the greatest IP address value will be the router ID.

Router ID is a 32-bit unsigned integer that uniquely identifies a router in an OSPF autonomous system. The user can specify the ID for a router. If the user doesn't specify router ID, the router will automatically select one from configured IP address as the ID of this router. If no IP address is configured for any interface of the router, the router ID must be configured in OSPF view. Otherwise, OSPF protocol cannot be enabled.

When the router ID is configured manually, the IDs of any two routers cannot be same in the autonomous system. So, the IP address of certain interface might as well be selected as the ID of this router.

The modified router ID will not be valid unless OSPF is re-enabled.

Related command: **ospf**.

Example

Set the router ID to 10.1.1.3.

```
[SW8800] router id 10.1.1.3
```

silent-interface

Syntax

silent-interface { **default** | **Vlan-interface** *Vlan-interface-number* }

undo silent-interface { **default** | **Vlan-interface** *Vlan-interface-number* }

View

OSPF view

Parameter

Vlan-interface*:* Specifies the VLAN interface

Vlan-interface-number: Specifies the VALAN interface number.

default: All interfaces.

Description

Use the **silent-interface** command to disable an interface to transmit OSPF packets. Use the **undo silent-interface** command to restore the default setting.

By default, the interface is enabled to transmit OSPF packets.

You can use this command to disable an interface to transmit OSPF packets, so as to prevent the router on some network from receiving the OSPF routing information. On a switch, this command can disable/enable a VLAN interface to send OSPF packets.

Example

Disable interface Vlan-interface 20 to transmit OSPF packets.

```
[3Com-ospf-1] silent-interface Vlan-interface 20
```

Disable all ports from sending OSPF packets.

```
[3Com-ospf-1] silent-interface default
```

sham-link

Syntax

sham-link *source-ip destination*-ip **dead minimal multi-hello** *packets*

undo sham-link *source-ip destination*-ip

View

OSPF area view

Parameter

sham-link: Sham-link link.

source-ip: Source IP address.

destination-ip: Destination IP address.

dead: Dead interval time.

minimal: Sends multiple Hello packets within 1 second. The fixed dead interval is 1 second.

multi-hello: Sends multiple Hello packets.

packets: Number of sent Hello packets, in the range of 3 to 10.

Description

Use the **sham-link** command to run Fast Hello function on the sham-link link, that is, to specify multiple Fast Hello packets to be sent within one second. The default dead interval time is one second.

Example

Specify the sham-link link 1.1.1.1 2.2.2.2 to run Fast Hello Function. The dead interval time is one second. Five Hello packets are sent within one second.

```
[3Com-ospf-1] area 0.0.0.0
[3Com-ospf-1-area-0.0.0.0] sham-link 1.1.1.1 2.2.2.2 dead minimal
multi-hello 5
```

snmp-agent trap enable ospf

Syntax

snmp-agent trap enable ospf [*process-id*] [**ifstatechange** | **virifstatechange** | **nbrstatechange** | **virnbrstatechange** | **ifcfgerror** | **virifcfgerror** | **ifauthfail** | **virifauthfail** | **ifrxbadpkt** | **virifrxbadpkt** | **iftxretransmit** | **viriftxretransmit** | **originatelsa** | **maxagelsa** | **lsdboverflow** | **lsdbapproachoverflow**]

undo snmp-agent trap enable ospf [*process-id*] [**ifstatechange** | **virifstatechange** | **nbrstatechange** | **virnbrstatechange** | **ifcfgerror** | **virifcfgerror** | **ifauthfail** | **virifauthfail** | **ifrxbadpkt** | **virifrxbadpkt** | **iftxretransmit** | **viriftxretransmit** | **originatelsa** | **maxagelsa** | **lsdboverflow** | **lsdbapproachoverflow**]

View

System view

Parameter

process-id: ID of an OSPF process. The command is applied to all current OSPF processes if you do not specify a process ID.

ifstatechange, **virifstatechange**, **nbrstatechange**, **virnbrstatechange**, **ifcfgerror**, **virifcfgerror**, **ifauthfail**, **virifauthfail**, **ifrxbadpkt**, **virifrxbadpkt**, **iftxretransmit**, **viriftxretransmit**, **originatelsa**, **maxagelsa**, **lsdboverflow**, **lsdbapproachoverflow**: Types of TRAP packets that the switch produces in case of OSPF anomalies.

Description

Use the **snmp-agent trap enable ospf** command to enable the OSPF TRAP function. Use the **undo snmp-agent trap enable ospf** command to disable the OSPF TRAP function.

This command cannot be applied to the OSPF processes that are started after the command is executed.

By default, the switch does not send TRAP packets in case of OSPF anomalies.

For detailed configuration of SNMP TRAP, refer to the module "System Management" in this manual.

Example

Enable the TRAP function for OSPF process 100.

```
[SW8800] snmp-agent trap enable ospf 100
```

spf-schedule-interval

Syntax

spf-schedule-interval *interval*

undo spf-schedule-interval

View

OSPF view

Parameter

interval: SPF calculation interval of OSPF, which is in the range of 1 to 10 and is measured in seconds. The default value is five seconds.

Description

Use the **spf-schedule-interval** command to configure the route calculation interval of OSPF.

Use the **undo spf-schedule-interval** command to restore the default setting.

According to the Link State Database (LSDB), the router running OSPF can calculate the shortest path tree taking itself as the root and determine the next hop to the destination network according to the shortest path tree. By adjusting SPF calculation interval, frequent network change can be restrained, which may lead to excessive bandwidth and router resource consumption.

Example

Set the OSPF route calculation interval of 3Com to six seconds.

```
[3Com-ospf-1] spf-schedule-interval 6
```

stub

Syntax

stub [**no-summary**]

undo stub

View

OSPF area view

Parameter

no-summary: ABR is disabled to transmit Summary LSAs to the Stub area.

Description

Use the **stub** command to configure an OSPF area as Stub area.

Use the **undo stub** command to cancel the settings.

By default, no area is set to be a Stub area.

If the router is an ABR, it will send a default route to the connected Stub area. Using the **default-cost** command, you can configure the default route cost value.

In addition, on an ABR, you can configure the **no-summary** argument in the **stub** command to prevent type-3 LSAs from entering the Stub area connected to this ABR.

Related command: **default-cost**.

Example

Set the type of OSPF area 1 to the Stub area.

```
[3Com-ospf-1] area 1
[3Com-ospf-1-area-0.0.0.1] stub
```

vlink-peer

Syntax

vlink-peer *router-id* [**dead** { *seconds* | **minimal multi-hello** *packets* } | **retransmit** *seconds* | **trans-delay** *seconds* | **hello** *seconds* | **simple** *password* | **md5** *keyid key*]*

undo vlink-peer *router-id*

View

OSPF area view

Parameter

route-id: Router ID of virtual link peer.

dead *seconds*: Specifies the interval of dead timer. It ranges from 1 to 8192 seconds. This value must equal the **dead** *seconds* of the router virtually linked to it and must be at least four times of **hello** *seconds*. The default value is 40 seconds.

dead minimal multi-hello *packets*: Specifies the virtual link to run Fast Hello function. The default dead is 1 second. The *packets* argument refers to the number of Hello packets sent within 1 second, in the range of 3 to 10.

retransmit *seconds:* Specifies the interval for re-transmitting the LSA packets on an interface. It ranges from 1 to 8192 seconds. The default value is 5 seconds.

trans-delay *seconds:* Specifies the interval for delaying transmitting LSA packets on an interface. It ranges from 1 to 8192 seconds. By default, the value is 1 second.

hello *seconds*: Specifies the interval for sending Hello packets on an interface. It ranges from 1 to 8,192 (in seconds). This value must equal the **hello** *seconds* value of the router virtually linked to the interface. By default, the value is 10 seconds.

simple *password:* Specifies the simple text authentication password, not exceeding 8 characters, of the interface. This value must equal the authentication key of the virtually linked peer.

keyid: Specifies the MD5 authentication key ID. Its value ranges from 1 to 255. It must be equal to the authentication key ID of the virtually linked peer.

key: Specifies the MD5 authentication key. If it is input in a plain text form, MD5 *key* is a character string in the range 1 to 16 characters. It will be displayed in a cipher text form in a length of 24 characters when the **display current-configuration** command is executed. Inputting the MD5 *key* in a cipher text form with 24 characters is also supported.

Description

Use the **vlink-peer** command to create and configure a virtual link.

Use the **undo vlink-peer** command to cancel an existing virtual link.

According to RFC2328, the OSPF area should be connected with the backbone network. You can use the **vlink-peer** command to keep the connectivity. Virtual link can be regarded as a common OSPF-enabled interface so that you can easily understand why to configure the parameters such as Hello, retransmit, and trans-delay on it.

One thing should be mentioned. When configuring virtual link authentication, the **authentication-mode** command is used to set the authentication mode as MD5 cipher text or simple text on the backbone network.

Related command: **authentication-mode**, **display ospf**.

Example

Create a virtual link to 10.110.0.3 and use the MD5 cipher authentication mode.

```
[3Com-ospf-1] area 10.0.0.0
[3Com-ospf-1-area-10.0.0.0] vlink-peer 10.110.0.3 md5 3 345
```

Specify this virtual link to run Fast Hello function and send five Hello packets.

```
[3Com-ospf-1-area-10.0.0.0] vlink-peer 10.110.0.3 dead minimal
multi-hello 5
```

26 INTEGRATED IS-IS CONFIGURATION COMMANDS

When a switch runs a routing protocol, it can perform the router functions. A router that is referred to in the following or its icon represents a generalized router or an Switch 8800 Family series routing switch running routing protocols. To improve readability, this will not be described in the other parts of the manual.

For the configuration of VPN instance, refer to the MPLS module in *3Com Switch 8800 Family Series Routing Switches Operation Manual*.

Integrated IS-IS Configuration Commands

area-authentication-mode

Syntax

area-authentication-mode { **simple** | **md5** } *password* [**ip** | **osi**]

undo area-authentication-mode { **simple** | **md5** } [**ip** | **osi**]

View

IS-IS view

Parameter

simple: Configures to transmit the password in simple text.

md5: Configures to transmit the password encrypted with MD5 algorithm.

password: Configures a password. If simple authentication is used, the *password* must be a simple-text password. If MD5 authentication is used, the *password* can be a simple-text or a cipher-text password. A simple-text password can be a character string with no more than 16 characters, for example, 3com918. Note that the simple-text password defined for MD5 authentication is displayed in cipher text. A cipher-text password must have 24 characters in cipher text, for example, (TT8F]Y5SQ=^Q'MAF4<1!!.

ip: If this argument is configured, the system checks the corresponding IP field in LSP.

osi: If this argument is configured, the system checks the corresponding OSI field in LSP.

The configuration of **ip** or **osi** authentication password is independent of the real network environment.

Description

Use the **area-authentication-mode** command to configure ISIS to authenticate the received Level-1 routing information packets (LSP, CSNP and PSNP), according to the pre-defined mode and password.

Use the **undo area-authentication-mode** command to configure ISIS not to authenticate the said packets.

In default configuration, the system will not authenticate the received Level-1 routing packets, and there is no password. As the result of this command, no Level-1 routing packets whose area authentication passwords are not consistent with the one set via this command will be received. At the same time, this command will let ISIS insert the area authentication password into all the level-1 routing packets sent by this node, in a certain mode.

Related command: **reset isis all**, **domain-authentication-mode**, **isis authentication-mode**.

Example

Set the area authentication password as "hello" and the authentication type as **simple**.

```
[SW8800] isis
[3Com-isis] area-authentication-mode simple hello
```

cost-style

Syntax

cost-style { **narrow** | **wide** | **wide-compatible** | { **compatible** | **narrow-compatible** } [**relax-spf-limit**] }

undo cost-style

View

IS-IS view

Parameter

narrow: Only receives/sends packets whose cost type is narrow

wide: Only receives/sends packets whose cost type is wide.

compatible: Receives/sends packets whose cost type is narrow or wide.

narrow-compatible: Receives packets whose cost type is narrow or wide, but only sends packets whose cost type is narrow

wide-compatible: Receives packets whose cost type is narrow or wide, but only sends packets whose cost type is wide.

relax-spf-metric: Permits to receive routes whose cost value is larger than 1024. If it is not set, routes whose metrics values are larger than 1024 will be discarded. This setting is only valid for **compatible**, **narrow-compatible** and **wide-compatible**.

Description

Use the **cost-style** command to set the cost type of an IS-IS packet received/sent by the router.

Use the **undo cost-style** command to restore the default settings.

By default, IS-IS only receives/sends packets whose cost type is narrow.

Related command: **isis cost**.

Example

Set IS-IS to receive packets whose cost type is narrow or wide, but only send packets whose cost type is narrow.

```
[SW8800] isis
[3Com-isis] cost-style narrow-compatible
```

debugging isis

Syntax

debugging isis { **adjacency** | **all** | **authentication-error** | **checksum-error** | **circuit-information** | **configuration-error** | **datalink-receiving-packet** | **datalink-sending-packet** | **general-error** | **interface-information** | **memory-allocating** | **receiving-packet-content** | **restart-events** | **self-originate-update** | **sending-packet-content** | **snp-packet** | **spf-event** | **spf-summary** | **spf-timer** | **task-error** | **timer** | **update-packet** }

undo debugging isis { **adjacency** | **all** | **authentication-error** | **checksum-error** | **circuit-information** | **configuration-error** | **datalink-receiving-packet** | **datalink-sending-packet** | **general-error** | **interface-information** | **memory-allocating** | **receiving-packet-content** | **restart-events** | **self-originate-update** | **sending-packet-content** | **snp-packet** | **spf-event** | **spf-summary** | **spf-timer** | **task-error** | **timer** | **update-packet** }

View

User view

Parameter

adjacency: IS-IS adjacency related packets.

all: All IS-IS related debugging information.

authentication-error: IS-IS authentication errors.

checksum-error: IS-IS checksum errors.

circuit-information: Information about IS-IS enabled interface.

configuration-error: IS-IS configuration errors.

datalink-receiving-packet: Data link layer's packets-receiving status.

datalink-sending-packet: Data link layer's packets-sending status.

general-error: IS-IS error information.

interface-information: Information about IS-IS enabled data link layer.

memory-allocating: IS-IS memory allocating status.

receiving-packet-content: Packets received through IS-IS protocol.

restart-events: IS-IS restart events.

self-originate-update: Packets locally updated through IS-IS protocol.

sending-packet-content: Packets sent through IS-IS protocol.

snp-packet: CSNP/PSNP packet of IS-IS.

spf-event: IS-IS SPF events.

spf-summary: Statistics about IS-IS performing SPF calculation.

spf-timer: IS-IS SPF trigger events.

task-error: IS-IS events status.

timer: IS-IS timer.

update-packet: Updated packets through IS-IS protocol.

Description

Use the **debugging isis** command to enable IS-IS debugging.

Use the **undo debugging isis** command to disable the function.

Example

Enable all the information debugging of IS-IS.

```
<SW8800> debugging isis all
```

default-route-advertise

Syntax

default-route-advertise [**route-policy** *route-policy-name*]

undo default-route-advertise [**route-policy** *route-policy-name*]

View

IS-IS view

Parameter

route-policy-name: Name of a route-policy.

Description

Use the **default-route-advertise** command to create the default route of L1, L2 router. Use the **undo default-route-advertise** command to cancel this configuration.

By default, this command uses the L2 router to create the default route. There is another mechanism for L1 routers. Namely, the system discovers the default route

by searching the nearest L1/L2 router. The nearest L1/L2 router can be found by searching the ATT bit in the L1 LSP.

This command can be set on L1 router or L2 router. By default, the route is generated on L2 LSP. If the **apply isis level-1** command is executed in route-policy view, the default route will be generated on L1 LSP. If the **apply isis level-2** command is executed in Route-policy view, the default route will be generated on L2 LSP. If the **apply isis level-1-2** command is executed in route-policy view, the default route will be generated on both L1 LSP and L2 LSP.

Example

Set the router to create the default route in the LSP of correspond level.

```
[3Com-isis] default-route-advertise
```

display isis interface

Syntax

display isis interface [**verbose**]

View

Any view

Parameter

verbose: If this parameter is used, the details of the interface will be displayed.

Description

Use the **display isis interface** command to view the information of the enabled IS-IS interface.

This command displays the information of the enabled IS-IS interface, including interface name, IP address of the interface, link state of the interface and so on. Besides displaying all the information shown by the **display isis interface** command, the **display isis interface verbose** command displays such information about the IS-IS parameters of the interface as CSNP packet broadcast interval, Hello packet broadcast interval and invalid number of Hello packet.

Example

Display the information about the enabled IS-IS interface.

```
<SW8800> display isis interface
Interface       IP Address Id  Link.Sta IP.Sta  MTU  Type  DIS
Vlan-interface1 172.16.1.2 001 Up   Up      1497    L1      Yes
```

Display the details of the IS-IS enabled interface.

```
<SW8800> display isis interface verbose
Interface       IP Address Id  Link.Sta IP.Sta  MTU  Type  DIS
Vlan-interface1 172.16.1.2 001 Up   Up      1497  L1    Yes
  Secondary IP Address        :
  SNPA Address                :  00e0.fc44.5f71
  Csnp Interval               :  L1    10  L2    10
  Hello Interval              :  L1    10  L2    10
  Hold Time                   :  L1    30  L2    30
  Lsp Interval                :        33
  Cost                        :  L1    10  L2    10
```

```
Priority                    :  L1     64  L2     64
Retransmission interval     :          5
```

display isis lsdb

Syntax

display isis lsdb [[**l1** | **l2** | **level-1** | **level-2**] | [[*LSPID* | **local**] | **verbose**]*]*

View

Any view

Parameter

l1 and **Level-1**: Both refer to the link state database of Level-1.

l2 and **level-2**: Both refer to the link state database of Level-2.

LSPID: Specifies the LSPID of the Network-entity-title.

local: Displays the LSP information generated locally.

verbose: Configures to display the verbose information of the link state database.

Description

Use the **display isis lsdb** command to view the link state database of the IS-IS.

Example

Display the information of an LSP.

```
<SW8800> display isis lsdb 0050.0500.5005.00-00
                      IS-IS Level-1 Link State Database

Lsp ID                    Sequence          Holdtime    A_P_O  Checksum
>0050.0500.5005.00-00    0x00000328        780         0_0_0    0xf211
```

display isis mesh-group

Syntax

display isis mesh-group

View

Any view

Parameter

None

Description

Use the **display isis mesh-group** command to view the IS-IS mesh group.

This command is used for displaying the configurations of the mesh-group of the current router interface.

Example

Add Interface Vlan-interface 10 and Interface Vlan-interface 20 running IS-IS into mesh group 100.

```
[3Com-Vlan-interface10] isis mesh-group 100
[SW8800] interface Vlan-interface 20
[3Com-Vlan-interface20] isis mesh-group 100
```

Display the information of IS-IS mesh-group.

```
[3Com-Vlan-interface20] display isis mesh-group
Interface           Mesh-group/Blocked
Vlan-interface 10            100
Vlan-interface 20            100
```

display isis peer

Syntax

display isis peer [**verbose**]

View

Any view

Parameter

verbose: When this parameter is configured, the area address carried in the Hello packet from the neighbor will be displayed. Otherwise, only the universal information will be displayed.

Description

Use the **display isis peer** command to view IS-IS peer information.

The **display isis peer verbose** command yields not only all the outputs of the **display isis peer** command, but also the area address, Uptime and IP address of the directly connected interface of the peer.

Example

Display detailed information about IS-IS neighbors.

```
<SW8800> display isis peer verbose
System ID      Interface           Circuit ID        State HoldTime  Type    Pri
0002.0000.0000 Vlan-interface251   0002.0000.0000.0a Up    6s        L1      64
  Area Address:  00.0001
  IP Address: 192.3.1.3  192.4.1.3  192.5.1.3  192.6.1.3  192.7.1.3  192.8.1.3
192.9.1.3  192.10.1.3  192.11.1.3
  Period: 22:27:42

System ID      Interface           Circuit ID        State HoldTime  Type    Pri
0003.0000.0000 Vlan-interface251   0002.0000.0000.0a Up    22s       L1      64
  Area Address:  00.0001
  IP Address: 192.3.1.2
  Period: 22:31:18
```

View IS-IS peer Information.

```
<SW8800> display isis peer
System ID      Interface          Circuit ID      State HoldTime Type Pri
0002.0000.0000 Vlan-interface251   0002.0000.0000.0a Up    6s        L1      64
0003.0000.0000 Vlan-interface251   0002.0000.0000.0a Up    22s       L1      64
```

display isis route

Syntax

display isis route

View

Any view

Parameter

None

Description

Use the **display isis route** command to view IS-IS routing information. .

Example

View IS-IS routing information.

```
<SW8800> display isis route
ISIS Level - 1 Forwarding Table :

          Type - D -Direct, C -Connected, I -ISIS, S -Static, O -OSPF
                 B -BGP, R -RIP

     Flags: R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set

  Destination/Mask  In.Met     Ex.Met NextHop         Interface         Flags
--------------------------------------------------------------------------------
I 3.3.3.0/24         20             7.7.7.7         Vlan-interface1000 R/-/-
                                    6.6.6.6         Vlan-interface1001
I 0.0.0.0/0          10             7.7.7.7         Vlan-interface1000 R/-/-
                                    6.6.6.6         Vlan-interface1001
D 7.7.7.0/25         10             Direct          Vlan-interface1000 R/L/-
D 6.6.6.0/24         10             Direct          Vlan-interface1001 R/L/-
I 10.1.1.0/24        10             7.7.7.7         Vlan-interface1000 R/-/-
                                    6.6.6.6         Vlan-interface1001
```

display isis spf-log

Syntax

display isis spf-log

View

Any view

Parameter

None

Description

Use the **display isis spf-log** command to view the SPF calculation log information of the IS-IS. .

Example

View the SPF calculation log of IS-IS.

```
<SW8800> display isis spf-log
Details of Level 1 SPF Run:
 --------------------------------------------------------------------------
      Trig.Event                 No.Of Nodes    Duration(ms)    StartTime
    IS_SPFTRIG_LSPCHANGE         2              19              1:12:1
    IS_SPFTRIG_LSPCHANGE         2              19              1:11:58
    IS_SPFTRIG_LSPCHANGE         2              18              1:11:53
    IS_SPFTRIG_CIRC_DOWN         2              19              1:11:46
    IS_SPFTRIG_NEWADJ            2              20              1:11:39
    IS_SPFTRIG_LSPCHANGE         2              19              1:11:35
    IS_SPFTRIG_PERIODIC          3              18              1:3:25
```

```
IS_SPFTRIG_LSPCHANGE          2               22              0:55:51
IS_SPFTRIG_LSPCHANGE          2               18              0:55:46
IS_SPFTRIG_ADJDOWN            2               19              0:55:23
IS_SPFTRIG_NEWADJ             2               18              0:54:16
IS_SPFTRIG_LSPCHANGE          2               20              0:54:12
IS_SPFTRIG_LSPCHANGE          3               19              0:54:7
IS_SPFTRIG_PERIODIC           3               21              0:48:25
IS_SPFTRIG_LSPEXPIRED         3               19              0:34:10
IS_SPFTRIG_PERIODIC           3               19              0:33:25
IS_SPFTRIG_PERIODIC           3               18              0:18:25
IS_SPFTRIG_LSPCHANGE          3               19              0:13:26
IS_SPFTRIG_PERIODIC           3               19              0:3:25
IS_SPFTRIG_LSPCHANGE          2               19              1:12:7
```

domain-authentication-mode

Syntax

domain-authentication-mode { **simple** | **md5** } *password* [**ip** | **osi**]

undo domain-authentication-mode { **simple** | **md5** } [**ip** | **osi**]

View

IS-IS view

Parameter

simple: Configures to transmit the password in plain text.

md5: Configures to transmit the password encrypted with MD5 algorithm.

password: Configures a password. If simple authentication is used, the *password* must be a simple-text password. If MD5 authentication is used, the *password* can be a simple-text or a cipher-text password. A simple-text password can be a character string with no more than 16 characters, for example, 3com918. Note that the simple-text password defined for MD5 authentication is displayed in cipher text. A cipher-text password must have 24 characters in cipher text, for example, (TT8F]Y5SQ=^Q‘MAF4<1!!.

password: Specifies the authentication password which can be a character string with 1 to 16 characters. If **md5** is specified, the password will be displayed in a cipher text form with 24 characters when the **display current-configuration** command is executed. Inputting *password* in a cipher text form with 24 characters is also supported.

ip: If this item is configured, the system checks the configuration of the corresponded field of the IP in LSP.

osi: If this item is configured, the system checks the configuration of the corresponded field of the OSI in LSP.

The configuration of **ip** or **osi** is independent of the real network environment.

Description

Use the **domain-authentication-mode** command to configure the IS-IS routing domain to authenticate the received Level-2 routing packets (LSP, CSNP, PSNP), according to the pre-defined mode and password.

Use the **undo domain-authentication-mode** command to configure IS-IS not to authenticate the said packets.

By default, the system will not authenticate the received level-2 routing packets, and there is no password. By using this command, all the level-2 routing packets, whose domain authentication passwords do not consist with the one set via this command will not be received. At the same time, this command will let IS-IS insert the domain authentication password into all the level-2 routing packets sent by this node, in a certain mode.

Related command: **area-authentication-mode**, **isis authentication-mode**.

Example

When you need to authenticate the level-2 routing packets, you can select the simple mode, and the password is "3com".

```
[SW8800] isis
[3Com-isis] domain-authentication-mode simple 3com
```

filter-policy export

Syntax

filter-policy *acl-number* **export** [*routing-protocol*]

undo filter-policy *acl-number* **export** [*routing-protocol*]

View

IS-IS view

Parameter

acl-number: Specifies the number of the access control list, ranging from 2000 to 3999.

routing-protocol: Specifies the protocols that distribute routing information, including direct, static, rip, bgp, ospf, ospf-nssa and ospf-ase. If it does not specify any protocol, the distributed routes of all the protocols will be filtered.

Description

Use the **filter-policy export** command to configure to filter the routes distributed by IS-IS.

Use the **undo filter-policy export** command to cancel the filtering for the exporting routes.

By default, IS-IS does not filter any distributed routing information.

In some cases, only the routing information meeting the specified conditions will be distributed. You can configure the filter-policy to specify the filter conditions so as to distribute the desired routing information only.

Related command: **filter-policy import**.

Example

Use ACL 2000 to filter all the routes advertised by IS-IS.

```
[3Com-isis] filter-policy 2000 export
```

filter-policy import

Syntax

filter-policy *acl-number* **import**

undo filter-policy *acl-number* **import**

View

IS-IS view

Parameter

acl-number: Specifies the number of the access control list, ranging from 2000 to 3999.

Description

Use the **filter-policy import** command to configure to filter the routes received by IS-IS. Use the **undo filter-policy import** command to configure not to filter the received routes.

By default, IS-IS does not filter the received routing information.

In some cases, only the routing information meeting the specified conditions will be accepted. You can configure the filter-policy to specify the filter conditions so as to accept the desired routing information only.

Related command: **filter-policy export**.

Example

Filter the received routes by using ACL 2000.

```
[3Com-isis] filter-policy 2000 import
```

graceful-restart

Syntax

graceful-restart

undo graceful-restart

View

IS-IS view

Parameter

None

Description

Use the **graceful-restart** command to enable the IS-IS restart signaling process of an IS-IS process.

Use the **undo graceful-restart** command to disable the restart process.

IS-IS restart signals are disabled by default

Example

Enable the restart signaling processes of IS-IS process 1.

```
<SW8800> system-view
[SW8800] isis 1
[3Com-isis-1] graceful-restart
```

graceful-restart interval

Syntax

graceful-restart interval *interval-value*

undo graceful-restart interval

View

IS-IS view

Parameter

interval-value: Interval of restart (expected restart time) in seconds, in the range of 30 to 1800. It is 300 seconds by default.

Description

Use the **graceful-restart interval** command to specify the restart interval.

Use the **undo graceful-restart interval** command to restore the restart interval to the default value.

The restart interval is 300 seconds by default.

Example

Set the restart interval of the IS-IS process 1 to two minutes.

```
<SW8800> system-view
[SW8800] isis 1
[3Com-isis-1] graceful-restart interval 120
```

graceful-restart suppress-sa

Syntax

graceful-restart suppress-sa

undo graceful-restart suppress-sa

View

IS-IS view

Parameter

None

Description

Use the **graceful-restart suppress-sa** command to suppress the suppress-advertisement (SA) bit of the restart TLV.

Use the **undo graceful-restart suppress-sa** command to disable the suppression on the SA bit.

Routers that are started for the first time (excluding routers being restarted) does not maintain the forwarding status. If this router is not started for the first time,

the LSP generated during the last run may still exist in the LSP database of other routers in the network.

Because LSP fragment sequence numbers are initialized when a router is reset, the LSP copy stored in the other routers in the network seems newer than the new LSPs generated after this router is restarted. This will cause temporary black-holes in the network until the router generates its own LSPs in normal update process and delivers these LSPs in the highest sequence number.

When this router is restarted, if neighbors of this router suppress sending adjacency relations to this router until this router delivers the updated LSP, black-holes can be avoided.

By default, the SA bit is not suppressed.

Example

Set to suppress the SA bit in the restart TLV of the ISIS process 1.

```
<SW8800> system-view
[SW8800] isis 1
[3Com-isis-1] graceful-restart suppress-sa
```

ignore-lsp-checksum-error

Syntax

ignore-lsp-checksum-error

undo ignore-lsp-checksum-error

View

IS-IS view

Parameter

None

Description

Use the **ignore-lsp-checksum-error** command to configure the IS-IS to discard LSPs with checksum errors.

Use the **undo ignore-lsp-checksum-error** command to configure the IS-IS to ignore the checksum error of LSP.

By default, the checksum error of LSP is ignored.

After receiving an LSP packet, the local IS-IS will calculate its checksum and compares the result with the checksum in the LSP packet. This process is the checksum authentication over the received LSP. By default, even if the checksum in the packet is found not in consistent with the calculated result, the LSP is processed as normal. However, after not ignoring LSP checksum error is set with the **ignore-lsp-checksum-error** command, the LSP packet will be discarded silently if the checksum error is found.

Example

Discard the LSPs with checksum errors.

```
[3Com-isis] ignore-lsp-checksum-error
```

import-route

Syntax

import-route *protocol* [**cost** *value* | **type** { **external** | **internal** } | [**level-1** | **level-1-2** | **level-2**] | **route-policy** *route-policy-name*]*

undo import-route *protocol* [**cost** *value* | **type** { **external** | **internal** } | [**level-1** | **level-1-2** | **level-2**] | **route-policy** *route-policy-name*]*

View

IS-IS view

Parameter

protocol: Specifies the source protocol for importing the routing information, which can be direct, static, rip, bgp, ospf, ospf-ase, and ospf-nssa.

value: Specifies the metric of the imported route, ranging from 0 to 63.

type: Type of routing cost: **internal** indicates the routing cost in the same area; **external** indicates the routing cost among areas. By default, the routing cost is **internal**.

level-1: Configures to import the route into Level-1 routing table.

level-2: Configures to import the route into Level-2 routing table. If the level is not specified, it defaults to importing the routes into **level-2**.

level-1-2: Configures to import the route into Level-1 and Level-2 routing table.

route-policy *route-policy-name*: Configures to import the routes matching the conditions defined in the specified route-policy only.

Description

Use the **import-route** command to configure IS-IS to import the routing information of other protocols.

Using the **undo import-route** command to disable IS-IS to import routing information from other protocols.

By default, IS-IS does not import the routing information of other protocols.

IS-IS regards all the routes imported into the routing domain as the external routes, which describe the way of routing outside the routing domain.

Related command: **import-route isis level-2 into level-1**.

Example

Import the static route. The cost value is 15.

```
[3Com-isis] import-route static ip cost 15
```

import-route isis level-2 into level-1

Syntax

import-route isis level-2 into level-1 [acl *acl-number*]

undo import-route isis level-2 into level-1 [acl *acl-number*]

View

IS-IS view

Parameter

acl-number: ACL number. It is in the range of 2000 to 3999, which means basic ACLs and advanced ACLs can be used.

Description

Use the **import-route isis level-2 into level-1** command to enable routing information in a Level-2 area to be imported to a Level-1 area.

Use the undo import-route isis level-2 into level-1 command to remove the function.

During routing leak configuration from Level-2 to Level-1, only the routes that are permitted by ACL can be imported to Level-1 area if an ACL has been specified.

By default, routing information in a Level-2 area is not imported to a Level-1 area.

Related command: **import-route**.

Example

Import routing information of a router from a Level-2 area to a Level-1 area through the ACL.

```
[SW8800] isis
[3Com-isis] import-route isis level2 into level1 acl 2100
```

isis

Syntax

isis [*tag*]

undo isis [*tag*]

View

System view

Parameter

tag: The name given to the ISIS process. The name length should be no longer than 128 characters, and it can be 0, which means null.

Description

Use the **isis** command to start the corresponding IS-IS routing process and enter the ISIS view.

Use the **undo isis** command to delete the specified IS-IS routing process.

By default, IS-IS routing process is not started

For the normal operation of the IS-IS protocol, the **isis** command must be used to enable the IS-IS process. Then the **network-entity** command is used to set a Network Entity Title (NET) for the router. And, at last, the **isis enable** command is

used to enable each interface which needs to run an IS-IS process. The IS-IS protocol is actually enabled upon the completion of these configurations.

Only one IS-IS routing process can be started on one router.

Related command: **isis enable**, **network-entity**.

Example

Start an IS-IS routing process, in which the system ID is 0000.0000.0002 and the area ID is 01.0001.

```
[SW8800] isis
[3Com-isis] network-entity 01.0001.0000.0000.0002.00
```

isis authentication-mode

Syntax

isis authentication-mode { **simple** | **md5** } *password* [{ **level-1** | **level-2** } [**ip** | **osi**]]

undo isis authentication-mode { **simple** | **md5** } *password* [{ **level-1** | **level-2** } [**ip** | **osi**]]

View

VLAN interface view

Parameter

simple: Configures to transmit the password in plain text.

md5: Configures to transmit the password encrypted with MD5 algorithm.

password: Configures a password. If simple authentication is used, the *password* must be a simple-text password. If MD5 authentication is used, the *password* can be a simple-text or a cipher-text password. A simple-text password can be a character string with no more than 16 characters, for example, 3com918. Note that the simple-text password defined for MD5 authentication is displayed in cipher text. A cipher-text password must have 24 characters in cipher text, for example, (TT8F]Y5SQ=^Q‘MAF4<1!!.

level-1: Configures authentication password for L1.

level-2: Configures authentication password for L2.

ip: If this item is configured, the system checks the configuration of the corresponded field of the IP in LSP.

osi: If this item is configured, the system checks the configuration of the corresponded field of the OSI in LSP.

The configuration of **ip** or **osi** is independent of the real network environment.

Description

Use the **isis authentication-mode** command to configure the IS-IS to authenticate the Hello packets of the corresponding level, in the specified mode and with the specified password on the IS-IS interface.

Use the **undo isis authentication-mode** command to cancel the authentication and delete the password at the same time.

By default, the password is not set and no authentication is executed.

If the password is set, but no parameter is specified, the default settings are Level-1, plaintext and osi.

Related command: **area-authentication-mode**, **domain-authentication-mode**.

Example

Set the authentication password "tangshi" in plain text for the Level-1 neighboring relationship on Interface Vlan-interface 10.

```
[SW8800] interface Vlan-interface 10
[3Com-Vlan-interface10] isis authentication-mode simple tangshi level-1
```

isis circuit-level

Syntax

isis circuit-level [**level-1** | **level-1-2** | **level-2**]

undo isis circuit-level

View

Interface view

Parameter

level-1: Configures Level-1, instead of Level-2, adjacency on the current interface only.

level-1-2: Configures Level-1-2 adjacency on the current interface.

level-2: Configures Level-2 adjacency on the current interface only.

Description

Use the **isis circuit-level** command to have the Level-1-2 router set up link adjacency with the peer router.

Use the **undo isis circuit-level** command to restore the default setting of the link adjacency on the Level-1-2 router.

By default, the value is **level-1-2**.

This command is only applicable to Level-1-2 routers. If the local router is a Level-1-2 router and it is required to establish a correlation with the peer router on a certain level (Level-1 or Level-2), this command can specify the interface to send and receive Hello packets of this level. Certainly, only one type of Hello packet is sent and received on the point-to-point link. In this way, excessive processing is avoided, and the bandwidth is saved.

Related command: **is-level**.

Example

When interface Vlan-interface 10 is connected with a non-backbone router in the same area, you can set this interface as level-1, prohibiting the sending and receiving of Level-2 Hello packets.

```
[SW8800] interface Vlan-interface 10
[3Com-Vlan-interface10] isis enable
[3Com-Vlan-interface10] isis circuit-level level-1
```

isis cost

Syntax

isis cost value [**level-1** | **level-2**]

undo isis cost [**level-1** | **level-2**]

View

Interface view

Parameter

value: Specifies the link cost used in the SPF calculation of corresponding level. Its range is 1 to 63. By default, the value is 10.

level-1: Indicates that the link cost corresponds to Level-1.

level-2: Indicates that the link cost corresponds to Level-2

Description

Use the **isis cost** command to configure the link cost of this interface when performing SPF calculation.

Use the **undo isis cost** command to restore the default link cost.

If neither Level 1 nor Level 2 is specified in the configuration, Level-1 will be the default value.

The user is recommended to configure the appropriate link cost for all the interfaces. Otherwise, the link cost in the calculation of IS-IS routes cannot reflect the link cost.

Example

Set the link cost of the Level-2 link on Interface Vlan-interface 10 to 5.

```
[SW8800] interface Vlan-interface 10
[3Com-Vlan-interface10] isis cost 5 level-2
```

isis dis-priority

Syntax

isis dis-priority *value* [**level-1** | **level-2**]

undo isis dis-priority [**level-1** | **level-2**]

View

Interface view

Parameter

value: The priority when selecting DIS. Its value ranges 0 to 127, and the default priority is 64.

level-1: Specifies the priority when selecting Level-1 DIS.

level-2: Specifies the priority when selecting Level-2 DIS.

If the level is not specified, the default priority level is Level-1.

Description

Use the **isis dis-priority** command to configure the priority of an interface for the DIS election.

Use the **undo isis dis-priority** command to restore the default priority.

The IS-IS protocol does not concern the concept of backup DIS. The router with the priority 0 can also run for the DIS, which is different from the DR election of OSPF.

Related command: **area-authentication-mode**, **domain-authentication-mode**.

Example

Set the priority of Interface Vlan-interface 10 to 127.

```
[SW8800] interface Vlan-interface 10
[3Com-Vlan-interface10] isis dis-priority 127 level-2
```

isis enable

Syntax

isis enable [*tag*]

undo isis enable [*tag*]

View

Interface view

Parameter

tag: The name given to an IS-IS routing process, when executing the **isis** command in the system view. If not specified, it is null.

Description

Use the **isis enable** command to configure the interface to activate the corresponding IS-IS routing process.

Use the **undo isis enable** command to cancel this designation.

By default, the IS-IS routing process is not enabled on an interface.

For the normal operation of the IS-IS protocol, the **isis** command must be used to enable the IS-IS process. Then the **network-entity** command is used to set a Network Entity Title (NET) for the router. And, at last, the **isis enable** command is

used to enable each interface which needs to run the IS-IS process. The IS-IS protocol is actually enabled upon the completion of these configurations.

Related command: **isis**, **network-entity**.

Example

Create an IS-IS routing process named "3com", and activate this routing process on interface Vlan-interface 10.

```
[SW8800] isis 3com
[3Com-isis] network-entity 10.0001.1010.1020.1030.00
[SW8800] interface Vlan-interface 10
[3Com-Vlan-interface10] isis enable 3com
```

isis mesh-group

Syntax

isis mesh-group { *mesh-group-number* | **mesh-blocked** }

undo isis mesh-group

View

Interface view

Parameter

mesh-group-number: Specifies the mesh group number, ranging from 1 to 4,294,967,295.

mesh-blocked: Configures to block a specified interface, so that it will not flood the received LSP to other interfaces.

Description

Use the **isis mesh-group** command to add an interface to a specified mesh group.

Use the **undo isis mesh-group** command to delete this interface from the mesh group.

By default, the interface does not belong to any mesh group and floods LSP normally.

The interface beyond the mesh group floods the received LSP to other interfaces, following the normal procedure.

The interface joining a mesh group only floods the received LSP to the interfaces beyond the local mesh group.

Make sure to provide some redundancy when adding an interface to a mesh group or blocking it, avoiding the affect to the normal flooding of the LSP due to link failure.

Example

Add Vlan-interface 20 running IS-IS to mesh group 3.

```
[3Com-Vlan-interface20] isis mesh-group 3
```

isis timer csnp

Syntax

isis timer csnp *seconds* [**level-1** | **level-2**]

undo isis timer csnp [**level-1** | **level-2**]

View

Interface view

Parameter

seconds: Specifies the CSNP packet interval on the broadcast network, ranging from 1 to 65535 and measured in seconds. By default, the value is 10 seconds.

level-1: Specifies the Level-1 CSNP packet interval.

level-2: Specifies the Level-2 CSNP packet interval.

Description

Use the **isis timer csnp** command to configure the interval of sending CSNP packets on the broadcast network.

Use the **undo isis timer csnp** command to restore the default value, that is, 10 seconds.

Only DIS can periodically send CSNP packets, therefore, this command is valid only for the router that is selected as the DIS. Furthermore, DIS is divided into level-1 and level-2, and their intervals of sending CSNP packets must be set respectively.

Example

Set the CSNP packet of Level-2 to be transmitted every 15 seconds on the interface Vlan-interface 10.

```
[SW8800] interface Vlan-interface 10
[3Com-Vlan-interface10] isis timer csnp 15 level-2
```

isis timer hello

Syntax

isis timer hello *seconds* [**level-1** | **level-2**]

undo isis timer hello [**level-1** | **level-2**]

View

Interface view

Parameter

seconds: Specifies the Hello interval, ranging from 3 to 255 and measured in seconds. The default value is 10 seconds.

level-1: Specifies the Level-1 Hello interval.

level-2: Specifies the Level-2 Hello interval.

If no level is not specified, the Hello interval is set to Level-1-2, that is, both Level-1 and Level-2 take effect.

Description

Use the **isis timer hello** command to configure the interval of sending Hello packet of the corresponding level.

Use the **undo isis timer hello** command to restore the default value.

On a broadcast link, level-1 and level-2 Hello packets will be sent respectively and their intervals should also be set respectively. Such settings are unnecessary on point-to-point links. The shorter the sending interval is, the more system resources are occupied to send Hello packets. Therefore, the interval should not be too short and should be set according to actual conditions.

Related command: **isis timer holding-multiplier**.

Example

Set the Hello packet of Level-2 to be transmitted every 20 seconds on Interface Vlan-interface 10.

```
[SW8800] interface Vlan-interface 10
[3Com-Vlan-interface10] isis timer hello 20 level-2
```

isis timer hello minimal

Syntax

isis timer hello minimal [**level-1** | **level-2**]

undo isis timer hello minimal [**level-1** | **level-2**]

View

Interface view

Parameter

minimal: Sets the sending interval to the minimum value. In this case, the hold time is 1 second.

level-1: Specifies that the sending interval resulting from this command is for level-1 Hello packets.

level-2: Specifies that the sending interval resulting from this command is for level-2 Hello packets.

If neither **level-1** nor **level-2** is specified, the sending interval is set for both Level-1 and Level-2 Hello packets by default, that is, this command takes effect on both Level-1 and Level-2 Hello packets.

Description

Use the **isis timer hello minimal** command to configure the IS-IS system to send the Hello packets at the corresponding level(s) in Fast Hello Mode. If the number of consecutively sent Hello packets is not specified, the system sends three Hello packets per second.

Use the **undo isis timer hello minimal** command to restore the default setting, that is, 10 seconds.

Related command: **isis timer holding-multiplier**.

isis timer holding-multiplier

Syntax

isis timer holding-multiplier *value* [**level-1** | **level-2**]

undo isis timer holding-multiplier [**level-1** | **level-2**]

View

Interface view

Parameter

value: Number of consecutive Hello packets that haven't been received from the IS-IS neighbor for it to be considered dead. It ranges from 3 to 1000.

level-1: Level-1 IS-IS neighbor.

level-2: Level-2 IS-IS neighbor.

If you do not specify Level-1 or Level-2, the command applies to both Level-1 and Level-2 IS-IS neighbors.

Description

Use the **isis timer holding-multiplier** command to set the number of consecutive Hello packets that haven't been received from the IS-IS neighbor for it to be considered dead.

Use the **undo isis timer holding-multiplier** command to restore the default setting.

By default, an IS-IS neighbor is considered dead if three consecutive Hello packets haven't been received from it.

Given a broadcast network, you may configure this command specific to Level-1 or Level-2 neighbors by specifying the keyword **level-1** or **level-2**.

Given a PPP link, you do not need to specify Level-1 or Level-2, because only one kind of Hello packet is available.

This command virtually specifies a hold-down time. If the local router does not receive any Hello packet from the peer within this time, the peer is considered dead.

The hold-down time is configured on a per-interface basis. Within one area, routers may have different holddown time settings.

To tune the hold-down time on a router, change the Hello timer setting of IS-IS or change the number of consecutive Hello packets that haven't been received from an IS-IS neighbor for it to be considered dead.

Related command: **isis timer hello**.

Example

On Vlan-interface 10, configure that the IS-IS neighbor is considered dead if five consecutive Hello packets haven't been received from it.

```
[SW8800] interface Vlan-interface 10
[3Com-Vlan-interface10] isis timer holding-multiplier 5
```

isis timer lsp

Syntax

isis timer lsp *time*

undo isis timer lsp

View

Interface view

Parameter

time: Specifies the LSP interval, ranging from 1 to 1000 and measured in milliseconds. The default value is 33 milliseconds.

Description

Use the **isis timer lsp** command to configure the interval at which IS-IS sends link-state packets on the interface.

Use the **undo isis timer lsp** command to restore the default setting.

Related command: **isis timer retransmit**.

Example

Set the LSP interval on Interface Vlan-interface 10 to 500 milliseconds.

```
[SW8800] interface Vlan-interface 10
[3Com-Vlan-interface10] isis timer lsp 500
```

timer lsp-generation

Syntax

timer lsp-generation *x y z* [**level-1** | **level-2**]

undo timer lsp-generation [**level-1** | **level-2**]

View

IS-IS view

Parameter

x: Maximum interval (in seconds) for generating LSP. It ranges from 1 to 120 and defaults to 5.

y: Interval (in milliseconds) between each trigger operation and each LSP generation operation. It ranges from 1 to 120,000 and defaults to 5,000.

z: Interval (in milliseconds) between two successive LSP generation operations. It ranges from 1 to 120,000 and defaults to 5,000.

level-1: Sets interval for Level-1 LSP only.

level-2: Sets interval for Level-2 LSP only.

If neither **level-1** nor **level-2** is specified in this command, this command takes effect on both levels by default.

Description

Use the **timer lsp-generation** command to set the time interval to generate LSPs (link state packets).

Use the **undo timer lsp-generation** command to restore the default setting.

When an event occurs, a new LSP needs to be generated for the IS-IS protocol. But the frequent generation of LSPs will result in the occupancy of huge resources and thus decrease the performance of the routing switch. To avoid the great decrease of the performance, an exponent decrement method is adopted for the generation of LSPs. You can set the intervals to generate LSPs as required.

Example

Set the intervals to generate LSPs to 10 500 2500.

```
[3Com-isis] timer lsp-generation 10 500 2500
```

isis timer retransmit

Syntax

isis timer retransmit *seconds*

undo isis timer retransmit

View

Interface view

Parameter

seconds: Specifies the retransmission interval of LSP packets, in the unit of second, in the range from 1 to 300 and the default value is five seconds.

Description

Use the **isis timer retransmit** command to configure the LSP retransmission interval over the point-to-point link.

Use the **undo isis timer retransmit** command to restore the default setting.

Use caution when setting this parameter to avoid unnecessary retransmission.

The response is required when sending LSP packets on the point-to-point link, not the broadcast link, and therefore this command is unnecessary for the broadcast link.

Related command: **isis timer lsp**.

Example

Set the LSP retransmission interval to 10 seconds on Interface Vlan-interface 10.

```
[SW8800] interface Vlan-interface 10
[3Com-Vlan-interface10] isis timer retransmit 10
```

is-level

Syntax

is-level { **level-1** | **level-1-2** | **level-2** }

undo is-level

View

IS-IS view

Parameter

level-1: Configures the router to operate at Level-1, only calculate the intra-area routes and maintain the LSDB of L1.

level-1-2: Configures the router to operate at Level-2, calculate both the L1 and L2 routes and maintain the LSDB of L1 and L2.

level-2: Configures the router to operate at Level-2, only switch L2 LSP and calculate the L2 routes and maintain the LSDB of L2.

Description

Use the **is-level** command to configure the level of the IS-IS router.

Use the **undo is-level** command to restore the default value.

By default, the value is **level-1-2**.

We recommend setting the system Level, when you configure IS-IS.

If there is only one area, you are recommended to set the level of all the routers as Level-1 or Level-2, because it is not necessary for all the routers to maintain two identical databases. You are recommended to set all the routers to Level-2 for convenient future extension, when applying them to IP network.

Related command: **isis circuit-level**.

Example

Set the current router to operate at Level-1.

```
[SW8800] isis
[3Com-isis] is-level level-1
```

log-peer-change

Syntax

log-peer-change

undo log-peer-change

View

IS-IS view

Parameter

None

Description

Use the **log-peer-change** command to log the peer changes.

Use the **undo log-peer-change** command to configure not to log the peer changes.

By default, peer changes log disabled.

After peer changes log is enabled, the IS-IS peer changes will be output on the configuration terminal until the log is disabled.

Example

Configure to output the IS-IS peer changes on the current router.

```
[3Com-isis] log-peer-change
```

md5-compatible

Syntax

md5-compatible

undo md5-compatible

View

IS-IS view

Parameter

None

Description

Use the **md5-compatible** command to set the IS-IS to use the MD5 algorithm which is compatible with that of the other vendors.

Use the **undo md5-compatible** command to return to the defaults.

By default, the system uses the MD5 algorithm in IS-IS which is compatible with that of 3Com.

To authenticate the devices of the vendors other than 3Com using MD5 algorithm in IS-IS, configure this command.

Example

Set the IS-IS to use the MD5 algorithm compatible with that of the other vendors.

```
[SW8800] isis
[3Com-isis] md5-compatible
```

network-entity

Syntax

network-entity network-entity-title

undo network-entity *network-entity-title*

View

IS-IS view

Parameter

network-entity-title: Specify the network entity title in the X...X.XXXX....XXXX.00 format, in which the first "X...X" is the area address, the twelve Xs in the middle is the System ID of the router, and the 00 in the end is SEL.

Description

Use the **network-entity** command to configure the name of Network Entity Title (NET) of the IS-IS routing process.

Use the **undo network-entity** command to delete a NET.

By default, no NET is defined.

NET means the Network Service Access Point (NSAP). An IS-IS NET is 8 to 20 bytes long.

It consists of three parts. Part one is area ID, which is variable (1 to 13 bytes), and the area IDs of the routers in the same area are identical. Part two is system ID (6 bytes) of this router, which must be unique in the whole area and backbone area. Part three, the last byte "SEL", whose value must be "00". Usually, one router can be configured with one NET. When the area is redesigned by combination or separation, after reconfiguration, the correctness and continuity of the routes must be ensured.

Related command: **isis**, **isis enable**.

Example

Specify NET as "10.0001.1010.1020.1030.00", in which the system ID is "1010.1020.1030", area ID is "10.0001".

```
[SW8800] isis
[3Com-isis] network-entity 10.0001.1010.1020.1030.00
```

preference

Syntax

preference *value*

undo preference

View

IS-IS view

Parameter

value: Specifies the preference, ranging from1 to 255. By default, the value is 15.

Description

Use the **preference** command to configure the preference of IS-IS protocol.

Use the **undo preference** command to restore the default value.

Several dynamic routing protocols could run simultaneously on a router. In this case, there is an issue of sharing and selecting the routing information among all the routing protocols. The system sets a preference for each routing protocol. When various routing protocols find the route to the same destination, the protocol with the higher preference will take effect.

Example

Configure the preference of IS-IS as 25.

```
[3Com-isis] preference 25
```

reset isis all

Syntax

reset isis all

View

User view

Parameter

None

Description

Use the **reset isis all** command to reset all the IS-IS data structures.

By default, IS-IS data structure will not be cleared.

This command is used when LSPs need refreshing immediately. For example, after the **area-authentication-mode** and **domain-authentication-mode** commands are executed, the old LSP still remain on the router. This command can be used to clear them.

Related command: **area-authentication-mode**, **domain-authentication-mode**.

Example

Reset all the IS-IS data structures.

```
<SW8800> reset isis all
```

reset isis peer

Syntax

reset isis peer system-id

View

User view

Parameter

system-id: Specifies the system ID of IS-IS neighbor.

Description

Use the **reset isis peer** command to reset the specified IS-IS peer.

By default, the IS-IS neighbor will not be cleared.

This command is used when you want to reconfigure a certain neighbor.

Example

Clear the IS-IS neighbor whose system ID is 0000.0c11.1111.

```
<SW8800> reset isis peer 0000.0c11.1111
```

set-overload

Syntax

set-overload

undo set-overload

View

IS-IS view

Parameter

None

Description

Use the **set-overload** command to set overload flag for the current router.

Use the **undo set-overload** command to cancel the overload flag.

By default, no overload flag is set.

If a router is configured with the overload flag, the routes it calculates will be ignored by other routers in SPF calculation. (However the directly connected routes will not be ignored.) And other routers should not send this router the packets which should be forwarded by it.

Example

Set overload flag on the current router.

```
[3Com-isis] set-overload
```

silent-interface

Syntax

silent-interface *silent-interface-type silent-interface-number*

undo silent-interface *silent-interface-type silent-interface-number*

View

IS-IS view

Parameter

silent-interface-type: Specifies the interface type.

silent-interface-number: Specifies the interface number.

Description

Use the **silent-interface** command to disable a specified interface to transmit IS-IS packet.

Use the **undo silent-interface** command to enable the interface to transmit IS-IS packet.

By default, all the interface are allowed to transmit/receive IS-IS packets.

The **silent-interface** command is only used to suppress the packets to be transmitted on the interface, but the routes of this interface will still be transmitted from other interfaces.

Example

Prohibit the IS-IS packets to be transmitted via Interface Vlan-interface 3.

```
[3Com-isis] silent-interface Vlan-interface 3
```

spf-delay-interval

Syntax

spf-delay-interval *number*

undo spf-delay-interval

View

IS-IS view

Parameter

number: Specifies number of routes to process before releasing CPU. It is in unit of piece with the range from 1000 to 50000. By default, the value is 2500 pieces.

Description

Use the **spf-delay-interval** command to configure the number of routes to process before releasing CPU in the SPF calculation.

Use the **undo spf-delay-interval** command to restore the default setting.

When there are a large number of routes in the routing table, this command can be used to set that CPU resources are released automatically after a certain number of routes are processed. The unprocessed routes will be processed in one second. In this way, SPF calculation will not occupy the system resources for a long time, which has impact on the responding speed of the console.

The value of the *number* argument can be adjusted according to the capacity of the routing table. If the **spf-slice-size** command is also configured, the SPF calculation will be paused when any setting item is met.

By default, CPU is released once when every 2500 pieces of routes are processed.

Related command: **spf-slice-size**.

Example

Set IS-IS to release CPU once after processing every 3000 pieces of routes.

```
[3Com-isis] spf-delay-interval 3000
```

spf-slice-size

Syntax

spf-slice-size *seconds*

undo spf-slice-size

View

IS-IS view

Parameter

seconds: Duration of one cycle in seconds of SPF calculation in the range from 0 to 120. When the calculation duration time reaches or exceeds the set value, the calculation of this time ends. If *seconds* is set to 0, it indicates that SPF calculation is not divided into slices and it will operate until the end. By default, the value is 0.

Description

Use the **spf-slice-size** command to enable IS-IS to calculate SPF routes in slices and configure the duration of each calculation.

Use the **undo spf-slice-size** command to restore the default setting.

When there are a large number of routes in the routing table, this command can be used to enable the SPF calculation in slices to prevent it from occupying the system resources for a long time.

The user is recommended to use the command when the number of routes reaches 150,000 or 200,000 and the value of seconds is recommended as 1. In other cases, the default setting should be used, that is, SPF runs to the end with no slice.

If the **spf-delay-interval** command is also configured, when SPF calculation is run, the SPF calculation will be paused if any setting item is met.

Related command: **spf-delay-interval**.

Example

Set the SPF duration time to one second.

```
[3Com-isis] spf-slice-size 1
```

summary

Syntax

summary *ip-address mask* [**level-1** | **level-1-2** | **level-2**]

undo summary *ip-address mask* [**level-1** | **level-1-2** | **level-2**]

View

IS-IS view

Parameter

ip-address: Summarized network segment address.

mask: Summarized network mask.

level-1: Summarizes the routes imported into Level-1.

level-1-2: Summarizes the routes imported into Level-1 and backbone area.

level-2: Summarizes the routes imported into backbone area.

Description

Use the **summary** command to configure to summarize IS-IS routes.

Use the **undo summary** command to cancel the summarization.

By default, no routes will be summarized.

Similarly, the routes with the same next hops can be summarized into one route. In this way, the sizes of the routing table, LSP packets and LSDB are reduced. Among them, the summarized route can be either a route found by IS-IS protocol, or an imported route. Furthermore, the cost value of the summarized route adopts the smallest cost among all the routes summarized.

Example

Set a summarized route of 202.0.0.0/8.

```
[3Com-isis] summary 202.0.0.0 255.0.0.0
```

timer lsp-max-age

Syntax

timer lsp-max-age *seconds*

undo timer lsp-max-age

View

IS-IS view

Parameter

seconds: Specifies the maximum lifetime of LSP, measured in seconds. The range is 1 to 65535. The default value is 1200 seconds.

Description

Use the **timer lsp-max-age** command to configure the maximum lifetime of an LSP generated by the current router.

Use the **undo timer lsp-max-age** command to restore the default value.

When the router generates an LSP for the system, it adds the maximum lifetime to it. When other routers receive this LSP, the lifetime of the LSP decreases continuously as time goes by. When this value reaches zero, the LSP times out. If no update is received before that, the timeout LSP will be deleted from the LSDB.

Related command: **timer lsp-refresh**.

Example

Set the lifetime of an LSP generated by the current system to 25 minutes, i.e., 1500 seconds.

```
[3Com-isis] timer lsp-max-age 1500
```

timer lsp-refresh

Syntax

timer lsp-refresh *seconds*

undo timer lsp-refresh

View

IS-IS view

Parameter

seconds: Specifies the LSP refreshment interval, measured in seconds. The range is 1 to 65535. The default value is 900 seconds.

Description

Use the **timer lsp-refresh** command to configure the refreshment interval of LSP.

Use the **undo timer lsp-refresh** command to restore the default value, that is, 900 seconds.

By this mechanism, the latest synchronization of the LSP within the entire area can be maintained.

Related command: **timer lsp-max-age**.

Example

Set the LSP refresh interval of the current system to 1500 seconds.

```
[3Com-isis] timer lsp-refresh 1500
```

timer spf

Syntax

timer spf *x y z* [**level-1** | **level-2**]

undo timer [**level-1** | **level-2**]

View

IS-IS view

Parameter

x: Maximum interval (in seconds) for SPF calculation. It ranges from 1 to 120 and defaults to 10.

y: Interval (in milliseconds) between a trigger operation and an SPF calculation operation. It ranges from 1 to 120,000 and defaults to 5,500.

z: Interval (in milliseconds) between two successive SPF calculation operations. It ranges from 1 to 120,000 and defaults to 5,500.

level-1: Sets Level-1 SPF calculation interval only.

level-2: Sets Level-2 SPF calculation interval only.

If the level is not specified, it defaults to setting Level-1 SPF calculation interval.

Description

Use the **timer spf** command to configure the interval for the SPF calculation of corresponding level.

Use the **undo timer spf** command to restore the system default value.

In IS-IS, when the LSDB of the corresponding level is changed, SPF calculation is required. However, if the SPF calculation is performed too frequently, the system efficiency will be lowered. By setting a proper interval for performing SPF calculation, you can avoid the above situation. This setting can be made according to actual conditions.

Example

Set the SPF calculation interval of the router to 3, 100 and 500 seconds.

```
[3Com-isis] timer spf 3 100 500
```

27
BGP CONFIGURATION COMMANDS

When a switch runs a routing protocol, it can perform the router functions. A router that is referred to in the following or its icon represents a generalized router or an Switch 8800 Family series routing switch running routing protocols. To improve readability, this will not be described in the other parts of the manual.

For the configuration of VPN instance, refer to the MPLS module in *3Com Switch 8800 Family Series Routing Switches Operation Manual*.

BGP Configuration Commands

aggregate

Syntax

aggregate *address mask* [**as-set** | **attribute-policy** *route-policy-name* | **detail-suppressed** | **origin-policy** *route-policy-name* | **suppress-policy** *route-policy-name*]*

undo aggregate *address mask* [**as-set** | **attribute-policy** *route-policy-name* | **detail-suppressed** | **origin-policy** *route-policy-name* | **suppress-policy** *route-policy-name*]*

View

BGP view

Parameter

address: Address of the aggregated route in dotted decimal format.

mask: Network mask of the aggregated route in dotted decimal format.

as-set: Creates a route with segment of AS_SET.

detail-suppressed: Only advertises the aggregated route.

suppress-policy *route-policy-name*: Suppresses the specific route selected and does not advertise part of the specific routes.

origin-policy *route-policy-name*: Selects the originate routes used for aggregation.

attribute-policy *route-policy-name:* Sets the attributes of the aggregated route.

Description

Use the **aggregate** command to establish an aggregated record in the BGP routing table.

Use the **undo aggregate** command to disable the function.

By default, there is no route aggregation.

The keywords are explained as follows:

Table 69 The use of the keywords

Keyword	Use
as-set	Used to produce an aggregated route, whose AS path information includes detailed routes. Use this keyword carefully when many AS paths need to be aggregated, for the frequent change of routes may lead to route vibration.
detail-suppressed	This keyword does not suppress any aggregated route, but it restrains the advertisement of all the specific routes. If only some specific routes are to be restrained, use the **peer filter-policy** command carefully.
suppress-policy	Create an aggregated route with this keyword. At the same time, the advertisement of the specified route is restrained. If you want to restrain some specific routes selectively and leaves other routes still being advertised, use the **if-match** sub-statement of the **route-policy** command.
origin-policy	Selects only the specific routes that are in accordance with route-policy to create an aggregated route.
attribute-policy	Sets aggregated route attributes. The same work can be done by using the **peer route-policy** command, etc.

Example

Create an aggregated record in BGP routing table.

```
[3Com-bgp] aggregate 168.328.0.0 255.255.0.0
```

Balance

Syntax

balance *balance-number*

undo balance

View

BGP view

Parameter

balance-number: Specifies the number of BGP equivalent routes.

Description

Use the **balance** command to set the number of BGP equivalent routes currently supported by the system.

Use the **undo balance** command to restore the default number of BGP equivalent routes.

By default, the system supports one BGP equivalent route.

Example

Set the number of supported BGP equivalent routes to 3.

```
[3Com-bgp] balance 3
```

bgp

Syntax

bgp as-number

undo bgp [*as-number*]

View

System view

Parameter

as-number: The specified local AS number, in the range of 1 to 65535.

Description

Use the **bgp** command to enable BGP and enter the BGP view.

Use the **undo bgp** command to disable BGP.

By default, the system does not run BGP.

This command is used to enable and disable BGP as well as to specify the local AS number of BGP.

Example

Enable BGP.

```
[SW8800] bgp 100
[3Com-bgp]
```

compare-different-as-med

Syntax

compare-different-as-med

undo compare-different-as-med

View

BGP view

Parameter

None

Description

Use the **compare-different-as-med** command to enable comparison of MED values from different AS neighboring routes.

Use the **undo compare-different-as-med** command to disable the comparison.

By default, it is disabled to compare the MED attribute values from the routing paths of different AS peers.

If there are several routes available to one destination address, the route with smaller MED parameter can be selected as the final route item.

Do not use this command unless it is determined that the same IGP and routing selection mode are adopted by different autonomous systems.

Example

[3Com-bgp] compare-different-as-med

confederation id

Syntax

confederation id *as-number*

undo confederation id

View

BGP view

Parameter

as-number: The ID of BGP AS confederation. It is equal to the AS number which contains the AS numbers of multiple sub-ASs. The range is 1 to 65535.

Description

Use the **confederation id** command to configure confederation identifier.

Use the **undo confederation id** command to cancel the BGP confederation specified by *as-number* argument.

By default, the confederation ID is not configured.

Confederation can be adopted to solve the problem of too many IBGP full connections in a large AS domain. The solution is, first dividing the AS domain into several smaller sub-ASs, and each sub-ASs remains full-connected. These sub-ASs form a confederation. Key BGP attributes of the route, such as next hop, MED, local preference, are not discarded across each sub-ASs. The sub-ASs still look like a whole from the point of view of a confederation although these sub-ASs have EBGP relations. This can assure the integrality of the former AS domain, and ease the problem of too many connections in the domain

Related command: **confederation nonstandard**, **confederation peer-as**.

Example

Confederation 9 consists of four sub-ASs, namely, 38, 39, 40 and 41. Here, the peer 10.1.1.1 is an internal member of the AS confederation while the peer 200.1.1.1 is an external member of the AS confederation. For external members, Confederation 9 is a unified AS domain.

```
[SW8800] bgp 41
[3Com-bgp] confederation id 9
[3Com-bgp] confederation peer-as 38 39 40
[3Com-bgp] group Confed38 external
[3Com-bgp] peer Confed38 as-number 38
[3Com-bgp] peer 10.1.1.1 group Confed38
[3Com-bgp] group Remote98 external
```

```
[3Com-bgp] peer Remote98 as-number 98
[3Com-bgp] peer 200.1.1.1 group Remote98
```

confederation nonstandard

Syntax

confederation nonstandard

undo confederation nonstandard

View

BGP view.

Parameter

None

Description

Use the **confederation nonstandard** command to configure the router to be compatible with routers not following RFC1965.

Use the **undo confederation nonstandard** command to disable this function.

By default, it is in accordance with RFC1965.

Related command: **confederation id**, **confederation peer-as**.

Example

AS100 contains routers following nonstandard, which is composed of two sub-ASs, 64000 and 65000.

```
[SW8800] bgp 64000
[3Com-bgp] confederation id 100
[3Com-bgp] confederation peer-as 65000
[3Com-bgp] confederation nonstandard
```

confederation peer-as

Syntax

confederation peer-as *as-number-1* [... *as-number-n*]

undo confederation peer-as [*as-number-1*] [... *as-number-n*]

View

BGP view

Parameter

as-number-1...as-number-n: Sub-AS number. The range is 1 to 65535. This command can configure a maximum of 32 Sub-ASs belonging to a confederation.

Description

Use the **confederation peer-as** command to configure a confederation consisting of which Sub-ASs.

Use the **undo confederation peer-as** command to delete the specified Sub-AS in the confederation.

By default, no autonomous system is configured as a member of the confederation.

Before this command is performed, the confederation ID should be configured by the **confederation id** command. Otherwise this configuration is invalid. The configured ASs in this command are inside the confederation and each AS uses fully meshed network. The confederation appears as a single AS to the routers outside it.

Related command: **confederation nonstandard**, **confederation id**.

Example

Configure the confederation contains AS 2001 and 2002.

```
[3Com-bgp]confederation peer-as 2000 2001
```

dampening

Syntax

dampening [*half-life-reachable half-life-unreachable reuse suppress ceiling*] [**route-policy** *policy-name*]

undo dampening

View

BGP view

Parameter

half-life-reachable: Specifies the semi-dampening when the route is reachable. The range is 1 to 45 minutes. By default, the value is 15 minutes.

half-life-unreachable: Specifies the semi-dampening when the route is unreachable. The range is 1 to 45 minutes. By default, the value is 15 minutes.

reuse: When the penalty is reduced under this value, the route is reused. The range is 1 to 20000. By default, the value is 750.

suppress: When the penalty exceeds this value, the route is suppressed. The range is 1 to 20000. By default, the value is 2000.

ceiling: The upper threshold of the penalty. The range is 1001 to 20000. By default, the value is 16000.

policy-name: Configures route policy name.

If these parameters are not set, their default values will be used.

The parameters are mutually dependent. Once one of these parameters is configured, all other parameters should also be specified.

Description

Use the **dampening** command to make BGP route attenuation valid or modify various BGP route attenuation parameters.

Use the **undo dampening** command to make the characteristics invalid.

By default, no route attenuation is configured.

Related command: **reset dampening**, **reset bgp flap-info**, **display bgp routing-table dampened**, **display bgp routing-table flap-info**.

Example

Modify the BGP route dampening parameters.

```
[3Com-bgp] dampening 15 15 1000 2000 10000
```

debugging bgp

Syntax

debugging bgp { **all** | **event** | **normal** | { **keepalive** | **mp-update** | **open** | **packet** | **route-refresh** | **update** } [**receive** | **send**] [**verbose**] }

undo debugging bgp { **all** | **event** | **normal** | **keepalive** | **mp-update** | **open** | **packet** | **route-refresh** | **update** }

View

User view

Parameter

all: Indicates to enable all BGP information debugging.

event: Indicates to enable BGP event information debugging.

normal: Indicates to enable information debugging of BGP normal functions.

keepalive: Indicates to enable BGP Keepalive packet information debugging.

mp-update: Indicates to enable MBGP Update packet information debugging.

open: Indicates to enable BGP Open packet information debugging.

packet: Indicates to enable BGP packet information debugging.

route-refresh: Indicates to enable BGP route-refresh packet information debugging.

update: Indicates to enable BGP Update packet information debugging.

receive: Information of received packets.

send: Information of sent packets.

verbose: Detailed information.

Description

Use the **debugging bgp all** command to enable all the information debugging of BGP packet and events.

Use the **debugging bgp event** command to enable the information debugging of BGP events

Use the **debugging bgp keepalive** command to enable the information debugging of BGP Keepalive packets.

Use the **debugging bgp packet** command to enable the information debugging of BGP packets.

Use the **undo debugging bgp** command to disable the debugging functions.

Example

Enable the information debugging of BGP packets.

```
<SW8800> debugging bgp packet
```

default local-preference

Syntax

default local-preference *value*

undo default local-preference

View

BGP view

Parameter

value: Default local preference to be configured. The range is 0 to 4294967295. By default, its value is 100.

Description

Use the **default local-preference** command to configure the local preference.

Use the **undo default local-preference** command to restore the default value.

Configuring different local preferences will affect BGP routing selection.

Example

The two routers RTA and RTB in the same autonomous area connect with external autonomous areas. The command can be used to configure the default local preference of RTB as 180 so that the route via RTB is selected first when the same route goes through RTA and RTB at the same time.

```
[3Com-bgp]default local-preference 180
```

default med

Syntax

default med *med-value*

undo default med

View

BGP view

Parameter

med-value: MED value to be specified. The range is 0 to 4294967295. By default, the *med-value* is 0.

Description

Use the **default med** command to configure the default system metric.

Use the **undo default med** command to restore the default metric of the system.

Multi-Exit Discriminators (MED) attribute is the external metric of a route. Different from local preference, MED is exchanged between ASs. However, this attribute is non-transitive. When a router running BGP gets routes with the same destination address but different next hops from different external peers, it selects the route with the smallest MED as the optimum route, provided that all other conditions are the same.

Example

Routers RTA and RTB belong to AS100 and router RTC belongs to AS200. RTC is the peer of RTA and RTB. So the MED of RTA can be configured as 25 to allow RTC to select the route transmitted by RTB first.

```
[3Com-bgp] default med 25
```

default-route imported

Syntax

default-route imported

undo default-route imported

View

BGP view

Parameter

None

Description

Use the **default-route imported** command to allow BGP to import the default routes of other routing protocols.

Use the **undo default-route imported** command to filter their default routes when BGP is importing other routing protocols.

When BGP is importing other routing protocols, BGP does not import their default routes by default.

Example

Configure a static default route.

```
<SW8800> system-view
[SW8800] ip route-static 0.0.0.0 0.0.0.0 NULL 0
```

Import static routes into BGP.

```
[SW8800] bgp 100
[3Com-bgp] import-route static
```

Find out that no static default route is imported into BGP.

```
[3Com -bgp]display bgp routing-table
Routes total: 0
```

Import the default routes of static routing protocols.

```
[3Com-bgp] default-route imported
```

Query the routing table.

```
[3Com-bgp] display bgp routing-table
Flags:   # - valid       ^ - active      I - internal
         D - damped      H - history     S - aggregate suppressed
         B - balance


    Dest/Mask          Next-Hop        Med        Local-pref Origin Path
   ------------------------------------------------------------------------
#^  0.0.0.0            0.0.0.0         0                     INC

  Routes total: 1
```

display bgp group

Syntax

display bgp group [*group-name*]

View

Any view

Parameter

group-name: Specified a peer group.

Description

Use the **display bgp group** command to view the information of peer groups.

Example

View the information of the peer group aaa.

```
<SW8800> display bgp group aaa
Group : aaa  type : external
  as-number : 200
members in this group :
                 10.1.1.1         11.1.1.1
  configuration within the group :
    no export policy route-policy
    no export policy filter-policy
    no export policy acl
    no export policy ip-prefix
    route-policy specified in import policy : aaa
    no import policy filter-policy
    no import policy acl
    no import policy ip-prefix
    no default route produce
```

Table 70 Description of the fields of the display bgp group command

Field	Description
Group	Name of peer group

Table 70 Description of the fields of the display bgp group command

Field	Description
type	Type of peer group: IBGP or EBGP
as-number	AS number of peer group
members in this group	Members in this peer group
route-policy	Name of configured route policy
filter-policy	Configured export and import route filter for BGP
acl	Configured access control list
ip-prefix	Configured IP address prefix list

display bgp network

Syntax

display bgp network

View

Any view

Parameter

None

Description

Use the **display bgp network** command to view the routing information that has been configured.

Example

Display the routing information that has been configured.

```
<SW8800> display bgp network
Network     Mask                Route-policy
133.1.1.0       255.255.255.0   None
112.1.0.0       255.255.0.0     None
```

Table 71 Description of the fields of the display bgp network command

Field	Description
Network	Network address
Mask	Mask
Route-policy	Configured route policy

display bgp paths

Syntax

display bgp paths *as-regular-expression*

View

Any view

Parameter

as-regular-expression: Matched AS path regular expression.

Description

Use the **display bgp paths** command to view the information about AS paths

Example

Display the information about the AS paths.

```
<SW8800> display bgp paths ^600$
Flags: # - valid,   ^ - best,
          D - damped,   H - history,
          I - internal,     S - aggregate suppressed
Id  Hash-Index  References  Aggregator  Origin     As-Path
------------------------------------------------------------------------
6    90              15       <null>      IGP        600
```

Table 72 Description of the fields of the display bgp paths command

Field	Description	
Flags	State flags: # - valid (valid) ^ - best (selected) D - damped (discarded) H - history (history) I - internal (interior gateway protocol) S - aggregate suppressed (suppressed)	
Id	Value of sequence number	
Hash-Index	Value of Hash-index	
References	Count of times that the route is referenced	
Aggregator	Mask length of aggregate route	
Origin	Origin attribute of route, which indicates that the route updates its origin relative to the route originating it from AS. It has three optional values:	
	IGP	The route belongs to inside of AS. BGP treats aggregate route and the route defined by the command **network** as inside of AS, and origin type as IGP.
	EGP	The route is learned from exterior gateway protocol (EGP).
	INC	Short for INCOMPLETE: indicates that the original source of the route information is unknown (learned by other methods). BGP sets the origin of the route imported through other IGP protocols as INCOMPLETE
As-path	AS-path attribute of route, which records all AS areas that the route passes. With it, route loop can be avoided	

display bgp peer

Syntax

display bgp peer [*peer-address*] [**verbose**]

View

Any view

Parameter

peer-address: Specifies the peer to be displayed.

verbose: Displays the detailed information of the peer.

Description

Use the **display bgp peer** command to view the information about BGP peers.

Example

Display the detail information of the peer 201.1.1.2.

```
<SW8800> display bgp peer 201.1.1.2 verbose
Peer: 201.1.1.2+179     Local: 200.1.1.1+1195
         Type: External
         State: Established      Flags: <>
         Expiring Time: 00:02:19
         Last State: OpenConfirm Last Event: RecvKeepAlive
         Last Error: None
         Options: <KeepAll Ttl>
         Peer Version: 4 Peer ID: 201.1.1.2      Local ID: 200.1.1.1
         Active Holdtime: 180s, Keepalive: 60s
         Last traffic (seconds): Received 41     Sent 41 Checked 41
         Input messages: Total 4 Updates 1       Octets 125
         Output messages: Total 4        Updates 1       Octets 148
         Route Queue Timer: unset
         Peer capabilities:
           Route refresh: advertised and received
           Ipv4-family Unicast: advertised and received

  Configuration within the peer :
    no export policy route-policy
    no export policy ip-prefix
    no export policy filter-policy
    no export policy acl
    no import policy route-policy
    no import policy ip-prefix
    no import policy filter-policy
    no import policy acl
    no default route produce
```

Table 73 Description of the fields of the display bgp peer verbose command

Field	Description
Peer	IP address of peer and port number used by the peer to establish TCP connection
Local	IP address and port number used to establish TCP connection of local end
Type	Type of peer: Internal for IBGP, and External for EBGP
State	State of peer
Flags	Flags of peer
Last State	Last state before entering the current state
Last Event	Last event of neighbor state machine
Last Error	Last error of neighbor state machine
Options	Options

display bgp routing-table

Syntax

display bgp routing-table [*ip-address* [*mask*]]

View

Any view

Parameter

ip-address: Destination of the network.

mask: Mask of the network.

Description

Use the **display bgp routing-table** command to view all the BGP routing information.

Example

Display all the BGP routing information.

```
<SW8800> display bgp routing-table
Flags:   # - valid       ^ - active      I - internal
         D - damped      H - history     S - aggregate suppressed
         B - balance

    Dest/Mask          Next-hop        Med        Local-pref Origin As-path
------------------------------------------------------------------------------
#^  129.1.1.0/24       5.5.5.5                               IGP   600
#^  129.1.2.0/24       5.5.5.5                               IGP   600
#^  129.1.3.0/24       5.5.5.5                               IGP   600
#^  129.1.4.0/24       5.5.5.5                               IGP   600
#^  129.1.5.0/24       5.5.5.5                               IGP   600
#^  129.1.6.0/24       5.5.5.5                               IGP   600
#^  129.1.7.0/24       5.5.5.5                               IGP   600
#^  129.1.8.0/24       5.5.5.5                               IGP   600
#^  129.1.9.0/24       5.5.5.5                               IGP   600
#^  129.1.10.0/24      5.5.5.5                               IGP   600
```

Table 74 Description of the fields of the display bgp routing-table command

Field	Description	
Flags	State flags: # - valid (valid) ^ - best (selected) D - damped (discarded) H - history (history) I - internal (interior gateway protocol) S - aggregate suppressed (suppressed) B - balance (equivalent route)	
Dest/Mask	Destination address/Mask	
Next Hop	IP address of next hop	
Med	MULTI_EXIT_DISC attribute value, which ranges from 0 to 4294967295	
Local-Pref	Local preference, which ranges from 0 to 4294967295	
Origin	Origin attribute of route, which indicates that the route updates its origin relative to the route originating it from AS. It has three optional values:	
	IGP	The route belongs to inside of AS. BGP treats aggregate route and the route defined by the command **network** as inside of AS, and origin type as IGP.
	EGP	The route is learned from exterior gateway protocol (EGP).
	INC	Short for INCOMPLETE: indicates that the original source of the route information is unknown (learned by other methods). BGP sets the origin of the route imported through other IGP protocols as INCOMPLETE

Table 74 Description of the fields of the display bgp routing-table command

Field	Description
As-path	AS-path attribute of route, which records all AS areas that the route passes. With it, route loop can be avoided

display bgp routing-table as-path-acl

Syntax

display bgp routing-table as-path-acl *acl-number*

View

Any view

Parameter

acl-number: Specifies matched AS path list number ranging from 1 to 199.

Description

Use the **display bgp routing-table as-path-acl** command to view routes that match an as-path acl.

Example

Display routes that match the as-path-acl 1.

```
<SW8800> display bgp routing-table as-path-acl 1
Flags:     # - valid,         ^ - best,
          D - damped,    H - history,
          I - internal,      S - aggregate suppressed
         B - balance

  Dest/Mask     Pref      Next-Hop       Med      Local-pref    Origin     As-path
------------------------------------------------------------------------------
#^ 1.1.1.0/24      256     10.10.10.1     0                      IGP       200
#^ 1.1.2.0/24      256     10.10.10.1     0                      IGP       200
#^ 1.1.3.0/24      256     10.10.10.1     0                      IGP       200
#^ 2.2.3.0/24      256     10.10.10.1     0                      INC       200
#^ 4.4.4.0/24      256     10.10.10.1     0                      INC       200
#^ 9.9.9.0/24      256     10.10.10.1     0                      INC       200
#^ 10.10.10.0/24   256     10.10.10.1     0                      IGP       200
#^  22.1.0.0/16    256     200.1.7.2     100                     INC       200
#   88.1.0.0/16    60      0.0.0.0                               IGP
```

Table 75 Description of the fields of the display bgp routing-table as-path-acl command

Field	Description
Dest/Mask	Destination address/Mask
Pref	Preference
Nexthop	IP address of next hop
Med	MULTI_EXIT_DISC attribute value
Local-pref	Local preference

Table 75 Description of the fields of the display bgp routing-table as-path-acl command

Field	Description	
Origin	Origin attribute of route, which indicates that the route updates its origin relative to the route originating it from AS. It has three optional values:	
	IGP	The route belongs to inside of AS. BGP treats aggregate route and the route defined by the command **network** as inside of AS, and origin type as IGP.
	EGP	The route is learned from exterior gateway protocol (EGP).
	INC	Short for INCOMPLETE: indicates that the original source of the route information is unknown (learned by other methods). BGP sets the origin of the route imported through other IGP protocols as INCOMPLETE
As-path	AS-path attribute of route, which records all AS areas that the route passes. With it, route loop can be avoided	

display bgp routing-table cidr

Syntax

display bgp routing-table cidr

View

Any view

Parameter

None

Description

Use the **display bgp routing-table cidr** command to view the routing information about the non-natural mask (namely classless interdomain routing, CIDR).

Example

```
<SW8800> display bgp routing-table cidr
Flags:     # - valid,        ^ - best,
          D - damped,   H - history,
          I - internal,     S - aggregate suppressed
       B - balance

       Dest/Mask    Pref     Next-Hop     Med     Local-pref   Origin    As-path
------------------------------------------------------------------------------
 #^  22.1.0.0/16   256      200.1.7.2              100       INC     200
 #   88.1.0.0/16   60       0.0.0.0                          IGP
```

For detailed description of the output information, see Table 74.

display bgp routing-table community

Syntax

display bgp routing-table community [*aa:nn*]* [**no-export-subconfed** | **no-advertise** | **no-export**]* [**whole-match**]

View

Any view

Parameter

aa:nn: Specifies a community number. It can be input up to 13 times.

no-export-subconfed: Does not send matched route outside AS.

no-advertise: Sends matched route to no peers.

no-export: Does not advertise the route to outside the AS or the confederation, but can advertise the route to other sub-Ass in the confederation.

whole-match: Configures to display the exactly matched routes.

Description

Use the **display bgp routing-table community** command to view the routing information related to the specified BGP community number in the routing table.

Example

Display the routing information matching BGP community number 11:22.

```
<SW8800> display bgp routing-table community 11:22
Flags:     # - valid,        ^ - best,
          D - damped,   H - history,
          I - internal,     S - aggregate suppressed
         B - balance

       Dest/Mask    Pref     Next-Hop     Med     Local-pref   Origin    As-path
------------------------------------------------------------------------------
 #^  1.0.0.0/8     256    172.10.0.2                100      IGP
 #^  2.0.0.0/8     256    172.10.0.2                100      IGP
```

For detailed description of the output information, see Table 74.

display bgp routing-table community-list

Syntax

display bgp routing-table community-list *community-list-number* [**whole-match**]

View

Any view

Parameter

community-list-number: Specifies a community-list.

whole-match: Configures to display the exactly matched routes.

Description

Use the **display bgp routing-table community-list** command to view the routing information matching the specified BGP community list.

Example

Display the routing information matching BGP community list 1.

```
[SW8800] display bgp routing-table community-list 1
Flags:     # - valid,        ^ - best,
          D - damped,   H - history,
          I - internal,     S - aggregate suppressed
         B - balance

Destination/Mask  Pref   Next-hop        Med      Local-Pref   Origin  As-Path
------------------------------------------------------------------------------
    1.1.1.0/24    256   10.10.10.1     0                    IGP      200
    1.1.2.0/24    256   10.10.10.1     0                    IGP      200
```

```
1.1.3.0/24     256   10.10.10.1     0                    IGP      200
2.2.3.0/24     256   10.10.10.1     0                    INC      200
4.4.4.0/24     256   10.10.10.1     0                    INC      200
9.9.9.0/24     256   10.10.10.1     0                    INC      200
10.10.10.0/24  0     10.10.10.2     0                    IGP
10.10.10.0/24  256   10.10.10.1     0                    IGP      200
```

For detailed description of the output information, see Table 74.

display bgp routing-table dampened

Syntax

display bgp routing-table dampened

View

Any view

Parameter

None

Description

Use the **display bgp routing-table dampened** command to view BGP dampened routes.

Example

View BGP dampened information.

```
<SW8800> display bgp routing-table dampened
Flags:     # - valid,      ^ - best,
      D - damped,   H - history,
      I - internal,    S - aggregate suppressed
      B - balance

Dest/Mask             Source    Damping-limit   Origin   As-path
------------------------------------------------------------------
#D  11.1.0.0/16       133.1.1.2   1:20:00       IGP      200
```

Table 76 Description of the fields of the display bgp routing-table dampened command

Field	Description
Flags	State flags: # - valid (valid) ^ - best (selected) D - damped (discarded) H - history (history) I - internal (interior gateway protocol) S - aggregate suppressed (suppressed)
#D	The valid and damped route
Dest/Mask	The dampened route to the destination network 11.1.0.0
Source	The nexthop of the route
Damping-limit	The time before dampening turns invalid and the route can be reused.

Table 76 Description of the fields of the display bgp routing-table dampened command

Field	Description	
Origin	Origin attribute of route, which indicates that the route updates its origin relative to the route originating it from AS. It has three optional values:	
	IGP	The route belongs to inside of AS. BGP treats aggregate route and the route defined by the command **network** as inside of AS, and origin type as IGP.
	EGP	The route is learned from exterior gateway protocol (EGP).
	INC	Short for INCOMPLETE: indicates that the original source of the route information is unknown (learned by other methods). BGP sets the origin of the route imported through other IGP protocols as INCOMPLETE
As-path	AS-path attribute of route, which records all AS areas that the route passes. With it, route loop can be avoided	

display bgp routing-table different-origin-as

Syntax

display bgp routing-table different-origin-as

View

Any view

Parameter

None

Description

Use the **display bgp routing-table different-origin-as** command to view routes that have different source autonomous systems

Example

View the routes that have different source ASs.

```
<SW8800> display bgp routing-table different-origin-as
Flags:     # - valid,        ^ - best,
          D - damped,   H - history,
          I - internal,     S - aggregate suppressed
       B - balance

Destination/Mask  Pref   Next-hop       Med       Local-Pref  Origin   As-Path
------------------------------------------------------------------------
   10.10.10.0/24  0      10.10.10.2     0                 IGP
   10.10.10.0/24  256    10.10.10.1     0                 IGP     200
```

For detailed description of the output information, see Table 74.

display bgp routing-table flap-info

Syntax

display bgp routing-table flap-info [**regular-expression** *as-regular-expression* | **as-path-acl** *acl-number* | *network-address* [*mask* [**longer-match**]]]

View

Any view

Parameter

as-regular-expression: The route flap-info matching AS path regular expression.

acl-number: Number of the specified AS path to be matched, ranging from 1 to 199.

network-address: Displays the flap information of this IP address.

mask: Network mask.

longer-match: Shows the route flap-info that is more specific than address, mask.

Description

Use the **display bgp routing-table flap-info** command to view BGP flap-info. If the *network-address mask* arguments are set to 0.0.0.0 0.0.0.0, this command displays the flap statistics of all BGP routes.

Example

Display BGP flap-info.

```
<SW8800> display bgp routing-table flap-info
Flags:     # - valid,         ^ - best,
          D - damped,   H - history,
          I - internal,     S - aggregate suppressed
       B - balance

Dest/Mask         Source  Keepup-time  Damping-limit  Flap-times  Origin  As-path
------------------------------------------------------------------------
#D  11.1.0.0/16 133.1.1.2   48     1:20:30        4           IGP    200
```

Table 77 Description of the fields of the display bgp routing-table flap-info command

Item	Description	
Flags	State flags: # - valid (valid) ^ - best (selected) D - damped (discarded) H - history (history) I - internal (interior gateway protocol) S - aggregate suppressed (suppressed)	
#D	The valid and damped route	
Dest/Mask	The dampened route to the destination network 11.1.0.0	
Source	The nexthop of the route	
Keepup-time	The time that route damping has continued	
Damping-limit	The time before dampening turns invalid and the route can be reused.	
Flap-times	The times of the route flap	
Origin	Origin attribute of route, which indicates that the route updates its origin relative to the route originating it from AS. It has three optional values:	
	IGP	The route belongs to inside of AS. BGP treats aggregate route and the route defined by the command **network** as inside of AS, and origin type as IGP.
	EGP	The route is learned from exterior gateway protocol (EGP).
	INC	Short for INCOMPLETE: indicates that the original source of the route information is unknown (learned by other methods). BGP sets the origin of the route imported through other IGP protocols as INCOMPLETE

Table 77 Description of the fields of the display bgp routing-table flap-info command

Item	Description
As-path	AS-path attribute of route, which records all AS areas that the route passes. With it, route loop can be avoided

display bgp routing-table peer

Syntax

display bgp routing-table peer *peer-address* { **advertised** | **received** } [*network-address* [*mask*] | **statistic**]

View

Any view

Parameter

peer-address: Specifies the peer to be displayed.

advertised: Routing information advertised by the specified peer.

received: Routing information the specified peer received.

network-address mask : IP address and address mask of destination network.

statistic: Statistic routing information of peer.

Description

Use the **display bgp routing-table peer** command to view the routing information the specified BGP peer advertised or received.

Related command: **display bgp peer**.

Example

Display the routing information advertised by BGP peer 10.10.10.1.

```
[SW8800] display bgp routing table peer 10.10.10.1 advertised
Flags:     # - valid,          ^ - best,
          D - damped,         H - history,
          I - internal,      S - aggregate suppressed
         B - balance

Dest/mask         Next -Hop    Med  Local-pref     Origin     As-path
*>  10.10.10.0/24     0.0.0.0                          INC
```

For detailed description of the output information, see Table 74.

display bgp routing-table regular-expression

Syntax

display bgp routing-table regular-expression *as-regular-expression*

View

Any view

Parameter

as-regular-expression: Matched AS regular expression.

Description

Use the **display bgp routing-table regular-expression** command to view the routing information matching the specified AS regular expression

Example

Display the routing information matched with ^600$.

```
<SW8800> display bgp routing-table regular-expression ^600$
Flags:     # - valid,        ^ - best,
          D - damped,   H - history,
          I - internal,     S - aggregate suppressed
        B - balance

Destination/Mask  Pref   Next-hop          Med        Local-Pref  Origin   Path
------------------------------------------------------------------------------
      1.1.1.0/24  256    10.10.10.1        0                  IGP   200
      1.1.2.0/24  256    10.10.10.1        0                  IGP   200
      1.1.3.0/24  256    10.10.10.1        0                  IGP   200
      2.2.3.0/24  256    10.10.10.1        0                  INC   200
      4.4.4.0/24  256    10.10.10.1        0                  IGP   200
      9.9.9.0/24  256    10.10.10.1        0                  INC   200
      10.10.10.0/24 256  10.10.10.1        0                  IGP   200
```

For detailed description of the output information, see Table 74.

display bgp routing-table statistic

Syntax

display bgp routing-table [**advertised** | **received**] **statistic**

View

Any view

Parameter

advertised: Routing information advertised by the peers.

received: Routing information received by the peers.

statistic: The total number of routes advertised or received by the peer.

Description

Use the **display bgp routing-table statistic** command to display the total number of routes advertised or received by all BGP peers.

Related command: **display bgp peer**.

Example

Display the routing information advertised by all BGP peers.

```
<SW8800> display bgp routing-table advertised statistic
Peer: 200.1.7.2+1062
Advertised routes total: 516
Peer: 150.1.1.2+179
Advertised routes total: 346
Peer: 2 133.1.1.2+179
Advertised routes total: 116
```

Display the routing information received by all BGP peers.

```
<SW8800> display bgp routing-table received statistic
Peer: 200.1.7.2+1062
Received routes total: 213
Peer: 150.1.1.2+179
Received routes total: 423
Peer: 2 133.1.1.2+179
Received routes total: 123
```

filter-policy export

Syntax

filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [*routing-protocol*]

undo filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [*routing-protocol*]

View

BGP view

Parameter

acl-number: Number of IP access control list, in the range of 2000 to 3999.

ip-prefix-name: Name of ip prefix list. Its length ranges from 1 to 19.

routing-protocol: Specified protocols advertising routing information which include direct, ospf, ospf-ase, ospf-nssa, rip, isis and static.

Description

Use the **filter-policy export** command to filter the advertised routes and only the routes passing the filter can be advertised by BGP.

Use the **undo filter-policy export** command to cancel the filtration to the advertised routes.

By default, the advertised routes are not filtered.

If the *protocol* argument is specified, only the imported route generated by the specified protocol is filtered and the imported routes generated by other protocols are not affected. If the *protocol* argument is not specified, the imported route generated by any protocol will be filtered.

Example

Use ACL 2000 to filter the routing information advertised by BGP.

```
[3Com-bgp] filter-policy 2000 export
```

filter-policy import

Syntax

filter-policy gateway *ip-prefix-name* **import**

undo filter-policy gateway *ip-prefix-name* **import**

filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name* } **import**

undo filter-policy { *acl-number* | ip-prefix *ip-prefix-name* } **import**

View

BGP view

Parameter

acl-number: Number of IP access control list, in the range of 2000 to 3999.

ip-prefix-name: Name of an address prefix list. It is used for filtering routing information by destination address. Its length ranges from 1 to 19.

gateway *ip-prefix-name*: Name of a peer-router address prefix list. It is used for filtering routing information by peer-router address. Its length ranges from 1 to 19.

Description

Use the **filter-policy gateway import** command to filter the learned routing information advertised by the peer with the specified address.

Use the **undo filter-policy gateway import** command to cancel the filtration to the routing information advertised by the peer with specified address.

Use the **filter-policy import** command to filter the received global routing information. Use the **undo filter-policy import** command to remove the filtration to the received global routing information.

By default, filtration to the received routing information is not configured.

This command can be used to filter the routes received by BGP and determines whether to add the routes to the BGP routing table.

Example

Use ACL 2000 to filter the routing information received by BGP.

```
[3Com-bgp] filter-policy 2000 import
```

group

Syntax

group *group-name* [**internal** | **external**]

undo group *group-name*

View

BGP view

Parameter

group-name: Specifies the name of the peer group. It can consist of numbers or letters with a length ranging from 1 to 47. *group-name* is locally significant.

internal: Specifies the type of the peer group as IBGP.

external: Specifies the type of the peer group as EBGP, including other groups of other sub-ASs in the confederation.

Description

Use the **group** *group-name* command to establish a peer group.

Use the **undo group** *group-name* command to cancel the configured peer group.

The default type of BGP peer group is **internal**.

Rather than existing alone, a BGP peer must belong to a peer group. Therefore, when creating a BGP peer, you must create a BGP peer group first and then add the peer into the group.

All member peers must use the same update policy as the peer group, but they may use different ingress policies.

Example

Create an IBGP group named test.

```
[3Com-bgp] group test
```

import-route

Syntax

import-route *protocol* [**med** *med-value* | **route-policy** *route-policy-name*]

undo import-route *protocol*

View

BGP view

Parameter

protocol: Specifies source routing protocols which can be imported, which include direct, ospf, ospf-nssa , ospf-ase, rip, isis and static at present.

med *med-value*: Specifies the MED value loaded by an imported route, ranging from 0 to 4294967295.

route-policy *route-policy-name*: Specifies a route-policy used for filtering imported routes of other protocols. It can consist of numbers and letters with a length ranging from 1 to 19.

Description

Use the **import-route** command to import routes of other protocols.

Use the **undo import-route** command to cancel importing routes of other protocols.

By default, BGP does not import routes of other protocols.

Note that when BGP is importing other routing protocols, BGP does not import their default routes.

Example

Import routes of RIP.

```
[3Com-bgp] import-route rip
```

network

Syntax

network *ip-address* [*address-mask*] [**route-policy** *route-policy-name*]

undo network *ip-address* [*address-mask*] [**route-policy** *route-policy-name*]

View

BGP view

Parameter

ip-address: Network address that BGP advertises.

address-mask: Mask of the network address.

route-policy-name: Route-policy applied to advertised routes.

Description

Use the **network** command to configure the network routes advertised by the local BGP.

Use the **undo network** command to cancel the existing configuration.

By default, the local BGP does not advertise any routes.

Example

Advertise routes to the network segment 10.0.0.0/16.

```
[3Com-bgp] network 10.0.0.1 255.255.0.0
```

log-peer-change

Syntax

log-peer-change

undo log-peer-change

View

BGP view

Parameter

None

Description

Use the **log-peer-change** command to enable the switch for reporting the BGP peer changes and print the BGP state change messages onto the screen. Use the **undo log-peer-change** command to disable this function.

The switch for reporting BGP peer changes is disabled by default.

Example

Enable the switch for reporting the BGP peer changes.

```
<SW8800> system-view
[SW8800] bgp
```

[3Com-bgp] log-peer-change

peer advertise-community

Syntax

peer *group-name* **advertise-community**

undo peer *group-name* **advertise-community**

View

BGP view

Parameter

group-name: Name of a peer group.

Description

Use the **peer advertise-community** command to enable the transmission of the community attribute to a peer group.

Use the **undo peer advertise-community** command to cancel the existing configuration.

By default, the community attribute is not transmitted to any peer group.

Related command: **if-match community-list**, **apply community**.

Example

Transmit community attribute to the peer group named test.

```
[3Com-bgp] peer test advertise-community
```

peer allow-as-loop

Syntax

peer { *group-name* | *peer-address* } **allow-as-loop** [*number*]

undo peer { *group-name* | *peer-address* } **allow-as-loop**

View

BGP view

Parameter

group-name: Specifies name of the peer group.

peer-address: Specifies IP address of the peer.

number: Specifies the repeating times of local AS, ranging from 1 to 10.

Description

Use the **peer allow-as-loop** command to configure the repeating time of local AS.

Use the **undo peer allow-as-loop** command to remove the repeating time of local AS.

Related command: **display current-configuration**, **display bgp routing-table peer**, **display bgp routing-table group**.

Example

Specify to configure the repeating times of local AS to 2.

```
[3Com-bgp] peer 1.1.1.1 allow-as-loop 2
```

peer as-number

Syntax

peer *group-name* **as-number** *as-number*

undo peer *group-name* **as-number**

View

BGP view

Parameter

group-name: Name of peer group.

as-number: Peer AS number of the peer group, the range is 1 to 65535.

Description

Use the **peer as-number** command to configure the peer AS number of the specified peer group.

Use the **undo peer as-number** command to delete the peer AS number of the specified peer group.

By default, no peer AS number of the specified peer group is configured.

Example

Specify the peer AS number for the peer group test as 100.

```
[3Com-bgp] peer test as-number 100
```

peer as-path-acl export

Syntax

peer *group-name* **as-path-acl** *acl-number* **export**

undo peer *group-name* **as-path-acl** *acl-number* **export**

View

BGP view

Parameter

group-name: Specifies name of the peer group.

acl-number: Number of an AS path list, in the range of 1 to 199.

export: Applies the AS path list to advertised routes.

Description

Use the **peer as-path-acl export** command to configure filtering Policy of BGP advertised routes based on AS path list.

Use the **undo peer as-path-acl** command to cancel the existing configuration.

By default, the peer group has no AS path list.

This command can only be configured on the peer group. The *acl-number* specifies the number of the AS path list. It is configured by the **ip as-path-acl** command rather than the **acl** command.

Related command: **peer as-path-acl import**, **ip as-path-acl**.

Example

Configure to filter the routes advertised by the peer group test using the AS path-list 1.

```
[3Com-bgp] peer test as-path-acl 1 export
```

peer as-path-acl import

Syntax

peer { *group-name* | *peer-address* } **as-path-acl** *acl-number* **import**

undo peer { *group-name* | *peer-address* } **as-path-acl** *acl-number* **import**

View

BGP view

Parameter

group-name: Specifies the name of the peer group.

peer-address: Specifies IP address of the peer, in dotted decimal format.

acl-number: Specifies the filter list number of an AS regular expression. The range is 1 to 199.

import: Applies the AS path list to received routes.

Description

Use the **peer as-path-acl import** command to configure filtering policy of BGP received routes based on AS path list.

Use the **undo peer as-path-acl import** command to cancel the existing configuration.

By default, the peer/peer group has no AS path list.

The priority of the inbound filter policy configured for the peer is higher than that configured for the peer group.

Related command: **peer as-path-acl export**.

Example

Set the AS path ACL of the peer group test to filter BGP received routes.

```
[3Com-bgp] peer test as-path-acl 1 import
```

peer connect-interface

Syntax

peer { *group-name* | *peer-address* } **connect-interface** *interface-type interface-number*

undo peer { *group-name* | *peer-address* } **connect-interface** *interface-type interface-name*

View

BGP view

Parameter

group-name: Specified peer group.

peer-address: IP address of the peer.

interface-type: Interface type.

interface-number: Interface number.

Description

Use the **peer connect-interface** command to specify the source interface of a route update packet.

Use the **undo peer connect-interface** command to restore the best source interface.

By default, BGP uses the best source interface.

Usually, BGP uses the optimal route to update the source interface of the packets. However, you can set the mode of the interface to Loopback in order to send route updates even if the interface is not work normally.

Example

Specify loopback0 as the source interface of a route update packet.

```
[3Com-bgp] peer test connect-interface loopback 0
```

peer default-route-advertise

Syntax

peer *group-name* **default-route-advertise**

undo peer *group-name* **default-route-advertise**

View

BGP view

Parameter

group-name: Specifies name of the peer group.

Description

Use the **peer default-route-advertise** command to configure a peer group to generate a default route for a peer.

Use the **undo peer default-route-advertise** command to cancel the existing configuration.

By default, a peer group does not import the default route.

For this command, no default route needs to exist in the routing table. A default route is sent unconditionally to a peer with the next hop as itself.

Example

Configure a peer group named test to generate a default route.

```
[3Com-bgp] peer test default-route-advertise
```

peer description

Syntax

peer { *group-name* | *peer-address* } **description** *description-line*

undo peer { *group-name* | *peer-address* } **description**

View

BGP view

Parameter

group-name: Group name.

peer-address: Address of the peer.

description-line: Description information configured, which can be letters or numbers with the maximum length of 79.

Description

Use the **peer description** command to configure the description information of the peer/peer group.

Use the **undo peer description** command to cancel the description information of the peer/peer group.

By default, description information of peers/peer group is not configured.

Related command: **display current-configuration**, **display bgp routing-table peer**, **display bgp routing-table group**.

Example

Configure the description information of the peer whose name is group1 as beijing1.

```
[3Com-bgp] peer group1 description beijing1
```

peer ebgp-max-hop

Syntax

peer *group-name* **ebgp-max-hop** [*ttl*]

undo peer *group-name* **ebgp-max-hop**

View

BGP view

Parameter

group-name: Specifies the name of the peer group.

ttl: Maximum hop value. The range is 1 to 255. By default, the value is 64.

Description

Use the **peer ebgp-max-hop** command to allow the router to establish EBGP connection with the peer on indirectly connected network.

Use the **undo peer ebgp-max-hop** command to cancel the existing configuration.

By default, this feature is disabled.

Example

Allow the router to establish EBGP connection with the peer group named test indirectly connected.

```
[3Com-bgp] peer test ebgp-max-hop
```

peer enable

Syntax

peer { *group-name* | *peer-address* } **enable**

undo peer { *group-name* | *peer-address* } **enable**

View

BGP view

Parameter

group-name: Specifies the name of the peer group which specifies the entire peer group.

peer-address: IP address of a peer, which specifies a certain peer.

Description

Use the **peer enable** command to enable the specified peer/peer group.

Use the **undo peer enable** command to disable the specified peer/peer group.

By default, BGP peer/peer group is enabled.

If the specified peer/peer group is disabled, the router will not exchange routing information with the specified peer/peer group.

Example

Disable the specified peer. After the configuration, the local router does not exchange BGP routing information with the specified peer.

```
[3Com-bgp] peer 18.10.0.9 group group1
[3Com-bgp] undo peer 18.10.0.9 enable
```

peer filter-policy export

Syntax

peer *group-name filter-policy acl-number export*

undo peer *group-name* **filter-policy** *acl-number* **export**

View

BGP view

Parameter

group-name: Specifies the name of the peer group.

acl-number: Specifies an IP acl number, ranging from 2000 to 3999.

export: Egress filter policy. It is only applicable to peer groups.

Description

Use the **peer filter-policy export** command to configure the filter-policy list of routes advertised by a peer group.

Use the **undo peer filter-policy export** command to cancel the existing configuration.

By default, a peer/peer group has no access control list (acl).

The **peer filter-policy export** command can only be configured on peer groups.

Related command: **peer filter-policy export**, **ip as-path-acl**, **peer as-path-acl**.

Example

Configure to use acl 2000 to filter the routes advertised by the peer group test.

```
[3Com-bgp] peer test filter-policy 2000 export
```

peer filter-policy import

Syntax

peer { *group-name* | *peer-address* } **filter-policy** *acl-number* **import**

undo peer { *group-name* | *peer-address* } **filter-policy** *acl-number* **import**

View

BGP view

Parameter

group-name: Specifies the name of the peer group.

peer-address: Specifies the IP address of the peer.

acl-number: Specifies an IP acl number, ranging from 2000 to 3999. That is, you can use basic ACLs or advanced ACLs.

import: Ingress filter policy. It is only applicable to peer groups.

Description

Use the **peer filter-policy import** command to configure the filter-policy list of the routes received by a peer/peer group.

Use the **undo peer filter-policy import** command to cancel the existing configuration.

By default, a peer/peer group has no access control list (acl).

Related command: **ip as-path-acl**, **peer as-path-acl export**, **peer as-path-acl import**.

The priority of the inbound filter policy configured for the peer is higher than that configured for the peer group.

Example

Configure to use acl 2000 to filter the routes received by the peer group test..

```
[3Com-bgp] peer test filter-policy 2000 import
```

peer graceful-restart

Syntax

peer { *peer-address* | *group-name* } **graceful-restart**

undo peer { *peer-address* | *group-name* } **graceful-restart**

View

BGP view

Parameter

group-name: Name of the peer group, which can consist of 1 to 47 alphabetic letters and numerals.

peer-address: IP address of the peer.

Description

Use the **peer graceful-restart** command to enable the Graceful-restart ability of the specified peer or peer group.

Use the **undo peer graceful-restart** command to disable the Graceful-restart ability of the specified peer or peer group.

If the Graceful-restart ability is enabled for a peer group first, peers added into this group afterwards also inherits the Graceful-restart ability of this group.

It is allowed that peers in a peer group have a different Graceful-restart ability than that configured for this peer group. For example, after configuring Graceful-restart for the whole peer group, you can disable the Graceful-restart ability of a specific peer. To do so, you must configure Graceful-restart for the peer group first, and then use the **undo graceful-restart** command on the peer.

Example

Enable Graceful-restart on a peer whose IP address is 10.2.2.2.

```
[3Com-bgp] peer 10.2.2.2 graceful-restart
```

Enable Graceful-restart on an EBGP peer group named "TEST", and disable Graceful-restart on Peer 10.1.1.1 in this group.

```
<SW8800>system-view
[3Com-bgp] group TEST external
[3Com-bgp] peer 10.1.1.1 group TEST as-number 200
[3Com-bgp] peer TEST graceful-restart
[3Com-bgp] undo peer 10.1.1.1 graceful-restart
```

peer group

Syntax

peer *peer-address* **group** *group-name* [**as-number** *as-number*]

undo peer *peer-address*

View

BGP view

Parameter

group-name: Specifies the name of the peer group, which can consist of letters and numbers with a length ranging from 1 to 47.

peer-address: Specifies the IP address of the peer.

as-number: Peer AS number of the peer/peer group, in the range of 1 to 65535.

Description

Use the **peer group** command to add a peer to the existing peer group.

Use the **undo peer group** command to delete the specified peer.

When you add a peer to an IBGP peer group, the **as-number** *as-number* argument is not available.

When a peer is added to an EBGP peer group that has been assigned an AS number, the peer inherits the configuration of the group. You cannot assign an AS number to the peer separately. If the peer group is not assigned an AS number, you need to assign an AS number to each peer when adding it to the group. The peers in the same peer group may use different AS numbers.

Example

Add a peer to the peer group TEST.

```
[3Com-bgp] group TEST
[3Com-bgp] peer TEST as-number 2004
[3Com-bgp] peer 10.1.1.1 group TEST
```

peer ip-prefix export

Syntax

peer *group-name* **ip-prefix** *prefixname* **export**

undo peer *group-name* **ip-prefix** *prefixname* **export**

View

BGP view

Parameter

group-name: Name of peer group.

prefixname: Name of the specified **ip-prefix**. It is a character string of 1 to 19 characters.

export: Applies the filtering policy on the route transmitted to the specified peer/peer group.

Description

Use the **peer ip-prefix export** command to configure the route filtering policy of routes advertised by the peer group based on the ip-prefix.

Use the **undo peer ip-prefix export** command to cancel the route filtering policy of the peer/peer group based on the ip-prefix.

By default, the route filtering policy of the peer group is not specified.

The **peer ip-prefix export** command can only be configured on peer groups.

Related command: **peer ip-prefix import**.

Example

Configure the route filtering policy of the peer group based on the ip-prefix 1.

```
[3Com-bgp] peer group1 ip-prefix list1 export
```

peer ip-prefix import

Syntax

peer *group-name* **ip-prefix** *prefixname* **import**

undo peer *group-name* **ip-prefix** *prefixname* **import**

View

BGP view

Parameter

group-name: Name of peer group.

prefixname: Name of the specified **ip-prefix.**

import: Applies the filtering policy on the route received by the specified peer/peer group.

Description

Use the **peer ip-prefix import** command to configure the route filtering policy of routes received by the peer/peer group based on the ip-prefix.

Use the **undo peer ip-prefix import** command to cancel the route filtering policy of the peer/peer group based on the ip-prefix.

By default, the route filtering policy of the peer/peer group is not specified.

The priority of the inbound filter policy configured for the peer is higher than that configured for the peer group.

Related command: **peer ip-prefix export**.

Example

Configure the route filtering policy of the peer group based on the ip-prefix 1.

```
[3Com-bgp] peer group1 ip-prefix list1 import
```

peer next-hop-local

Syntax

peer *group-name* **next-hop-local**

undo peer *group-name* **next-hop-local**

View

BGP view

Parameter

group-name: Specifies the name of the peer group.

Description

Use the **peer next-hop-local** command to configure to perform the process of the next hop in the route to be advertised to the peer/peer group and take the address of itself as the next hop.

Use the **undo peer next-hop-local** command to cancel the existing configuration.

Example

When BGP distributes the routes to the peer group "test", it will take its own address as the next hop.

```
[3Com-bgp] peer test next-hop-local
```

peer password

Syntax

peer { *group-name* | *peer-address* } **password** { **cipher** | **simple** } *password*

undo peer { *group-name* | *peer-address* } **password**

View

BGP view

Parameter

group-name: Name of the peer group.

peer-address: IP address of the peer, in dotted decimal format.

cipher: Displays the configured password in cipher text mode.

simple: Displays the configured password in simple text mode.

password: Password in character string form with 1 to 16 characters when parameter **simple** is configured in the command or in the event of inputting the password in simple text mode but parameter **cipher** is configured in the command; with 24 characters in the event of inputting the password in cipher text mode when parameter **cipher** is configured in the command.

Description

Use the **peer password** command to configure MD5 authentication for BGP during TCP connection setup.

Use the **undo peer password** command to cancel the configuration.

By default, BGP does not perform MD5 authentication when TCP connection is set up.

Once MD5 authentication is enabled, both parties involved in the authentication must be configured with identical authentication modes and passwords. Otherwise, TCP connection will not be set up because of the failed authentication.

This command is used to configure MD5 authentication for the specific peer only when the peer group to which the peer belongs is not configured with MD5 authentication. Otherwise, the peer should be consistent with the peer group.

Example

Adopt MD5 authentication on the TCP connection set up between the local router at 10.1.100.1 and the peer router at 10.1.100.2.

```
[3Com-bgp] peer 10.1.100.2 password simple 3com
```

Perform the similar configuration on the peer.

```
[3Com-bgp] peer 10.1.100.1 password simple 3com
```

peer public-as-only

Syntax

peer *group-name* **public-as-only**

undo peer *group-name* **public-as-only**

View

BGP view

Parameter

group-name: Name of a peer group.

Description

Use the **peer public-as-only** command to configure not to carry the AS number when transmitting BGP update packets.

Use the **undo peer public-as-only** command to configure to carry the AS number when transmitting BGP update packets.

By default, private AS number is carried when transmitting BGP update packets.

Generally, BGP transmits BGP update packets with the AS number (either public AS number or private AS number). To enable some outbound routers to ignore the AS number when transmitting update packets, you can configure not to carry the AS number when transmitting BGP update packets.

Example

Configure not to carry the private AS number when transmitting BGP update packets to the peer named test.

```
[3Com-bgp] peer test public-as-only
```

peer restart-timer

Syntax

peer *group-name* **restart-timer** *time-value*

undo peer *group-name* **restart-timer**

View

BGP view

Parameter

group-name: Name of the peer group, which can consist of 1 to 47 alphabetic letters and numerals.

time-value: Restart-time value of the peer, in seconds.

Description

Use the **peer restart-timer** command to configure the Graceful-restart Restart-time of a peer or peer group.

Use the **undo peer restart-timer** command to restore the default value of the Graceful-restart Restart-time of a peer or peer group.

The setting of the Restart-time value is not directly related to the configuration of Graceful-restart. That is, Restart-time can be configured before the configuration of the Graceful-restart ability.

The default value of Restart-time is 180 seconds.

Example

Set the Restart-time of peer group "TEST" to 100 seconds.

```
<SW8800>system-view
[3Com-bgp] group TEST external
[3Com-bgp] peer TEST restart-timer 100
```

peer reflect-client

Syntax

peer *group-name* **reflect-client**

undo peer *group-name* **reflect-client**

View

BGP view

Parameter

group-name: Name of peer group.

Description

Use the **peer reflect-client** command to configure a peer group as the route reflector client.

Use the **undo peer reflect-client** command to cancel the existing configuration.

By default, there is no route reflector in an AS.

This command only applies to IBGP peer groups.

Related command: **reflect between-clients**, **reflector cluster-id**.

Example

Configure the peer group "test" as the route reflector client.

```
[3Com-bgp] peer test reflect-client
```

peer route-policy export

Syntax

peer *group-name* **route-policy** *route-policy-name* **export**

undo peer *group-name* **route-policy** *route-policy-name* **export**

View

BGP view

Parameter

group-name: Name of peer group.

route-policy-name: The specified Route-policy.

Description

Use the **peer route-policy export** command to assign the Route-policy to the routes advertised to the peer group.

Use the **undo peer route-policy export** command to delete the specified Route-policy.

By default, the peer/peer group has no Route-policy association.

The **peer route-policy export** command only applies to peer groups.

Related command: **peer route-policy import**.

Example

Apply the Route-policy named test-policy to the route going out of the peer group test.

```
[3Com-bgp] peer test route-policy test-policy export
```

peer route-policy import

Syntax

peer { *group-name* | *peer-address* } **route-policy** *route-policy-name* **import**

undo peer { *group-name* | *peer-address* } **route-policy** *route-policy-name* **import**

View

BGP view

Parameter

group-name: Name of peer group.

peer-address: IP address of the peer.

route-policy-name: The specified Route-policy.

Description

Use the **peer route-policy import** command to assign the Route-policy to the route coming from the peer/peer group.

Use the **undo peer route-policy import** command to delete the specified Route-policy.

By default, the peer/peer group has no Route-policy association.

The priority of the inbound filter policy configured for the peer is higher than that configured for the peer group.

Related command: **peer route-policy export**.

Example

Apply the Route-policy named test-policy to the route coming from the peer group test.

```
[3Com-bgp] peer test route-policy test-policy import
```

peer route-update-interval

Syntax

peer *group-name* **route-update-interval** *seconds*

undo peer *group-name* **route-update-interval**

View

BGP view

Parameter

group-name: Specifies the name of the configured peer group.

seconds: The minimum interval of sending route update message. The range is from 0 to 600 seconds. By default, the advertisement interval is 5 seconds for internal peer/peer group, and 30 seconds for external peer/peer group.

Description

Use the **peer route-update-interval** command to configure the interval for the transmission route of a peer group.

Use the **undo peer route-update-interval** command to restore the interval to the default value.

Example

Configure the interval of sending the route update packet of the BGP peer group "test" as 10 seconds.

```
[3Com-bgp] peer test as-number 100
[3Com-bgp] peer test route-update-interval 10
```

peer shutdown

Syntax

peer { *peer-address* | *group-name* } **shutdown**

undo peer { *peer-address* | *group-name* } **shutdown**

View

BGP view, BGP multicast view, BGP L2VPN view and BGP VRF view

Parameter

group-name: Peer group names, which contain letters and numbers. The name length ranges from 1 to 47.

peer-address: Peer IP address.

Description

Use the **peer shutdown** command to disconnect and not to reconnect BGP connections, without deleting BGP configurations.

Example

Disconnect without reconnecting Peer 1.1.1.1 in the BGP unicast view.

```
[3Com-bgp] peer 1.1.1.1 shutdown
```

Disconnect without reconnecting the Group Out in the BGP unicast view.

```
[3Com-bgp] peer out shutdown
```

Disconnect without reconnecting Peer 1.1.1.1 in the BGP vrf view.

```
[3Com-bgp-af-vpn-instance] peer 1.1.1.1 shutdown
```

Disconnect but not reconnect the out group in the BGP vrf view.

```
[3Com-bgp-af-vpn-instance] peer out shutdown
```

peer timer

Syntax

peer { *group-name* | *peer-address* } **timer keep-alive** *keepalive-interval* **hold** *holdtime-interval* }

undo peer { *group-name* | *peer-address* } **timer**

View

BGP view

Parameter

group-name: Name of peer group.

peer-address: IP address of the peer.

keepalive-interval: Keepalive interval to be specified. The range is 1 to 4294967295. By default, its value is 60 seconds.

holdtime-interval: Holdtime interval to be specified. The range is 3 to 4294967295. By default, its value is 180 seconds.

Description

Use the **peer timer** command to configure the Keepalive and Holdtime intervals for the specified peer/peer group.

Use the **undo peer timer** command to restore the default timer settings.

The timer configured by using this command has a higher priority than the one configured by using the **timer** command.

Example

Configure Keepalive and Holdtime intervals of the peer group "test".

```
[3Com-bgp] peer test timer keep-alive 60 hold 180
```

preference

Syntax

preference *ebgp-value ibgp-value local-value*

undo preference

View

BGP view

Parameter

ebgp-value: Sets preference value for routes learned from external peers.

ibgp-value: Sets preference value for routes learned from internal peers.

local-value: Sets preference value for local-originated routes.

The *ebgp-value*, *ibgp-value* and *local-value* arguments are in the range of 1 to 256. By default, the first two is 256 and the last one is 130.

Description

Use the **preference** command to configure BGP preference.

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

Three types of routes may be involved in BGP: routes learned from external peers, routes learned from internal peers and local-originated routes. You can set preference values for the three types of route.

Example

Set the preference of EBGP routes, IBGP routes and local-originated routes all to 170.

```
[3Com-bgp] preference 170 170 170
```

reflect between-clients

Syntax

reflect between-clients

undo reflect between-clients

View

BGP view

Parameter

None

Description

Use the **reflect between-clients** command to configure the between-client reflection of a route.

Use the **undo reflect between-clients** command to disable this function.

After the route reflector is configured, the route reflector reflects the routes of one client to other clients by default.

By default, the clients of a route reflector need not be fully connected. If the clients are fully connected, a route reflector is not required.

Related command: **reflector cluster-id**, **peer reflect-client**.

Example

Disable the reflection between clients.

```
[3Com-bgp] undo reflect between-clients
```

reflector cluster-id

Syntax

reflector cluster-id { *cluster-id* | *address* }

undo reflector cluster-id

View

BGP view

Parameter

cluster-id: Specifies the cluster ID of the route reflector with the range from 1 to 4294967295. It is an integer.

address: Used as the interface address of the route reflector's cluster ID.

Description

Use the **reflector cluster-id** command to configure the cluster ID of the route reflector.

Use the **undo reflector cluster-id** command to delete the cluster ID of the route reflector.

By default, each route reflector uses its Router ID as the cluster ID.

Usually, there is only one route reflector in a cluster. In this case, the cluster is identified by the router ID of the route reflector. You can configure multiple route reflectors to improve network stability. If there are multiple route reflectors, you can use this command to configure the same cluster ID for all these route reflectors.

Related command: **reflect between-clients**, **peer reflect-client**.

Example

Set the cluster ID of the route reflector as 80.

```
[3Com-bgp] reflector cluster-id 80
[3Com-bgp] peer 172.38.160.10 reflect-client
```

refresh bgp

Syntax

refresh bgp { **all** | *peer-address* | **group** *group-name* } [**multicast** | **vpn-instance** *instance-name* **| vpnv4**] { **import** | **export** }

View

User view

Parameter

all: Resets all the connections with BGP.

peer-address: Resets the connection with a specified BGP peer.

group-name: Resets the connection with a specified BGP peer group.

import: Requests the peer for all its routes by sending Route-refresh packets to the peer.

export: Refreshes routes advertised to the peers.

multicast: Refreshes multicast routes.

vpn-instance: VPN instance route.

vpnv4: VPNv4 route.

Description

Use the **refresh bgp** command to request the peers to refresh the routes.

After the BGP connection is established, only incremental routes are sent. However, some special cases exist. For example, when the routing policy changes, the routes advertised to the peer or the advertised routes from the peer need refreshing so that they can be filtered according to the new policy.

Example

Request all peers to re-send the routes.

```
<SW8800>refresh bgp all import
```

reset bgp

Syntax

reset bgp { **all** | *peer-address* [**flap-info**] }

View

User view

Parameter

peer-address: Resets the connection with a specified BGP peer.

all: Resets all the connections with BGP.

flap-info: Resets the flap-info of a record at this peer address.

Description

Use the **reset bgp** *peer-address* command to reset the connection of BGP with a specified BGP peer.

Use the **reset bgp all** command to reset all the connections with BGP.

If the BGP policy or the protocol configuration changes, resetting the BGP connection can make the newly configured policy take effect immediately.

Example

Reset all the BGP connections to enable the new configuration (after configuring the new Keepalive interval and Holdtime interval using the **timer** command).

```
<SW8800> reset bgp all
```

reset bgp flap-info

Syntax

reset bgp flap-info [**regular-expression** *as-regular-expression* | **as-path-acl** *acl-number* } | *network-address* [*mask*]]

View

User view

Parameter

regular-expression *as-regular-expression*: Resets the flap-info matching the AS path regular expression.

as-path-acl *acl-number:* Resets the flap-info in consistency with a specified filter list. The range of the *acl-number* argument is 1 to 199.

flap-info of a record at this IP address.

network-address: Resets the flap-info of a record at this IP address.

mask: Network mask.

Description

Use the **reset bgp flap-info** command to reset the flap-info of a route.

Related command: **dampening**.

Example

Reset the flap-info of all the routes that go through filter list 1.

```
<SW8800> reset bgp flap-info as-path-acl 1
```

reset bgp group

Syntax

reset bgp group *group-name*

View

User view

Parameter

group-name: Specifies the name of the peer group. It is a character string of 1 to 47 characters.

Description

Use the **reset bgp group** command to reset the connections between the BGP and all the members of a group.

Related command: **peer group**.

Example

Reset BGP connections of all members from group1.

```
<SW8800> reset bgp group group1
```

reset dampening

Syntax

reset bgp dampening [*network-address* [*mask*]]

View

User view

Parameter

network-address: Network IP address related to the clearing attenuation information.

mask: Network mask.

Description

Use the **reset dampening** command to reset route attenuation information and release suppressed routes.

Related command: **dampening**, **display bgp routing-table dampened**.

Example

Reset the route attenuation information of the specified route 20.1.0.0, and release the suppression of a suppressed route.

```
<SW8800> reset dampening 20.1.0.0 255.255.0.0
```

summary

Syntax

summary

undo summary

View

BGP view

Parameter

None

Description

Use the **summary** command to configure auto aggregation of sub-network routes.

Use the **undo summary** command to disable auto aggregation of sub-network routes.

By default, no auto aggregation of sub-network routes is executed.

After the **summary** is configured, BGP cannot receive the sub-network routes imported from the IGP, so the amount of the routing information can be reduced.

Example

Make the auto aggregation of the sub-network routes.

```
[3Com-bgp] summary
```

timer

Syntax

timer keep-alive *keepalive-interval* **hold** *holdtime-interval*

undo timer

View

BGP view

Parameter

keepalive-interval: Sets the interval time value for keepalive time which ranges from 1 to 65535. By default, its value is 60 seconds.

holdtime-interval: Sets the interval time value for hold time which ranges from 3 to 65535. By default, its value is 180 seconds.

Description

Use the **timer** command to configure the Keep-alive and Hold-time timer of BGP.

Use the **undo timer** command to restore the default value of the Keep-alive and Hold-time of the timer.

Example

Configure the Keep-alive timer as 120 seconds and Hold-time timer as 360 seconds.

```
[3Com-bgp] timer keep-alive 120 hold 360
```

28

IP ROUTING POLICY CONFIGURATION COMMANDS

In this chapter, a router refers to a general router or an Ethernet switch. To improve readability, such a description of a router will not be given in the other parts of the manual.

IP Routing Policy Configuration Commands

In some situations, it may be required that only some routing information meeting a certain condition be received. In this case, you can define a Filter-policy to filter advertised routing information so that only the routing information having passed the filtration can be received.

*For the details about the **apply mpls-label**, **if-match mpls-label** and **if-match vpn-target** commands, refer to the 08-MPLS command module in the 3Com Switch 8800 Family Series Routing Switches Command Manual.*

apply as-path

Syntax

apply as-path *as-number* [*as-number* [*as-number* ...]]

undo apply as-path

View

Route policy view

Parameter

as-number-1... *as-number-n*: AS number to be added.

Description

Use the **apply as-path** command to configure AS number to be added in front of the original AS path in Route-policy.

Use the **undo apply as-path** command to cancel the AS sequence number added in front of the original AS path.

By default, no AS number is set.

If the match condition of Route-policy is met, the AS attribute of the transmitting route will be changed. You can add up to 10 AS numbers.

Example

Configure AS 200 to be added in front of the original AS path in Route-policy.

```
[3Com-route-policy] apply as-path 200
```

apply community

Syntax

apply community [*aa:nn*]* [[**no-export-subconfed** | **no-export** | **no-advertise**] * [**additive**] | **additive** | **none**]

undo apply community

View

Route policy view

Parameter

none: Deletes the community attribute of the route. This keyword can be input up to 13 times.

aa:nn: Community number.

no-export-subconfed: Does not send matched route outside the sub-AS.

no-advertise: Does not send matched route to any peer.

no-export: Does not advertise the route to outside the AS or the confederation, but can advertises to other sub-Ass in the confederation.

additive: Community attribute of the additive route.

Description

Use the **apply community** command to configure the set BGP community attribute of Route-policy.

Use the **undo apply community** command to cancel the set BGP community attribute.

By default, BGP community attribute is not set.

If the matching conditions defined in the Route-policy are satisfied, the BGP community attribute is set.

Related command: **ip community-list**, **if-match community-list**, **route-policy**, **display bgp routing-table community**.

Example

Configure one Route-policy setcommunity, whose node serial number is 16 and match mode is permit, and enter Route policy view to set match conditions and attribute modification actions to be executed.

```
[SW8800] route-policy permit node 16
[3Com-route-policy] if-match as-path 8
[3Com-route-policy] apply community no-export
```

apply cost

Syntax

apply cost *value*

undo apply cost

View

Route policy view

Parameter

value: Specifies the route cost value of route information.

Description

Use the **apply cost** command to configure the route cost value of route information. Use the **undo apply cost** command to cancel the Apply sub-statement.

By default, no Apply sub-statement is defined.

This command is one Apply sub-statement of Route-policy. It configures the route cost value of the routing information that passes the filtration.

Related command: **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 next-hop**, **apply local-preference**, **apply origin**, **apply tag**.

Example

Define one Apply sub-statement. When it is used for setting route information attribute, it sets the route metric value of route information as 120.

```
[3Com-route-policy] apply cost 120
```

apply cost-type

Syntax

apply cost-type [**internal** | **external**]

undo apply cost-type

View

Route policy View

Parameter

internal: For BGP, it indicates when a BGP peer advertises routes to its EBGP peer, the peer uses the cost value of IGP as the MED value of BGP. For IS-IS, it indicates the internal cost. For other protocols, it is invalid.

external: It is only valid for IS-IS and it indicates external cost type of IS-IS.

Description

Use the **apply cost-type** command to configure the route cost type of route information. Use the **undo apply cost-type** command to cancel the Apply sub-statement.

By default, route cost type is not set.

Example

Set the cost type of IGP as MED value of BGP.

```
[3Com-route-policy] apply cost-type internal
```

apply ip next-hop

Syntax

apply ip next-hop *ip-address*

undo apply ip next-hop

View

Route policy view

Parameter

ip-address: The next-hop address.

Description

Use the **apply ip next-hop** command to configure the next hop address in the route information.

Use the **undo apply ip next-hop** command to cancel the Apply sub-statement.

By default, no Apply sub-statement is defined.

This command is one of the Apply sub-statements of Route-policy. When it is used for setting route information attribute, it sets the next hop address area of route information passing filtration.

Related command: **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**, **apply tag**.

Example

Define an Apply sub-statement. Set the next hop address of route information as 193.1.1.8 when it is used for setting route information attribute.

```
[3Com-route-policy] apply ip next-hop 193.1.1.8
```

apply isis

Syntax

apply isis [**level-1** | **level-2** | **level-1-2**]

undo apply isis

View

Route policy view

Parameter

level-1: Sets to import the matched route to Level-1 area.

level-2: Sets to import the matched route to Level-2 area.

level-1-2: Sets to import the matched route to both Level-1 and Levle-2 area.

Description

Use the **apply isis** command to configure to apply the level of a matched route to be imported to Level-1, Level-2 or Level-1-2.

Use the **undo apply isis** command to cancel the Apply sub-statement.

By default, no apply clause is defined.

Related command: **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 next-hop**, **apply cost**, **apply origin**, **apply tag**.

Example

Define an apply clause, setting to import the route to a level-2 area.

```
[3Com-route-policy] apply isis level-2
```

apply local-preference

Syntax

apply local-preference *local-preference-value*

undo apply local-preference

View

Route policy view

Parameter

local-preference: Newly set local preference.

Description

Use the **apply local-preference** command to configure to apply the local preference of route information.

Use the **undo apply local-preference** command to cancel the Apply sub-statement.

Related command: **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 next-hop**, **apply local-preference**, **apply origin**, **apply tag**.

Example

Define an Apply sub-statement. Apply the local preference level of route information as 130 when this Apply sub-statement is used for setting route information attribute. .

```
[3Com-route-policy] apply local-preference 130
```

apply origin

Syntax

apply origin { **igp** | **egp** *as-number* | **incomplete** }

undo apply origin

View

Route policy view

Parameter

igp: Sets the BGP route information source as internal route.

egp: Sets the BGP route information source as external route

as-number: Specifies AS number of external route.

incomplete: Sets the BGP route information source as unknown source.

Description

Use the **apply origin** command to configure to apply the route source.

Use the **undo apply origin** command to cancel the Apply sub-statement.

Related command: **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 next-hop**, **apply local-preference**, **apply cost**, **apply tag**.

Example

Define an Apply sub-statement. When it is used for setting route information attribute, it sets the route source of BGP route information as IGP.

```
[3Com-route-policy] apply origin igp
```

apply tag

Syntax

apply tag *value*

undo apply tag

View

Route policy view

Parameter

value: Specifies the tag value of route information.

Description

Use the **apply tag** command to configure to set the tag area of OSPF route information. Use the **undo apply tag** command to cancel the Apply sub-statement.

Related command: **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 next-hop**, **apply local-preference**, **apply cost**, **apply origin**.

Example

Define one Apply sub-statement. When it is used for setting route information attribute, it sets the tag area of route information as 100.

```
[3Com-route-policy] apply tag 100
```

display ip ip-prefix

Syntax

display ip ip-prefix [*ip-prefix-name*]

View

Any view

Parameter

ip-prefix-name: Specifies displayed address prefix list name.

Description

Use the **display ip ip-prefix** command to view the address prefix list.

If no *ip-prefix-name* is specified, all configured address prefix lists are displayed.

Related command: **ip ip-prefix**.

Example

Display the information of the address prefix list named as p1.

```
<SW8800> display ip ip-prefix p1
name                index   conditions  ip-prefix / mask    GE  LE
p1                  10      permit      10.1.0.0/16         17  18
```

Table 78 Description of the fields of the display ip ip-prefix command

Field	Description
name	Name of ip-prefix
index	Internal sequence number of ip-prefix
conditions	Mode: permit or deny
ip-prefix / mask	Address and network segment length of ip-prefix
GE	Greater-equal value of ip-prefix network segment length
LE	Less-equal value of ip-prefix network segment length

display route-policy

Syntax

display route-policy [*route-policy-name*]

View

Any view

Parameter

route-policy-name: Specifies displayed Route-policy name.

Description

Use the **display route-policy** command to view the configured Route-policy.

If the *route-policy-name* argument is not specified, all configured Route-policies are displayed.

Related command: **route-policy**.

Example

Display the information of Route-policy named as policy1.

```
<SW8800> display route-policy policy1
Route-policy : policy1
  Permit 10 : if-match (prefixlist) p1
              apply cost 100
              matched : 0     denied : 0
```

Table 79 Description of the fields of the display route-policy command

Field	Description	
Route-policy	Name of ip-prefix	
Permit 10	Information of the route-policy with mode configured as permit and node as 10:	
	if-match (prefixlist) p1	The configured if-match clause
	apply cost 100	Apply routing cost 100 to the routes matching the conditions defined by if-match clause
	matched	Number of routes matching the conditions set by if-match clause
	denied	Number of routes not matching the conditions set by if-match clause

filter-policy export

Syntax

filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [*routing-protocol*]

undo filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [*routing-protocol*]

View

Routing protocol view

Parameter

acl-number: Number of the access control list used for matching the destination address field of the routing information.

ip-prefix-name: Address prefix list used for matching the routing information destination address field.

routing-protocol: The routing information of which kind of route protocol to be filtered.

Description

Use the **filter-policy export** command to configure to set the filtering conditions of the routing information advertised by a certain type of routing protocols.

Use the **undo filter-policy export** command to cancel the filtering conditions set.

By default, the advertised routing information is not filtered.

In some cases, it may be required that only the routing information meeting some conditions can be advertised. Then, the **filter-policy** command can be used to set

the filtering conditions for the routing information to be advertised. Only the routing information passing the filtration can be advertised.

Related command: **filter-policy import**.

Example

Define the filtering rules for advertising the routing information of RIP. Only the routing information passing the filtering of address prefix list p1 will be advertised by RIP.

```
[3Com-rip] filter-policy ip-prefix p1 export
```

filter-policy import

Syntax

filter-policy gateway *ip-prefix-name* **import**

undo filter-policy gateway *ip-prefix-name* **import**

filter-policy { *acl-number* | ip-prefix *ip-prefix-name* [**gateway** *ip-prefix-name*] } **import**

undo filter-policy { *acl-number* | ip-prefix *ip-prefix-name* [**gateway** *ip-prefix-name*] } **import**

View

Routing protocol view

Parameter

acl-number: The access control list number used for matching the destination address field of the routing information.

ip-prefix *ip-prefix-name:* The prefix address list name. Its matching object is the destination address field of the routing information.

gateway *ip-prefix-name:* The prefix address list name of the neighbor router address. Its matching object is the routing information advertised by the specified neighbor router.

Description

Use the **filter-policy gateway import** command to filter the received routing information advertised by a specified router.

Use the **undo filter-policy gateway import** command to cancel the setting of the filtering condition.

Use the **filter-policy import** command to set the condition for filtering the routing information.

Use the **undo filter-policy import** command to cancel the setting of filter condition.

By default, the received routing information is not filtered. To ignore some routing information received, you can use the **filter-policy** command to set the filter condition.

Related command: **filter-policy export**.

Example

Define the filtering rule for receiving routing information of RIP. Only the routing information filtered through the address prefix list p1 can be received by RIP.

```
[3Com-rip] filter-policy ip-prefix p1 import
```

if-match { acl | ip-prefix }

Syntax

if-match { **acl** *acl-number* | **ip-prefix** *ip-prefix-name* }

undo if-match { **acl** | **ip-prefix** }

View

Route policy view

Parameter

acl-number: Specifies the number of the access control list used for filtration.

ip-prefix-name: Specifies the name of the prefix address list used for filtration.

Description

Use the **if-match** { **acl** | **ip-prefix** } command to specify one matching rule for the route-policy and configure the IP address range to match the Route-policy.

Use the **undo if-match** { **acl** | **ip-prefix** } command to cancel the setting of the match rule.

Filtration is performed by quoting an ACL or a prefix address list.

Related commands: **if-match interface**, **if-match ip next-hop**, **if-match cost**, **if-match tag**, **route-policy**, **apply ip next-hop**, **apply cost**, **apply local-preference**, **apply origin**, **apply tag**.

Example

Define an if-match sub-statement. When the sub-statement is used for filtering route information, the route information filtered by route destination address through address prefix list p1 can pass the if-match sub-statement.

```
[3Com-route-policy] if-match ip-prefix p1
```

if-match as-path

Syntax

if-match as-path *acl-number*

undo if-match as-path

View

Route policy view

Parameter

acl-number: AS path list number, ranging from 1 to 199.

Description

Use the **if-match as-path** command to match the AS path domain of the BGP routing information.

Use the **undo if-match as-path** command to cancel the match of AS path domain.

By default, AS path list number is not matched.

This command is an if-match sub-statement of route-policy, used to filter BGP routing information and specify the match condition according to the AS path attribute of the routing information.

Example

First define an as-path numbered 2, allowing it to contain the routing information of AS 200 and AS 300. Then define a route-policy named "test". An if-match sub-statement is defined for Node 10 of this route-policy, which quotes the definition of as-path.

```
[SW8800] ip as-path-acl 2 permit 200:300
[SW8800] route-policy test permit node 10
[3Com-route-policy] if-match as-path 2
```

if-match community

Syntax

if-match community { *basic-community-number* [**whole-match**] | *adv-community-number* }

undo if-match community

View

Route policy view

Parameter

basic-community-list-number: Basic community list number, ranging from 1 to 99.

adv-community-list-number: Advanced community list number, ranging from 100 to 199.

whole-match: Exact match. That is, all specified communities must be present and only these communities are present.

Description

Use the **if-match community** command to match the community attribute of the BGP information.

Use the **undo if-match community** command to cancel the match of the community attribute.

By default, no match operation is done on the community attribute of BGP routes.

This if-match sub-statement of route-policy is used to filter BGP routing information and specify the match condition according to the community attributes of the routing information.

Related command: **route-policy**, **ip community-list**.

Example

First define a community-list numbered 1, allowing it to contain the routing information of AS 100 and AS 200. Then, define a route-policy named "test". An if-match sub-statement is defined for Node 10 of the route-policy, which quotes the definition of the community-list.

```
[SW8800] ip community-list 1 permit 100:200
[SW8800] route-policy test permit node 10
[3Com-route-policy] if-match community 1
```

if-match cost

Syntax

if-match cost *value*

undo if-match cost

View

Route policy view

Parameter

value: Specifies the required route metric value, ranging from 0 to 4294967295.

Description

Use the **if-match cost** command to configure one of the match rules of the route-policy to match the cost of the routing information.

Use the **undo if-match cost** command to cancel the configuration of the match rule.

By default, no if-match sub-statement is defined.

This is an if-match sub-statement of Route-policy, used to specify the cost of a route matches the specified condition.

Related command: **if-match interface**, **if-match acl**, **if-match ip-prefix**, **if-match ip next-hop**, **if-match tag**, **route-policy**, **apply ip next-hop**, **apply local-preference**, **apply cost**, **apply origin**, **apply tag**.

Example

Define an if-match sub-statement, allowing the routing information with routing cost of 8 to pass this if-match sub-statement.

```
[3Com-route-policy] if-match cost 8
```

if-match interface

Syntax

if-match interface *interface-type interface-number*

undo if-match interface

View

Route policy view

Parameter

interface-type: Specifies interface type.

interface-number: Specifies interface number.

Description

Use the **if-match interface** command to configure to match the route whose next hop is designated interface.

Use the **undo if-match interface** command to cancel the setting of matching condition.

By default, no if-match sub-statement is defined.

This command is an if-match sub-statement of route-policy, used to match the interface corresponding to the route next hop in route filtering.

Related commands: **if-match acl**, **if-match ip-prefix**, **if-match ip next-hop**, **if-match cost**, **if-match tag**, **route-policy**, **apply ip next-hop**, **apply cost**, **apply local-preference**, **apply origin**, **apply tag**.

Example

Define an if-match sub-statement to match the route whose next hop interface is Vlan-interface 1

```
[3Com-route-policy] if-match interface Vlan-interface 1
```

if-match ip next-hop

Syntax

if-match ip next-hop { **acl** *acl-number* | **ip-prefix** *ip-prefix-name* }

undo if-match ip next-hop [**ip-prefix**]

View

Route policy view

Parameter

acl-number: Specifies the number of the access control list used for filtration. The range is 2000 to 2999.

ip-prefix-name: Specifies the name of the prefix address list used for filtration. Its length ranges from 1 to 19.

Description

Use the **if-match ip next-hop** command to configure one match rule on next hop address of routing information for the route-policy.

Use the **undo if-match ip next-hop** command to cancel the setting of ACL matching condition.

Use the **undo if-match ip next-hop ip-prefix** command to cancel the setting of address prefix list matching condition.

Filtration is performed by quoting an ACL or an address prefix list.

By default, no if-match sub-statement is defined.

This command is an if-match sub-statement of route-policy used to filter the routing information based on next hop address by referencing an ACL or an address prefix list.

Related command: **if-match interface**, **if-match acl**, **if-match ip-prefix**, **if-match cost**, **if-match tag**, **route-policy**, **apply ip next-hop**, **apply cost**, **apply local-preference**, **apply origin**, **apply tag**.

Example

Define an if-match sub-statement, allowing the routing information whose route next hop address passes the filtration of the prefix address list p1 to pass this if-match sub-statement.

```
[3Com-route-policy] if-match ip next-hop ip-prefix p1
```

if-match tag

Syntax

if-match tag *value*

undo if-match tag

View

Route policy view

Parameter

value: Specifies the value in tag field of OSPF route information.

Description

Use the **if-match tag** command to configure to match the tag field of OSPF route information.

Use the **undo if-match tag** command to cancel the existing matching rules.

Related command: **if-match interface**, **if-match acl**, **if-match ip-prefix**, **if-match ip next-hop**, **if-match cost**, **route-policy**, **apply ip next-hop**, **apply cost**, **apply local-preference**, **apply origin**, **apply tag**.

Example

Define an if-match sub-statement, allowing the OSPF routing information whose tag is 8 to pass the if-match sub-statement.

```
[3Com-route-policy] if-match tag 8
```

ip as-path-acl

Syntax

ip as-path-acl *acl-number* { **permit** | **deny** } *as-regular-expression*

undo ip as-path-acl *acl-number*

View

System view

Parameter

acl-number: Number of AS path list, ranging from 1 to 199.

as-regular-expression: AS regular expression.

Description

Use the **ip as-path-acl** command to configure an AS path regular express.

Use the **undo ip as-path-acl** command to disable the defined regular expression.

The configured AS path list can be used on BGP policy.

Related command: **peer as-path-acl**, **display bgp routing-table as-path-acl**.

Example

Configure an AS path list.

```
[SW8800] ip as-path-acl 10 permit 200,300
```

ip community-list

Syntax

ip community-list *basic-comm-list-number* { **permit** | **deny** } [*aa:nn*]* [**internet** | **no-export-subconfed** | **no-advertise** | **no-export**]*

ip community-list *adv-comm-list-number* { **permit** | **deny** } *comm-regular-expression*

undo ip community-list { *basic-comm-list-number* | *adv-comm-list-number* }

View

System view

Parameter

basic-comm-list-number: Number of the basic community list, ranging from 1 to 99.

adv-comm-list-number: Number of the advanced community list, ranging from 100 to 199.

permit: Permits those that match conditions to access.

deny: Denies those that match conditions to access.

aa:nn: Community number. This argument can be input up to 13 times.

internet: Advertises all routes.

no-export-subconfed: Used not to advertise the matched route beyond the sub-ASs.

no-advertise: Used not to send the matched route to any peer.

no-export: Does not advertise routes beyond the AS or the confederation, but can advertise routes to other sub-ASs within the confederation.

comm-regular-expression: Community attribute in regular expression format.

Description

Use the **ip community-list** command to configure a BGP community list.

Use the **undo ip community-list** command to cancel the configured BGP community list.

The configured community list can be used in BGP policy.

Related command: **apply community**, **display bgp routing-table community-list**.

Example

Define a community attribute list, not allowing to advertise routes with the community attribute beyond the local AS.

```
[SW8800] ip community-list 6 permit no-export-subconfed
```

ip ip-prefix

Syntax

ip ip-prefix *ip-prefix-name* [**index** *index-number*] { **permit** | **deny** } *network len* [**greater-equal** *greater-equal* | **less-equal** *less-equal*]

undo ip ip-prefix *ip-prefix-name* [**index** *index-number* | **permit** | **deny**]

View

System view

Parameter

ip-prefix-name: The specified address prefix list name. It identifies one address prefix list uniquely.

index-number: Identifies an item in the prefix address list. The item with a smaller index-number will be tested first.

permit: Specifies the match mode of the defined address prefix list items as permit mode. In this case, if the IP address of the route to be filtered matches an entry in the address prefix list, the route passes the filtering and no further check is performed. If not, it is check against the next entry.

deny: Specifies the match mode of the defined address prefix list items as deny mode. In this case, if the IP address of the route to be filtered matches an entry in the address prefix list, the route is denied without further check. If otherwise, the IP address is checked against the next address prefix entry.

network: The IP address prefix range (IP address). If it is 0.0.0.0 0, all the IP addresses are matched.

len: The IP address prefix range (mask length). If it is 0.0.0.0 0, all the IP addresses are matched.

greater-equal, less-equal: The address prefix range [greater-equal, *less-equal*] to be matched after the address prefix *network len* has been matched. The meaning of **greater-equal** is "larger than or equal to", and the meaning of **less-equal** is "less than or equal to". The range is *len* <= *greater-equal* <= *less-equal* <= 32. When only **greater-equal** is used, it denotes the prefix range [*greater-equal*, 32]. When only **less-equal** is used, it denotes the prefix range [*len*, *less-equal*].

Description

Use the **ip ip-prefix** command to configure an address prefix list or one of its items.

Use the **undo ip ip-prefix** command to delete an address prefix list or one of its items.

The address prefix list is used for IP address filtering. An address prefix list may contain several items, and each item specifies one address prefix range. The inter-item filtering relation is "OR", i.e. passing an item means passing the filtering of this address prefix list. Not passing the filtering of any item means not passing the filtration of this prefix address list.

The address prefix range may contain two parts, which are determined by *len* and [*greater-equal*, *less-equal*] respectively. If the prefix ranges of these two parts are both specified, the IP to be filtered must match the prefix ranges of these two parts.

If you specify *network len* as 0.0.0.0 0, it only matches the default route.

If you specify *network len* as 0.0.0.0 0 *less-equal* 32, it matches all routes.

Example

Define an address prefix list named "p1", permitting the routes of the network segment 10.0.192.0 8 with a mask length of 17 or 18 to pass.

```
[SW8800] ip ip-prefix p1 permit 10.0.192.0 8 greater-equal 17 less-equal 18
```

route-policy

Syntax

route-policy *route-policy-name* { **permit** | **deny** } **node** *node-number*

undo route-policy *route-policy-name* [**permit** | **deny** | **node** *node-number*]

View

System view

Parameter

route-policy-name: Specifies the Route-policy name to identify one Route-policy uniquely.

permit: Specifies the match mode of the defined Route-policy node as permit mode. When a route satisfy all if-match sub-statements of this node and pass the filtration, the Apply sub-statement of this node will be executed on the route. Otherwise, the route will be tested by the next node.

deny: Specifies the match mode of the defined Route-policy node as deny mode. When a route satisfy all if-match sub-statements of this node and fails to pass the filtration, it will not tested by the next node.

node: Node of the route policy.

node-number: Index of the node in the route-policy. When this route-policy is used for routing information filtration, the node with a smaller *node-number* will be tested first.

Description

Use the **route-policy** command to create a route-policy and enter its view.

Use the **undo route-policy** command to delete the established Route-policy.

By default, no Route-policy is defined.

Route-policy is used for route information filtration or policy routing. One Route-policy comprises of some nodes and each node comprises of some match and Apply sub-statements. The if-match sub-statement defines the match rules of this node and the Apply sub-statement defines the actions after passing the filtration of this node. The filtering relationship between the if-match sub-statements of the node is "and", i.e., all if-match sub-statements that meet the node. The filtering relation between Route-policy nodes is "OR", i.e. passing the filtering of one node means passing the filtering of this Route-policy. If the information does not pass the filtration of any nodes, it cannot pass the filtration of this Route-policy.

Related command: **if-match interface**, **if-match acl**, **if-match ip-prefix**, **if-match ip next-hop**, **if-match cost**, **if-match tag**, **apply ip next-hop**, **apply local-preference**, **apply cost**, **apply origin**, **apply tag**.

Example

Configure a Route-policy named policy1, whose node number is 10 and match mode is permit, and enter Route policy view.

```
[SW8800] route-policy policy1 permit node 10
[3Com-route-policy]
```

29

ROUTE CAPACITY CONFIGURATION COMMANDS

Route Capacity Configuration Commands

router route-limit

Syntax

router route-limit { **128K** | **256K** | **512K** }

View

System view

Parameter

128K: Sets the maximum number of route entries supported by current system to 128 K.

256K: Sets the maximum number of route entries supported by current system to 256 K.

512K: Sets the maximum number of route entries supported by current system to 512 K.

Description

Use the **router route-limit** command to set the maximum number of route entries supported by the current system. If the maximum number of route entries supported by a card is less than this number, the system will inhibit the card from working.

By default, the maximum number of route entries is 128 K.

Example

Set the maximum number of route entries supported by the current system to 256 K.

```
<SW8800>system-view

System View: return to User View with Ctrl+Z.
[SW8800] router route-limit 256K
```

router VRF-limit

Syntax

router VRF-limit { **256** | **512** | **1024** }

View

System view

Parameter

256: Sets the maximum number of VPN routing & forwarding instances (VRFs) supported by current system to 256.

512: Sets the maximum number of VRFs supported by current system to 512.

1024: Sets the maximum number of VRFs supported by current system to 1024.

Description

Use the **router VRF-limit** command to set the maximum number of VPN routing and forwarding instances (VRFs) supported by current system. If the number of VRFs supported by a card is less than this number, the system will inhibit the card from working. This number is 256 by default.

Example

Set the maximum number of VRFs supported by current system to 512.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] router VRF-limit 512
```

30 RECURSIVE ROUTING CONFIGURATION

Recursive Routing Configuration Commands

route-rely

Syntax

route-rely [**bgp** | **static**]

undo route-rely [**bgp** | **static**]

View

System view

Parameter

bgp: Specifies routes learned by the BGP as the type of routes to be controlled.

static: Specifies static routes as the type of routes to be controlled.

Description

Use the **route-rely** command to enable recursive routing.

Use the **undo route-rely** command to disable the recursive routing.

By default, both routes learned by the BGP and static routes support recursive routing.

Example

Disable recursive routing for static routes.

```
<SW8800>system-view
[SW8800] undo route-rely static
```

Restore the default recursive routing function.

```
[SW8800] route-rely
```

31 IGMP SNOOPING CONFIGURATION COMMANDS

IGMP Snooping Configuration Commands

debugging mpm

Syntax

debugging mpm { **abnormal** | **all** | **event** | **forward** | **groups** | **packets** | **timer** }

undo debugging mpm { **abnormal** | **all** | **event** | **forward** | **groups** | **packets** | **timer** }

View

User view

Parameter

abnormal: Enables IGMP snooping abnormal debugging

all: Turns on all IGMP snooping debugging switches

events: Enables IGMP snooping events debugging

forward: Enables IGMP snooping forwarding debugging

groups: Enables IGMP snooping multicast groups debugging

packets: Enables IGMP snooping packets debugging

timers: Enables IGMP snooping timers debugging

Description

Use the **debugging mpm** command to enable IGMP snooping debugging.

Use the **undo debugging mpm** to disable IGMP snooping debugging.

By default, IGMP snooping debugging is disabled.

Example

Enable IGMP snooping timers debugging.

```
<SW8800> debugging mpm timers
MPM timers debugging switch is on.
```

display igmp-snooping configuration

Syntax

display igmp-snooping configuration

View

Any view

Parameter

None

Description

Use the **display igmp-snooping configuration** command to view the IGMP Snooping configuration information.

When IGMP Snooping is enabled, the information displayed includes whether IGMP Snooping is enabled, router port aging time, maximum response time of a query, multicast group port aging time, and whether unknown multicast packets are disabled from flooding within VLANs.

Related command: **igmp-snooping**.

Example

Display the IGMP Snooping configuration information of the switch.

```
<SW8800> display igmp-snooping configuration
Enable IGMP-Snooping.
Enable IGMP-Snooping.
The router port timeout  is 105 second(s).
The max response timeout is 1 second(s).
The host port timeout is 260 second(s).
Enable IGMP-Snooping Non-Flooding.
```

The information above tells us that: IGMP Snooping is enabled; the router port aging time is set to be 105 seconds; the max response time of a query is set to be 1 seconds; the aging time of a multicast group member is set to be 260 seconds. Non-broadcasting of unknown multicast data packets in a VLAN is enabled.

display igmp-snooping group

Syntax

display igmp-snooping group [**vlan** *vlan-id* [*group-address*]]

View

Any view

Parameter

vlan *vlan-id*: Specifies the VLAN where the multicast group to be viewed is located. When the parameter is not provided, the command will display the information about all the multicast groups on the VLAN.

group-address: Address of the multicast group, the information of which is to be displayed. If this argument is not provided, the command displays information of all the multicast groups in the specified VLAN.

Description

Use the **display igmp-snooping group** command to view the IP multicast group and MAC multicast group information of a VLAN or all the VLAN where the Ethernet switch is located. It displays the information such as VLAN ID, router port,

IP multicast group address, member ports in the IP multicast group, MAC multicast group, MAC multicast group address, and the member ports in the MAC multicast group.

Example

Display the multicast group information about VLAN2.

```
<SW8800> display igmp-snooping group vlan 2
***************Multicast group table***************
Vlan(id):2.
Router port(s):Ethernet3/1/1
IP group(s):the following ip group(s) match to one mac group.
IP group address:230.45.45.1
Member port(s):Ethernet3/1/12
MAC group(s):
MAC group address:01-00-5e-2d-2d-01
Member port(s):Ethernet3/1/12
```

We can know from the information listed above that:

- There is a multicast group in VLAN 2;
- The router port is Ethernet 2/1/1;
- The IP multicast group address is 230.45.45.1;
- The member port of the IP multicast group is Ethernet 2/1/2;
- MAC multicast group is 0100-5e2d-2d01;
- The member of the MAC multicast group is Ethernet 2/1/2.

display igmp-snooping statistics

Syntax

display igmp-snooping statistics

View

Any view

Parameter

None

Description

Use the **display igmp-snooping statistics** command to view the statistics information on IGMP Snooping.

This command displays the information such as the number of received general IGMP query packets, received IGMP group-specific query packets, received IGMP v1 packets, received IGMP v2 packets, received IGMP leave packets and error packets, and sent IGMP group-specific query packets.

Related command: **igmp-snooping**.

Example

Display statistics information about IGMP Snooping.

```
<SW8800> display igmp-snooping statistics
Received IGMP general query packet(s) number:1.
```

```
Received IGMP specific query packet(s) number:2.
Received IGMP V1 report packet(s) number:2.
Received IGMP V2 report packet(s) number:0.
Received IGMP leave packet(s) number:3.
Received error IGMP packet(s) number:0.
Sent IGMP specific query packet(s) number:5.
```

The information above shows that:

IGMP Snooping receives:

- 1 IGMP general query packets
- 2 IGMP group-specific query packets
- 2 IGMP v1 report packets
- 0 IGMP v2 report packets
- 3 IGMP leave packets
- 0 IGMP error packets

IGMP Snooping sends:

- 5 IGMP group-specific query packets

igmp-snooping

Syntax

igmp-snooping { **enable** | **disable** }

View

System view, VLAN view

Parameter

enable: Enables IGMP Snooping.

disable: Disables IGMP Snooping;

Description

Use the **igmp-snooping enable** command to enable IGMP Snooping.

Use the **igmp-snooping disable** command to disable IGMP Snooping.

By default, the switch disables IGMP Snooping.

CAUTION:

- When configuring IGMP Snooping, first enable global IGMP Snooping in system view, and then enable IGMP Snooping in VLAN view. Otherwise the IGMP Snooping function will not take effect.
- If the VLAN VPN is enabled on a port, the IGMP Snooping feature cannot be enabled on the VLAN for the port or the IGMP feature cannot be enabled on the corresponding VLAN interface.
- If IGMP Snooping feature is enabled on a VLAN, or IGMP is enabled on the VLAN interface, you cannot add the member port on which VLAN VPN is enabled into the VLAN.

- Isolate-user-VLAN supports the IGMP-Snooping function. After IGMP-Snooping is enabled under isolate-user-VLAN, all secondary VLANs are IGMP-Snooping enabled. It makes no sense to enable IGMP-Snooping for a secondary VLAN.
- In a secondary VLAN, IGMP packets will be directly converted and processed in isolate-user-VLAN, namely all the multicast services are implemented within isolate-user-VLAN.
- Ports in secondary VLANs cannot be used as source addresses of multicast.

Example

Enable IGMP Snooping in system view.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] igmp-snooping enable
```

Enable IGMP Snooping on VLAN 10

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] vlan 10
[3Com-vlan10] igmp-snooping enable
```

igmp-snooping fast-leave

Syntax

igmp-snooping fast-leave [**vlan** { *vlan-id* [**to** *vlan-id*] }&<1-10>]

undo igmp-snooping fast-leave [**vlan** { *vlan-id* [**to** *vlan-id*] } &<1-10>]

View

System view, Ethernet port view

Parameter

vlan { *vlan-id* [**to** *vlan-id*] }&<1-10>: Specifies any VLAN or VLAN scope for port you want to enable/disable the IGMP Snooping fast leave feature on. The *vlan-id* argument ranges from 1 to 4094.

Description

Use the **igmp-snooping fast-leave** command to enable IGMP Snooping fast leave on ports or VLANs.

Use the **undo igmp-snooping fast-leave** command to disable IGMP Snooping fast leave.

You can optionally specify multiple **vlan** keywords for the **igmp-snooping fast-leave** command, through which you can enable IGMP Snooping fast leave in corresponding VLANs. If you do not specify the **vlan** keyword, IGMP Snooping fast leave is enabled in all VLANs. As mentioned earlier, the **igmp-snooping fast-leave** command can be executed in both system view and Ethernet port view. When you execute the command in system view, fast leave is enabled on all ports of the specified VLANs, otherwise, it is only enabled on the current port in the specified VLANs.

- Fast leaves that are configured in system view and Ethernet port view operate separately.
- Fast leave works on all ports of the specified VLANs if you configure it in system view. However, it only works on the current port (e.g., a port operates as a trunk of multiple VLANs) in the specified VLANs if you configure it in Ethernet port view.

CAUTION:

- Fast leave configured for a port takes effect only when the VLAN it belongs to is IGMP Snooping-enabled.
- Fast leave does not work if the corresponding specified VLANs do not exist, the port does not belongs to any of the specified VLANs, or the VLANs do not have IGMP Snooping enabled.
- A newly configured IGMP Snooping clears all existing fast leave configurations.
- The **igmp-snooping fast-leave** command is useless if you do not enable IGMP Snooping globally. (You can enable IGMP Snooping globally by executing the **igmp-snooping enable** command in system view.)
- When you configure IGMP Snooping fast leave on aggregation ports, the configuration takes effect only on primary aggregation ports.
- If you add an IGMP V1 host of the same multicast group to the port, the switch does not remove the port when the port receives an IGMP Leave packet of the multicast group even you enable IGMP Snooping fast leave for the port.

Fast leave is disabled by default.

Related command: **igmp-snooping**.

Example

Enable IGMP Snooping fast leave on the Ethernet2/1/1 port in VLAN 5 only.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface Ethernet2/1/1
[3Com-Ethernet2/1/1] igmp-snooping fast-leave vlan 5
```

Enable IGMP Snooping fast leave on the Ethernet2/1/1 port in VLAN 5, VLAN 7, VLAN 8, VLAN 30 through VLAN 40, VLAN 50, VLAN 55, VLAN 60, and VLAN 61.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface Ethernet2/1/1
[3Com-Ethernet2/1/1] igmp-snooping fast-leave vlan 5 7 to 8 30 to 40
 50 55 60 to 61
```

Enable IGMP Snooping fast leave on the Ethernet2/1/1 port in all VLANs.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800]interface Ethernet2/1/1
[3Com-Ethernet2/1/1] igmp-snooping fast-leave
```

Enable IGMP Snooping fast leave on the Ethernet2/1/1 port in all VLANs. Then disable the feature in VLAN 3.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface Ethernet2/1/1
[3Com-Ethernet2/1/1] igmp-snooping fast-leave
[3Com-Ethernet2/1/1] undo igmp-snooping fast-leave vlan 3
```

Disable IGMP Snooping fast leave on the Ethernet2/1/1 port in all VLANs.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface Ethernet2/1/1
[3Com-Ethernet2/1/1] undo igmp-snooping fast-leave
```

Enable IGMP Snooping fast leave on all Ethernet ports in VLAN 5.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] igmp-snooping fast-leave vlan 5
```

Enable IGMP Snooping fast leave on all Ethernet ports in all VLANs.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] igmp-snooping fast-leave
```

Enable IGMP Snooping fast leave for all Ethernet ports except those in VLAN 5.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] igmp-snooping fast-leave
[SW8800] undo igmp-snooping fast-leave vlan 5
```

Disable IGMP Snooping fast leave in all VLANs.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] undo igmp-snooping fast-leave
```

igmp-snooping group-policy

Syntax

igmp-snooping group-policy *acl-number*

undo igmp-snooping group-policy

View

VLAN view

Parameter

acl-number: Number of basic ACL, in the range of 2,000 to 2,999.

Description

Use the **igmp-snooping group-policy** command to configure the filtering rule of multicast groups on a specified VLAN so as to control the access to IP multicast

groups. You can configure only one ACL rule for each VLAN, and the new configured rule will replace the old one.

Use the **undo igmp-snooping group-policy** command to cancel the configuration.

By default, no filtering rule is set in a VLAN. In this case, a host can join any multicast group.

Example

Create ACL2001 and configure the flow rule for basic ACL, using the source IP address serves as the destination multicast address.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800]acl number 2001
[3Com-acl-basic-2001]rule 0 permit source 224.1.1.1 0
[3Com-acl-basic-2001]quit
```

Create VLAN 2.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800]vlan 2
```

Configure the filtering rule of multicast groups in VLAN2.

```
[3Com-vlan2]igmp-snooping group-policy 2001
```

Cancel the filtering rule in VLAN2.

```
[3Com-vlan2]undo igmp-snooping group-policy
```

igmp-snooping host-aging-time

Syntax

igmp-snooping host-aging-time *seconds*

undo igmp-snooping host-aging-time

View

System view

Parameter

seconds: Port aging time for the multicast group member, ranging from 200 to 1000 seconds. By default, it is 260 seconds.

Description

Use the **igmp-snooping host-aging-time** command to configure the port aging time of the multicast group members.

Use the **undo igmp-snooping host-aging-time** command to restore the default value.

This command is used to set the aging time of the multicast group member so that the refresh frequency can be controlled. When the group members change frequently, the aging time should be comparatively short, and vice versa.

Related command: **igmp-snooping**.

Example

Set the aging time to 300 seconds.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] igmp-snooping host-aging-time 300
```

igmp-snooping max-response-time

Syntax

igmp-snooping max-response-time *seconds*

undo igmp-snooping max-response-time

View

System view

Parameter

seconds: Maximum response time for a query, ranging from 1 to 25 seconds. By default, it is 1 second.

Description

Use the **igmp-snooping max-response-time** command to configure the maximum response time for a query.

Use the **undo igmp-snooping max-response-time** command to restore the default value.

The set maximum response time decides the time limit for the switch to respond to IGMP Snooping query packets.

Related command: **igmp-snooping** and **igmp-snooping router-aging-time**.

Example

Set the maximum response time for the IGMP Snooping packet to 15s.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] igmp-snooping max-response-time 15
```

igmp-snooping nonflooding-enable

Syntax

igmp-snooping nonflooding-enable

undo igmp-snooping nonflooding-enable

View

System view

Parameter

None

Description

Use the **igmp-snooping nonflooding-enable** command to enable unknown multicast data packets not to be broadcasted within a VLAN.

Use the **undo igmp-snooping nonflooding-enable** command to disable unknown multicast data packets not to be broadcasted within a VLAN.

Note that if IGMP snooping is not enabled on the VLAN (nor Layer 3 multicast), unknown multicast packets are broadcasted within the VLAN no matter whether this function is enabled or not. To make unknown multicast data packets not be broadcasted within the VLAN, you need to enable igmp-snooping in this VLAN and enable **igmp-snooping nonflooding-enable** globally.

By default, unknown multicast data packets are broadcasted within the VLAN.

Example

Enable multicast packets not to be broadcasted within the VLAN.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] igmp-snooping nonflooding-enable
```

igmp-snooping router-aging-time

Syntax

igmp-snooping router-aging-time *seconds*

undo igmp-snooping router-aging-time

View

System view

Parameter

seconds: Router port aging time, ranging from 1 to 1000 measured in seconds; By default, it is 105.

Description

Use the **igmp-snooping router-aging-time** command to configure the router port aging time of IGMP Snooping.

Use the **undo igmp-snooping router-aging-time** command to restore the default value.

The port here refers to the Ethernet switch port connected to the multicast router. The Layer-2 Ethernet switch receives general query packets from the router via this port. The timer should be set to about 3.5 times of the general query period of the router.

Related command: **igmp-snooping** and **igmp-snooping max-response-time**.

Example

Set the aging time of the IGMP Snooping router port to 500 seconds.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] igmp-snooping router-aging-time 500
```

reset igmp-snooping statistics

Syntax

reset igmp-snooping statistics

View

User view

Parameter

None

Description

Use the **reset igmp-snooping statistics** command to reset the IGMP Snooping statistic information.

Related command: **igmp-snooping**.

Example

Clear IGMP Snooping statistic information.

```
<SW8800> reset igmp-snooping statistics
```

Multicast Static Routing Port Configuration Commands

multicast static-router-port

Syntax

In VLAN view:

multicast static-router-port *port-number*

undo multicast static-router-port *port-number*

In Ethernet port view:

multicast static-router-port vlan *vlan-id*

undo multicast static-router-port vlan *vlan-id*

View

VLAN view, Ethernet port view

Parameter

port-number: Port number of the port to be configured as a static routing port. Provide this argument in the format of *interface-type interface-number*, where the *interface-type* argument can only be Ethernet port type.

vlan-id: ID of the VLAN where the port belongs to.

Description

Use the **multicast static-router-port** command to configure a port in a VLAN as a static routing port, through which IGMP packets can be transparently transmitted, so as to meet the requirements of specific networks.

Use the **undo multicast static-router-port** command to remove static routing port configuration.

By default, no static routing port is configured.

Example

Configure GigabitEthernet 5/1/1 port to be a static routing port (assuming that GigabitEthernet 5/1/1 port belongs to VLAN 10).

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] vlan 10
[3Com-vlan10] multicast static-router-port GigabitEthernet 5/1/1
```

Cancel the static routing port GigabitEthernet 5/1/1 port in VLAN10.

```
[3Com-vlan10] undo multicast static-router-port GigabitEthernet 5/1/1
# Configure Ethernet 5/1/1 port in VLAN 11 to be a static routing port.
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800]_interface Ethernet 5/1/1
[3Com-Ethernet5/1/1 multicast static-router-port vlan 11
# Cancel the Ethernet 5/1/1static routing port in VLAN 11
[3Com-Ethernet5/1/1] undo multicast static-router-port vlan 11
```

32 MULTICAST VLAN CONFIGURATION COMMANDS

Multicast VLAN Configuration Commands

service-type multicast

Syntax

service-type multicast

undo service-type multicast

View

VLAN view

Parameter

None

Description

Use the **service-type multicast** command to configure the current VLAN as multicast VLAN.

Use the **undo service-type multicast** command to remove the configuration.

By default, all VLANs are not multicast VLANs.

If you configure multicast VLAN, add the corresponding switch ports to the multicast VLAN and enable IGMP Snooping, users in different VLANs can share one multicast VLAN, and multicast flow can be transmitted in the multicast VLAN only, thus saving bandwidth. The completely isolated multicast VLAN and user VLAN can effectively ensure security.

- A port can belong to only one multicast VLAN.
- The type of port connected with user terminals must be hybrid untagged.
- The current system supports up to three multicast VLANs.

Example

Configure VLAN 2 as multicast VLAN.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] vlan 2
[3Com-vlan2] service-type multicast
```

33 MULTICAST COMMON CONFIGURATION COMMANDS

Multicast Common Configuration Commands

broadcast-suppression

Syntax

broadcast-suppression { *ratio* | **bandwidth** *bandwidth* }

undo broadcast-suppression

View

Ethernet port view

Parameter

ratio: Maximum wire speed ratio of the broadcast traffic allowed on the port. The value range is 1 to 100, and the default value is 50. The smaller the ratio is, the smaller the broadcast traffic is allowed to pass.

bandwidth: Broadcast suppression bandwidth on the port. The value range is 1 to the maximum value of port bandwidth.

Description

Use the **broadcast-suppression** command to set the broadcast suppression ratio or broadcast suppression bandwidth.

Use the **undo broadcast-suppression** command to disable the broadcast suppression function.

The default broadcast suppression ratio is 50%.

You can use the **broadcast-suppression** command repeatedly. The effective broadcast suppression ratio value is the one last updated.

CAUTION:

- You cannot enable both broadcast suppression and multicast suppression simultaneously on the same card. Namely, once you have enabled broadcast suppression on some ports of a card, you cannot enable multicast suppression on the other ports of the card, and vice versa.

If multicast suppression is enabled, broadcast packets are also suppressed at the same time, while broadcast suppression does not work on multicast packets.

No distinction is made between known multicast and unknown multicast for multicast suppression.

Related command: **multicast-suppression**.

Example

Set the broadcast suppression ratio to 40%.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface Ethernet 2/1/1
[3Com-Ethernet2/1/1] broadcast-suppression 40
```

Set the broadcast suppression bandwidth to 40Mbit.

```
[3Com-Ethernet2/1/1] broadcast-suppression bandwidth 40
```

Disable broadcast suppression.

```
[3Com-Ethernet2/1/1] undo broadcast-suppression
```

debugging multicast forwarding

Syntax

debugging multicast forwarding

undo debugging multicast forwarding

View

User view

Parameter

None

Description

Use the **debugging multicast forwarding** command to enable multicast packet forwarding debugging functions.

Use the **undo debugging multicast forwarding** command to disable the debugging functions.

By default, the debugging function is disabled.

Example

Enable multicast packet forwarding debugging functions.

```
<SW8800> debugging multicast forwarding
```

debugging multicast kernel-routing

Syntax

debugging multicast kernel-routing

undo debugging multicast kernel-routing

View

User view

Parameter

None

Description

Use the **debugging multicast kernel-routing** command to enable multicast kernel routing debugging functions.

Use the **undo debugging multicast kernel-routing** command to disable the debugging functions.

By default, the multicast kernel routing debugging is disabled.

Example

Enable multicast kernel routing debugging functions.

```
<SW8800> debugging multicast kernel-routing
```

debugging multicast status-forwarding

Syntax

debugging multicast status-forwarding

undo debugging multicast status-forwarding

View

User view

Parameter

None

Description

Use the **debugging multicast status-forwarding** command to enable multicast forwarding status debugging functions.

Use the **undo debugging multicast status-forwarding** command to disable the debugging functions.

By default, the multicast forwarding status debugging is disabled.

Example

Enable multicast forwarding status debugging functions.

```
<SW8800> debugging multicast status-forwarding
```

display mpm forwarding-table

Syntax

display mpm forwarding-table [*group-address* | *source-address*]

View

Any view

Parameter

group-address: Multicast group address, used to specify a multicast group, ranging from 224.0.0.0 to 239.255.255.255.

source-address: IP address of the multicast source.

Description

Use the **display mpm forwarding-table** command to view the port-carrying multicast forwarding table information.

When a group address or a source address is specified, this command shows only the matched (S, G) entry; otherwise, this command shows all entries.

Related command: **display multicast forwarding-table**

Example

View the port-carrying multicast forwarding table information.

```
<SW8800> display mpm forwarding-table
Multicast Forwarding Cache Table
Total 1 entry (entries)

00001. (10.11.113.110, 226.1.1.1)
 in-vlan Vlan1
 2 out-vlan(s):
  Vlan20
   Ethernet5/1/33
  Vlan10
   Ethernet5/1/31

Total 1 entry(entries) Listed
```

The descriptions about the displayed information are shown in Table 82.

Table 80 Description of information generated by the command display mpm forwarding-table

Field	Description
Multicast Forwarding Cache Table	Multicast forwarding cache table
Total 1 entry (entries)	Total number of entries
00001	Sequence number of entries
(10.11.113.110, 226.1.1.1)	(s,g), namely (source address, group address)
in-vlan Vlan1	The in-VLAN of the multicast forwarding table is VLAN 1
2 out-vlan(s):	The multicast forwarding table has two out-VLANs
Vlan20	The first out-VLAN is VLAN 20, of which the egress port is Ethernet 5/1/33
Ethernet5/1/33	
Vlan10	The second out-VLAN is VLAN 10, of which the egress port is Ethernet5/1/31
Ethernet5/1/31	
Total 1 entry(entries) Listed	Totally 1 (S, G) entry is listed.

display mpm group

Syntax

display mpm group [**vlan** *vlan-id* [*ip-address*]]

View

Any view

Parameter

vlan *vlan-id*: Specifies the VLAN the desired multicast group information resides in. If this key word and argument combination is not provided the command displays the information of all the multicast groups in the VLAN.

ip-address: IP address of the desired multicast group.

Description

Use the **display mpm group** command to display the information about the IP multicast groups or MAC multicast groups in a specified VLAN. If you do not specify the *vlan-id* argument, this command displays the information about multicast groups in all VLANs.

The information displayed contains the following fields:

- VLAN ID
- Router port
- IP multicast group
- IP multicast group address
- Member port of IP multicast group
- MAC multicast group
- MAC multicast group address
- Member port of MAC multicast group

CAUTION:

- The information displayed by this command includes that displayed by the **display igmp group** command and port information.
- The information displayed by this command is the same as that displayed by the **display igmp-snooping group** command except the VLAN properties. The **display igmp-snooping group** command displays the information about the ports that join Layer 2 multicast groups in VLANs that have the IGMP-snooping function enabled. The **display mpm group** command displays the information about the ports that join Layer 3 multicast groups in VLANs that have the IGMP function enabled.

Example

Display the multicast group information about VLAN 2.

```
<SW8800> display mpm group vlan 2
Vlan(id):2.
Router port(s):Ethernet2/1/1
IP group(s):the following ip group(s) match to one mac group.
IP group address:230.45.45.1
Member port(s):Ethernet2/1/2
MAC group(s):
MAC group address:01-00-5e-2d-2d-01
Member port(s):Ethernet2/1/2
```

Table 81 Description on the fields of the display mpm group command

Field	Description
Vlan(id):2.	The output information is about VLAN 2.
Router port(s):Ethernet2/1/1	The router port concerned is Ethernet2/1/1.
IP group(s):the following ip group(s) match to one mac group.	Lists the IP multicast groups matching the same MAC multicast group.
IP group address:230.45.45.1	The IP address of the IP multicast group is 230.45.45.1.
Member port(s):Ethernet2/1/2	Ethernet2/1/2 port is a member port of the IP multicast group.
MAC group address:01-00-5e-2d-2d-01	The MAC address of the MAC multicast group is 01-00-5e-2d-2d-01.
Member port(s):Ethernet2/1/2	Ethernet2/1/2 port is a member port of the MAC multicast group.

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* | **null** *NULL-interface-number* | **register**}] *

View

Any view

Parameter

group-address: Multicast group address, used to specify a multicast group, ranging from 224.0.0.0 to 239.255.255.255.

source-address: Unicast IP address of the multicast source.

incoming-interface: Incoming interface of the multicast forwarding table entry.

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

null: Incoming-interface is null.

NULL-interface-number: The only number is 0.

register: Register interface of PIM-SM.

Description

Use the **display multicast forwarding-table** command to view the information of multicast forwarding table.

CAUTION: *You must use* ***multicast routing-enable*** *command in system view to enable IP multicast routing before you can view the multicast forwarding table information.*

Related command: **display multicast routing-table**.

Example

View the multicast forwarding table information.

```
<SW8800> display multicast forwarding-table
Multicast Forwarding Cache Table
Total 2 entries

00001. (4.4.4.4, 224.2.254.84), iif Vlan-interface1, 0 oifs
     Matched 240 pkts(11288 bytes), Wrong If 0 pkts
     Forwarded 232 pkts(11288 bytes)
00002. (4.4.4.4, 224.2.149.17), iif Vlan-interface1, 1 oifs
     List of outgoing interface:
       01: Vlan-interface2
     Matched 236 pkts(3267 bytes), Wrong If 0 pkts
     Forwarded 233 pkts(3267 bytes)

Matched 2 entries
```

The descriptions about the displayed information are shown in Table 82.

Table 82 Description on the fields of display multicast forwarding-table

Field	Description
Multicast Forwarding Cache Table	Multicast forwarding cache table
Total 2 entries	Total number of entries
00002	Sequence number of entries
(4.4.4.4, 224.2.149.17)	(s,g), source IP address and multicast group
iif Vlan-interface1, 1 oifs	Multicast forwarding cache table has an incoming interface Vlan-interface 1 and one outgoing interface
List of outgoing interface: 01: Vlan-interface2	List of outgoing interface has an outgoing interface Vlan-interface 2
Matched 236 pkts(3267 bytes), Wrong If 0 pkts	236 matched packets (3267 bytes); 0 matched packets means wrong; 233 forwarded packets (3267 bytes)
Forwarded 233 pkts(3267 bytes)	
Matched 2 entries	2 matched entries

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 vlan-interface* | **register** }]*

View

Any view

Parameter

group-address: Multicast group address, used to specify a multicast group and display the corresponding routing table information of the group. The value ranges from 224.0.0.0 to 239.255.255.255.

source-address: Unicast IP address of the multicast source.

incoming-interface: Incoming interface of the multicast route entry.

vlan-interface interface-number: VLAN interface number.

register: Register interface of PIM-SM.

Description

Use the **display multicast routing-table** command to view the information of IP multicast routing table.

CAUTION: *You must use* ***multicast routing-enable*** *command in system view to enable IP multicast routing before you can view the multicast routing table information.*

Related command: **display multicast forwarding-table**

Example

View the route entry information in the multicast routing table.

```
<SW8800> display multicast routing-table
Multicast Routing Table
Total 3 entries

(4.4.4.4, 224.2.149.17)
    Uptime: 00:15:16, Timeout in 272 sec
    Upstream interface: Vlan-interface1(4.4.4.6)
    Downstream interface list:
      Vlan-interface2(2.2.2.4), Protocol 0x1: IGMP

(4.4.4.4, 224.2.254.84)
    Uptime: 00:15:16, Timeout in 272 sec
    Upstream interface: Vlan-interface1(4.4.4.6)
    Downstream interface list: NULL

(4.4.4.4, 239.255.2.2)
    Uptime: 00:02:57, Timeout in 123 sec
    Upstream interface: Vlan-interface1(4.4.4.6)
    Downstream interface list: NULL

Matched 3 entries
```

The descriptions about the displayed information are shown in Table 83.

Table 83 Description on the fields of the display multicast routing-table command

Field	Description
Multicast Routing Table	Multicast routing table
Total 3 entries	3 entries in total
(4.4.4.4, 224.2.149.17)	(s, g)
Uptime: 00:15:16, Timeout in 272 sec	Multicast routing table lasts 15’16" and times out in 272 seconds.
Upstream interface: Vlan-interface1(4.4.4.6)	Upstream interface vlan-interface 1 (its IP address is 4.4.4.6).
Downstream interface list: Vlan-interface2(2.2.2.4), Protocol 0x1: IGMP	Downstream interface list: has an interface Vlan-interface 2 (its IP address is 2.2.2.4). The downstream interface is configured with IGMP groups.

Table 83 Description on the fields of the display multicast routing-table command

Field	Description
Matched 3 entries	3 entries in total meeting the requirement

ip managed-multicast

Syntax

ip managed-multicast

undo ip managed-multicast

View

System view

Parameter

None

Description

Use the **ip managed-multicast** command to enable the managed multicast function of the system.

Use the **undo ip managed-multicast** to disable the managed multicast function.

Related command: **display local-user, service-type lan-access**.

Example

Enable the managed multicast function of the system.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800]ip managed-multicast
```

local-user multicast

Syntax

local-user multicast [**domain** *domain-name*] *ip-address* [*mask-length*]

undo local-user [**domain** *domain-name*] *ip-address*

View

System view

Parameter

ip-address: IP address of the multicast group.

mask-length: Mask length of the multicast group.

domain *domain-name*: Domain name of the multicast group.

Description

Use the **local-user multicast** command to specify the multicast group(s) that users in a specified domain can join.

Use the **undo local-user multicast** command to cancel the configuration.

Related command: **display local-user, service-type lan-access, multicast**.

Example

Grant users permission to join the multicast group with the IP address of 225.10.10.10.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] local-user multicast 225.10.10.10.
```

multicast

Syntax

multicast *ip-address* [*ip-address* &<1-9> | *mask-length*]

undo multicast { *ip-address* [*ip-address* &<1-9>] | **all** }

View

Local user view

Parameter

ip-address &<1-9>: Multicast group IP address. &<1-9> implies that the preceding parameter can repeatedly input up to 9 times.

mask-length: Mask length. The default value of this argument is to 32. If you do not specify this argument, this command specifies a specific multicast group instead of a network segment.

Description

Use the **multicast** command to configure the multicast groups so that users can join the multicast group (the managed multicast).

Use the **undo multicast** command to remove the configuration.

If you do not specify the *mask-length* argument, you can configure up to ten multicast group addresses at one time. And if you specify the *mask-length* argument, you can configure only one multicast group address at one time. You can configure up to 64 network segments.

Managed multicast is based on the port mode. It implements authority control for users to a multicast group. Users must pass the 802.1x authentication for the port first. Moreover, users can only join the multicast group configured particularly for them. The port-based managed multicast prohibits users without authority from joining, controlling users' access to the specific multicast group.

CAUTION: *In local user view, before configuring this command, you must configure user service type as LAN-ACCESS, which the managed multicast supports exclusively at present.*

You can use the **service-type lan-access** command to configure service type in local user view.

Related command: **display local-user, service-type lan-access**.

Example

Allow users to join the multicast group with the IP address of 225.10.10.10.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800]local-user test
[3Com-luser-test] multicast 225.10.10.10.
```

multicast route-limit

Syntax

multicast route-limit *limit*

undo multicast route-limit

View

System view

Parameter

limit: Capacity of multicast routing table.

Description

Use the **multicast route-limit** command to limit the capacity of multicast routing table. When the preset capacity is exceeded, the router will discard new (S, G) protocol and data packets.

Use the **undo multicast route-limit** command to restore the limit to the default value.

By default, the capacity of multicast routing table is set to 512.

Example

Limit multicast routing table capacity at 128.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] multicast route-limit 128
```

Limit multicast routing table capacity at 800, here the default value of the multicast routing table capacity is 512, and all interface I/O Modules in the current system support this specification.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] multicast route-limit 800
```

Limit multicast routing table capacity at 1000, here the default value of the multicast routing table capacity is 512, and interface I/O modules with slot 5 in the current system do not support the specification.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] multicast route-limit 1000
Slot 5 does not support the limit, configuration failed.
```

multicast routing-enable

Syntax

multicast routing-enable

undo multicast routing-enable

View

System view

Parameter

None

Description

Use the **multicast routing-enable** command to enable multicast routing.

Use the **undo multicast routing-enable** command to disable multicast routing.

By default, multicast routing is disabled.

Related commands: **pim dm**, **pim sm**, **igmp enable**.

Example

Enable multicast routing.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] multicast routing-enable
```

multicast-suppression

Syntax

multicast-suppression { *ratio* | **bandwidth** *bandwidth* }

undo multicast-suppression

View

Ethernet port view

Parameter

ratio: Maximum wire speed ratio of the multicast traffic allowed on the port. The value range is 1 to 100, and the default value is 50. The smaller the ratio is, the smaller the multicast traffic is allowed to pass.

bandwidth: Multicast suppression bandwidth on the port. The value range is 1 to the maximum value of port bandwidth.

Description

Use the **multicast-suppression** command to set the multicast suppression ratio or multicast suppression bandwidth.

Use the **undo multicast-suppression** command to disable the multicast suppression function.

The default multicast suppression ratio is 100%.

You can use the **multicast-suppression** command repeatedly. The effective multicast suppression ratio value is the one last updated.

CAUTION:

- You cannot enable both broadcast suppression and multicast suppression simultaneously on the same card. Namely, once you have enabled broadcast suppression on some ports of a card, you cannot enable multicast suppression on the other ports of the card, and vice versa. Although the commands are based on ports, the mutual exclusion between these two commands is based on cards.
- If multicast suppression is enabled, broadcast packets are also suppressed at the same time, while broadcast suppression does not work on multicast packets.
- No distinction is made between known multicast and unknown multicast for multicast suppression.

Related command: **broadcast-suppression**.

Example

Set the multicast suppression ratio to 40%.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800]interface Ethernet 2/1/1
[3Com-Ethernet2/1/1] multicast-suppression 40
```

Set the multicast suppression bandwidth to 40Mbit.

```
[3Com-Ethernet2/1/1] multicast-suppression bandwidth 40
```

Disable multicast suppression.

```
[3Com-Ethernet2/1/1] undo multicast-suppression
```

reset multicast forwarding-table

Syntax

reset multicast forwarding-table [**statistics**] { **all** | { *group-address* [**mask** { *group-mask* | *group-mask-length* }] | *source-address* [**mask** { *source-mask* | *source-mask-length* }] | **incoming-interface** { **null** *NULL-interface-number* | *interface-type interface-number* } }* }

View

User view

Parameter

statistics: If it is selected, the system clears the statistic information of MFC forward entries. Otherwise, the system clears MFC forward entries.

all: All MFC forward entries.

group-address: Multicast group address.

group-mask: Mask of multicast group address

group-mask-length: Mask length of multicast group address.

source-address: Source address.

source-mask: Mask of source address.

source-mask-length: Mask length of source address.

incoming-interface: Specifies incoming interface for the multicast forward entry.

null: Incoming-interface is null.

NULL-interface-number: The only number is 0.

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

Description

Use the **reset multicast forwarding-table** command to clear MFC forwarding entries or the statistic information of MFC forwarding entries.

You can type in *source address* first and *group address* after in the command, as long as they both are valid addresses. The system prompts error information if you type in invalid addresses.

Related command:: **reset pim routing-table**, **reset multicast routing-table**, **display multicast forwarding-table**.

Example

Clear the forwarding entry with address of 225.5.4.3 from the MFC forwarding table.

```
<SW8800> reset multicast forwarding-table 225.5.4.3
```

Clear statistic information of the forwarding entry with address of 225.5.4.3 from the MFC forwarding table.

```
<SW8800> reset multicast forwarding-table statistics 225.5.4.3
```

reset multicast routing-table

Syntax

reset multicast routing-table { **all** | { *group-address* [**mask** { *group-mask* | *group-mask-length* }] | *source-address* [**mask** { *source-mask* | *source-mask-length* }] | **incoming-interface vlan-interface** *interface-num*ber } * }

View

User view

Parameter

all: All route entries in the core multicast routing table.

group-address: Multicast group address.

group-mask: Mask of multicast group address

group-mask-length: Mask length of multicast group address.

source-address: Source address.

source-mask: Mask of source address.

source-mask-length: Mask length of source address.

incoming-interface: Specifies incoming interface for the multicast forward entry.

vlan-interface *interface-number*: VLAN virtual interface number.

Description

Use the **reset multicast routing-table** command to clear route entries from the core multicast routing table, as well as MFC forwarding entries.

You can type in *source address* first and *group address* after in the command, as long as they both are valid addresses. The system prompts error information if you type in invalid addresses.

Related command: **reset pim routing-table**, **reset multicast forwarding-table** and **display multicast forwarding-table**.

Example

Clear the route entry with address of 225.5.4.3 from the core multicast routing table.

```
<SW8800> reset multicast routing-table 225.5.4.3
```

34 STATIC MULTICAST MAC ADDRESS CONFIGURATION COMMAND

Static Multicast MAC Address Configuration Command

mac-address multicast

Syntax

mac-address multicast *mac-addr* **interface** { { *interface-type interface-number* } [**to** { *interface-type interface-number* }] } &<1-10> **vlan** *vlan-id*

undo mac-address multicast [[*mac-addr*] **vlan** *vlan-id*]

undo mac-address multicast *mac-addr* **interface** { { *interface-type interface-number* } [**to** { *interface-type interface-number* }] } &<1-10> **vlan** *vlan-id*

View

System view

Parameter

mac-addr: Multicast group address.

interface-type interface-number: Interface type and interface number. Refer to the Port Configuration part of the book.

to: Defines a range of multicast MAC ports. Before **to** is the initial interface and after **to** is the terminal interface. Interfaces from the initial interface to the terminal interface form an interface list.

vlan-id: ID of the VLAN

Description

Use the **mac-address multicast** command to add multiple ports into static multicast MAC group.

Use the **undo mac-address multicast** command to delete the specified static multicast MAC group or to delete multiple ports from the static multicast MAC group.

Only Ethernet ports supported, and the ports must not join an aggregation group and must not be LACP enabled.

The configured multicast MAC should not be any multicast MAC address used by a known protocol. For example, 0100-5E00-0005 is the multicast MAC address used by the OSPF protocol.

The PIM protocol must not be enabled on the corresponding virtual interface of the specified VLAN.

Related command: **display mac-address multicast static**.

Example

Add a new multicast MAC address. The MAC address is 0100-1000-1000. Ports are from Ethernet 1/1/1 to Ethernet 1/1/5, and these ports belong to Vlan 2

```
[SW8800] mac-address multicast 0100-1000-1000 interface Ethernet 1/1
/1 to Ethernet 1/1/5 vlan 2
```

display mac-address multicast static

Syntax

display mac-address multicast static [[*mac-addr*] **vlan** *vlan-id*]

View

Any view

Parameter

mac-addr: Multicast MAC address.

vlan-id: ID of the VLAN.

Description

Use the **display mac-address multicast static** command to display the information of a static multicast group. The information includes multicast MAC address, VLAN ID, address status, port name, and aging time.

If all ports in the configured static multicast MAC group are out of position (the corresponding module has been pulled out after configuration), the port name in the MAC information is displayed as N/A when you use this command.

Example

Display all static multicast MAC address information

```
<SW8800> display mac-address multicast static
MAC ADDR        VLAN ID   STATE           PORT INDEX           AGING TIME(s)
0100-5e01-0101     3      Config static   Ethernet0/1/23       N/A
                                                Ethernet0/1/24

  ---  1 mac address(es) found  ---
```

Table 84 Description on the fields of display mac-address multicast static

Field	Description
MAC ADDR	Multicast MAC address
VLAN ID	The ID of the VLAN where the MAC address is located.
STATE	Status of MAC address.
	The status of the static multicast MAC address is always "Config static".
PORT INDEX	Port name.
	When no valid port is in position, the port name is displayed as N/A
AGING TIME(s)	Aging time.
	The aging time of a static multicast MAC address is always "N/A".

reset mac-address multicast

Syntax

reset mac-address multicast

View

User view

Parameter

None

Description

Use the **reset mac-address multicast** command to delete all static multicast MAC groups.

Related command: **mac-address multicast**

Example

Delete all the static multicast MAC groups.

```
<SW8800> reset mac-address multicast
```

35 IGMP CONFIGURATION COMMANDS

IGMP Configuration Commands

debugging igmp

Syntax

debugging igmp { **all** | **event** | **host** | **packet** | **timer** }

undo debugging igmp { **all** | **event** | **host** | **packet** | **timer** }

View

User view

Parameter

all: All the debugging information of IGMP.

event: Debugging information of IGMP event.

host: Debugging information of IGMP host.

packet: Debugging information of IGMP packets.

timer: Debugging information of IGMP timers.

Description

Use the **debugging igmp** command to enable IGMP debugging functions.

Use the **undo debugging igmp** command to disable the debugging functions.

By default, IGMP debugging functions are disabled.

Example

Enable all IGMP debugging functions

```
<SW8800> debugging igmp all
```

display igmp group

Syntax

display igmp group [*group-address* | **interface vlan-interface** *interface-number*]

View

Any view

Parameter

group-address: Address of the multicast group.

vlan-interface *interface-number*: VLAN interface number.

Description

Use the **display igmp group** command to view the member information of the IGMP multicast group.

You can specify to show the information of a group or the member information of the multicast group on a VLAN interface. The information displayed contains the multicast groups which the downstream hosts join through IGMP or through command line.

Related command: **igmp host-join**.

Example

Display the IGMP group members in a directly-connected subnet.

```
<SW8800> display igmp group
LoopBack0 (20.20.20.20): Total 3 IGMP Groups reported:
  Group Address      Last Reporter   Uptime      Expires
  225.1.1.1           20.20.20.20     00:02:04    00:01:15
  225.1.1.3           20.20.20.20     00:02:04    00:01:15
  225.1.1.2           20.20.20.20     00:02:04    00:01:17
```

Table 85 Description of the fields of the display igmp group command

Field	Description
Group address	Multicast group address
Last Reporter	The last host reporting to join the multicast group
Uptime	Time passed since multicast group is discovered (hh: mm: ss).
Expires	Specifies when the member will be removed from the multicast group (hh: mm: ss).

display igmp interface

Syntax

display igmp interface [**vlan-interface** *interface-number*]

View

Any view

Parameter

vlan-interface *interface-number*: VLAN interface number of the router, used to specify the interface. If the parameters are not provided, information about all the interfaces running IGMP will be displayed.

Description

Use the **display igmp interface** command to view the IGMP configuration and running information on an interface.

Example

View the IGMP configuration and running information of all interfaces.

```
<SW8800> display igmp interface
Vlan-interface1 (10.153.17.99):
  IGMP is enabled
  Current IGMP version is 2
  Value of query interval for IGMP(in seconds): 60
  Value of other querier time out for IGMP(in seconds): 120
  Value of maximum query response time for IGMP(in seconds): 10
  Value of robust count for IGMP: 2
  Value of startup query interval for IGMP(in seconds): 15
  Value of last member query interval for IGMP(in seconds): 1
  Value of query timeout for IGMP version 1(in seconds): 400
  Policy to accept IGMP reports: none
  Querier for IGMP: 10.153.17.99 (this router)
  IGMP group limit is 1024
  No IGMP group reported
```

Table 86 Description on the fields of the display igmp interface command

Field	Description
IGMP version	IGMP version
query interval	General query interval
querier timeout	Querier timeout time
max query response time	Maximum query response time
robust count	IGMP robust count, namely the number of times IGMP querier sends IGMP specific group query packet when it receives an IGMP Leave packet from a host
startup query interval	Startup query interval
last member query interval	The interval at which the IGMP querier sends IGMP specific group query packets when it receives an IGMP leave packet from a host
query timeout	Query timeout for IGMP V1
Policy to accept IGMP reports	Filter policy for the IGMP multicast group to control the accesses to the IP multicast group
Querier for IGMP	IGMP querier
IGMP group limit	Quantity limit of IGMP groups added to the interface. After the limit is reached, the router does not process the IGMP join messages

igmp enable

Syntax

igmp enable

undo igmp enable

View

VLAN interface view

Parameter

None

Description

Use the **igmp enable** command to enable IGMP on an interface.

Use the **undo igmp enable** command to disable IGMP on the interface.

By default, IGMP is disabled on an interface.

You must enable the multicast function before this command can work, you must use this command first before you can configure other IGMP features.

Related command: **multicast routing-enable**.

CAUTION:

- If the VLAN VPN is enabled on a port, the IGMP Snooping feature cannot be enabled on the VLAN to which the port belongs, and the IGMP feature cannot be enabled on the corresponding interface.
- If IGMP Snooping feature is enabled on a VLAN, or IGMP is enabled on the interface, you cannot add VLAN VPN enabled ports into the VLAN, and vice versa.

Example

Enable IGMP on Vlan-interface 10.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800]interface vlan-interface 10
[3Com-Vlan-interface10] igmp enable
```

igmp fast-leave

Syntax

igmp fast-leave [**vlan** { *vlan-id* [**to** *vlan-id*] } &<1-10>]

undo igmp fast-leave [**vlan** { *vlan-id* [**to** *vlan-id*] } &<1-10>]

View

Ethernet port view, system view

Parameter

vlan-id: VLAN ID, which you want to configure the IGMP Snooping fast leave feature on. The *value* range is from 1 to 4094.

Description

Use the **igmp fast-leave** command to enable IGMP fast leave on ports or VLANs.

Use the **undo igmp fast-leave** command to disable IGMP fast leave.

An IGMP-enabled Layer 3 switch does not query packets of the specific multicast group to a fast leave-enabled port any longer when the port receives an IGMP leave packet. Instead, the switch peels off the port from the multicast group immediately.

You can optionally specify multiple **vlan** keywords for the **igmp fast-leave** command, through which you can enable IGMP fast leave in corresponding VLANs. If you do not specify the **vlan** keyword, IGMP fast leave is enabled in all VLANs. As mentioned earlier, the **igmp fast-leave** command can be executed in both system view and Ethernet port view. When you execute the command in system view, fast leave is enabled on all ports of the specified VLANs, otherwise, it is only enabled on the current port in the specified VLANs.

- Fast leaves that are configured in system view and Ethernet port view operate separately.
- Fast leave works on all ports of the specified VLANs if you configure it in system view. However, it only works on the current port (e.g., when a Trunk port belong to multiple VLANs) in the specified VLANs if you configure it in Ethernet port view.

CAUTION:

- Fast leave configured for a port takes effect only when the VLAN it belongs to is IGMP-enabled.
- Fast leave does not work if the corresponding specified VLANs do not exist, the port does not belongs to any of the specified VLANs, or the VLANs do not have IGMP enabled.
- You can enable multicast routing globally by executing the **multicast routing-enable** command before you can configure the fast leave feature.
- Disabling globally-enabled multicast routing results in all existing IGMP fast leave-related configurations being cleared.
- When you configure IGMP fast leave on aggregation ports, the configuration takes effect only on primary aggregation ports.
- If you add an IGMP V1 host of the same multicast group to the port, or configure a static host of the same multicast group by using the **igmp host-join** command, the switch does not remove the port when the port receives an IGMP Leave packet of the multicast group even you enable IGMP fast leave for the port.

Fast leave is disabled by default.

Example

Enable IGMP fast leave on the Ethernet2/1/1 port in VLAN 5 only.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800]interface Ethernet2/1/1
[3Com-Ethernet2/1/1] igmp fast-leave vlan 5
```

Disable IGMP fast leave on the Ethernet2/1/1 port in all VLANs.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface Ethernet2/1/1
[3Com-Ethernet2/1/1] undo igmp fast-leave
```

Enable IGMP fast leave on all Ethernet ports in VLAN 5.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] igmp fast-leave vlan 5
```

Enable IGMP fast leave for on all Ethernet ports except those in VLAN 5.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] igmp fast-leave
[SW8800] undo igmp fast-leave vlan 5
```

Disable IGMP fast leave in all VLANs.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] undo igmp fast-leave
```

igmp group-limit

Syntax

igmp group-limit *limit*

undo igmp group-limit

View

Interface view

Parameter

limit: Quantity of multicast groups, in the range of 0 to 512.

Description

Use the **igmp group-limit** command to limit multicast groups to be added on an interface. After the limit is reached, the router does not process IGMP join messages.

Use the **undo igmp group-limit** command to restore the default setting.

By default, the maximum number is 512.

The new configuration overwrites the old one if you run the command for a second time.

Example

Limit the maximum number of IGMP groups to be added on Vlan-interface10 to 100.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800]interface vlan-interface 10
[3Com-Vlan-interface10] igmp group-limit 100
```

igmp group-policy

Syntax

igmp group-policy *acl-number*

undo igmp group-policy

View

VLAN view

Parameter

acl-number: Number of basic ACL, in the range of 2,000 to 2,999.

Description

Use the **igmp group-policy** command to configure the filtering rule of multicast groups on a specified VLAN so as to control the access to IP multicast groups. You can configure only one ACL rule for each VLAN, and the new configured rule will replace the old one.

Use the **undo igmp group-policy** command to cancel the configuration.

By default, no filtering rule is set in a VLAN. In this case, a host can join any multicast group.

Example

Create ACL2001 and configure the flow rule for basic ACL, using the source IP address serves as the destination multicast address.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800]acl number 2001
[3Com-acl-basic-2001]rule 0 permit source 224.1.1.1 0
[3Com-acl-basic-2001]quit
```

Create VLAN 2.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800]vlan 2
```

Configure the filtering rule of multicast groups on VLAN2.

```
[3Com-vlan2]igmp group-policy 2001
```

Cancel the filtering rule in VLAN2.

```
[3Com-vlan2]undo igmp group-policy
```

igmp host-join port

Syntax

igmp host-join *group-address* **port** *interface-type interface- number* [**to** { *interface-type interface- number*]

undo igmp host-join *group-address* **port** { *interface-type interface-number* [**to** { *interface-type interface- number*]

View

Interface view

Parameter

group-address: Multicast address of the multicast group that an interface will join.

interface-type interface-number [**to** *interface-type interface-number*]: Specifies the port under the interface.

Description

Use the **igmp host-join** command to enable a port in the interface of an Ethernet switch to join a multicast group.

Use the **undo igmp host-join** command to disable the configuration.

By default, an interface does not join any multicast group.

Related command: **igmp group-policy**.

Example

Add port Ethernet 2/1/1 under VLAN-interface10 to the multicast group 225.0.0.1.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800]interface vlan-interface 10
[3Com-Vlan-interface10] igmp host-join 225.0.0.1 port Ethernet 2/1/1
```

igmp host-join vlan

Syntax

igmp host-join *group-address* **vlan** *vlan-id*

undo igmp host-join *group-address* **vlan** *vlan-id*

View

Ethernet port view

Parameter

group-address: Address of the multicast group to be joined.

vlan-id: VLAN where the port belongs to.

Description

Use the **igmp host-join vlan** command to make an Ethernet join a multicast group.

Use the **undo igmp host-join vlan** command to cancel the configuration.

By default, an Ethernet port does not join any multicast group.

Related command: **igmp group-policy**.

Example

Add port Ethernet 2/1/1 to the multicast group at 225.0.0.1

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800]interface vlan-interface 10
[3Com-Vlan-interface10] igmp enable
[3Com-Vlan-interface10] quit
[SW8800] interface Ethernet 2/1/1
[3Com-Ethernet2/1/1] port access vlan 10
[3Com-Ethernet2/1/1] igmp host-join 225.0.0.1 vlan 10
```

igmp lastmember-queryinterval

Syntax

igmp lastmember-queryinterval *seconds*

undo igmp lastmember-queryinterval

View

Interface view

Parameter

seconds: Time interval before IGMP query router sends the IGMP group query message after it receives the IGMP Leave message from the host. It is in the range of 1 to 5 seconds. By default, it is 1 second.

Description

Use the **igmp lastmember-queryinterval** command to set the time interval at which IGMP query router sends the IGMP group query message after it receives the IGMP Leave message from the host.

Use the **undo igmp lastmember-queryinterval** command to restore the default value.

This command is valid only when the query router runs IGMP v2. If the host runs IGMP v1 , it does not send an IGMP Leave message when it leaves a group, so this command is invalid for the IGMP query router.

Related command: **igmp robust-count** and **display igmp interface**.

Example

Set the query interval at the Vlan-interface10 as 3 seconds.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800]interface vlan-interface 10
[3Com-Vlan-interface10] igmp lastmember-queryinterval 3
```

igmp max-response-time

Syntax

igmp max-response-time *seconds*

undo igmp max-response-time

View

Interface view

Parameter

seconds: Maximum response time in the IGMP query messages in second in the range from 1 to 25. By default, the value is 10 seconds.

Description

Use the **igmp max-response-time** command to configure the maximum response time contained in the IGMP query messages.

Use the **undo igmp max-response-time** command to restore the default value.

The maximum query response time determines the period for a router to quickly detect that there are no more directly connected group members in a LAN.

Related command: **display igmp group**.

Example

Set the maximum response time carried in host-query message to 8 seconds.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800]interface vlan-interface 10
[3Com-Vlan-interface10] igmp max-response-time 8
```

igmp-report enhance enable

Syntax

igmp-report enhance enable

igmp-report enhance disable

View

System view

Parameter

None

Description

Use the **igmp-report enhance enable** command to enable the compatibility control function of the switch.

Use the **igmp-report enhance disable** command to disable the function.

With the compatibility control function enabled, the switch processes the protocol packet with the destination IP address 224.0.0.1 **among** IGMP Report packets. Otherwise, the switch drops this kind of packets.

By default, the compatibility control function of the switch is disabled.

This command is often executed after IGMP or IGMP Spooning protocol is enabled in the system.

Related command: **igmp** { **enable** | **disable** } and **igmp-snooping** { **enable** | **disable** }

Example

Enable the compatibility control function of the switch.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] igmp-report enhance enable
```

igmp robust-count

Syntax

igmp robust-count *robust-value*

undo igmp robust-count

View

Interface view

Parameter

robust-value: IGMP robust value, number of times the IGMP query router sends IGMP group query message after it receives the IGMP Leave message from the host. the value range is 2 to 5. The default value is 2.

Description

Use the **igmp robust-count** command to set the number of times the IGMP query router sends IGMP group query message after it receives the IGMP Leave message from the host.

Use the **undo igmp robust-count** command to restore the default value.

Related commands: **igmp lastmember-queryinterval, display igmp interface**.

Example

Set the robust value at the Vlan-interface 10 to 3.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800]interface vlan-interface 10
[3Com-Vlan-interface10] igmp robust-count 3
```

igmp timer other-querier-present

Syntax

igmp timer other-querier-present *seconds*

undo igmp timer other-querier-present

View

Interface view

Parameter

seconds: IGMP querier present timer value in second ranging from 1 to 131070. By default, the value is twice the value of IGMP query message interval, i.e., 120 seconds.

Description

Use the **igmp timer other-querier-present** command to configure the timer of presence of the IGMP querier.

Use the **undo igmp timer other-querier-present** command to restore the default value.

On a shared network, i.e., there are multiple multicast routers on the same network segment, the query router (querier for short) takes charge of sending query messages periodically on the interface. If other non-queriers receive no query messages within the valid period, the router will consider the previous query to be invalid and the router itself becomes a querier.

In IGMP version 1, the selection of a query is determined by the multicast routing protocol. In IGMP version 2, the router with the smallest IP address on the shared network segment acts as the querier.

Related command: **igmp timer query** and **display igmp interface**.

Example

Set querier to expire after 300 seconds.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800]interface vlan-interface 10
[3Com-Vlan-interface10] igmp timer other-querier-present 300
```

igmp timer query

Syntax

igmp timer query *seconds*

undo igmp timer query

View

Interface view

Parameter

seconds: Interval at which a router transmits IGMP query messages in second in the range from 1 to 65535. By default, the value is 60 seconds.

Description

Use the **igmp timer query** command to configure the interval at which a router interface sends IGMP query messages.

Use the **undo igmp timer query** command to restore the default value.

A multicast router periodically sends out IGMP query messages to check whether there are multicast group members on the network. The query interval can be modified according to the practical conditions of the network.

Related command: **igmp timer other-querier-present**.

Example

Configure to transmit the host-query message every 150 seconds via VLAN-interface2.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800]interface vlan-interface 2
[3Com-Vlan-interface2] igmp timer query 150
```

igmp version

Syntax

igmp version { **1** | **2** }

undo igmp version

View

Interface view

Parameter

1: IGMP version 1.

2: IGMP version 2. The default setting is IGMP version 2.

Description

Use the **igmp version** command to specify the version of IGMP that a router uses.

Use the **undo igmp version** command to restore the default value.

The system does not automatic switching between different IGMP versions. Therefore, all routers on a subnet must be configured to run the same IGMP version.

Example

Run IGMP Version 1 on VLAN-interface10.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800]interface vlan-interface 10
[3Com-Vlan-interface10] igmp version 1
```

reset igmp group

Syntax

reset igmp group { **all** | **interface** *vlan-interface interface-number* { **all** | *group-address* [*group-mask*] } }

View

User view

Parameter

all: All IGMP groups.

interface *vlan-interface interface-number*: VLAN virtual interface type and number.

group-address: IGMP group address.

group-mask: Segment mask of the IGMP group address.

Description

Use the **reset igmp group** command to delete an existing IGMP group from the interface. The deleted group can added again on the interface.

Example

Delete all IGMP groups on all the interfaces.

```
<SW8800> reset igmp group all
```

Delete all IGMP groups on the Vlan-intrface10.

```
<SW8800> reset igmp group interface Vlan-interface10 all
```

Delete the group 225.0.0.1 from the Vlan-interface10.

```
<SW8800> reset igmp group interface Vlan-interface10 225.0.0.1
```

Delete the IGMP groups ranging from 225.1.1.0 to 225.1.1.255 on the Vlan-interface10.

```
<SW8800> reset igmp group interface Vlan-interface10 225.1.1.0 255.2
55.255.0
```

IGMP Proxy Configuration Commands

igmp proxy

Syntax

igmp proxy *interface-type interface-number*

undo igmp proxy

View

Interface view

Parameter

interface-type: Proxy interface type.

interface-number: Proxy interface number.

Description

Use the **igmp proxy** command to enable IGMP proxy for the VLAN interface and specify the IGMP proxy interface of the VLAN interface.

Use the **undo igmp proxy** command to remove IGMP proxy configuration.

By default, IGMP proxy is disabled on the interface.

CAUTION:

- You need to enable PIM protocol for a VLAN interface before executing the **igmp proxy** command in its VLAN interface view.
- If you configure the IGMP proxy interface for a VLAN interface multiple times, the latest configured IGMP proxy interface will take effect.
- A VLAN interface cannot be the IGMP proxy interface for two or more other VLAN interfaces simultaneously.

Example

Enable IGMP proxy for the interface of VLAN 100 and specify the interface of VLAN 200 to be its IGMP proxy interface.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface vlan-interface 100
[3Com-vlan-interface100] igmp proxy vlan-interface 200
```

36 PIM CONFIGURATION COMMANDS

PIM Configuration Commands

bsr-policy

Syntax

bsr-policy *acl-number*

undo bsr-policy

View

PIM view

Parameter

acl-number: ACL number imported in BSR filtering policy, in the range of 2000 to 2999.

Description

Use the **bsr-policy** command to limit the range of legal BSRs to prevent BSR proofing.

Use the **undo bsr-policy** command to restore the default setting, that is, no range limit is set and all received messages are taken as legal.

In the PIM SM network using BSR (bootstrap router) mechanism, every router can set itself as C-BSR (candidate BSR) and take the authority to advertise RP information in the network once it wins in the contention. To prevent the legal BSR from being replaced maliciously in the network, the following two measures need to be taken:

- Prevent the router from being spoofed by hosts though faking legal BSR messages to modify RP mapping. BSR messages are of multicast type and their TTL is 1, so this type of attacks often hit edge routers. Fortunately, BSRs are inside the network, while assaulting hosts are outside, therefore neighbor and RPF checks can be used to stop this type of attacks.
- If a router in the network is manipulated by an attacker, or an illegal router is accessed into the network, the attacker may set itself as C-BSR and try to win the contention and gain authority to advertise RP information among the network. Since the router configured as C-BSR shall propagate BSR messages, which are multicast messages sent hop by hop with TTL as 1, among the network, then the network cannot be affected as long as the peer routers do not receive these BSR messages. One way is to configure **bsr-policy** on each router to limit legal BSR range, for example, only 1.1.1.1/32 and 1.1.1.2/32 can

be BSR, thus the routers cannot receive or forward BSR messages other than these two. Even legal BSRs cannot contest with them.

Problems may still exist if a legal BSR is attacked, though these two measures can effectively guarantee high BSR security.

The **source** parameter in the **rule** command is translated as BSR address in the **bsr-policy** command.

Related command: **acl** and **rule**.

Example

Configure BSR filtering policy on routers, only 101.1.1.1/32 can be BSR and all others are illegal.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] multicast routing-enable
[SW8800]pim
[3Com-pim] bsr-policy 2000
[3Com-pim] quit
[SW8800] acl number 2000
[3Com-acl-basic-2000] rule 0 permit source 101.1.1.1 0
```

c-bsr

Syntax

c-bsr *interface-type interface-number hash-mask-len* [*priority*]

undo c-bsr

View

PIM view

Parameter

interface-type interface-number:. Interface type and interface number, used to specify the interface. The candidate BSR is configured on the interface. PIM-SM must be enabled on the interface first.

hash-mask-len: Length of the mask. The value ranges from 0 to 32.

priority: Priority of the candidate BSR. The larger the value of the priority, the higher the priority of the BSR. The value ranges from 0 to 255. By default, the priority is 0.

Description

Use the **c-bsr** command to configure a candidate BSR.

Use the **undo c-bsr** command to remove the candidate BSR configured.

By default, no candidate BSR is set.

When configure the candidate BSR, the larger bandwidth should be guaranteed since a great amount of information will be exchanged between BSR and other devices in the PIM domain.

Related command: **pim sm**.

Example

Configure the Ethernet switch as C-BSR with priority 2 (the C-BSR address is designated as the IP address of VLAN-interface10 and the PIM SM protocol is enabled on VLAN-interface 10).

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] multicast routing-enable
[SW8800] pim
[3Com-pim] c-bsr vlan-interface 10 24 2
```

c-rp

Syntax

c-rp *interface-type interface-number* [**group-policy** *acl-number* | **priority** *priority-value*]*

undo c-rp { *interface-type interface-number* | **all** }

View

PIM view

Parameter

interface-type interface-number: Interface type and interface number, used to specify the interface whose IP address is advertised as a candidate RP address.

acl-number: Number of the basic ACL that defines a group range, which is the service range of the advertised RP. The value ranges from 2000 to 2999.

priority-value: Priority value of candidate RP, in the range of 0 to 255. By default, it is 0. The greatest value corresponds to the lowest priority level

all: Removes all candidate RP configurations.

Description

Use the **c-rp** command to configure the router to advertise itself as a candidate RP.

Use the **undo c-rp** command to remove the configuration.

By default, no candidate RP is configured.

When configuring the candidate RP, a relatively large bandwidth should be reserved for the router and other devices in the PIM domain.

Related command: **c-bsr**.

Example

Configure the switch to advertise itself as a C-RP in the PIM domain to BSR. The standard access list 2000 defines the groups related to the RP. The address of C-RP is designated as the IP address of VLAN-interface10.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] acl number 2000
```

```
[3Com-acl-basic-2000] rule permit source 225.0.0.0 0.255.255.255
[3Com-acl-basic-2000]quit
[SW8800] multicast routing-enable
[SW8800] pim
[3Com-pim] c-rp vlan-interface 10 group-policy 2000
```

crp-policy

Syntax

crp-policy *acl-number*

undo crp-policy

View

PIM view

Parameter

acl-number: ACL number imported in C-RP filtering policy, ranging from 3000 to 3999.

Description

Use the **crp-policy** command to limit the range of legal C-RP, as well as target service group range of each C-RP, and prevent C-RP proofing.

Use the **undo crp-policy** command to restore the default setting, that is, no range limit is set and all received messages are taken as legal.

In the PIM SM network using BSR mechanism, every router can set itself as C-RP (candidate rendezvous point) servicing particular groups. If elected, a C-RP becomes the RP servicing the current group.

In BSR mechanism, a C-RP router unicasts C-RP messages to the BSR, which then propagates the C-RP messages among the network by BSR message.

To prevent C-RP spoofing, you need to configure **crp-policy** on the BSR to limit legal C-RP range and their service group range. Since each C-BSR has the chance to become BSR, you must configure the same filtering policy on each C-BSR router.

This command uses the ACLs numbered between 3000 and 3999. The **source** parameter in the **rule** command is translated as C-RP address in the **crp-policy** command, and the **destination** parameter as the service group range of this C-RP address. For the C-RP messages received, only when their C-RP addresses match the **source** address and their server group addresses are subset of those in ACL, can the be considered as matched.

Related command: **acl** and **rule**.

Example

Configure C-RP filtering policy on the C-BSR routers, allowing only 1.1.1.1/32 as C-RP and to serve only for the groups 225.1.0.0/16.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] multicast routing-enable
[SW8800] pim
```

```
[3Com-pim] crp-policy 3000
[3Com-pim] quit
[SW8800] acl number 3000
[3Com-acl-adv-3000] rule 0 permit source 1.1.1.1 0 destination 225.1
.0.0 0.0.255.255
```

debugging pim common

Syntax

debugging pim common { **all** | **event** | **packet** | **timer** }

undo debugging pim common { **all** | **event** | **packet** | **timer** }

View

User view

Parameter

all: All the common debugging information of PIM.

event: Debugging information of common PIM event.

packet: Debugging information of PIM hello packet.

timer: Debugging information of common PIM timer.

Description

Use the **debugging pim common** command to enable common PIM debugging functions.

Use the **undo debugging pim common** command to disable the debugging functions.

By default, common PIM debugging functions are disabled.

Example

Enable all common PIM debugging functions

```
<SW8800> debugging pim common all
```

debugging pim dm

Syntax

debugging pim dm { **alert** | **all** | **mrt** | **timer** | **warning** | { **recv** | **send** } { **all** | **assert** | **graft** | **graft-ack** | **join** | **prune** } }

undo debugging pim dm { **alert** | **all** | **mrt** | **timer** | **warning** | { **recv** | **send** } { **all** | **assert** | **graft** | **graft-ack** | **join** | **prune** } }

View

User view

Parameter

alert: Interoperation event debugging information of PIM-DM

all: All the debugging information of PIM-DM.

mrt: Debugging information of PIM-DM multicast routing table.

timer: Debugging information of PIM-DM timer.

warning: Debugging information of PIM-DM warning message.

recv: Debugging information of PIM-DM receiving packets.

send: Debugging information of PIM-DM sending packets.

assert | **graft** | **graft-ack** | **join** | **prune**: Packets type.

Description

Use the **debugging pim dm** command to enable PIM-DM debugging functions.

Use the **undo debugging pim dm** command to disable the debugging functions.

By default, PIM-DM debugging functions are disabled.

Example

Enable all PIM-DM debugging functions

```
<SW8800> debugging pim dm all
```

debugging pim sm

Syntax

debugging pim sm { **all** | **mbr** { **alert** | **fresh** } | **verbose** | **mrt** | **msdp** | **timer** { **assert** | **bsr** | **crpadv** | **jp** | **jpdelay** | **mrt** | **probe** | **spt** } | **warning** | { **recv** | **send** } { **assert** | **bootstrap** | **crpadv** | **jp** | **reg** | **regstop** } }

undo debugging pim sm { **all** | **mbr** { **alert** | **fresh** } | **verbose** | **mrt** | **msdp** | **timer** { **assert** | **bsr** | **crpadv** | **jp** | **jpdelay** | **mrt** | **probe** | **spt** } | **warning** | { **recv** | **send** } { **assert** | **bootstrap** | **crpadv** | **jp** | **reg** | **regstop** } }

View

User view

Parameter

all: All debugging information of PIM-SM.

mbr: Debugging information of PIM-SM multicast border router event. **Alert** stands for debugging alert information of PIM-SM multicast border router **fresh** stands for debugging renew information of PIM-SM multicast.

verbose: Debugging detail information of PIM-SM.

mrt: Debugging information of PIM-SM multicast routing table.

msdp: Debugging information of correspondence between PIM SM and MSDP.

timer: Debugging information of PIM-SM timer.

assert | **bsr** | **crpadv** | **jp** | **jpdelay** | **mrt** | **probe** | **spt**: PIM-SM timer type.

warning: Debugging information of PIM-SM warning message.

recv: Debugging information of PIM-SM receiving packets.

send: Debugging information of PIM-SM sending packets.

assert | **bootstrap** | **crpadv** | **jp** | **reg** | **regstop**: Packets type.

Description

Use the **debugging pim sm** command to enable PIM-SM debugging functions.

Use the **undo debugging pim sm** command to disable the debugging functions.

By default, PIM-SM debugging functions are disabled.

Example

Enable all PIM-SM debugging functions

```
<SW8800> debugging pim sm all
```

display pim bsr-info

Syntax

display pim bsr-info

View

Any view

Parameter

None

Description

Use the **display pim bsr** command to view the BSR information.

Related command: **c-bsr**, **c-rp**.

Example

```
<SW8800> display pim bsr-info
  Current BSR Address: 192.168.1.1
              Priority: 0
           Mask Length: 30
               Expires: 00:01:26
     Bootstrap-Period: 60 seconds
    Bootstrap-Timeout: 130 seconds
  Local host is BSR
```

Table 87 Description on the fields of the display pim bsr command

Field	Description
BSR	Boot strap router
Priority	Priority of BSR
Mask Length: 30	Length of mask
Expires: 00:01:55	Expire time
BootStrap-Period: 60 seconds	Boot strap interval
Bootstrap-timeout: 130 second	Boot strap timeout

display pim interface

Syntax

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

View

Any view

Parameter

interface-type interface-number: Interface type and interface number, used to specify the interface.

Description

Use the **display pim interface** command to view the PIM interface configuration information.

If no interface type or interface number is specified, this command displays the PIM configurations on all interfaces. If the interface type and interface number are specified, only the PIM configuration on the specified interface is displayed.

Example

Display the PIM configuration information on an interface.

```
<SW8800> display pim interface vlan 2
PIM information of VLAN-interface 2:
  IP address of the interface is 10.10.1.20
  PIM is enabled on interface
  PIM version is 2
  PIM mode is Sparse
  PIM query interval is 30 seconds
  PIM neighbor hold-time is 105 seconds
PIM neighbor limit is 128
  PIM neighbor policy is none
  Total 1 PIM neighbor on interface
  PIM DR(designated router) is 10.10.1.20
```

Table 88 Description on the fields of the display pim interface command

Field	Description
PIM version	Version of PIM
PIM mode	PIM mode enabled on the interface (DM or SM)
PIM query interval	Hello packet interval
PIM neighbor hold-time	Hold-time of PIM neighbor
PIM neighbor limit	Limit of the PIM neighbors on an interface. No neighbor can be added any more when the limit is reached
PIM neighbor policy	Filtering policy of the PIM neighbors on the current interface
PIM DR	Designated router

display pim neighbor

Syntax

display pim neighbor [**interface** *interface-type interface-number*]

View

Any view

Parameter

interface *interface-type interface-number*: Interface type and interface number, used to specify the interface.

Description

Use the **display pim neighbor** command to view the PIM neighbor information discovered by the switch interface. If the interface type and interface number are specified, this command only displays the PIM neighbor information on the specified interface.

Example

Display PIM neighbor information discovered by the switch interface.

```
<SW8800> display pim neighbor
Neighbor's Address  Interface Name               Uptime    Expires
90.0.0.2            Vlan-interface90             00:00:36  00:01:40
```

Table 89 Description on the fields of display pim neighbor command

Field	Description
Neighbor Address	Neighbor address
Interface	Interface where the neighbor has been discovered
Uptime	Time passed since the multicast group has been discovered
Expires	Specifies when the member will be removed from the group

display pim routing-table

Syntax

display pim routing-table [{ { ***g** [*group-address* [**mask** { *mask-length* | *mask* }]] | ****rp** [*rp-address* [**mask** { *mask-length* | *mask* }]] } | { *group-address* [**mask** { *mask-length* | *mask* }] | *source-address* [**mask** { *mask-length* | *mask* }] } ***** | **incoming-interface** { **interface** *interface-type interface-number* | **null** } | { **dense-mode** | **sparse-mode** }] *****

View

Any view

Parameter

***g**: (*, G) route entry.

mask: IP address mask.

mask-length: Length of the IP address mask.

****rp**: (*, *, p) route entry.

rp-address: Address of the RP.

group-address: Address of the multicast group.

source-address: IP address of the multicast source.

incoming-interface interface *interface-type interface-number*: Route entry with the specified incoming interface.

null: Specifies the incoming interface type as Null.

dense-mode: Specifies the multicast routing protocol as PIM-DM.

sparse-mode: Specifies the multicast routing protocol as PIM-SM.

Description

Use the **display pim routing-table** command to view the contents of the PIM multicast routing table. The displayed information of the PIM multicast routing table includes the SPT and RPF information.

Example

View the contents of the PIM multicast routing table on the router.

```
<SW8800> display pim routing-table
PIM-SM Routing Table
Total 0 (*,*,RP)entry, 0 (*,G)entry, 2 (S,G)entries

(192.168.1.2, 224.2.178.130),
Protocol 0x20: PIMSM, Flag 0x4: SPT
UpTime: 23:59, Timeout after 196 seconds
Upstream interface: VLAN-interface2, RPF neighbor: NULL
Downstream interface list: NULL

(192.168.1.2, 224.2.181.90),
Protocol 0x20: PIMSM, Flag 0x4: SPT
UpTime: 23:59, Timeout after 196 seconds
Upstream interface: VLAN-interface2, RPF neighbor: NULL
Downstream interface list: NULL
Total 2 entries listed
```

Table 90 Description on the fields of display pim routing-table

Field	Description
RP	Rendezvous Point
(S,G)	(source address, multicast group)
PIM-SM	PIM Sparse Mode
SPT	Shortest Path Tree
RPF	Reverse Path Forwarding

display pim rp-info

Syntax

display pim rp-info [*group-address*]

View

Any view

Parameter

group-address: Group address to display. If no multicast group is specified, the RP information about all multicast groups will be displayed.

Description

Use the **display pim rp-info** command to view the RP information of multicast group.

In addition, this command can also display the BSR and static RP information.

Example

View the RP information of multicast group.

```
<SW8800> display pim rp-info
PIM-SM RP-SET information:
    BSR is: 20.20.20.20

    Group/MaskLen: 224.0.0.0/4
      RP 20.20.20.20
        Version: 2
        Priority: 0
        Uptime: 00:00:05
        Expires: 00:02:25
        Adv-Period: 60 seconds
        Holdtime: 150 seconds
```

The following table details the display information.

Table 91 Description on the fields of display pim rp-info

Field	Description
PIM-SM RP-SET information:	RP information
BSR is: 4.4.4.6	BSR is the virtual interface of the node 4.4.4.6.
Group/MaskLen: 224.0.0.0/4 RP 4.4.4.6 Version: 2 Priority: 0 Uptime: 00:39:50 Expires: 00:01:40 Adv-Period: 60 seconds Holdtime: 150 seconds	The RP with IP address 224.0.0.0 and mask length of 4 is the virtual interface of the node 4.4.4.6, in version 2 and priority 0; it has been active for 39 minutes and 50 seconds and shall expire in one minute and 40 seconds; the advertisement interval is 60 seconds and holdtime is 150 seconds.

pim

Syntax

pim

undo pim

View

System view

Parameter

None

Description

Use the **pim** command to enter the PIM view and configure the PIM global parameters. Note that the command does not enable the PIM protocol.

Use the **undo pim** command to return to system view, clear the PIM global parameters configured before and clear the PIM view.

Example

Enter the PIM view.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] multicast routing-enable
[SW8800] pim
[3Com-pim]
```

pim bsr-boundary

Syntax

pim bsr-boundary

undo pim bsr-boundary

View

Interface view

Parameter

None

Description

Use the **pim bsr-boundary** command to configure an interface to be the PIM domain border.

Use the **undo pim bsr-boundary** command to remove the border.

By default, no domain border is set.

You can use this command to set border of bootstrap messages, that is to say, bootstrap messages cannot pass interfaces that are configured with **pim bsr-boundary** command while other PIM messages can. In this way, the network is divided into different BSR domains. Each domain uses a different bootstrap router.

CAUTION: *The **pim bsr-boundary** command cannot build a multicast boundary. It just sets up a PIM bootstrap message boundary.*

Related command: **c-bsr**.

Example

Configure domain border on VLAN-interface10.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800]interface vlan-interface 10
[3Com-Vlan-interface10] pim bsr-boundary
```

pim dm

Syntax

pim dm

undo pim dm

View

VLAN interface view

Parameter

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.

Before enabling PIM-DM, you must execute the **multicast routing-enable** command in system view to enable the multicast routing first.

Example

Enable PIM-DM on VLAN-interface10 of the Ethernet switch.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] multicast routing-enable
[SW8800]interface vlan-interface 10
[3Com-Vlan-interface10] pim dm
```

pim neighbor-limit

Syntax

pim neighbor-limit *limit*

undo pim neighbor-limit

View

Interface view

Parameter

limit: Limits of PIM neighbors on the interface, in the range of 0~128.

Description

Use the **pim neighbor-limit** command to limit the PIM neighbors on an interface. No neighbor can be added any more when the limit is reached.

Use the **undo pim neighbor-limit** command to restore the default setting.

By default, the PIM neighbors on the interface are limited to 128.

If the existing PIM neighbors exceed the configured value during configuration, they will not be deleted.

Example

Limit the PIM neighbors on the Vlan-interface10 to 50.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
```

```
[SW8800]interface vlan-interface 10
[3Com-Vlan-interface10] pim neighbor-limit 50
```

pim neighbor-policy

Syntax

pim neighbor-policy *acl-number*

undo pim neighbor-policy

View

Interface view

Parameter

acl-number: Basic ACL number, in the range of 2000 to 2999.

Description

Use the **pim neighbor-policy** command to set to filter the PIM neighbors on the current interface.

Use the **undo pim neighbor-policy** command to remove the setting.

Only the routers that match the filtering rule in the ACL can serve as a PIM neighbor of the current interface.

The new configuration overwrites the old one if you run the command for a second time.

Example

Configure that 10.10.1.2 can serve as a PIM neighbor of the Vlan-interface10, but not 10.10.1.1.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800]interface vlan-interface 10
[3Com-Vlan-interface10] pim neighbor-policy 2000
[3Com-Vlan-interface10] quit
[SW8800] acl number 2000
[3Com-acl-basic-2000] rule permit source 10.10.1.2 0
[3Com-acl-basic-2000] rule deny source 10.10.1.1 0
```

pim sm

Syntax

pim sm

undo pim sm

View

Interface view

Parameter

None

Description

Use the **pim sm** command to enable the PIM-SM protocol on an interface.

Use the **undo pim sm** command to disable the PIM-SM protocol.

By default, PIM-SM is disabled.

Users need to configure the PIM-SM protocol on each interface. Generally, the PIM-SM protocol needs to be enabled on each interface.

Related command: **multicast routing-enable**.

Example

Enable PIM-SM on VLAN-interface10.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800]interface vlan-interface 10
[3Com-Vlan-interface10] pim sm
```

pim timer hello

Syntax

pim timer hello *seconds*

undo pim timer hello

View

Interface view

Parameter

seconds: Time interval for a port to send Hello packets, in the range of 1 to 18,000 (in seconds). By default, the time interval is 30 seconds.

Description

Use the **pim timer hello** command to configure the time interval for a port to send Hello packets.

Use the **undo pim timer hello** command to restore the default time interval.

After the protocol independent multicast-sparse mode (PIM-SM) protocol is enabled for a port, a switch sends Hello packets periodically to all network devices supporting protocol independent multicast (PIM) to find its neighbors. If a port receives the Hello packets, it indicates the port has a neighbor network device supporting PIM, and the port adds the neighbor to its port neighbor list. If a port does not receive the Hello packets from the existing neighbors in its neighbor list in the specified time, the system assumes the neighbor has left the multicast group.

- You must enable a PIM protocol (PIM-DM or PIM-SM) in interface view before you can proceed with this configuration.
- When you configure the time interval for a port to send Hello packets, the PIM neighbor hold-time value is automatically set to 3.5 times the Hello interval. Therefore you need not configure the PIM neighbor hold-time separately.

Example

Set the time interval to send Hello packets for VLAN-interface10 to 40 seconds.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800]interface vlan-interface 10
[3Com-Vlan-interface10] pim timer hello 40
```

register-policy

Syntax

register-policy *acl-number*

undo register-policy

View

PIM view

Parameter

acl-number: Number of IP advanced ACL, defining the rule of filtering the source and group addresses. The value ranges from 3000 to 3999.

Description

Use the **register-policy** command to configure a RP to filter the register messages sent by the DR (the last-hop router) in the PIM-SM network and to accept the specified messages only.

Use the **undo register-policy** command to remove the configured message filtering.

Example

If the local device is the RP in the network, using the following command can only accept multicast message register of the source sending multicast address in the range of 225.1.0.0/16 on network segment 10.10.0.0/16.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] acl number 3010
[3Com-acl-adv-3010] rule permit ip source 10.10.0.0 0.0.255.255 dest
ination 225.1.0.0 0.0.255.255
[3Com-acl-adv-3010] quit
[SW8800] multicast routing-enable
[SW8800] pim
[3Com-pim] register-policy 3010
```

reset pim neighbor

Syntax

reset pim neighbor { **all** | { *neighbor-address* | **interface** *interface-type interface-number* } * }

View

User view

Parameter

all: All PIM neighbors

neighbor-address: Neighbor address.

interface *interface-type interface-number*: Specifies interface.

Description

Use the **reset pim neighbor** command to clear a PIM neighbor.

Related command: **display pim neighbor**.

Example

Clear the PIM neighbor 25.5.4.3.

```
<SW8800> reset pim neighbor 25.5.4.3
```

reset pim routing-table

Syntax

reset pim routing-table { **all** | { *group-address* [**mask** *group-mask* | **mask-length** *group-mask-length*] | *source-address* [**mask** *source-mask* | **mask-length** *source-mask-length*] | { **incoming-interface** *interface-type interface number* | **null** } } * }

View

User view

Parameter

all: All PIM neighbors.

group-address: Group address.

mask *group-mask*: Specifies group mask.

mask-length *group-mask-length*: Mask length of the group address.

source-address: Source address.

mask *source-mask*: Specifies source mask.

mask-length *source-mask-length*: Specifies mask length of the group address.

incoming-interface: Specifies incoming interface for the route entry in PIM routing table.

interface-type interface-number: Interface type and interface number, used to specify the interface.

Description

Use the **reset pim routing-table** command to clear a PIM route entry.

You can type in *source address* first and *group address* after in the command, as long as they are valid. Error information will be given if you type in invalid addresses.

If in this command, the *group-address* is 224.0.0.0/24 and *source-address* is the RP address (where group address can have a mask, but the resulted IP address

must be 224.0.0.0, and source address has no mask), then it means only the (*, *, RP) item will be cleared.

If in this command, the *group-address* is any a group address, and *source-address* is 0 (where group address can have a mask, and source address has no mask), then only the (*, G) item will be cleared.

This command shall clear not only multicast route entries from PIM routing table, but also the corresponding route entries and forward entries in the multicast core routing table and MFC.

Related command: **reset multicast routing-table**, **reset multicast forwarding-table** and **display pim routing-table**.

Example

Clear the route entries with group address 225.5.4.3 from the PIM routing table.

```
<SW8800> reset pim neighbor 25.5.4.3
```

source-policy

Syntax

source-policy *acl-number*

undo source-policy

View

PIM view

Parameter

acl-number: Basic or advanced ACL, in the range of 2000 to 3999.

Description

Use the **source-policy** command to set the router to filter the multicast data packets based on source (or group) address.

Use the **undo static-rp** command to remove the configuration.

If resource address filtering is configured, as well as basic ACLs, then the router filters the resource addresses of all multicast data packets received. Those not matched will be discarded.

If resource address filtering is configured, as well as advanced ACLs, then the router filters the resource and group addresses of all multicast data packets received. Those not matched will be discarded.

When this feature is configured, the router filters not only multicast data, but the multicast data encapsulated in the registration packets.

The new configuration overwrites the old one if you run the command for a second time.

Example

Set to receive the multicast data packets from source address 10.10.1.2, but discard those from 10.10.1.1.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] multicast routing-enable
[SW8800] pim
[3Com-pim] source-policy 2000
[3Com-pim] quit
[SW8800] acl number 2000
[3Com-acl-basic-2000] rule permit source 10.10.1.2 0
[3Com-acl-basic-2000] rule deny source 10.10.1.1 0
```

static-rp

Syntax

static-rp *rp-address* [*acl-number*]

undo static-rp

View

PIM view

Parameter

rp-address: Static RP address, only being legal unicast IP address.

acl-number: Basic ACL, used to control the range of multicast group served by static RP, which ranges from 2000 to 2999. If an ACL is not specified upon configuration, static RP will serve all multicast groups; if an ACL is specified, static RP will only serve the multicast group passing the ACL.

Description

Use the **static-rp** command to configure static RP.

Use the **undo static-rp** command to remove the configuration.

Static RP functions as the backup of dynamic RP so as to improve the network robustness. If the RP elected by BSR mechanism is valid, static RP will not work.

All routers in the PIM domain should be configured with this command and be specified with the same RP address.

The new configuration overwrites the old one if you run the command for a second time.

CAUTION:

- When the BSR-elected RP is effective, the static RP does not work.
- All routers in the PIM domain must be configured with this command simultaneously, with the same RP address specified.
- The system supports up to ten different static RP addresses. When more than ten static RP addresses are configured, the system will give this prompt information:

  ```
  "Cannot config static-rp, exceeded static-rp limit 10".
  ```

Related command: **display pim rp-info**.

Example

Configure 10.110.0.6 as a static RP.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] multicast routing-enable
[SW8800] pim
[3Com-pim] static-rp 10.110.0.6
```

Remove the static RP with the IP address of 10.110.0.6.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] multicast routing-enable
[SW8800] pim
[3Com-pim] undo static-rp 10.110.0.6
```

37 MSDP CONFIGURATION COMMANDS

An Ethernet switch functions as a router when it supports the layer 3 protocols. A router that is referred to in the following represents a generalized router or a layer 3 Ethernet switch running related protocols.

MSDP Configuration Commands

cache-sa-enable

Syntax

cache-sa-enable

undo cache-sa-enable

View

MSDP view

Parameter

None

Description

Use the **cache-sa-enable** command to enable the router to cache SA state.

Use the **undo cache-sa-enable** command to remove the cache from the router.

By default, the router caches the SA state, i.e., (S, G) entry after it receives SA messages.

If the router is in cache state, it will not send SA request message to the specified MSDP peer when it receives a new group join message.

Example

Configure the router to cache all the SA states.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] msdp
[3Com-msdp] 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

Parameter

all: All the debugging information of MSDP.

connect: Debugging information of MSDP peer connection reset.

event: Debugging information of MSDP event.

packet: Debugging information of MSDP packet.

source-active: Debugging information of active MSDP source.

Description

Use the **debugging msdp** command to enable MSDP debugging functions.

Use the **undo debugging msdp** command to disable MSDP debugging functions.

By default, MSDP debugging functions are disabled.

Example

Enable all common MSDP debugging functions.

```
<SW8800> debugging msdp all
```

display msdp brief

Syntax

display msdp brief

View

Any view

Parameter

None

Description

Use the **display msdp brief** command to view the state of MSDP peer.

Example

Display the state of MSDP peer.

```
<SW8800> display msdp brief
MSDP Peer Brief Information
  Peer's Address     State   Up/Down time   AS     SA Count  Reset Count
  20.20.20.20        Up       00:00:13        100    0          0
```

display msdp peer-status

Syntax

display msdp peer-status [*peer-address*]

View

Any view

Parameter

peer-address: Address of MSDP peer.

Description

Use the **display msdp peer-status** command to view the detailed information of MSDP peer.

Related command: **peer**.

Example

Display the detailed information of the MSDP peer 10.110.11.11.

```
<SW8800> display msdp peer-status 10.110.11.11
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
```

display msdp sa-cache

Syntax

display msdp sa-cache [*group-address* | *source-address* | *autonomous-system-number*]*

View

Any view

Parameter

group-address: Group address of (S, G) entry.

source-address: Source address of (S, G) entry. With no source address specified, all the source information of the specified group will be displayed.

If neither group address nor source address is determined, all SA caches will be displayed.

autonomous-system-number: Autonomous system number. Displays (S, G) entries from specified autonomous system.

Description

Use the **display msdp sa-cache** command to view (S, G) state learnt from MSDP peer.

Only **cache-sa-enable** command is configured, can cache state be displayed.

Example

Display the (S, G) state learned from MSDP peer.

```
<SW8800> 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
```

display msdp sa-count

Syntax

display msdp sa-count [*as-number*]

View

Any view

Parameter

as-number: Number of sources and groups from the specified autonomous system.

Description

Use the **display msdp sa-count** command to view the number of sources and groups in MSDP cache.

The **cache-sa-enable** command must be configured before the configuration of this command.

Example

view the number of sources and groups in MSDP cache.

```
<SW8800> 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 Source-Active entries: 5
```

import-source

Syntax

import-source [**acl** *acl-number*]

undo import-source

View

MSDP view

Parameter

acl-number: Number of basic or advanced IP ACL, ranging from 2000 to 3999, controlling which sources SA messages will advertise and to which groups it will be sent in the domain. Basic ACL performs filtering to source and advanced ACL performs filtering to source/group. If no ACL is specified, no multicast source will be advertised.

Description

Use the **import-source** command to configure which (S, G) entries in the domain need to be advertised when a MSDP originates an SA message.

Use the **undo import-source** command to remove the configuration.

By default, all the (S, G) entries in the domain are advertised by the SA message.

Besides controlling SA messages creation, you can filter the forwarded SA messages by the commands **peer sa-policy import** and **peer sa-policy export**.

Example

Specify that the MSDP peer, when creating an SA message, advertises (S,G) entries with their source addresses in the range of 10.10.0.0/16 and multicast group addresses in the range of 225.1.0.0/16 in the multicast routing table.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] acl number 3001
[3Com-acl-adv-3001] rule permit ip source 10.10.0.0 0.0.255.255 dest
ination 225.1.0.0 0.0.255.255
[3Com-acl-adv-3001] quit
[SW8800] msdp
[3Com-msdp] import-source acl 3001
```

msdp

Syntax

msdp

undo msdp

View

System view

Parameter

None

Description

Use the **msdp** command to enable MSDP and enter the MSDP view.

Use the **undo msdp** command to clear all configurations of MSDP, release all resources that MSDP occupies, and restore the initial state.

Related command: **peer**.

Example

Clear all configurations of MSDP.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] undo msdp
```

msdp-tracert

Syntax

msdp-tracert *source-address group-address rp-address* [**max-hops** *max-hops* | **next-hop-info** | **sa-info** | **peer-info** | **skip-hops** *skip-hops*]*

View

Any view

Parameter

source-address: Multicast source address.

group-address: Multicast group address.

rp-address: IP address of RP.

max-hops: The maximum number of hops that are traced, ranging from 1 to 255. By default, the value is 16.

next-hop-info: Specifies flag bit for collecting the next hop information.

sa-info: Specifies flag bit for collecting SA entity information.

peer-info: Specifies flag bit for collecting MSDP peer information.

skip-hops: Number of hops that are skipped before collecting detailed information, ranging from 0 to 255. By default, the value is 0.

Description

Use the **msdp-tracert** command to trace the transmission path of SA messages in the network, which helps to locate the faults such as information loss and configuration error. After the transmission path of SA messages is determined, correct configuration can avoid the overflow of SA messages.

Example

Trace (10.10.1.1, 225.2.2.2, 20.20.20.20) path information.

```
<SW8800> msdp-tracert 10.10.1.1 225.2.2.2 20.20.20.20
```

Specify the maximum number of hops that are traced and collect detailed information of SA and MSDP peer.

```
<SW8800> msdp-tracert 10.10.1.1 225.2.2.2 20.20.20.20 max-hops 10 sa-
info peer-info
MSDP tracert: press CTRL_C to break
 D-bit:  set if have this (S,G) in cache but with a different RP
 RP-bit: set if this router is an RP
 NC-bit: set if this router is not caching SA's
 C-bit:  set if this (S,G,RP) tuple is in the cache
 MSDP Traceroute path information:
   Router Address:  20.20.1.1
     Fixed-length response info:
       Peer Uptime: 10 minutes,  Cache Entry Uptime: 30 minutes
       D-bit: 0,  RP-bit: 1,  NC-bit: 0,  C-bit: 1
       Return Code: Reached-max-hops
     Next Hop info:
       Next-Hop Router Address: 0.0.0.0
     SA info:
       Count of SA messages received for this (S,G,RP): 0
       Count of encapsulated data packets received for this (S,G,RP):0
       SA cache entry uptime: 00:30:00 ,  SA cache entry expiry time: 00:03:32
     Peering info:
       Peering Uptime: 10 minutes,  Count of Peering Resets: 3
```

Table 92 Description of msdp-tracert command domain

Item	Description
Router Address	Address where the local router creates Peering session with Peer-RPF neighbor.
Peer Uptime	Time for which the local router performs Peering session with Peer-RPF neighbor in minute, with the maximum value of 255.
Cache Entry Uptime	Present time of (S, G, RP) entry in SA cache of the local router, in minute, with the maximum value of 255.
D-bit: 1	(S, G, RP) entry existing in SA cache of the local router.
	But the RP is different from the RP specified in the request message.
RP-bit: 1	The local router is an RP, but it is not necessarily the source RP in (S, G, RP) entry.
NC-bit: 0	The local router enables SA cache.
C-bit: 1	(S, G, RP) entry exists in SA cache of the local router.
Return Code: Reached-max-hops	Return reason is the reached maximum hops and other possible value includes:
	Hit-src-RP: The local hop router is the source RP in (S, G, RP) entry.
Next-Hop Router Address: 0.0.0.0	If the parameter next-hop-info is used, Peer-RPF neighbor address will be displayed.
Count of SA messages received for this (S,G,RP)	Number of SA messages received for tracing this (S, G, RP) entry.
Count of encapsulated data packets received for this (S,G,RP)	Number of encapsulated data packets received for tracing this (S, G, RP) entry.
SA cache entry uptime	Present time of SA cache entry.
SA cache entry expiry time	Expiry time of SA cache entry.
Peering Uptime: 10 minutes	Time for which the local router performs Peering session with Peer-RPF neighbor.
Count of Peering Resets	Number of Peering session resets.

originating-rp

Syntax

originating-rp *interface-type interface-number*

undo originating-rp

View

MSDP view

Parameter

interface-type: Interface type.

interface-number: Interface number.

Description

Use the **originating-rp** command to allow a MSDP to use the IP address of specified interface as the RP address when the SA message originated.

Use the **undo originating-rp** command to remove the configuration.

By default, the RP address in the SA message is the RP address configured by PIM.

Configure logical RP by using this command.

Example

Configure IP address of the interface Vlan-interface10 as the RP address in the SA message originated.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] msdp
[3Com-msdp] originating-rp Vlan-interface 10
```

peer

Syntax

peer *peer-address* **connect-interface** *interface-type interface-number*

undo peer *peer-address*

View

MSDP view

Parameter

peer-address: Address of MSDP peer.

connect-interface *interface-type interface-number*: Interface type and number whose primary address is used by the local router as the source IP address to establish TCP connection with remote MSDP peers.

Description

Use the **peer** command to configure an MSDP peer.

Use the **undo peer** command to remove the MSDP peer configured.

If the local router is also in BGP peer relation with a MSDP peer, the MSDP peer and the BGP peer should use the same IP address.

Related command: **static-rpf-peer**.

Example

Configure the router using IP address 125.10.7.6 as an MSDP peer of the local router.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] msdp
[3Com-msdp] peer 125.10.7.6 connect-interface Vlan-interface 10
```

peer description

Syntax

peer *peer-address* **description** *text*

undo peer *peer-address* **description**

View

MSDP view

Parameter

peer-address: Address of MSDP peer.

text: Descriptive text, being case sensitive. The maximum length is 80 characters.

Description

Use the **peer description** command to configure descriptive text to MSDP peer.

Use the **undo peer description** command to remove the descriptive text configured.

By default, an MSDP peer has no descriptive text.

Administrator can conveniently differentiate MSDP peers by configuring descriptive text.

Related command: **display msdp peer-status**.

Example

Add descriptive text CstmrA to router 125.10.7.6 to specify that the router is Client A.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] msdp
[3Com-msdp] peer 125.10.7.6 description router CstmrA
```

peer mesh-group

Syntax

peer *peer-address* **mesh-group** *name*

undo peer *peer-address* **mesh-group** *name*

View

MSDP view

Parameter

name: Name of a Mesh Group, being case sensitive. The maximum length is 32 characters.

peer-address: Address of an MSDP peer to be a member of the Mesh Group.

Description

Use the **peer mesh-group** command to configure an MSDP peer to join an Mesh Group.

Use the **undo peer mesh-group** command to remove the configuration.

By default, an MSDP peer is not a member of any Mesh Group.

Example

Configure the MSDP peer with address 125.10.7.6 to be a member of the Mesh Group Grp1.

```
<SW8800> system-view
[SW8800] msdp
[3Com-msdp] peer 125.10.7.6 mesh-group Grp1
```

peer minimum-ttl

Syntax

peer *peer-address* **minimum-ttl** *ttl*

undo peer *peer-address* **minimum-ttl**

View

MSDP view

Parameter

peer-address: Address of the MSDP peer to which the TTL limitation applies.

ttl: TTL threshold, ranging from 0 to 255.

Description

Use the **peer minimum-ttl** command to configure the minimum TTL (Time-to-Live) value of the multicast data packets encapsulated in SA messages to be sent to specified MSDP peer.

Use the **undo peer minimum-ttl** command to restore the default TTL threshold.

By default, the value of TTL threshold is 0.

Related command: **peer**.

Example

Configure the TTL threshold value to 10, i.e., only those multicast data packets with a TTL value greater than or equal to 10 can be forwarded to the MSDP peer 110.10.10.1.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
```

```
[SW8800] msdp
[3Com-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

Parameter

peer-address: Address of MSDP peer.

Description

Use the **peer request-sa-enable** command to enable the router to send SA request message to the specified MSDP peer when receiving a new group join message.

Use the **undo peer request-sa-enable** command to remove the configuration.

By default, when receiving a new group join message, the router sends no SA request messages to MSDP peers but waits to receive the next SA message.

Related command: **cache-sa-enable**.

Example

Configure to send SA request message to the MSDP peer 125.10.7.6.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] msdp
[3Com-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

Parameter

peer-address: Address of MSDP peer.

sa-limit: Maximum value that the SA cache allows, ranging from 1 to 2048.

Description

Use the **peer sa-cache-maximum** command to limit the number of caches originated when the router receives SA messages from an MSDP peer.

Use the **undo peer sa-cache-maximum** command to restore the default configuration.

By default, the maximum number of SA caches is 2048.

This configuration is recommended for all MSDP peers in the networks possibly attacked by DoS.

Related command: **display msdp**, **sa-count**, **display msdp peer-status**, **display msdp brief**.

Example

Limit the number of caches originated to 100 when the router receives SA messages from the MSDP peer 125.10.7.6.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] msdp
[3Com-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

Parameter

import: Receives SA messages from the specified MSDP peer.

export: Forwards SA messages from the specified MSDP peer.

peer-address: Address of the MSDP peer whose SA messages need to be filtered.

acl *acl-number*: Number of advanced IP ACL, ranging from 3000 to 3999. If no ACL is specified, all (S, G) entries are filtered.

Description

Use the **peer sa-policy** command to configure a filter list for SA messages received or forwarded from the specified MSDP peer.

Use the **undo peer sa-policy** command to remove the configuration.

By default, messages received or forwarded will not be filtered. All SA messages are received or forwarded from an MSDP peer.

Related command: **peer**.

Example

Forward only those SA messages that passed the advanced IP ACL.

```
<SW8800> system-view
[SW8800] acl number 3000
```

```
[3Com-acl-adv-3000] rule permit ip source 170.15.0.0 0.0.255.255
destination 225.1.0.0 0.0.255.255
[3Com-acl-adv-3000] quit
[SW8800] msdp
[3Com-msdp] peer 125.10.7.6 connect-interface Vlan-interface 10
[3Com-msdp] peer 125.10.7.6 sa-policy export acl 3000
```

peer sa-request-policy

Syntax

peer *peer-address* **sa-request-policy** [**acl** *acl-number*]

undo peer *peer-address* **sa-request-policy**

View

MSDP view

Parameter

peer-address: Address from which the local router receives SA request messages sent by the specified MSDP peer.

acl *acl-number*: Number of basic IP ACL, describing multicast group address, ranging from 2000 to 2999. If no ACL is specified, all SA request messages will be ignored.

Description

Use the **peer sa-request-policy** command to limit SA request messages that the router receives from MSDP peers.

Use the **undo peer sa-request-policy** command to remove the limitation.

By default, the router receives all SA request messages from the MSDP peer.

If no ACL is specified, all SA requests will be ignored. If ACL is specified, only those SA request messages from the groups permitted by the ACL will be processed and all the others will be ignored.

Related command: **peer**.

Example

Configure the ACL for filtering SA request messages from the MSDP peer 175.58.6.5. The SA request messages from group address range 225.1.1.0/8 will be received and all the others will be ignored.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] acl number 2000
[3Com-acl-basic-2000] rule permit source 225.1.1.0 0.255.255.255
[3Com-acl-basic-2000] quit
[SW8800] msdp
[3Com-msdp] peer 175.58.6.5 sa-request-policy acl 2000
```

reset msdp peer

Syntax

reset msdp peer *peer-address*

View

User view

Parameter

peer-address: Address of MSDP peer.

Description

Use the **reset msdp peer** command to reset TCP connection with the specified MSDP peer, and clear all the statistics of the specified MSDP peer.

Related command: **peer**.

Example

Clear TCP connection and statistics of the MSDP peer 125.10.7.6.

```
<SW8800> reset msdp peer 125.10.7.6
```

reset msdp sa-cache

Syntax

reset msdp sa-cache [*group-address*]

View

User view

Parameter

group-address: Address of the group, (S, G) entries matching this address are cleared from the SA cache. If no multicast group address is specified, all SA cache entries will be cleared.

Description

Use the **reset msdp sa-cache** command to clear SMDP SA cache entries.

Related command: **cache-sa-enable** and **display msdp sa-cache**.

Example

Clear the cache entries with group address 225.5.4.3 from the SA cache.

```
<SW8800> reset msdp sa-cache 225.5.4.3
```

reset msdp statistics

Syntax

reset msdp statistics [*peer-address*]

View

User view

Parameter

peer-address: Address of the MSDP peer whose statistics, resetting information and input/output information will be cleared. If no MSDP peer address is specified, all MSDP peers statistics will be cleared.

Description

Use the **reset msdp statistics** command to clear statistics of one or more MSDP peers without resetting the MSDP peer.

Example

Clear the statistics of the MSDP peer 25.10.7.6.

```
<SW8800> reset msdp statistics 125.10.7.6
```

shutdown

Syntax

shutdown *peer-address*

undo shutdown *peer-address*

View

MSDP view

Parameter

peer-address: IP address of MSDP peer.

Description

Use the **shutdown** command to disable the MSDP peer specified.

Use the **undo shutdown** command to remove the configuration.

By default, no MSDP peer is disabled.

Related command: **peer**.

Example

Disable the MSDP peer 125.10.7.6.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] msdp
[3Com-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

Parameter

peer-address: Address of the static RPF peer to receive SA messages.

rp-policy *ip-prefix-name*: Filter policy based on RP address, which filters the RP in SA messages. If the parameter is not specified, all SA messages from static RPF peer will be accepted. If the parameter **rp-policy** *ip-prefix-name* is specified and filter policy is configured, the router will only accept SA messages from the RP

which passes filtering. If no filter policy is configured, the router will still accept all SA messages from the static RPF peer.

Description

Use the **static-rpf-peer** command to configure static RPF peer.

Use the **undo static-rpf-peer** command to remove the static RPF peer.

By default, no static RPF peer is configured.

- You must configure the **peer** command before using the **static-rpf-peer** command.
- If only one MSDP peer is configured on a router, this MSDP peer will be regarded as a static RPF peer.

Related command: **peer** and **ip prefix-list**.

Example

Configure two static RPF peers.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] ip ip-prefix list1 permit 130.10.2.3 32
[SW8800] ip ip-prefix list2 permit 130.10.2.4 32
[SW8800] msdp
[3Com-msdp] peer 130.10.7.6 connect-interface Vlan-interface 10
[3Com-msdp] peer 130.10.7.5 connect-interface Vlan-interface 10
[3Com-msdp] static-rpf-peer 130.10.7.6 rp-policy list1
[3Com-msdp] static-rpf-peer 130.10.7.5 rp-policy list2
```

In the above commands, 130.10.2.3 is the IP address of the RP for 130.10.7.5 and 130.10.2.4 is the IP address of the RP of 130.10.7.6.

timer retry

Syntax

timer retry *seconds*

undo timer retry

View

MSDP view

Parameter

seconds: Value of connection request retry period in second, ranging from 1 to 60.

Description

Use the **timer retry** command to configure the value of connection request re-try period.

Use the **undo timer retry** command to restore the default value.

By default, the value of connection request re-try period is 30 seconds.

peer.

Related command:

Example

Configure the connection request re-try period to 60 seconds.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.


[SW8800] msdp
[3Com-msdp] timer retry 60
```

38

MBGP MULTICAST EXTENSION CONFIGURATION COMMANDS

MBGP Multicast Extension Configuration Commands

aggregate

Syntax

aggregate *address mask* [**as-set** | **attribute-policy** *route-policy-name* | **detail-suppressed** | **origin-policy** *route-policy-name* | **suppress-policy** *route-policy-name*]*

undo aggregate *address mask* [**as-set** | **attribute-policy** *route-policy-name* | **detail-suppressed** | **origin-policy** *route-policy-name* | **suppress-policy** *route-policy-name*]*

View

IPv4 multicast sub-address family view

Parameter

address: Address of the aggregated route.

mask: Network mask of the aggregated route.

as-set: Generates a route with AS_SET segment. This parameter is not recommended when aggregating many AS paths.

attribute-policy *route-policy-name*: Sets aggregate attribute.

detail-suppressed: Advertises the aggregated routes rather than the specific routes.

origin-policy *route-policy-name*: Filters the originate routes of the aggregate.

suppress-policy *route-policy-name*: Does not advertise the specific routes selected.

Description

Use the **aggregate** command to create a multicast aggregated record in the BGP routing table.

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

By default, no route is aggregated.

Use the **aggregate** command without parameters to create one local aggregated route and set atomic aggregation attributes.

Example

Create an aggregation entry in the MBGP routing table, with aggregated route address as 192.213.0.0.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] bgp 100
[3Com-bgp] ipv4-family multicast
[3Com-bgp-af-mul] aggregate 192.213.0.0 255.255.0.0
```

compare-different-as-med

Syntax

compare-different-as-med

undo compare-different-as-med

View

IPv4 multicast sub-address family view

Parameter

None

Description

Use the **compare-different-as-med** command to enable to compare the route MED values of neighbors from different ASs.

Use the **undo compare-different-as-med** command to disable this function.

By default, the comparison function is disabled.

If there are multiple routes available to the same destination address, you can select the route with the smallest MED value.

This command is not recommended unless you make sure that different ASs use the same IGP and route selection modes.

Example

Enable to compare the route MED values of neighbors from different ASs.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] bgp 100
[3Com-bgp] ipv4-family multicast
[3Com-bgp-af-mul] compare-different-as-med
```

debugging bgp mp-update

Syntax

debugging bgp mp-update [**receive** | **send**] [**verbose**]

undo debugging bgp mp-update

View

User view

Parameter

receive: Debugs the MBGP Update messages received.

send: Debugs the MBGP Update messages sent.

verbose: Debugs detailed information.

Description

Use the **debugging bgp mp-update** command to enable to debug MBGP Update messages.

Use the **undo debugging bgp mp-update** command to disable the debugging.

By default, the debugging function is disabled.

Example

Enable MBGP Update message debugging.

```
<SW8800> debugging bgp mp-update
```

default local-preference

Syntax

default local-preference *value*

undo default local-preference

View

IPv4 multicast sub-address family view

Parameter

value: Default local precedence you configured, in the range of 0 to 4294967295. By default, it is 100. The greatest value corresponds to the highest precedence level.

Description

Use the **default local-preference** command to configure the default local precedence.

Use the **undo default local-preference** command to restore the default value.

You can affect BGP route selection by configuring different local precedence values.

Example

Configure the default local precedence value as 180.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] bgp 100
```

```
[3Com-bgp] ipv4-family multicast
[3Com-bgp-af-mul] default local-preference 180
```

default med

Syntax

default med *med-value*

undo default med

View

IPv4 multicast sub-address family view

Parameter

med-value: MED value, in the range of 0 to 4294967295. By default, it is 0.

Description

Use the **default med** command to configure system MED value.

Use the **display bgp multicast group** command to restore the default value.

Multi-exit discriminator (MED) attribute is the external metric for a route. Unlike local precedence attribute, MED is exchanged, between ASs, and one it enters an AS, it does not leave the AS. MED attribute is used in best route selection. When a router running BGP travels through different external peers and get the routes with identical destination, but different next-hop addresses, it selects these routes according to their MED values. The route with smaller MED value will be selected as the external AS route if other attributes are the same.

Example

Configure system MED value as 25.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] bgp 100
[3Com-bgp] ipv4-family multicast
[3Com-bgp-af-mul] default med 25
```

display bgp multicast group

Syntax

display bgp multicast group [*group-name*]

View

Any view

Parameter

group-name: Peer group. If no peer group is specified, the information about all peer groups will be displayed.

Description

Use the **display bgp multicast group** command to view the information about peer groups.

Example

View the information about the peer group named my_peer.

```
<SW8800> display bgp multicast group my_peer
```

display bgp multicast network

Syntax

display bgp multicast network

View

Any view

Parameter

None

Description

Use the **display bgp multicast network** command to view the routing information that MBGP advertises.

Example

View the network segment routing information MBGP advertises.

```
<SW8800> display bgp multicast network
```

display bgp multicast peer

Syntax

display bgp multicast peer [*peer-address*] [**verbose**]

View

Any view

Parameter

peer-address: Peer address, in dotted decimal format.

verbose: Displays detailed information.

Description

Use the **display bgp multicast peer** command to view the MBGP peer information.

Example

View the MBGP peer detailed information.

```
<SW8800> display bgp multicast peer verbose
```

display bgp multicast routing-table

Syntax

display bgp multicast routing-table [*ip-address* [*mask*]]

View

Any view

Parameter

ip-address: IP address of the network segment whose MBGP routing information with specified IP address.

Description

Use the **display bgp multicast routing-table** command to view MBGP routing information.

Example

Display MBGP routing information of network segment 14.1.0.0.

```
<SW8800> display bgp multicast routing-table 14.1.0.0
```

display bgp multicast routing-table as-path-acl

Syntax

display bgp multicast routing-table as-path-acl *acl-number*

View

Any view

Parameter

acl-number: Matched AS path list number, ranging from 1 to 199.

Description

Use the **display bgp multicast routing-table as-path-acl** command to view routes that match an as-path acl.

Example

Display routes that match the as-path-acl 2.

```
<SW8800> display bgp multicast routing-table as-path-acl 2
```

display bgp multicast routing-table cidr

Syntax

display bgp multicast routing-table cidr

View

Any view

Parameter

None

Description

Use the **display bgp multicast routing-table cidr** command to view the non-natural network mask, namely the classless inter-domain routing (CIDR) information.

Example

View CIDR routing information.

```
<SW8800> display bgp multicast routing-table cidr
```

display bgp multicast routing-table community

Syntax

display bgp multicast routing-table community [*aa*:*nn* | **no-export-subconfed** | **no-advertise** | **no-export**]* [**whole-match**]

View

Any view

Parameter

aa:*nn*: Community number.

no-export-subconfed: Does not send matched routes outside the local autonomous system.

no-advertise: Does not advertise matched routes to any peer.

no-export: Does not advertise routes outside the local autonomous system but advertise routes to other sub-autonomous systems.

whole-match: Exact match.

Description

Use the **display bgp multicast routing-table community** command to view routing information of a specified MBGP community.

Example

Display routing information of the specified MBGP community

```
<SW8800> display bgp multicast routing-table community 600:1
```

display bgp multicast routing-table community-list

Syntax

display bgp multicast routing-table community-list *community-list-number* [**whole-match**]

View

Any view

Parameter

community-list-number: Number of the specified community list.

exact-match: Exact match.

Description

Use the **display bgp multicast routing-table community-list** command to view the routing information of a specified MBGP community list.

Example

Display routing information of the specified MBGP community list.

```
<SW8800> display bgp multicast routing-table community-list 1
```

display bgp multicast routing-table different-origin-as

Syntax

display bgp multicast routing-table different-origin-as

View

Any view

Parameter

None

Description

Use the **display bgp multicast routing-table different-origin-as** command to view AS routes of different origins.

Example

Display AS routes of different origins.

```
<SW8800> display bgp multicast routing-table different-origin-as
```

display bgp multicast routing-table peer

Syntax

display bgp multicast routing-table peer *peer-address* { **received** | **advertised** } [*network-address* [*mask*] | *statistic*]

View

Any view

Parameter

peer-address: Peer address, in dotted decimal format.

received: Routing information received from a specified peer.

advertised: Routing information advertised from a specified peer.

network-address: IP address of the destination network.

mask: Mask of the destination network.

statistic: Statistic information of the route.

Description

Use the **display bgp multicast routing-table peer** command to view the routes received/advertised at/to the specified peer.

Example

Display routing information advertised to the peer 10.10.1.11.

```
<SW8800> display bgp multicast routing-table peer 10.10.1.11 advertised
```

display bgp multicast routing-table regular-expression

Syntax

display bgp multicast routing-table regular-expression *as-regular-expression*

View

Any view

Parameter

as-regular-expression: AS regular expression matched.

Description

Use the **display bgp multicast routing-table regular-expression** command to view the routing information matching the specified AS regular expression.

Example

Display routing information matching AS regular expression ^600$.

```
<SW8800> display bgp multicast routing-table regular-expression ^600
$
```

filter-policy export

Syntax

filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [*protocol*]

undo filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [*protocol*]

View

IPv4 multicast sub-address family view

Parameter

acl-number: Number of ACL used in matching the destination address domain of routing information, in the range of 2000 to 3999.

ip-prefix-name: Name of the IP prefix used in matching the destination address domain of routing information, in the range of 1 to 19.

Protocol: Protocol specifing which kind of routing information shall be filtered out, with options currently available include **direct**, **ospf**, **ospf-ase**, **ospf-nssa**, **rip, is-is** and **static**.

Description

Use the **filter-policy export** command to set to filter the advertised routes. Only those pass through the filter can be advertised by BGP.

Use the **undo filter-policy export** command to cancel route filtering.

By default, filtering the advertised routes is not enabled.

The command affects route advertising by BGP. If you specify the *protocol* parameter, the router only filters the routes with the specified protocol imported, without influence on the routes importing other protocols. Otherwise, the router filters the routes importing any protocols.

Example

Filter all BGP-advertised routes using ACL 2000.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
```

```
[SW8800] bgp 100
[3Com-bgp] ipv4-family multicast
[3Com-bgp-af-mul] filter-policy 2000 export
```

filter-policy import

Syntax

filter-policy gateway *ip-prefix-name* **import**

undo filter-policy gateway *ip-prefix-name* **import**

filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name* } **import**

undo filter-policy { *acl-number* | ip-prefix *ip-prefix-name* } **import**

View

IPv4 multicast sub-address family view

Parameter

acl-number: Number of ACL used in matching the destination address domain of routing information, in the range of 2000 to 3999.

ip-prefix *ip-prefix-name*: Specifies the IP prefix used in matching the destination address domain of routing information, in the range of 1 to 19.

gateway *ip-prefix-name*: Specifies IP prefix of the neighbor router, in the range of 1 to 19, to filter the routing information advertised by a specified neighbor router.

Description

Use the **filter-policy gateway import** command to set to filter the routes advertised by a specified neighbor router. Only those pass through the filter can be advertised by BGP.

Use the **undo filter-policy gateway import** command to cancel route filtering.

Use the **filter-policy import** command to set to filter the global routes received.

Use the **undo filter-policy import** command to cancel route filtering.

By default, filtering the received routes is not enabled.

This configuration determines whether to add the routes into the BGP routing table.

Example

Filter all BGP-received routes using ACL 2000.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] bgp 100
[3Com-bgp] ipv4-family multicast
[3Com-bgp-af-mul] filter-policy 2000 import
```

import-route

Syntax

import-route *protocol* [**route-policy** *route-policy-name* | **med** *med-value*]*

undo import-route *protocol*

View

IPv4 multicast sub-address family view

Parameter

protocol: Source routing protocols that can be imported, which can be direct, ospf, ospf-ase, ospf-nssa, rip, isis and static.

med-value: Metric value loaded by an imported route, ranging from 0 to 4,294,967,295.

route-policy-name: Route policy used for importing routes.

Description

Use the **import-route** command to import routing information of other protocols into MBGP.

Use the **undo import-route** command to cancel the importing.

By default, MBGP will not import routing information of other protocols.

Example

Import static routes.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] bgp 100
[3Com-bgp] ipv4-family multicast
[3Com-bgp-af-mul] import-route static
```

ipv4-family multicast

Syntax

ipv4-family multicast

undo ipv4-family multicast

View

BGP view, VPN instance sub-address family view, VPNv4 sub-address family view

Parameter

None

Description

Use the **ipv4-family multicast** command to enter the IPv4 multicast sub-address family view.

Use the **undo ipv4-family multicast** command to exit the IPv4 multicast sub-address family view, return to the unicast view and remove all the information in multicast.

Example

Enter the IPv4 multicast sub-address family view.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] bgp 100
[3Com-bgp] ipv4-family multicast
[3Com-bgp-af-mul]
```

network

Syntax

network *ip-address* [*address-mask*] [**route-policy** *route-policy-name*]

undo network *ip-address* [*address-mask*] [**route-policy** *route-policy-name*]

View

IPv4 multicast sub-address family view

Parameter

ip-address: Network address that BGP advertises.

address-mask: Mask of the network address.

route-policy *policy-name*: Route-policy applied to the routes advertised.

Description

Use the **network** command to configure the network addresses to be sent by the local MBGP.

Use the **undo network** command to remove the configuration.

By default, the local MBGP does not send any route.

Example

Advertise routes to network segment 10.0.0.0/16.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] bgp 100
[3Com-bgp] ipv4-family multicast
[3Com-bgp-af-mul] network 10.0.0.1 255.255.0.0
```

peer advertise-community

Syntax

peer *group-name* a**dvertise-community**

undo peer *group-name* **advertise-community**

View

IPv4 multicast sub-address family view

Parameter

group-name: Name of the peer group.

Description

Use the **peer advertise-community** command to set to send community attributes to a peer group.

Use the **undo peer advertise-community** command to remove the configuration.

By default, no community attribute is sent to any peer group.

Example

Set to send community attributes to peer group "test".

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] bgp 100
[3Com-bgp] ipv4-family multicast
[3Com-bgp-af-mul] peer test advertise-community
```

peer allow-as-loop

Syntax

peer { *group-name* | *peer-address* } **allow-as-loop** [*number*]

undo peer { *group-name* | *peer-address* } **allow-as-loop**

View

IPv4 multicast sub-address family view

Parameter

group-name: Name of the peer group.

peer-address: IP address of the peer.

number: Repetition number of local AS IDs, in the range of 1 to 10. By default ,the repetition number is 3.

Description

Use the **peer allow-as-loop** command to specify repetition number of local AS IDs.

Use the **undo peer allow-as-loop** command to remove the configuration.

Related command: **display current-configuration**, **display bgp routing-table peer** and **display bgp routing-table group**.

Example

Configure repetition number of local AS IDs as 2.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] bgp 100
[3Com-bgp] ipv4-family multicast
[3Com-bgp-af-mul] peer 1.1.1.1 allow-as-loop 2
```

peer as-path-acl export

Syntax

peer { *group-name* | *peer-address* } **as-path-acl** *acl-number* **export**

undo peer { *group-name* | *peer-address* } **as-path-acl** *acl-number* **export**

View

IPv4 multicast sub-address family view

Parameter

group-name: Name of the peer group.

peer-address: IP address of the peer; uses dotted decimal notation.

acl-number: Filter list number of an AS regular expression, In the range of 1 to 199.

export: Uses the AS path list to filter the advertised routes.

Description

Use the **peer as-path-acl export** command to configure filtering Policy of MBGP advertised routes based on AS path list.

Use the **undo peer as-path-acl** command to cancel the existing configuration.

By default, the peer group has no AS path list.

This command can only be configured on peer group.

Related command: **peer as-path-acl import**, **ip as-path-acl** (refer to the "Routing Protocol" part).

Example

Configure the peer group test to use AS path list 2 to filter the advertised routes.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] bgp 100
[3Com-bgp] ipv4-family multicast
[3Com-bgp-af-mul] peer test as-path-acl 2 export
```

peer as-path-acl import

Syntax

peer { *group-name* | *peer-address* } **as-path-acl** *acl-number* **import**

undo peer { *group-name* | *peer-address* } **as-path-acl** *acl-number* **import**

View

IPv4 multicast sub-address family view

Parameter

group-name: Name of the peer group.

peer-address: IP address of the peer.

acl-number: Filter list number of an AS regular expression, in the range 1 to 199.

import: Uses the AS path list to filter the received routes.

Description

Use the **peer as-path-acl import** command to configure filtering Policy of MBGP received routes based on AS path list.

Use the **undo peer as-path-acl import** command to cancel the existing configuration.

By default, the peer/peer group has no AS path list.

The inbound filter policy configured for the peer takes precedence over the configurations for the peer group.

Related command: **peer as-path-acl export**, **ip as-path-acl** (refer to the "Routing Protocol" part).

Example

Set the AS path ACL of the peer group test to filter BGP received routes.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] bgp 100
[3Com-bgp] ipv4-family multicast
[3Com-bgp-af-mul] peer test as-path-acl 3 import
```

peer enable

Syntax

peer *group-name* **enable**

undo peer *group-name* **enable**

View

IPv4 multicast sub-address family view

Parameter

group-name: Name of the multicast peer group.

Description

Use the **peer enable** command to enable the MBGP peer group.

Use the **undo peer enable** command to disable the MBGP peer group.

By default, the MBGP peer group is disabled.

Only after the peer group is enabled, can the router establishes connection with the multicast peer.

Example

Enable peer group group1.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] bgp 100
[3Com-bgp] ipv4-family multicast
[3Com-bgp-af-mul] peer group1 enable
```

peer filter-policy export

Syntax

peer *group-name* **filter-policy** *acl-number* **export**

undo peer *group-name* **filter-policy** *acl-number* **export**

View

IPv4 multicast sub-address family view

Parameter

group-name: Name of the peer group.

acl-number: Number of IP ACL ranging from 2000 to 3999. That is, you can use basic ACLs or advanced ACLs.

export: Applies the filter policy to the advertised routes. This keyword is only valid for the peer groups.

Description

Use the **peer filter-policy export** command to configure the peer group to apply the ACL-based filter policy to the advertised routes.

Use the **undo peer filter-policy export** command to cancel the existing configuration.

By default, no ACL-based filter policy is configured.

The **peer filter-policy export** command can only be configured on peer groups.

Related command: **peer filter-policy import, acl** .

Example

Configure the peer group test to use ACL 2000 to filter the advertised routes.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] bgp 100
[3Com-bgp] ipv4-family multicast
[3Com-bgp-af-mul] peer test filter-policy 2000 export
```

peer filter-policy import

Syntax

peer { *group-name* | *peer-address* } **filter-policy** *acl-number* **import**

undo peer { *group-name* | *peer-address* } **filter-policy** *acl-number* **import**

View

IPv4 multicast sub-address family view

Parameter

group-name: Name of the peer group.

peer-address: IP address of the peer.

acl-number: Number of IP ACL, ranging from 2000 to 3999. That is, you can use basic ACLs or advanced ACLs.

Description

Use the **peer filter-policy import** command to configure the peer to apply the ACL-based filter policy to the received routes.

Use the **undo peer filter-policy import** command to cancel the existing configuration.

By default, no ACL-based filter policy is configured.

Related command: **peer filter-policy export, acl**.

The inbound filter policy configured for the peer takes precedence over the configurations for the peer group.

Example

Configure the peer group test to use ACL 2000 to filter the received routes.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] bgp 100
[3Com-bgp] ipv4-family multicast
[3Com-bgp-af-mul] peer test filter-policy 2000 import
```

peer group

Syntax

peer *peer-address* **group** *group-name*

undo peer *peer-address*

View

IPv4 multicast sub-address family view

Parameter

peer-address: IP address of the peer, in dotted decimal format.

group-name: Name of the peer, consisting of one to 47 alphanumeric characters.

Description

Use the **peer group** command to add a peer into a peer group.

Use the **undo peer group** command to delete the peer.

CAUTION: *You must first add the specific peer in the peer group in BGP view and enable the peer group in the IPv4 multicast sub-address family view before you can issue this command.*

Example

Add peer 10.1.1.1 to EBGP peer group TEST.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] bgp 100
```

```
[3Com-bgp] group TEST external.
[3Com-bgp] peer TEST as-number 2004
[3Com-bgp] peer 10.1.1.1 group TEST
[3Com-bgp] ipv4-family multicast
[3Com-bgp-af-mul] peer TEST enable
[3Com-bgp-af-mul] peer 10.1.1.1 group TEST
```

peer ip-prefix export

Syntax

peer *group-name* **ip-prefix** *prefixname* **export**

undo peer *group-name* **ip-prefix** *prefixname* **export**

View

IPv4 multicast sub-address family view

Parameter

group-name: Name of peer group.

prefixname: Name of the specified **ip-prefix.**

Description

Use the **peer ip-prefix export** command to configure the route filtering policy of routes advertised by the peer group based on the ip-prefix.

Use the **undo peer ip-prefix export** command to cancel the route filtering policy of the peer/peer group based on the ip-prefix.

By default, the route filtering policy of the peer group is not specified.

The **peer ip-prefix export** command can only be configured on the peer groups.

Related command: **ip ip-prefix, peer ip-prefix import**.

Example

Configure the route filtering policy of the peer group1 based on the ip-prefix list1.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] bgp 100
[3Com-bgp] ipv4-family multicast
[3Com-bgp-af-mul] peer group1 ip-prefix list1 export
```

peer ip-prefix import

Syntax

peer { *group-name* | *peer-address* } **ip-prefix** *prefixname* **import**

undo peer { *group-name* | *peer-address* } **ip-prefix** *prefixname* **import**

View

IPv4 multicast sub-address family view

Parameter

group-name: Name of peer group.

peer-address: IP address of the peer, in dotted decimal format.

prefixname: Name of the specified ip-prefix, a character string of 1 to 19 characters.

Description

Use the **peer ip-prefix import** command to configure the route filtering policy of routes received by the peer based on the ip-prefix.

Use the **undo peer ip-prefix import** command to cancel the route filtering policy of the peer based on the ip-prefix.

By default, the route filtering policy of the peer is not specified.

The inbound route policy configured for the peer takes precedence over the configurations for the peer group.

Related command: **peer ip-prefix export**.

Example

Configure the route filtering policy of the peer group1 based on the ip-prefix list1.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] bgp 100
[3Com-bgp] ipv4-family multicast
[3Com-bgp-af-mul] peer group1 ip-prefix list1 import
```

peer next-hop-local

Syntax

peer *group-name* **next-hop-local**

undo peer *group-name* **next-hop-local**

View

IPv4 multicast sub-address family view

Parameter

group-name: Name of the peer group.

Description

Use the **peer next-hop-local** command to remove the processing of the next hop in routes which BGP will advertise to the peer group and set the local address as the next hop.

Use the **undo peer next-hop-local** command to cancel the configuration.

Example

Specify the local address as next-hop when advertising routes to peer group named test.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] bgp 100
```

```
[3Com-bgp] ipv4-family multicast
[3Com-bgp-af-mul] peer test next-hop-local
```

peer public-as-only

Syntax

peer *group-name* **public-as-only**

undo peer *group-name* **public-as-only**

View

IPv4 multicast sub-address family view

Parameter

group-name: Name of the peer group.

Description

Use the **peer public-as-only** command to set to contain only public AS IDs in the MBGP Update message, but not private AS IDs.

Use the **undo peer public-as-only** command to restore the default setting, the router contains only private AS IDs in the MBGP Update message.

By default, the private AS ID is carried when BGP sends MBGP Update message.

Generally, MBGP sends MBGP Update message with the AS ID (which can be either the public AS number or private AS number) contained. To enable some egress routers to ignore the private AS ID when sending MBGP Update message, you can configure not to carry the private AS IDs when sending MBGP Update message.

Example

Set not to carry private AS IDs when sending MBGP Update message to peer group "test".

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] bgp 100
[3Com-bgp] ipv4-family multicast
[3Com-bgp-af-mul] peer test public-as-only
```

peer reflect-client

Syntax

peer *group-name* **reflect-client**

undo peer *group-name* **reflect-client**

View

IPv4 multicast sub-address family view

Parameter

group-name: Name of the peer group.

Description

Use the **peer reflect-client** command to configure a peer (group) as a client of the route reflector.

Use the **undo peer reflect-client** command to remove the configuration.

By default, there is no route reflector in the autonomous system.

Example

Configure peer group "test" as the client of the route reflector.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] bgp 100
[3Com-bgp] ipv4-family multicast
[3Com-bgp-af-mul] peer test reflect-client
```

peer route-policy export

Syntax

peer *group-name* **route-policy** *policy-name* **export**

undo peer *group-name* **route-policy** *policy-name* **export**

View

IPv4 multicast sub-address family view

Parameter

group-name: Name of peer group.

peer-address: IP address of the peer.

Description

Use the **peer route-policy export** command to assign the Route-policy to the routes advertised to the peer group.

Use the **undo peer route-policy export** command to delete the specified Route-policy.

By default, the peer/peer group has no Route-policy association.

Related command: **peer route-policy import**.

Example

Apply the Route-policy named test-policy to the route coming from the peer group test.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] bgp 100
[3Com-bgp] ipv4-family multicast
[3Com-bgp-af-mul] peer test route-policy test-policy export
```

peer route-policy import

Syntax

peer { *group-name* | *peer-address* } **route-policy** *policy-name* **import**

undo peer { *group-name* | *peer-address* } **route-policy** *policy-name* **import**

View

IPv4 multicast sub-address family view

Parameter

group-name: Name of peer group.

peer-address: IP address of the peer.

policy-name: Name of the applied route policy.

Description

Use the **peer route-policy import** command to assign the Route-policy to the route coming from the peer.

Use the **undo peer route-policy import** command to delete the specified Route-policy.

By default, the peer has no Route-policy association.

The inbound route policy configured for the peer takes precedence over the configurations for the peer group.

Related command: **peer route-policy export**.

Example

Apply the Route-policy named test-policy to the route coming from the peer group test.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] bgp 100
[3Com-bgp] ipv4-family multicast
[3Com-bgp-af-mul] peer test route-policy test-policy import
```

preference

Syntax

preference *ebgp-value ibgp-value local-vlaue*

undo preference

View

IPv4 multicast sub-address family view

Parameter

ebgp-value: EBGP route priority, in the range of 1 to 256. By default, it is 256.

ibgp-value: IBGP route priority, in the range of 1 to 256. By default, it is 256.

local-value: Local route priority, in the range of 1 to 256. By default, it is 130.

Description

Use the **preference** command to configure MBGP protocol priority.

Use the **undo preference** command to restore the default priority.

You can configure different priority values for different types of MBGP routes.

Example

Set the priority of EBGP, IBGP and local routes all to 170.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] bgp 100
[3Com-bgp] ipv4-family multicast
[3Com-bgp-af-mul] preference 170 170 170
```

reflect between-clients

Syntax

reflect between-clients

undo reflect between-clients

View

IPv4 multicast sub-address family view

Parameter

None

Description

Use the **reflect between-clients** command to enable route reflection between clients.

Use the **undo reflect between-clients** command to disable route reflection between clients.

When configured, the route reflector can reflect routes of a client to other clients.

By default, all-connection is not required for the clients with route reflectors configured, since the routes are by default reflected from one client to others. For all-connection clients, route reflection is unnecessary.

Related command: **reflector cluster-id** and **peer reflect-client**.

Example

Disable route reflection function.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] bgp 100
[3Com-bgp] ipv4-family multicast
[3Com-bgp-af-mul] undo reflect between-clients
```

refresh bgp multicast

Syntax

refresh bgp { **all** | *peer-address* | **group** *group-name* } **multicast** { **import** | **export** }

View

User view

Parameter

all: Refreshes multicast sub-address family router of all peer .

peer-address: Multicast sub-address family router of the specified address peer.

group-name: Multicast sub-address family router of all members of the specified peer group.

import: Sends ROUTE-REFRESH packets, request the peer to send all multicast sub-address family router again .

export: Sends all multicast sub-address family router again .

Description

Use the **refresh bgp multicast** command to request the peer to send multicast sub-address family router again, or send multicast sub-address family router again.

Example

Request all the peers to send multicast sub-address family router again.

```
<SW8800> refresh bgp all multicast import
```

reflector cluster-id

Syntax

reflector cluster-id { *cluster-id* | *address* }

undo reflector cluster-id

View

IPv4 multicast sub-address family view

Parameter

cluster-id: Route reflector cluster ID, in integer number or IP address format, range 1 to 4294967295.

address: Route reflector cluster ID in IP address format.

Description

Use the **reflector cluster-id** command to configure route reflector cluster ID.

Use the **undo reflector cluster-id** command to delete route reflector cluster ID.

By default, each route reflector uses its own route ID as cluster ID.

In general, one cluster has only one route reflector, and then the router ID for the route reflector can be used to identify the cluster. If a cluster has several route reflectors, for multiple route reflectors can improve network stability, then you can use this command to specify the same cluster ID for them all.

Related command: **reflect between-clients** and **peer reflect-client**.

Example

Specify cluster ID for local router, one of the router reflectors.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] bgp 100
[3Com-bgp] ipv4-family multicast
[3Com-bgp-af-mul] reflector cluster-id 80
[3Com-bgp-af-mul] peer test reflect-client
```

summary

Syntax

summary

undo summary

View

IPv4 multicast sub-address family view

Parameter

None

Description

Use the **summary** command to set to auto-aggregate subnet routes.

Use the **undo summary** command to remove the configuration.

By default, subnet routes cannot be aggregated automatically.

After the **summary** command is executed, MBGP cannot receive the subnet routes imported by IGP. You can use this command to reduce route selection information.

Example

Enable subnet route auto-aggregation.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] bgp 100
[3Com-bgp] ipv4-family multicast
[3Com-bgp-af-mul] summary
```

39 MPLS BASIC CONFIGURATION COMMANDS

MPLS Basic Configuration Commands

debugging mpls lspm

Syntax

debugging mpls lspm { **agent** | **all** | **event** | **ftn** | **interface** | **packet** | **policy** | **process** | **vpn** }

undo debugging mpls lspm { **agent** | **all** | **event** | **ftn** | **interface** | **packet** | **policy** | **process** | **vpn** }

View

User view

Parameter

agent: Enables all MPLS Agent debugging.

all: Enables all MPLS-related debugging.

event: Enables debugging for various MPLS events.

ftn: Enables MPLS FTN debugging.

interface: Enables the MPLS debugging on the message sending/receiving interface.

packet: Enables MPLS packet debugging.

policy: Enables MPLS policy debugging.

process: Enables debugging of MPLS internal processing.

vpn: Enables all MPLS VPN debugging.

Description

Use the **debugging mpls lspm** command to enable various LSPM debugging.

Use the **undo debugging mpls lspm** command to disable the corresponding debugging.

By default, all debugging is disabled.

This command is used to the debug MPLS LSPM. As running the debugging will affect the performance of the 3Com Switch 8800 Family Series Routing Switches, you are recommended to use the command with caution.

Example

Enable all MPLS VPN debugging.

```
<SW8800> debugging mpls lspm vpn
```

display mpls interface

Syntax

display mpls interface

View

Any view

Parameter

None

Description

Use the **display mpls interface** command to view the information of all MPLS-enabled interfaces.

Related command: **display mpls lsp**, **display mpls statistics** and **display static-lsp**.

Example

Display the information of all MPLS-enabled interfaces.

```
<SW8800> display mpls interface
MPLS interface information:
  Interface Vlan-interface12 ( Label Range : 0-44800 )
  Interface Vlan-interface23 ( Label Range : 0-44800 )
  Interface Vlan-interface21 ( Label Range : 0-44800 )
  Interface Vlan-interface20 ( Label Range : 0-44800 )
  Interface Vlan-interface194 ( Label Range : 0-44800 )
  Interface Vlan-interface104 ( Label Range : 0-44800 )
  Interface Vlan-interface76 ( Label Range : 0-44800 )
  Interface Vlan-interface22 ( Label Range : 0-44800 )
  Interface Vlan-interface193 ( Label Range : 0-44800 )
  Interface Vlan-interface27 ( Label Range : 0-44800 )
```

display mpls lsp

Syntax

display mpls lsp [**include** *text* | **verbose**]

View

Any view

Parameter

include *text*: Displays the matching string including the specified information.

verbose: Displays detailed information.

Description

Use the **display mpls lsp** command to display LSP information.

By default, the **display mpls lsp** command displays all LSP information.

Related command: **display mpls interface**, **display mpls statistics** and **display static-lsp**.

Example

Display all the LSPs including "----------".

```
<SW8800> display mpls lsp include -----
------------------------------------------------------------------
LSP Information: Ldp                Lsp
NO      FEC               NEXTHOP         I/O-LABEL    OUT-INTERFACE

1     10.110.1.0/24       10.110.1.1      3/-----          -------

2     10.10.10.0/24       10.10.10.1      3/-----          -------

3     10.100.20.20/32     127.0.0.1       3/-----          -------

4     5.5.5.5/32           127.0.0.1       3/-----          -------

5     10.100.20.0/24      10.100.20.20    3/-----         -------
6     80.80.80.80/32      127.0.0.1        3/-----         -------
7     70.70.70.70/32      200.5.5.4       -----/3         Vlan2000
TOTAL:  7 Record(s) Found.
```

display mpls static-lsp

Syntax

display mpls static-lsp [**include** *text* | **verbose**]

View

Any view

Parameter

include *text*: Displays the matching string including the specified information .

verbose: Displays detailed information.

Description

Use the **display mpls static-lsp** command to view the information of one static LSP or all.

Related command: **display mpls interface**, **display mpls lsp** and **display mpls statistics**.

Example

Display the static LSP information.

```
<SW8800> display mpls static-lsp
------------------------------------------------------------------
                LSP Information: Static Lsp
------------------------------------------------------------------
```

```
NO         FEC              NEXTHOP         I/O-LABEL     OUT-INTERFACE

1      1.1.1.1/32           200.5.5.4       -----/1000    Vlan2000
TOTAL:   1 Record(s) Found.
```

display mpls statistics

Syntax

display mpls statistics { **interface** { *Vlan-interface* | **all** } | **lsp** { *lsp-Index* | **all** | *lsp-name* }}

View

Any view

Parameter

interface { *Vlan-interface* | **all** }: Specifies one interface or all interfaces.

lsp { *lsp-Index* | **all** | *lsp-name* }: Specifies one label switching path or all label switching paths. Where *lsp-Index* is an LSP index, *lsp-name* is an LSP name, and **all** represents all LSPs.

Description

Use the **display mpls statistics** command to view the MPLS statistics about one specific VLAN interface/LSP or all interfaces/LSPs.

Related command: **display mpls interface** and **display mpls lsp**.

Example

Display MPLS statistics about all LSPs

```
<SW8800> display mpls statistics lsp all
Building the information...
  LSP Index/LSP Name :  10240/dynamic-lsp
  There is no information of LSP incoming segment!
  The statistics of lsp Out :
    OutSegment octets of LSP is: 162876
    OutSegment packets of LSP is: 2943
    OutSegment errors of LSP is: 0
    OutSegment discard packets of LSP is: 0
```

lsp-trigger

Syntax

lsp-trigger { **all** | **ip-prefix** *ip-prefix* }

undo lsp-trigger { **all** | **ip-prefix** *ip-prefix* }

View

MPLS view

Parameter

all: Triggers LSPs at any route.

ip-prefix: Triggers LSPs only at the routes matching the specified IP prefix list.

ip-prefix: IP prefix list, ranging from 1 to 19.

Description

Use the **lsp-trigger** command to configure topology-triggered LSP creation policy.

Use the **undo lsp-trigger** command to remove the filtering conditions specified by parameters and disable LSP trigger creation at any route.

By default, all kinds of routing protocols are filtered out.

If no route-triggered policy is configured, LSPs can be triggered at all host routes with 32-bit masks.

If you import an IP-prefix rule without contents, LSPs can be triggered at all routes.

Related command: **ip ip-prefix**.

Example

Triggers LSPs at all routes.

```
<SW8800> system-view
[SW8800] mpls
[3Com-mpls] lsp-trigger all
```

mpls

Syntax

mpls

undo mpls

View

System view, VLAN interface view

Parameter

None

Description

In system view, input the **mpls** command for an initial use to enable MPLS function globally and enter MPLS view. Later you can go straight to the MPLS view with this command.

Use the **mpls** command in VLAN interface view to enable MPLS on the VLAN interface.

Use the **undo mpls** command to disable MPLS function in the system view or on the VLAN interface.

By default, you cannot enter this view.

After executing the command, you are in MPLS view. You can configure other MPLS commands only when you are in MPLS view.

You must configure the **mpls lsr-id** command before you can enter MPLS view.

Example

Enter MPLS view from system view.

```
<SW8800> system-view
[SW8800] mpls
[3Com-mpls]
```

Execute the **mpls** command in interface view.

```
[SW8800] vlan 201
[3Com-Vlan201] port gigabitethernet 2/1/1
[3Com-Vlan201] quit
[SW8800] interface vlan-interface 201
[3Com-vlan-interface201] mpls
% Info: MPLS in the interface is starting, please wait...OK
```

mpls lsr-id

Syntax

mpls lsr-id *ip-address*

undo mpls lsr-id

View

System view

Parameter

ip-address: LSR ID, in the format of IP address, used to identify an LSR.

Description

Use the **mpls lsr-id** command to configure an LSR ID.

Use the **undo mpls lsr-id** command to delete an LSR ID.

By default, no LSR has an ID.

You must configure the **mpls lsr-id** command first and then you can use the other MPLS-related commands.

An LSR ID is in the format of IP address, thus a loopback address is recommended.

Related command: **display mpls interface**.

Example

Set the LSR ID to 202.17.41.246.

```
<SW8800> system-view
[SW8800] mpls lsr-id 202.17.41.246
% Info: Mpls lsr-id changed.
```

snmp-agent trap enable ldp

Syntax

snmp-agent trap enable ldp

undo snmp-agent trap enable ldp

View

System view

Parameter

None

Description

Use the **snmp-agent trap enable ldp** command to enable Trap function in MPLS LDP creation.

Use the **undo snmp-agent trap enable ldp** command to disable Trap function in MPLS LDP creation.

By default, Trap function is not enabled during MPLS LDP creation.

Example

Enable the Trap function during MPLS LDP creation.

```
<SW8800> system-view
[SW8800] snmp-agent trap enable ldp
```

snmp-agent trap enable lsp

Syntax

snmp-agent trap enable lsp

undo snmp-agent trap enable lsp

View

System view

Parameter

None

Description

Use the **snmp-agent trap enable lsp** command to enable Trap function in MPLS LSP creation.

Use the **undo snmp-agent trap enable lsp** command to disable Trap function in MPLS LSP creation.

By default, Trap function is disabled during MPLS LSP creation.

Example

Enable the Trap function during MPLS LSP creation.

```
<SW8800> system-view
[SW8800] snmp-agent trap enable lsp
```

static-lsp egress

Syntax

static-lsp egress *lsp-name* [**l2vpn**] **incoming-interface** *interface-type interface-number* **in-label** *in-label-value*

undo static-lsp egress *lsp-name*

View

MPLS view

Parameter

lsp-name: LSP name

interface-type Interface-number: Interface type, interface number.

in-label-value: Value of inbound label, ranging 3 (implicit empty label) and from 16 to 1023.

Description

Use the **static-lsp egress** command to configure a static LSP for an egress LSR.

Use the **undo static-lsp egress** command to delete an LSP for an egress LSR.

Related command: **static-lsp ingress**, **static-lsp transit** and **debugging mpls**.

Example

Configure a static LSP named bj-sh on the egress LSR.

```
<SW8800> system-view
[3Com-mpls] static-lsp egress bj-sh incoming-interface vlan-
interface 201 in-label 233
```

static-lsp ingress

Syntax

static-lsp ingress *lsp-name* { **destination** *dest-addr* { *addr-mask* | *mask-length* } | **l2vpn** } **nexthop** *next-hop-addr* } } **out-label** *out-label-value*

undo static-lsp ingress *lsp-name*

View

MPLS view

Parameter

lsp-name: LSP name

dest-addr: Destination IP address.

addr-mask: Destination IP address mask.

mask-length: Mask length of destination IP address

next-hop-addr: Next-hop address.

out-label-value: Value of outbound label, ranging 3 (implicit empty label) and from 16 to 1023.

Description

Use the **static-lsp ingress** command to configure a static LSP for an ingress LSR.

Use the **undo static-lsp ingress** command to delete an LSP for an ingress LSR.

Related command: **static-lsp egress**, **static-lsp transit** and **debugging mpls**.

Example

Configure a static LSP for the ingress LSR heading for the destination address 202.25.38.1.

```
<SW8800> system-view
[SW8800] mpls
[3Com-mpls] static-lsp ingress bj-sh destination 202.25.38.1 24
nexthop 202.55.25.33 out-label 237
```

static-lsp transit

Syntax

static-lsp transit *lsp-name* [**l2vpn**] **incoming-interface** *interface-type interface-number* **in-label** *in-label-value* **nexthop** *next-hop-addr* **out-label** *out-label-value*

undo static-lsp transit *lsp-name*

View

MPLS view

Parameter

lsp-name: LSP name

interface-type Interface-number: Interface type, interface number.

next-hop-addr: Next-hop address.

in-label-value: Value of inbound label, ranging from 16 to 1023.

out-label-value: Value of outbound label, ranging 3 (implicit empty label) and from 16 to 1023.

Description

Use the **static-lsp transit** command to configure a static LSP for a transit LSR.

Use the **undo static-lsp transit** command to delete an LSP for a transit LSR.

Related command: **static-lsp egress** and **static-lsp ingress**.

Example

Configure a static LSP for the VLAN201 interface on a transit LSR, with an inbound label of 123 and an outbound label of 253.

```
<SW8800> system-view
[SW8800] mpls
[3Com-mpls] static-lsp transit bj-sh incoming-interface vlan-
interface 201 in-label 123 nexthop 202.34.114.7 out-label 253
```

LDP Configuration Commands

debugging mpls ldp

Syntax

debugging mpls ldp { **all** | **main** | **advertisement** | **session** | **pdu** | **notification** | **remote** | **filter** } [**interface** *interface-type interface-number*]

undo debugging mpls ldp { **all** | **main** | **advertisement** | **session** | **pdu** | **notification** | **remote** | **filter** } [i**nterface** *interface-type interface-number*]

View

User view

Parameter

all: Displays all debugging information related to LDP.

main: Displays the debugging information of LDP main tasks.

advertisement: Displays the debugging information during LDP advertising.

session: Displays debugging information during LDP session processing.

pdu: Displays the debugging information during PDU packet processing.

notification: Displays the debugging information during notification.

remote: Displays debugging information of all Remote Peers.

filter: Displays debugging information of all filters.

interface-type interface-number: Interface type, interface number.

Description

Use the **debugging ldp** command to enable the debugging of various LDP messages. Use the **undo debugging ldp** command to disable the debugging of various LDP messages.

You are advised to use the debugging command cautiously.

Example

Enable LDP debugging.

```
<SW8800> debugging mpls ldp all
```

display mpls ldp

Syntax

display mpls ldp

View

Any view

Parameter

None

Description

Use the **display mpls ldp** command to display LDP and LSR information.

By default, it displays information of LDP and LSR.

Related command: **mpls ldp**, **mpls ldp hops-count**, **mpls ldp loop-detection** and **mpls ldp path-vectors**.

Example

Display LDP and LSR information.

```
<SW8800> display mpls ldp
Label Distribution Protocol: V1
LSR ID: 10.10.10.10      LSR Status: Active
Loop Detection: Disabled.
Path Vector Limit: 32              Hop Count Limit: 32
DU Readvertisement: On             Request   Retry: Off
Label Retention Mode: Liberal      DU Explicit Request: Off
Label Distribution Control Mode: Ordered.
```

display mpls ldp buffer-info

Syntax

display mpls ldp buffer-info

View

Any view

Parameter

None

Description

Use the **display mpls ldp buffer-info** command to view the LDP buffer information.

Example

Display the LDP buffer information.

```
<SW8800> display mpls ldp buffer-info
-----------------------------------------------------------------
Buffer-Name     Buffer-ID    Buffer-Size  Total-Count  Free-Count
ENTITY              0            292          199          195
LOCAL-IF            1            36           200          196
PEER-IF             2            40           201          195
PDU                     3            204          249          249
ADJACENCY       4            56           201          198
PEER-INF            5            116          201          198
SESSION             6            176          201          198
US-BLK              7            264          1052         1028
DS-BLK              8            240          1052         1042
FEC                 9            40           1042         1032
US-LIST             10           16           1052         1028
TRIG-BLK            11           56           2076         2071
LABEL-RANGE         12           20           198          198
CR-TUNNEL           13           124          128          128
ER-HOP              14           40           4096         4096
IF-MSG              15           24           9999         9999
```

```
----------------------------------------------------------------
Buffer no error.
```

display mpls ldp interface

Syntax

display mpls ldp interface [| **begin** *text* | **exclude** *text* | **include** *text*]

View

Any view

Parameter

|: Displays matched outputs.

begin: Displays the outputs matching the regular expression from the first line.

exclude: Displays the outputs excluding those lines matching the regular expression.

include: Displays only those outputs matching the regular expression.

text: Contents of the regular expression.

Description

Use the **display mpls ldp interface** command to display information of the interface with LDP enabled and in the Up state.

Related command: **mpls ldp enable** and **display mpls ldp session**.

Example

Display the information of the interface with LDP enabled and in the UP state.

```
<3Com-Ethernet3/1/0> display mpls ldp interface
Displaying information about all Ldp interface:
    Interface Vlan-interface12(address=12.12.12.2):
    Label distributing enabled,bound to entity:2.2.2.2:0
    Generic label range configured:16 -  44800
    Label Advertisement Mode: Downstream-Unsolicited
    Configured KeepAlive hold time:60, Configured Hello hold time:15
    Negotiated Hello hold time:15
    Hello packets sent/rcv:21158/21136

    Interface Vlan-interface21(address=21.21.21.2):
    Label distributing enabled,bound to entity:2.2.2.2:0
    Generic label range configured:16 -  44800
    Label Advertisement Mode: Downstream-Unsolicited
    Configured KeepAlive hold time:60, Configured Hello hold time:15
    Negotiated Hello hold time:0
    Hello packets sent/rcv:16929/0

    Interface Vlan-interface22(address=22.22.22.2):
    Label distributing enabled,bound to entity:2.2.2.2:0
    Generic label range configured:16 -  44800
    Label Advertisement Mode: Downstream-Unsolicited
    Configured KeepAlive hold time:60, Configured Hello hold time:15
    Negotiated Hello hold time:15
    Hello packets sent/rcv:21175/21159
```

```
Interface Vlan-interface23(address=23.23.23.2):
Label distributing enabled,bound to entity:2.2.2.2:0
Generic label range configured:16 -  44800
Label Advertisement Mode: Downstream-Unsolicited
Configured KeepAlive hold time:60, Configured Hello hold time:15
Negotiated Hello hold time:15
Hello packets sent/rcv:20970/20949
Interface Vlan-interface194(address=192.4.1.1):
Label distributing enabled,bound to entity:2.2.2.2:0
Generic label range configured:16 -  44800
Label Advertisement Mode: Downstream-Unsolicited
Configured KeepAlive hold time:60, Configured Hello hold time:15
Negotiated Hello hold time:0
Hello packets sent/rcv:15296/0
```

display mpls ldp lsp

Syntax

display mpls ldp lsp [| **begin** *text* | **exclude** *text* | **include** *text*]

View

Any view

Parameter

|: Displays matched outputs.

begin: Displays the outputs matching the regular expression from the first line.

exclude: Displays the outputs excluding those lines matching the regular expression.

include: Displays only those outputs matching the regular expression.

text: Contents of the regular expression.

Description

Use the **display mpls ldp lsp** command to view relevant LSP information created via LDP.

Related command: **display mpls lsp**.

Example

Display LSP.

```
<3Com-Ethernet3/1/0> display mpls ldp lsp
-------------------------------------------------------------------------------
                            LDP LSP Information
-------------------------------------------------------------------------------
No.  FECType  DestAddress        InLab OLab  UHC DHC Next-Hop       OutInterface
1    PREFIX   2.2.2.2            3     ----  0   1   127.0.0.1      InLoop0
2    PREFIX   2.2.2.2            3     ----  0   1   127.0.0.1      InLoop0
3    PREFIX   192.4.1.0/24       3     ----  0   1   192.4.1.1      Vlan194
4    PREFIX   192.4.1.0/24       3     ----  0   1   192.4.1.1      Vlan194
     Liberal  12.12.12.0/24      ----  3     --- 1   --------       Vlan22
5    PREFIX   12.12.12.0/24      3     ----  0   1   12.12.12.2     Vlan12
6    PREFIX   12.12.12.0/24      3     ----  0   1   12.12.12.2     Vlan12
     Liberal  16.16.16.0/24      ----  1026  --- 2   --------       Vlan23
     Liberal  16.16.16.0/24      ----  3     --- 1   --------       Vlan22
```

```
7    PREFIX   16.16.16.0/24      3     ----  0   1   16.16.16.16    Vlan16
8    PREFIX   16.16.16.0/24      3     ----  0   1   16.16.16.16    Vlan16
9    PREFIX   22.22.22.0/24      3     ----  0   1   22.22.22.2     Vlan22
     Liberal  1.1.0.5/32         ----  1024  --- 2   --------        ------
10   PREFIX   1.1.0.5            1024  3     0   1   23.23.23.3     Vlan23
11   PREFIX   1.1.0.5            ----  3     1   1   23.23.23.3     Vlan23
     Liberal  85.12.0.1/32       ----  1025  --- 2   --------        ------
12   PREFIX   85.12.0.1          1025  3     0   1   23.23.23.3     Vlan23
13   PREFIX   85.12.0.1          ----  3     1   1   23.23.23.3     Vlan23
```

display mpls ldp peer

Syntax

display mpls ldp peer [| **begin** *text* | **exclude** *text* | **include** *text*]

View

Any view

Parameter

|: Displays matched outputs.

begin: Displays the outputs matching the regular expression from the first line.

exclude: Displays the outputs excluding those lines matching the regular expression.

include: Displays only those outputs matching the regular expression.

text: Contents of the regular expression.

Description

Use the **display mpls ldp peer** command to view peer information.

By default, it displays all the peer information.

Example

Display peer information.

```
<SW8800> display mpls ldp peer
Displaying information about all peers:

   Local LDP ID: 2.2.2.2:0
   Peer LDP ID: 1.1.1.1:0
   Internetwork Address Type: IPv4
   Internetwork Address: 1.1.1.1
   Maximum Peer PDU length: 4096
   Peer KeepAlive hold time: 60
   Peer Distribution Method: Downstream Unsolicited
   Peer Type: Remote
   Peer RowStatus: Active

   Local LDP ID: 2.2.2.2:0
   Peer LDP ID: 3.3.3.3:0
   Internetwork Address Type: IPv4
   Internetwork Address: 3.3.3.3
   Maximum Peer PDU length: 4096
   Peer KeepAlive hold time: 60
   Peer Distribution Method: Downstream Unsolicited
```

```
Peer Type: Remote
Peer RowStatus: Active

Local LDP ID: 2.2.2.2:0
Peer LDP ID: 1.1.1.1:0
Internetwork Address Type: IPv4
Internetwork Address: 1.1.1.1
Maximum Peer PDU length: 4096
Peer KeepAlive hold time: 60
Peer Distribution Method: Downstream Unsolicited
Peer Type: Local
Peer RowStatus: Active

Local LDP ID: 2.2.2.2:0
Peer LDP ID: 1.1.1.1:0
Internetwork Address Type: IPv4
Internetwork Address: 1.1.1.1
Maximum Peer PDU length: 4096
Peer KeepAlive hold time: 60
Peer Distribution Method: Downstream Unsolicited
Peer Type: Local
Peer RowStatus: Active

Local LDP ID: 2.2.2.2:0
Peer LDP ID: 3.3.3.3:0
Internetwork Address Type: IPv4
Internetwork Address: 3.3.3.3
Maximum Peer PDU length: 4096
Peer KeepAlive hold time: 60
Peer Distribution Method: Downstream Unsolicited
Peer Type: Local
Peer RowStatus: Active
```

display mpls ldp remote

Syntax

display mpls ldp remote [| **begin** *text* | **exclude** *text* | **include** *text*]

View

Any view

Parameter

|: Displays matched outputs.

begin: Displays the outputs matching the regular expression from the first line.

exclude: Displays the outputs excluding those lines matching the regular expression.

include: Displays only those outputs matching the regular expression.

text: Contents of the regular expression.

Description

Use the **display mpls ldp remote** command to view the configured Remote-peer information.

By default, you can view all the Remote-peer configurations.

Related command: **mpls ldp remote-peer** and **remote-ip**.

Example

Display the Remote-peer configuration.

```
<SW8800> display mpls ldp remote
Displaying information about all Ldp Remote Peers:
    Remote Index: 1
    Peer Address: 1.1.1.1  Transport Address: 2.2.2.2
    Configured KeepAlive hold time:60, Configured Hello hold time:45
    Negotiated Hello hold time:45
    Hello packets sent/rcv:6515/6509

    Remote Index: 3
    Peer Address: 3.3.3.3  Transport Address: 2.2.2.2
    Configured KeepAlive hold time:60, Configured Hello hold time:45
    Negotiated Hello hold time:45
    Hello packets sent/rcv:6457/6453

    Remote Index: 4
    Peer Address: 1.1.0.3  Transport Address: 2.2.2.2
    Configured KeepAlive hold time:60, Configured Hello hold time:45
    Negotiated Hello hold time:0
    Hello packets sent/rcv:0/0

    Remote Index: 7
    Peer Address: 1.1.1.7  Transport Address: 2.2.2.2
    Configured KeepAlive hold time:60, Configured Hello hold time:45
    Negotiated Hello hold time:0
    Hello packets sent/rcv:0/0
```

display mpls ldp session

Syntax

display mpls ldp session [| **begin** *text* | **exclude** *text* | **include** *text*]

View

Any view

Parameter

|: Displays matched outputs.

begin: Displays the outputs matching the regular expression from the first line.

exclude: Displays the outputs excluding those lines matching the regular expression.

include: Displays only those outputs matching the regular expression.

text: Contents of the regular expression.

Description

Use the **display mpls ldp session** command to know the session between peer entities.

By default, it displays the session between peer entities.

Related command: **mpls ldp enable**.

Example

Display the session between peer entities.

```
<SW8800> display mpls ldp session
Displaying information about all sessions

Local LDP ID: 1.1.1.9:5;   Peer LDP ID: 4.4.4.9:0
   TCP Connection: 1.1.1.9 <- 4.4.4.9
   Session State: Operational
   Session Role: Passive
   Session existed time:
   Basic Hello Packets Sent/Received: 85/67
   KeepAlive Packets Sent/Received: 1/1
   Negotiated Keepalive hold time: 60   Peer PV Limit: 0
   LDP Basic Discovery Source((A) means active):
   Inter vlan113(A)            Inter vlan112
   Inter vlan111
```

mpls ldp

Syntax

mpls ldp

undo mpls ldp

View

System view

Parameter

None

Description

Use the **mpls ldp** command to enable LDP.

Use the **undo mpls ldp** command to disable LDP.

By default, LDP is disabled.

Before enabling LDP, you must enable MPLS and configure LSR ID first.

Related command: **mpls lsr-id**.

Example

Enable LDP.

```
<SW8800> system-view
[SW8800] mpls ldp
```

mpls ldp enable

Syntax

mpls ldp enable

mpls ldp disable

View

VLAN interface view

Parameter

None

Description

Use the **mpls ldp enable** command to enable LDP on a VLAN interface.

Use the **mpls ldp disable** command to disable LDP on a VLAN interface.

By default, LDP is disabled on an interface.

To enable an interface, you must enable LDP first. After LDP is enabled on an interface, peer discovery and session creation proceed.

Example

Enable LDP on a VLAN interface.

```
<SW8800> system-view
[SW8800] vlan 201
[3Com-Vlan201] port gigabitethernet 2/1/1
[3Com-Vlan201] quit
[SW8800] interface vlan-interface 201
[3Com-Vlan-interface201] mpls
[3Com-vlan-interface201] mpls ldp enable
```

mpls ldp hops-count

Syntax

mpls ldp hops-count *hop-number*

undo mpls ldp hops-count

View

System view

Parameter

hop-number: Maximum hop count of loop detection, ranging from 1 to 32.

Description

Use the **mpls ldp hops-count** command to set the maximum hop count of loop detection.

Use the **undo mpls ldp hops-count** command to restore the default value of the maximum hop count of loop detection.

By default, the maximum hop count of loop detection is 32.

If you need to enable loop detection, configure this command before LDP is enabled on all interfaces. Its value, which depends on actual networking, determines the loop detection speed during LSP creation

Related command: **mpls ldp loop-detection** and **mpls ldp path-vector**.

Example

Set the maximum hop count of loop detection to 22.

```
<SW8800> system-view
[SW8800] mpls ldp hops-count 22
```

Set the maximum hop count of loop detection to its default value 32.

```
[SW8800] undo mpls ldp hops-count
```

mpls ldp loop-detect

Syntax

mpls ldp loop-detect

undo mpls ldp loop-detect

View

System view

Parameter

None

Description

Use the **mpls ldp loop-detect** command to enable loop detection.

Use the **undo mpls ldp loop-detect** command to disable loop detection.

By default, loop detection is not enabled in the system.

If you need to enable loop detection, configure this command before LDP is enabled on any interface.

Related command: **mpls ldp hops-count** and **mpls ldp path-vectors**.

Example

Enable loop detection.

```
<SW8800> system-view
[SW8800] mpls ldp loop-detect
```

Disable loop detection.

```
[SW8800] undo mpls ldp loop-detect
```

mpls ldp label-accept

Syntax

mpls ldp label-accept *ip-prefix-name*

undo mpls ldp label-accept *ip-prefix-name*

View

System view

Parameter

label-accept: Specifies an ingress label filtering policy.

ip-prefix-name: Name of IP address prefix list.

Description

Use the **mpls ldp label-accept** command to control the acceptance of label binding through the IP address prefix filtering policy when a Label Mapping event is received.

Use the **undo mpls ldp label-accept** command to cancel the configuration.

Example

Configure to deny the Label Mapping information of 1.1.1.1 through 1.1.1.3. First, configure the corresponding IP Prefix.

```
<SW8800> system-view
[SW8800] ip ip-prefix fec index 1 deny 1.1.1.1 32
[SW8800] ip ip-prefix fec index 2 deny 1.1.1.2 32
[SW8800] ip ip-prefix fec index 3 deny 1.1.1.3 32
[SW8800] ip ip-prefix fec index 100 permit 0.0.0.0 0 greater-equal 0

less-equal 32
```

Then, configure a specific IP Prefix that will be used in the policy for filtering ingress label mapping.

```
[SW8800] mpls ldp label-accept fec
```

mpls ldp label-advertise

Syntax

mpls ldp label-advertise *fec-ip-prefix* [*lsr-ip-prefix*] [**swap-only**]

undo mpls ldp label-advertise { *fec-ip-prefix* | **all** }

View

System view

Parameter

label-advertise: Specifies a filtering policy for label mapping advertisement

fec-ip-prefix: FEC address prefix list

lsr-ip-prefix: LSR IP address prefix list

swap-only: Creates no Ingress LSP but Swap entries (only when the advertisement control policy is passed).

all: Deletes all filtering policies for label mapping advertisement.

Description

Use the **mpls ldp label-advertise** command to control the advertisement of locally distributed labels; that is, control which label mapping is advertised to which LDP peer.

Use the **undo mpls ldp label-advertise** command to cancel the configuration. By default, the labels of all destination addresses are advertised to all LDP peers.

Example

First, configure the IP Prefix corresponding to the FEC address prefix.

```
<SW8800> system-view

[SW8800]ip ip-prefix fec1 index 1 permit 1.1.1.1 32
[SW8800]ip ip-prefix fec1 index 2 permit 1.1.1.2 32
```

Then, configure the IP Prefix for the peer address used for advertisement.

```
<SW8800> system-view

[SW8800]ip ip-prefix peer1 index 1 permit  2.1.1.1 32
[SW8800]ip ip-prefix peer1 index 2 permit  2.1.1.2 32
[SW8800]ip ip-prefix fec2 index 1 permit 2.2.2.1 32
[SW8800]ip ip-prefix fec2 index 2 permit 2.2.2.2 32
[SW8800]ip ip-prefix peer2 index 1 permit  4.1.1.1 32
[SW8800]ip ip-prefix peer2 index 2 permit  4.1.1.2 32
```

Apply the configured IP Prefix of FEC address and the configured IP Prefix of the peer address in the filtering policy for outgoing label mapping advertisement.

```
<SW8800> system-view

[SW8800] mpls ldp label-advertise fec1 to peer1
```

Configure to advertise the FEC message corresponding to FEC2 but not to create Ingress LSP.

```
[SW8800] mpls ldp label-advertise fec2 to peer2 swap-only
```

mpls ldp password

Syntax

mpls ldp password [**cipher** | **simple**] *password*

undo mpls ldp password

View

VLAN interface view, remote-peer view

Parameter

cipher: Specifies that the password in configuration file will be displayed in cipher-text.

simple: Specifies that the password in configuration file will be displayed in plain-text.

password: User password.

Description

Use the **mpls ldp password** command to configure MD5 authentication password for the LDP. After this configuration, the MD5 authentication is adopted for LDP on the interface.

Use the **undo mpls ldp password** command to delete the configuration.

Example

Configure the LDP authentication mode as MD5, plain-text password 123.

```
<SW8800> system-view
[SW8800] interface vlan-interface 201
[3Com-vlan-interface201] mpls ldp password simple 123
```

mpls ldp path-vectors

Syntax

mpls ldp path-vectors *pv-number*

undo mpls ldp path-vectors

View

System view

Parameter

pv-number: Maximum value of path vector, ranging from 1 to 32.

Description

Use the **mpls ldp path-vectors** command to set the maximum value of path vector.

Use the **undo mpls ldp path-vectors** command to restore the default maximum value of path vector.

By default, *pv-number* is 32.

If you need to enable loop detection, configure this command before LDP is enabled on all interfaces. Its value, which depends on actual networking situation, determines the loop detection speed during LSP creation.

Related command: **mpls ldp loop-detection** and **mps ldp hops-count**.

Example

Set the maximum value of path vector to 23.

```
<SW8800> system-view
[SW8800] mpls ldp path-vectors 23
```

Restore the default maximum value of path vector.

```
[SW8800] undo mpls ldp path-vectors
```

mpls ldp remote-peer

Syntax

mpls ldp remote-peer *index*

undo mpls ldp remote-peer *index*

View

System view or remote-peer view

Parameter

index: Index that identifies a remote peer entity, ranging from 0 to 99.

Description

Use the **mpls ldp remote-peer** command to create a Remote-peer entity and enter remote-peer view.

Use the **undo mpls ldp remote-peer** command to delete a Remote-peer entity.

You can use this command to create a Remote-peer and accordingly create a Remote-session.

Related command: **remote-ip**.

Example

Create a Remote-peer.

```
<SW8800> system-view
[SW8800] mpls ldp remote-peer 22
[3Com-mpls-remote22]
```

Delete a Remote-peer.

```
[3Com-mpls-remote22] undo mpls ldp remote-peer 22
[SW8800]
```

mpls ldp reset-session

Syntax

mpls ldp reset-session *peer-address*

View

VLAN interface view

Parameter

peer-address: Corresponding remote LDP Peer address (in IP address format).

Description

Use the **mpls ldp reset-session** command to reset a specified session on an interface.

After LDP is configured on an interface and LDP session is created, this command can be used to reset a specific session on the interface. You only need to specify the address of the peer corresponding to the session to be reset.

Related command: **mpls ldp** and **mpls ldp enable**.

Example

Reset a specified session on the VLAN201 interface.

```
<SW8800> system-view
[SW8800] interface vlan-interface 201
[3Com-Vlan-interface201] mpls ldp reset-session 10.1.1.1
```

mpls ldp timer

Syntax

In VLAN interface view:

mpls ldp timer { **session-hold** *session-holdtime* | **hello** *hello-holdtime* }

undo mpls ldp timer { **session-hold** | **hello** }

In remote-peer view:

mpls ldp timer { **targeted-session-hold** | **targeted-hello** } { **holdtime** *holdtime* | **interval** *interval* }

undo mpls ldp timer { **targeted-session-hold** | **targeted-hello** } { **holdtime** | **interval** }

View

VLAN interface view, remote-peer view

Parameter

hello *hello-holdtime*: Specifies the hold time (i.e. timeout time) of the Hello hold timer, in the range of 6 to 65535 (seconds). By default it is 15 seconds.

session-hold *session-holdtime*: Specifies the time interval for Session hold timer to send a session packet, in the range of 1 to 65535 (seconds). By default it is 60 seconds.

targeted-hello: Specifies the hold time (i.e. timeout time) of the Targeted-hello hold timer, in the range of 1 to 65535 (seconds). By default *holdtime* is 45 seconds and *interval* is 13 seconds.

targeted-session-hold: Specifies the time interval for Targeted-session hold timer to send a session packet, in the range of 1 to 65535 (seconds). By default *holdtime* is 60 seconds and *interval* is 24 seconds.

holdtime: Time interval for the hold timer.

interval: Time interval to send a Keepalive packet.

Description

Use the **mpls ldp timer** command to set the hold time for the Hello hold timer and Session hold timer.

Use the **undo mpls ldp timer** command to restore the default values.

The timeout of the Hello hold timer means that the adjacency with the peer goes down; the timeout of the Session hold timer means the session with the peer goes down.

targeted-hello *interval* refers to the time interval to send a targeted-hello packet. It cannot be greater than (targeted-hello holdtime) × 0.3, so the maximum value is 65535 × 0.3 = 19660.5.

targeted-session-hold *interval* refers to the time interval to send a Keepalive packet. It cannot be greater than (targeted-session-hold holdtime) × 0.4.

In general, the time interval to send a hello/keepalive packet is one third of the hold time of Hello/Session hold timer.

You can usually use the default values if not in special cases, Note that you must reset the session to validate new values if you do modify these timer parameters.

Related command: **mpls ldp** and **mpls ldp enable**.

Example

Modify the hold time of the Hello timer to 30 seconds.

```
<SW8800> system-view
[SW8800] interface vlan-interface 201
[3Com-Vlan-interface201] mpls ldp timer hello 30
```

mpls ldp transport-ip

Syntax

mpls ldp transport-ip { **interface** | *ip-address* }

undo mpls ldp transport-ip

View

VLAN interface

Parameter

interface: Sets the IP address of the current interface as the transport address.

ip-address: Sets the IP address as the transport address.

Description

Use the **mpls ldp transport-ip** command to configure an LDP transport address.

Use the **undo mpls ldp transport-ip** command to restore the default LDP transport address.

By default, LSR ID is set as a transport address.

When there are multiple directly-connected and MPLS LDP-enabled links between two LSR neighbors, all these links must be configured with the same transport address (it is recommended to adopt the default LSR ID as the transport address). Otherwise, the system may be unable to set up a steady LDP session.

For a Remote-peer, the transport address cannot be configured and is fixed to the LSR ID.

By default, an LSR ID is the address of some Loopback interface and the Remote peer can route to this address for a session. For a Local peer, the address of the local interface or the Router ID of LSR can be adopted as its transport address.

Example

Set the address of the current interface as a transport address.

```
<SW8800> system-view
[SW8800] interface vlan-interface 201
[Quidwa-Vlan-interface201] mpls ldp transport-ip interface
```

Set the address of another interface as a transport address.

```
[3Com-Vlan-interface201] mpls ldp transport-ip 10.1.11.2
```

remote-ip

Syntax

remote-ip *remoteip*

View

remote-peer view

Parameter

remoteip: IP address of the Remote-peer.

Description

Use the **remote-ip** command to configure a Remote-IP address. The address should be the lsr-id of the remote LSR. As Remote Peers adopt LSR ID as their transport addresses, the last two Remote Peers use the lsr-id as their transport addresses for creating TCP connection.

Related command: **mpls ldp remote-peer**.

Example

Configure the address of remote-peer.

```
<SW8800> system-view
[SW8800] mpls ldp remote-peer 12
[3Com-mpls-remote12] remote-ip 192.168.1.1
```

40 BGP/MPLS VPN CONFIGURATION COMMANDS

*Refer to the 05-Routing Protocol Commands Module of the 3Com Switch 8800 Family Command Manual for the details about the **if-match interface**, **if-match acl**, **if-match ip-prefix**, **if-match ip next-hop**, **if-match cost**, **if-match tag**, **apply ip next-hop**, **apply local-preference**, **apply origin**, **apply tag** commands and the related commands.*

aggregate

Syntax

aggregate *address mask* [**as-set** | **attribute-policy** *route-policy-name* | **detail-suppressed** | **origin-policy** *route-policy-name* | **suppress-policy** *route-policy-name*]*

undo aggregate *address mask* [**as-set** | **attribute-policy** *route-policy-name* | **detail-suppressed** | **origin-policy** *route-policy-name* | **suppress-policy** *route-policy-name*]*

View

VPN-instance sub-address family view

Parameter

address: IP address of an aggregated route, in dotted decimal notation.

mask: Network mask of an aggregated route, in dotted decimal notation.

as-set: Generates routes with AS sets.

detail-suppressed: Advertises only aggregated routes.

suppress-policy *route-policy-name*: Suppresses advertisement of some selected specific routes.

origin-policy *route-policy-name*: Selects source route for aggregation.

attribute-policy *route-policy-name*: Sets the attributes of an aggregated route.

Description

Use the **aggregate** command to create an aggregation entry in the BGP routing table of VPN instance.

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

By default, route aggregation is not enabled.

The function of the keywords involved in the above commands is shown in the following table.

Table 93 Keywords function

Keyword	Function
as-set	By setting this keyword, you can create an aggregated route whose AS path contains the information of all the aggregation routes. This keyword is not recommended when aggregating many AS paths because frequent changes of the specific route may result in routing oscillation.
detail-suppressed	This keyword suppresses advertisement of all the specific routes, but not of the aggregated routes. Using the **peer filter-policy** command, you can suppress some specific routes.
suppress-policy	This keyword enables the creation of an aggregate route but disables the advertising of the specified routes. Using the **if-match** clause in the **route-policy** command, you can choose to suppress advertisement of some specific routes.
origin-policy	Using this command, you can only choose the specific routes matching the Route-policy to create aggregated route.
attribute-policy	Using this keyword, you can set the attributes of the aggregation route. The **peer route-policy** command can also enables you to complete the same setting.

Example

Create an aggregation entry in the BGP routing table of VPN instance.

```
[3Com-bgp-af-vpn-instance] aggregate 192.213.0.0 255.255.0.0
```

apply mpls-label

Syntax

apply mpls-label

undo apply mpls-label

View

Route-policy view

Parameter

None

Description

Use the **apply mpls-label** command to configure the system to assign MPLS labels to the public network routes that meet the filer condition of Route-policy.

Use the **undo apply mpls-label** command to cancel this configuration.

By default, the public network routes carry no labels.

Related command: **if-match mpls-label**.

Example

Define an Apply clause to assign labels to routes meeting the Route-policy filter condition.

```
[3Com-route-policy] apply mpls-label
```

debugging bgp

Syntax

debugging bgp { **all** | **event** | **normal** | { **keepalive** | **mp-update** | **open** | **packet** | **route-refresh** | **update** } [**receive** | **send**] [**verbose**] }

undo debugging bgp { **all** | **event** | **normal** | **keepalive** | **mp-update** | **open** | **packet** | **route-refresh** | **update** }

View

User view

Parameter

all: Enables all types of BGP debugging.

event: Enables BGP event debugging.

normal: Enables BGP common function debugging.

keepalive: Enables BGP Keepalive packet debugging.

mp-update: Enables multi-protocol BGP Update packet debugging.

open: Enables BGP Open packet debugging.

packet: Enables BGP packet debugging.

route-refresh: Enables BGP Route-Refresh packet debugging.

update: Enables BGP Update packet debugging.

receive: Displays receive information.

send: Displays send information.

verbose: Displays detailed information.

Description

Use the **debugging bgp** command to enable BGP debugging.

Use the **undo debugging bgp** command to disable BGP debugging.

Caution should be taken in deciding to enable BGP debugging, since debugging affects system performance. Remember to disable the debugging when it is completed.

Example

Enable the debugging on the detailed information about BGP Keepalive packets.

```
<SW8800> debugging bgp keepalive verbose
```

default local-preference

Syntax

default local-preference *value*

undo default local-preference

View

VPNv4 sub-address family view

Parameter

value: Value of the local precedence, ranging from 0 to 4294967295. A greater value enjoys higher precedence. The default local precedence is 100.

Description

Use the **default local-preference** command to configure the local precedence for BGP routing in VPN.

Use the **undo default local-preference** command to restore the default configuration.

The value of the local precedence is advertised between IBGP peers and you can affect the BGP routing in VPN by changing the precedence.

Example

Set the local precedence to be 180, so that the system-advertised routing information will be preferred.

```
[3Com-bgp-af-vpn] default local-preference 180
```

default med

Syntax

default med *med-value*

undo default med

View

VPNv4 sub-address family view, VPN-instance sub-address family view

Parameter

med-value: MED value, ranging from 0 to 4294967295. The default value is 0.

Description

Use the **default med** command to configure the MED value of the system.

Use the **undo default med** command to restore the default value.

MED attributes, switched between autonomous system (AS), is an external measurement for routes and does not leave AS once entering it. The route with smaller MED value will be selected as the external one for AS when other conditions hold.

Example

The routers RTA and RTB belong to AS100 and the router RTC belongs to AS200. RTC associates with RTA and RTB. Set the MED value of RTA 25. This makes the RTC prefer the route sent by RTB.

```
[3Com-bgp-af-vpn-instance] default med 25
```

description

Syntax

description *vpn-instance-description*

undo description

View

VPN-instance view

Parameter

vpn-instance-description: Specifies the description of a specified VPN instance.

Description

Use the **description** command to configure description for a specified VPN instance.

Use the **undo description** command to remove the description of this VPN instance.

Example

Display the VPN description.

```
[3Com-vpn-vpna] description 3com
```

display bgp vpnv4

Syntax

display bgp vpnv4 { **all** | **route-distinguisher** *rd-value* | **vpn-instance** *vpn-instance-name* } { **group** [*group-name*] | **network** | **peer** [[*peer-address*] **verbose**] | **routing-table** [*options*] }

View

Any view

Parameter

all: Displays all the VPNv4 routings.

route-distinguisher *rd-value*: Displays the information related to RD.

vpn-instance *vpn-instance-name*: Displays the information related to VPN instance.

group: Displays the information of a neighbor peer group.

network: Displays the advertised routing information.

peer: Displays the peer information.

verbose: Displays detailed peer information.

routing-table: Displays routing information.

options: Options for viewing the routing information.

Description

Use the **display bgp vpnv4** command to view the VPN address in BGP table.

Example

Display all the BGP VPNv4 routing tables.

```
<SW8800> display bgp vpnv4 all routing-table
Flags:   # - valid       ^ - active      I - internal
         D - damped      H - history     S - aggregate suppressed
In/out   As
    Dest/mask       Next-hop        Med Local-pref      label   path
------------------------------------------------------------------
    Route Distinguisher:1.1.1.1:1 (VPN instance:v1)
#^  1.0.0.0     0.0.0.0                      -/1024
  Routes total: 1
```

display bgp routing-table label

Syntax

display bgp routing-table label

View

Any view

Parameters

None

Description

Use the **display bgp routing-table label** command to view the routing information and label information in the BGP routing table. For an unlabelled common IPv4 route, the label in the displayed information is null. If you use the **display bgp routing-table** address [mask] command to view the BGP routing information, the label information will be displayed if the route has a label.

Example

View the BGP routing information.

```
<SW8800> display bgp routing-table label
Flags:   # - valid       ^ - active      I - internal
          D - damped      H - history     S - aggregate suppressed
                                          In/out
    Dest/Mask          Next-Hop        Label
-------------------------------------------------------------
#^  9.0.0.1/32         0.0.0.0        1024/-
```

View the detailed BGP routing information.

```
<SW8800> display bgp routing-table 9.0.0.1
BGP routing table entry information of 9.0.0.1/32
Age          : 00:00:32
From         : local
State        : valid, sourced, active,
Nexthop      : 0.0.0.0
Origin       : INC
As-path      : (null)
```

```
Med          : 1563
In/Out label :   1024/-
```

display ip routing-table vpn-instance

Syntax

display ip routing-table vpn-instance *vpn-instance-name* [[*ip-address*] | [**verbose**] **statistics**]

View

Any view

Parameter

vpn-instance-name: Name assigned to VPN-instance.

ip-address: Displays information of the specified address

statistics: Displays statistics of routes.

verbose: Displays detailed information.

Description

Use the **display ip routing-table VPN-instance** command to view the specified information in the IP routing table of vpn-instance.

Example

Display the IP routing table associated with the VPN-instance.

```
<PEA> disp ip routing-table vpn-instance vpna-ce1
 vpna-ce1   Route Information
 Routing Table:  vpna-ce1   Route-Distinguisher:   100:1
Destination/Mask  Protocol Pre    Cost     Nexthop         Interface
20.20.20.0/24       BGP     256     0      40.40.40.40  Vlan-interface24
40.40.40.0/24       DIRECT  0       0      40.40.40.10  Vlan-interface24
40.40.40.10/32      DIRECT  0           0      127.0.0.1      InLoopBack0
80.80.80.0/24       BGP         256     0      40.40.40.40  Vlan-interface24
200.200.200.0/24   BGP      256     0      40.40.40.40  Vlan-interface24
 VPN Routing Table:   Route-Distinguisher:   100:2
20.20.20.0/24       BGP         256     0      2.2.2.2
 InLoopBack0
30.30.30.0/24       BGP         256     0      2.2.2.2
 InLoopBack0
```

display ip vpn-instance

Syntax

display ip vpn-instance [*vpn-instance-name* | **verbose**]

View

Any view

Parameter

vpn-instance-name: Name assigned to VPN-instance.

verbose: Displays detailed information.

Description

Use the **display ip vpn-instance** command to view the information related to VPN-instance, such as RD, description, and interfaces of the VPN instance.

Example

Display the information about VPN-instance VPN 1.

```
<SW8800> display ip vpn-instance vpn1
VPN-Instance : vpn1
   No description
   Route-Distinguisher :    100:6
   Interfaces :
   Vlan-interface1100
```

display mpls l3vpn-lsp

Syntax

display mpls l3vpn-lsp [**vpn-instance** *vpn-instance-name*] [**transit** | **egress** | **ingress**] [**include** *text* | **verbose**]

View

Any view

Parameter

transit: LSP for the ASBR (Autonomous System Boundary Router).

egress: LSP of egress VPN.

ingress: LSP of ingress VPN.

vpn-instance: Specifies the name of VPN routing/forwarding VPN-instance

include *text*: Only matches the string including the specified information.

verbose: Displays detailed information.

Description

Use the **display mpls l3vpn-lsp** command to view the information of MPLS L3VPN LSPs of the specified VPN-instance.

Example

Display MPLS L3VPN transit lsp information on the ASBR.

```
<SW8800> display mpls l3vpn-lsp transit
------------------------------------------------------------------
                 LSP Information: Ebgp Transit Lsp
------------------------------------------------------------------
NO     I/O-LABEL        NEXTHOP         IN-INTERFACE    OUT-INTERFACE
1      1025/3             30.30.1.2         -------       Vlan20
2      1024/3             10.10.1.2         -------       Vlan10
3      1026/1024          30.30.1.2         -------       Vlan20
TOTAL:  3 Record(s) Found.
```

Table 94 Description on the fields of the command

Field	Description
NO	Number

Table 94 Description on the fields of the command

Field	Description
I/O-LABEL	Incoming/Outgoing label. VPN labels (labels advertised with VPNV4 routes) will be displayed in case of uni-hop EBGP cross-AS MPLS L3 VPN networking, and tunneling labels (labels advertised with unicast routes and labels advertised by LDP protocol) will be displayed in case of multi-hop EBGP cross-AS MPLS L3 VPN networking.
NEXTHOP	Next hop
IN-INTERFACE	Ingress interface
OUT-INTERFACE	Egress interface

Display MPLS L3VPN ingress lsp information on PE (Provider Edge).

```
<SW8800> display mpls l3vpn-lsp ingress
------------------------------------------------------------------------
                  LSP Information: L3vpn Ingress Lsp
------------------------------------------------------------------------

Vpn-instance Name: vpna     Route Distinguisher: 100:1
NO     FEC                 NEXTHOP       OUTER-LABEL OUT-INTERFACE
1      168.3.1.0/24        10.10.1.1        1026(vpn)     Vlan10

TOTAL:  1 Record(s) Found.
```

Table 95 Description on the fields of the command

Field	Description
NO	Number
FEC	Forwarding equivalent class
NEXTHOP	Next hop
OUTER-LABEL	Outer label (MPLS Tunneling Label)
OUT-INTERFACE	Egress interface

Display MPLS L3VPN egress lsp information on PE.

```
<SW8800> display mpls l3vpn-lsp egress
---------------------  ----------------------------------------
                  LSP Information: L3vpn Egress Lsp
------------------------------------------------------------------------
NO     VRFNAME              INNER-LABEL   NEXTHOP         OUT-INTERFACE
1         vpna               4096         0.0.0.0            InLoop0

TOTAL:  1 Record(s) Found.
```

Table 96 Description on the fields of the command

Field	Description
NO	Number
VRFNAME	Name of VPN Instance
INNER-LABEL	Inner label (VPN label)
NEXTHOP	Next hop
OUT-INTERFACE	Egress interface

display rip vpn-instance

Syntax

display rip vpn-instance *vpn-instance-name*

View

Any view

Parameter

vpn-instance *vpn-instance-name*: Specifies a VPN instance name.

Description

Use the **display rip vpn-instance** command to view the configuration related to VPN instance of RIP.

Example

View the specified VPN instance configuration of RIP.

```
<SW8800> disp rip vpn vpn1
  RIP is running
  private net VPN-Instance: vpn1
    Checkzero is on         Default cost : 1
    Summary is on           Preference : 100
    Period update timer : 30
    Timeout timer : 180
    Garbage-collection timer : 120
    No peer router
    Network :
    192.168.0.0
```

domain-id

Syntax

domain-id { *id-number* | *id-addr* }

undo domain-id

View

OSPF protocol view

Parameter

id-number: Domain-id for a VPN instance, an integer in the range of 0 to 4294967295. By default, it is 0.

id-addr: IP address format of Domain-id for a VPN instance. By default, it is 0.0.0.0.

Description

Use the **domain-id** command to specify Domain-id for a VPN instance.

Use the **undo domain-id** command to restore the default Domain-id.

For standard BGP/OSPF interoperability, when BGP routes are imported to OSPF at PE, their original OSPF attributes cannot be restored. As these BGP VPN IP routes are issued to CE as ASE LSA (type-5 LSA), OSPF cannot distinguish them from the routes imported from other route domains. In order to distinguish external routes

from OSPF internal routes, it is required to restore the attributes of BGP routes when they are imported to OSPF at the remote end. To achieve this goal, we can configure a Domain-id for each OSPF domain. A Domain-id is attached to a BGP/VPN route when an OSPF route is imported into BGP/VPN for transmission over BGP/VPN routes. Then when BGP routes are imported to the peer PE, LAS values are filled in according to the extended community attributes. If the received BGP VPN IP routes have the same Domain-id, they are from the same VPN instance route.

By default, Domain-id is 0.

CAUTION: *The specified Domain-id will not take effect until the* ***reset ospf*** *command is executed.*

Example

Set Domain-id 100 to OSPF process 100.

```
[3Com-ospf-100] domain-id 100
[3Com-ospf-100] domain-id 0.0.0.100
```

filter-policy export

Syntax

filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [*protocol*]

undo filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [*protocol*]

View

VPNv4 sub-address family view, VPN instance sub-address family view

Parameter

acl-number: ACL number, ranging from 2000 to 3999, matching the destination address of routing.

ip-prefix-name: Name of IP prefix to match the destination of routing information.

protocol: Routing protocol whose routing information will be filtered. You can specify one of the following protocols: direct, static, isis, ospf, ospf-ase, ospf-nssa, or rip. If you specify ospf, ospf-ase, or ospf-nssa, the OSPF process ID is needed.

Description

Use the **filter-policy export** command to configure to filter routing information redistribute by a certain protocol. Only the filtered routing information can be advertised. Use the **undo filter-policy export** command to cancel the configuration.

By default, the redistribute routing will not be filtered.

Related command: **filter-policy import**.

Example

Define that only the routes that can pass the filtering of ACL 3 can be received by BGP.

```
[3Com-bgp-af-vpn-instance] filter-policy 3 export
```

filter-policy import

Syntax

filter-policy [**ip-prefix** *ip-prefix-name*] **gateway** *ip-prefix-name* **import**

undo filter-policy [**ip-prefix** *ip-prefix-name*] **gateway** *ip-prefix-name* **import**

filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name* } **import**

undo filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name* } **import**

View

VPNv4 sub-address family view, VPN instance sub-address family view

Parameter

acl-number: ACL number, ranging from 2000 to 3999 to match the destination address of routing.

ip-prefix *ip-prefix-name*: Specifies the name of IP prefix list to match destination of routing.

gateway *ip-prefix-name*: Specifies the name of the IP prefix list for the neighboring routers whose routing information will be filtered.

Description

Use the **filter-policy gateway import** command to filter the information imported from specified routers.

Use the **undo filter-policy gateway import** command to cancel the setting.

Use the **filter-policy import** command to set the filtering conditions to filter routing information.

Use the **undo filter-policy import** command to cancel the setting on filtering conditions.

By default, no filtering is performed on the received information.

Related command: **filter-policy export**.

Example

Define a filtering rule for receiving routing information: Only the routing information matching the IP prefix ACL P1 can it be received by VPN.

```
[3Com-bgp-af-vpn-instance] filter-policy ip-prefix p1 import
```

group

syntax

group *group-name* [**internal** | **external**]

undo group *group-name*

View

VPN-instance sub-address family view

Parameter

group-name: Name of a neighbor peer group. It can be expressed in string of letters and numbers from 1 to 47 in length.

internal: Creates an internal peer group.

external: Creates an external peer group including other sub-AS groups in federation.

Description

Use the **group** command to create a BGP peer group in VPN-instance.

Use the **undo group** command to delete a specified BGP peer group.

By default, the MP-IBGP peer is created.

Members in one peer group must have the same routing export policy as the group does, but can have different ingress policies.

Example

Create an MP-EBGP peer group named test.

```
[3Com-bgp-af-vpn-instance] group test external
```

if-match mpls-label

Syntax

if-match mpls-label

undo if-match mpls-label

View

Route-policy view

Parameter

None

Description

Use the **if-match mpls-label** command to configure the system to match only the public network routes that carries an MPLS label.

Use the **undo if-match mpls-label** command to cancel this configuration.

Related command: **apply mpls-label**.

Example

Define an if-match clause to allow label-carrying routes to pass the filtering of this clause.

```
[3Com-route-policy] if-match mpls-label
```

if-match vpn-target

Syntax

if-match vpn-target { *vpn-target* | **begin** *vpn-target count* }

undo if-match vpn-target

View

Route-policy view

Parameter

vpn-target: Route VPN-target attribute values used for matching, in ASN:nn or IP-address:nn format.

count: Number of the route VPN-target values used for matching, in the range of 2 to 65535.

Description

Use the **if-match vpn-target** command to match the route's **vpn-target** attribute. The match for a route succeeds only when the route's **vpn-target** attribute is a subset of the configured values, otherwise, if the route has no **vpn-target** attribute or has at least one attribute value that is not in the configuration range, the match fails. The **if-match vpn-target** command is applicable only to the PE devices on nested VPN network to limit VPNV4 routes with the VPN-Target attribute from the CE devices.

Use the **undo if-match vpn-target** command to cancel the configuration.

Use the **if-match vpn-target** *vpn-target* command to list up to 10 vpn-target attribute values to be matched.

Use the **if-match vpn-target begin** *vpn-target count* command to set the start value and the total number of the vpn-target values to be matched.

Example

Define an if-match clause to match the following VPN-target attribute values: 100:1, 200:1, 300:1, 300:2 and 400:3.

```
[3Com-route-policy] if-match vpn-target 100:1 200:1 300:1 300:2 400:3
```

With the above-mentioned configuration, if a route's attribute value is 100:1 300:1, the route will pass the matching; if the route's attribute value is 200:1 500:1, it will not pass the matching because 500:1 is not one of the attribute values that have been configured.

Define an if-match clause to match ten VPN-target attribute values starting from 100:1, that is, 100:1 to 100:10.

```
[3Com-route-policy] if-match vpn-target begin 100:1 10
```

Define an if-match clause to match five VPN-target attribute values starting from 1.1.1.1:65533, that is, 1.1.1.1:65533, 1.1.1.1:65534, 1.1.1.1:65535, 1.1.1.2:0, and 1.1.1.2:1.

```
[3Com-route-policy] if-match vpn-target begin 1.1.1.1:65533 5
```

import-route

syntax

import-route { { **ospf** | **ospf-ase** | **ospf-nssa** } [*process-id*] | **direct** | **rip** | **static** } [**med** *value* | **route-policy** *route-policyname*]

undo import-route { { **ospf** | **ospf-ase** | **ospf-nssa** } [*process-id*] | **direct** | **rip** | **static** }

View

VPN-instance sub-address family view

Parameter

process-id: OSPF process ID, ranging from 1 to 65535. By default, it is 1.

ospf: Imports only the ASE internal route discovered by the OSPF process *process-id* as the external route.

ospf-ase: Imports only the OSPF-ASE route discovered by OSPF process with *process-id* as the external route.

ospf-nssa: Imports only the OSPF-NSSA route discovered by OSPF process with *process-id* as the external route.

med *value*: Specifies a route cost value, which ranges from 0 to 4294967295.

route-policyname: Name of Route-policy, consisting of 1 to 19 characters.

Description

Use the **import-route ospf** command to enable OSPF route import.

Use the **undo import-route ospf** command to disable OSPF route import.

CAUTION: *By default, the process ID is 1.*

Example

Configure to import an OSPF route with process ID 100.

```
[SW8800]ip vpn-instance sphinx
[3Com-vpn-sphinx]route-distinguisher 168.168.55.1:85
[3Com-vpn-sphinx]quit
[SW8800]bgp 352
[3Com-bgp]ip vpn-instance sphinx
[3Com-bgp-af-vpn-instance] import-route ospf 100
```

ip binding vpn-instance

Syntax

ip binding vpn-instance *vpn-instance-name*

undo ip binding vpn-instance *vpn-instance-name*

View

VLAN interface view

Parameter

vpn-instance-name: Name assigned to VPN-instance.

Description

Use the **ip binding vpn-instance** command to bind a VLAN interface to a VPN-instance.

Use the **undo ip binding vpn-instance** command to delete the binding.

By default, global routing table is used.

You need to reconfigure the IP address for an interface since this command deletes the original IP address.

Example

Bind the VLAN201 interface to the VPN-instance VPN 1.

```
[SW8800] interface vlan-interface 201
[3Com-Vlan-interface201] ip binding vpn-instance vpn1
```

ip route-static vpn-instance

Syntax

ip route-static vpn-instance *vpn-instance-name* [*vpn-instance-name*] *... destination-ip-address* { *mask* | *mask-length* } [*interface-name* | **vpn-instance** *vpn-nexthop-name*] *nexthop-ip-address* [**preference** *preference-value* | **public**] [**reject** | **blackhole**]

undo ip route-static vpn-instance *vpn-instance-name* [*vpn-instance-name*] *... destination-ip-address* { *mask* | *mask-length* } [*interface-name* | **vpn-instance** *vpn-nexthop-name*] *nexthop-ip-address* [**preference** *preference-value*| **public**] [**reject** | **blackhole**]

View

System view

Parameter

vpn-instance-name: Name of VPN-instance. 6 names can be configured at most, and this value of character string is ranging from 1 to 19 characters.

destination-ip-address: Destination address of a static route.

mask: Subnet mask.

mask-length: Length of the mask, ranging to 0 to 32. As it requires consecutive 1s in a 32-bit mask, the mask in dotted decimal notation can be substituted by *mask-length* (*mask-length* is represented by the number of consecutive 1s in the mask).

interface-name: Outgoing interface name of a static route. You can specify the interface of a public network or other VPN-instance as the outgoing-interface of the static route .NULL 0 shows the outgoing-interface is null.

vpn-nexthop-name: Specifies VPN-instance of the next hop for the static route.

nexthop-ip-address: Specifies IP address of the next hop for the static route.

preference-value: Specifies preference value, ranging from 1 to 255, By default it is 60.

public: Configures a route as public network route.

reject: Configures a route as unreachable.

blackhole: Configures a route as blackhole.

Description

Use the **ip route-static vpn-instance** command to configure a static route by specifying an interface of a private network as an egress interface.

Use the **undo ip route-static vpn-instance** command to delete the configuration of this static route.

Example

Configure a static route with destination address 100.1.1.1 and next hop address 1.1.1.2.

```
[SW8800] ip route-static vpn-instance vpn1 100.1.1.1 16 vpn-instance

vpn1 1.1.1.2
```

ip vpn-instance

Syntax

ip vpn-instance vpn-instance-name

undo ip vpn-instance *vpn-instance-name*

View

System view

Parameter

vpn-instance-name: Name assigned to VPN-instance.

Description

Use the **ip vpn-instance** command to create a VPN instance and enter VPN instance view.

Use the **undo ip vpn-instance** command to delete the specified VPN instance.

By default, VPN-instance is not defined. Neither input nor output list is associated with VPN-instance. No Route-map is associated with VPN-instance.

Use the **ip vpn-instance** command to create a VPN-instance named *vpn-name*.

Example

Create the VPN instance VPN 1.

```
[SW8800] ip vpn-instance vpn1
[3Com-vpn-vpn1]
```

ipv4-family

Syntax

BGP view, VPN-instance sub-address family view or VPNv4 sub-address family view:

ipv4-family { **vpn-instance** *vpn-instance-name* | **vpnv4** [**unicast**] }

undo ipv4-family { **vpn-instance** *vpn-instance-name* | **vpnv4** [**unicast**] }

RIP view:

ipv4-family [**unicast**] **vpn-instance** *vpn-instance-name*

undo ipv4-family [**unicast**] **vpn-instance** *vpn-instance-name*

View

BGP view, VPN-instance sub-address family view or VPNv4 sub-address family view, and RIP view.

Parameter

vpn-instance *vpn-instance-name*: Associates a specified VPN-instance with the MBGP address family. This parameter is used to enter MBGP VPN-instance sub-address family view.

vpnv4: Enters MBGP VPNv4 address family view.

unicast: Uses unicast sub-address family.

Description

Use the **ipv4-family vpn-instance** command to enter MBGP VPN-instance sub-address family view.

Use the **undo ipv4-family vpn-instance** command to delete the association of a VPN-instance with MBGP address family, and return to BGP unicast view.

Use the **ipv4-family vpnv4** command to enter MBGP VPNv4 sub-address family view. Use the **undo ipv4-family vpnv4** command to delete the configuration of MBGP VPNv4 sub-address family view.

By default, unicast address is used when VPNv4 address family is configured.

By default, use the unicast address when configuring the MBGP address family.

Use this command to enter address family view and configure parameters related to BGP address family in this view.

Related command: **peer enable**.

Example

Associate a specified VPN-instance with MBGP address family to enter MBGP VPN-instance sub-address family view. You must first configure VPN-instance before you perform that configuration.

```
[SW8800] bgp 100
[3Com-bgp] ipv4-family vpn-instance abc
[3Com-bgp-af-vpn-instance]
```

Enter VPNv4 sub-address family view.

```
[SW8800] bgp 100
[3Com-bgp] ipv4-family vpnv4 unicast
[3Com-bgp-af-vpn]
```

nesting-vpn

Syntax

nesting-vpn

undo nesting-vpn

View

BGP-VPNv4 sub-address family view

Parameter

None

Description

Use the **nesting-vpn** command to enable the nested VPN function.

Use the **undo nesting-vpn** command to disable this function.

By default, the nested VPN function is disabled.

If VPNv4 route advertisement is needed for a CE connected to a PE, the nested VPN function must be enabled on the PE.

Example

Enable the nested VPN function.

```
[3Com-bgp-af-vpn] nesting-vpn
```

network

Syntax

network *ip-address* [*address-mask*] [**route-policy** *policy-name*]

undo network *ip-address* [*address-mask*] [**route-policy** *policy-name*]

View

VPN-instance sub-address family view

Parameter

ip-address: Network address advertised by BGP in dotted decimal notation.

address-mask: Mask of the network address.

policy-name: Name of the routing policy applied to the advertised route.

Description

Use the **network** command to configure the network route advertised to the outside by local BGP.

Use the **undo network** command to cancel the configuration.

By default, local BGP does not advertise any route to the outside.

Example

Configure local router to advertise the routing with the destination network segment 10.0.0.0/16.

```
[3Com-bgp-af-vpn-instance] network 10.0.0.1 255.255.0.0
```

ospf

Syntax

ospf *process-id* [**router-id** *router-id-number*] [**vpn-instance** *vpn-instance-name*]

undo ospf *process-id*

View

System view

Parameter

process-id: OSPF Process ID. The default process ID is 1.

router-id-number: Router ID for an OSPF process. It is optional.

vpn-instance-name: VPN instance bound to an OSPF process.

Description

Use the **ospf** command to enable an OSPF process.

Use the **undo ospf** command to disable an OSPF process.

After enabling an OSPF process, you can perform the configuration related to OSPF in the OSPF protocol view.

By default, OSPF protocol is not used in the system.

Comware supports multiple OSPF processes, so you can specify different process IDs to enable multiple OSPF processes on a router.

You are recommended to specify Route-id in a process using *Router-id* when enabling the OSPF process. If you want to enable multiple processes on a router, you are recommended to specify different Router IDs for different processes.

To enable an OSPF process belonging to a public network without a Router ID, the following conditions should be satisfied:

- RM (Route Manage) is configured with a Router ID.
- There is an interface that is configured with an IP address.

If you enable an OSPF process without specifying a Router ID, and the process is to be bound to a VPN instance, the VPN instance should have an interface that is configured with an IP address.

If you want to bind a process to a VPN instance, you must specify the VPN instance name.

One VPN instance may include several processes. For example, for VPN1, you can configure the commands **OSPF 1 VPN-instance VPN1**, **OSPF2 VPN-instance VPN1**, and **OSPF3 VPN-instance VPN1**. Accordingly, VPN instance VPN1 will include the OSPF processes 1, 2, and 3.

However, one process belongs to one instance only. If you have configured **OSPF 1 VPN-instance VPN1**, you cannot configure **OSPF 1 VPN-instance VPN2**. Otherwise, the system prompts: "Wrong configuration. Process 1 has been bound to VPN-instance VPN-instance 1". If you configure **OSPF 1** first and then **OSPF 1 VPN-instance VPN1**, the system prompts: "Wrong configuration. Process 1 has been running in public domain".

If you configure **OSPF 1 VPN-instance VPN1** first and then **OSPF 1**, the system enters OSPF 1 VPN-instance VPN1 mode. That is, the **OSPF 1** and **OSPF 1 VPN-instance VPN1** commands are equivalent.

When an OSPF process is bound to a VPN instance, the default OSPF router is PE router. After executing the **display OSPF** *process-id* **brief** command, you will view the information: "PE router, connected to VPN backbone".

CAUTION:

- A router can run no more than 1024 OSPF processes, with up to 10 processes enabled in each VPN instance.
- If you bind an OSPF process to a nonexistent VPN instance, the configuration for the command fails and display the errors: The specified VPN-Instance does not exist, or the VPN-Instance's Route-Distinguisher is not specified.
- When a VPN instance is deleted, all the related OSPF processes will be deleted. For example, the VPN instance VPN 1 includes the OSPF processes 1, 2 and 3. If VPN instance VPN 1 is deleted, the OSPF processes 1, 2 and 3 will all be deleted at the same time.

Related command: **network**.

Example

Enable OSPF protocol with the default process ID 1.

```
[SW8800] router id 10.110.1.8
[SW8800] ospf
```

Enable OSPF protocol with the process ID 120.

```
[SW8800] router id 10.110.1.8
[SW8800] ospf 120
[3Com-ospf-120]
```

Enable OSPF process with the process ID 100, specify its Route ID to 2.2.2.2, and bind it to VPN instance VPN1.

```
[SW8800] ospf 100 router-id 2.2.2.2 vpn-instance vpn1
[3Com-ospf-100]
```

peer advertise-community

Syntax

peer *group-name* **advertise-community**

undo peer *group-name* **advertise-community**

View

VPNv4 sub-address family view, VPN-instance sub-address family view

Parameter

group-name: Name of a neighbor peer group, consisting of 1 to 47 alphanumeric characters.

Description

Use the **peer advertise-community** command to configure to transmit the community attributes to a specified peer group.

Use the **undo peer advertise-community** command to cancel this configuration.

By default, the BGP advertiser does not transmit the community attributes to peer group.

Related command: **if-match community-list** and **apply community**.

Example

Transmit the community attributes to the peer group test.

```
[3Com-bgp] ipv4-family vpnv4
[3Com-bgp-af-vpn] peer test advertise-community
```

peer allow-as-loop

Syntax

peer { *group-name* | *peer-address* } **allow-as-loop** [*asn-limit*]

undo peer { *group-name* | *peer-address* } **allow-as-loop**

View

VPNv4 sub-address family view, VPN-instance sub-address family view

Parameter

group-name: Name of a peer group, consisting of 1 to 47 alphanumeric characters.

peer-address: IP address of a specified peer.

asn-limit: Maximum times for which autonomous system (AS) number is allowed to receive in route updates.

Description

Use the **peer allow-as-loop** command to allow loop in the route updates in the Hub & Spoke networking mode.

Use the **undo peer allow-as-loop** command to prohibit loop in the route updates.

By default, loop is prohibited in the received routing updates; by using the **peer allow-as-loop** command, loop is allowed in the received routing updates. The default value of *asn-limit* argument is 3.

Standard BGP tests loop using AS number. However, on a Hub & Spoke network running EBGP between PE and CE, PE carries its own AS number when advertising route information to CE. Accordingly, the updated route information will contain PE's AS number when it is sent from CE. In this case, PE will not accept the route updates.

You can avoid this by using the **peer allow-as-loop** command, which makes PE router allow the route updates from CE to contain its AS number. You can define *asn-imit* to control the maximum times for which AS number is received by PE.

Example

Enable route loop.

```
[3Com-bgp] ipv4-family vpnv4
[3Com-bgp-af-vpn] peer 1.1.1.1 allow-as-loop 1
```

peer as-number

Syntax

peer { *group-name* | [*peer-address* **group** *group-name*] }**as-number** *as-number*

undo peer { *group-name* | [*peer-address* **group** *group-name*] }**as-number** *as-number*

View

VPN-instance sub-address family view

Parameter

group-name: Name of a peer group, consisting of 1 to 47 alphanumeric characters.

peer-address: IP address of peer group.

as-number: Opposite AS number of a peer (group).

Description

Use the **peer as-number** command to configure the opposite AS number of a specified peer (group).

Use the **undo peer as-number** command to remove the opposite AS number of a specified peer (group).

By default, the opposite end of a peer (group) has no AS number.

Example

Set the opposite AS number of a specified peer (group) to 100.

```
[3Com-bgp] ipv4-family vpn-instance test
[3Com-bgp-af-vpn-instance] peer test as-number 100
```

peer as-path-acl export

Syntax

peer *group-name* **as-path-acl** *acl-number* **export**

undo peer *group-name* **as-path-acl** *acl-number* **export**

View

VPNv4 sub-address family view, VPN-instance sub-address family view

Parameter

group-name: Name of a neighbor peer group, consisting of 1 to 47 alphanumeric characters.

acl-number: AS regular expression ACL number, ranging 1 to 199.

Description

Use the **peer as-path-acl export** command to apply the routing filtering policy based on AS path list to the advertised routing information.

Use the **undo peer as-path-acl export** command to cancel the configuration.

By default, there is no filtering policy based on AS path list.

You can only use the **peer as-path-acl export** command in the peer group.

Related command: **peer as-path-acl import**.

Example

Configure the test peer group to filter the advertised routing information with the AS path ACL 3.

```
[3Com-bgp] ipv4-family vpnv4
[3Com-bgp-af-vpn] peer test as-path-acl 3 export
```

peer as-path-acl import

Syntax

peer { *group-name* | *peer-address* } **as-path-acl** *acl-number* **import**

undo peer { *group-name* | *peer-address* } **as-path-acl** *acl-number* **import**

View

VPNv4 sub-address family view, VPN-instance sub-address family view

Parameter

group-name: Name of a neighbor peer group, consisting of 1 to 47 alphanumeric characters.

peer-address: IP address of the peer group in dotted decimal notation.

acl-number: AS regular expression ACL number, ranging 1 to 199.

import: Filters the received routes with AS path list.

Description

Use the **peer as-path-acl import** command to configure peers from filter received routing information with routing filtering policy based on AS path list.

Use the **undo peer as-path-acl import** command to cancel the configuration.

By default, there is no filtering policy based on AS path list.

The incoming filtering policy applied to peers takes precedence over the configuration to peer groups.

Example

Configure the test peer group to filter the received routes with AS path ACL 3.

```
[3Com-bgp] ipv4-family vpnv4
[3Com-bgp-af-vpn] peer test as-path-acl 3 import
```

peer connect-interface

Syntax

peer { *group-name* | *ip-address* } **connect-interface** { *interface-type interface_num* }

undo peer { *group-name* | *ip-address* } **connect-interface**

View

VPN-instance sub-address family view

Parameter

group-name: Name of a neighbor peer group, consisting of 1 to 47 alphanumeric characters.

ip-address: Peer IP address.

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

Description

Use the **peer connect-interface** command to configure to allow the internal BGP session to use any operable interface for a TCP connection.

Use the **undo peer connect-interface** command to restore the optimum local address for a TCP connection.

By default, BGP uses the optimum local address to implement a TCP connection.

Generally, BGP uses the optimum local address to implement a TCP connection. In order to make the TCP connection valid even when the interface fails, you can configure to allow the internal BGP session to use any operable interface for the TCP connection. Usually, loopback interface is used.

Example

Allow the internal BGP session to use any operable interface for a TCP connection.

```
[3Com-bgp] ipv4-family vpn-instance test
[3Com-bgp-af-vpn-instance] peer 1.1.1.1 connect-interface loopback 0
```

peer default-route-advertise

Syntax

peer *group-name* **default-route-advertise**

undo peer *group-name* **default-route-advertise**

View

VPN-instance sub-address family view

Parameter

group-name: Name of a neighbor peer group, consisting of 1 to 47 alphanumeric characters.

Description

Use the **peer default-route-advertise** command to enable a peer (group) to transmit a default route.

Use the **undo peer default-route-advertise** command to remove the existing configuration.

By default, a peer (group) does not transmit a default route.

This command does not require any default route in the routing table but transmits a default route whose next hop address is itself to the peer unconditionally.

Example

Enable the peer group test to transmit a default route.

```
[3Com-bgp] ipv4-family vpn-instance a
[3Com-bgp-af-vpn-instance] peer test default-route-advertise
```

peer default-route-advertise vpn-instance

Syntax

peer *ip-address* **default-route-advertise vpn-instance** *vpn-instance name*

undo peer *ip-address* **default-route-advertise vpn-instance** *vpn-instance name*

View

VPNv4 sub-address family view

Parameter

ip-address: Peer IP address.

vpn-instance name: Name of the created VPN instance.

Description

Use the **peer default-route-advertise vpn-instance** command to enable a peer to import a default route.

Use the **undo peer default-route-advertise vpn-instance** to restore the configuration.

By default, a peer does not import a default route.

This command does not require any default route in the routing table but transmits a default route whose next hop address is itself to the peer unconditionally.

Example

Enable the peer test to import a default route.

```
[3Com-bgp] ipv4-family vpnv4
[3Com-bgp-af-vpn] peer 10.1.1.1 default-route-advertise vpn-instance
 test
```

peer description

Syntax

peer { *group-name* | *peer-address* } **description** *description-line*

undo peer { *group-name* | *peer-address* } **description**

View

VPN-instance sub-address family view

Parameter

group-name: Name of a neighbor peer group, consisting of 1 to 47 alphanumeric characters.

peer-address: Peer IP address, in dotted decimal notation.

description-line: Description of the configuration, up to 79 characters in length.

Description

Use the **peer description** command to set the description of a peer (group).

Use the **undo peer description** command to delete the description.

By default, there is no description for a peer (group).

The peer description is independent of the peer's group description.

Related command: **display bgp peer verbose** and **display bgp group**.

Example

Set description of the peer group group1 to be city 1.

```
[3Com-bgp-af-vpn-instance] peer group1 description city1
```

peer ebgp-max-hop

Syntax

peer *group-name* **ebgp-max-hop** [*ttl*]

undo peer *group-name* **ebgp-max-hop**

View

VPN-instance sub-address family view

Parameter

group-name: Name of a neighbor peer group, consisting of 1 to 47 alphanumeric characters.

peer-address: Peer IP address.

ttl: Maximum hops, in the rang of 1 to 255 and is 64 by default.

Description

Use the **peer ebgp-max-hop** command to establish an EBGP connection with a specified neighbor which is attached to the network indirectly.

Use the **undo peer ebgp-max-hop** command to restore the default setting.

By default, you can only make a connection with a direct accessing EBGP neighbor.

Example

Enable the router to connect the EBGP peer group test that is attached to the network indirectly.

```
[3Com-bgp] ipv4-family vpn-instance test
[3Com-bgp-af-vpn-instance] peer test ebgp-max-hop
```

peer enable

Syntax

peer *group-name* **enable**

undo peer *group-name* **enable**

View

VPNv4 sub-address family view

Parameter

group-name: Name of a neighbor peer group, consisting of 1 to 47 alphanumeric characters.

Description

Use the **peer enable** command to enable a specified peer group.

Use the **undo peer enable** command to disable a specified peer group.

For IPv4 address family, address switching is enabled by default.

Example

Enable the peer group 168.

```
[3Com-bgp] ipv4-family vpnv4
[3Com-bgp-af-vpn] peer 168 enable
```

peer filter-policy export

Syntax

peer *group-name* **filter-policy** *acl-number* **export**

undo peer *group-name* **filter-policy** *acl-number* **export**

View

VPNv4 sub-address family view, VPN-instance sub-address family view

Parameter

group-name: Name of a neighbor peer group, consisting of 1 to 47 alphanumeric characters.

acl-number: IP ACL number ranging from 2000 to 3999. That is, you can use basic ACL or advanced ACL.

export: Uses the filtering policy for the advertised route and this policy is only effective for peer groups.

Description

Use the **peer filter-policy export** command to apply the ACL-based filtering policy to the advertised route for the peer group.

Use the **undo peer filter-policy export** command to cancel the configuration.

By default, there is no ACL-based filtering policy.

You can only use the **peer filter-policy export** command to configure peer group.

Related command: **ip as-path-acl**, **peer as-path-acl** and **peer filter-policy export**.

Example

Configure the test peer group to filter the advertised route with ACL 3000.

```
[3Com-bgp] ipv4-family vpnv4
[3Com-bgp-af-vpn] peer test filter-policy 3000 export
```

peer filter-policy import

Syntax

peer { *group-name* | *peer-address* } **filter-policy** *acl-number* **import**

undo peer { *group-name* | *peer-address* } **filter-policy** *acl-number* **import**

View

VPNv4 sub-address family view, VPN-instance sub-address family view

Parameter

group-name: Name of a neighbor peer group, consisting of 1 to 47 alphanumeric characters.

peer-address: Peer IP address, in dotted decimal notation.

acl-number: IP ACL number from 2000 to 3999, that is, you can use basic or advanced ACL.

import: Performs the filtering policy on the received routes.

Description

Use the **peer filter-policy import** command to apply the ACL-based filtering policy to the received routing information for peers.

Use the **undo peer filter-policy import** command to cancel the application.

By default, there is no ACL-based filtering policy.

Related command: **ip as-path-acl** and **peer as-path-acl**.

The incoming filtering policy configured for peers take precedence over the configuration for peer groups.

Example

Configure the test peer group to filter the received route with ACL 3000.

```
[3Com-bgp] ipv4-family vpnv4
[3Com-bgp-af-vpn] peer test filter-policy 3000 import
```

peer group

Syntax

peer *peer-address* **group** *group-name* [**as-number** *as-number*]

undo peer *peer-address*

View

VPNv4 sub-address family view, VPN-instance sub-address family view

Parameter

group-name: Name of a neighbor peer group, consisting of 1 to 47 alphanumeric characters.

peer-address: Peer IP address in dotted decimal notation.

as-number: Peer AS number in the range of 1 to 65535. This parameter is only effective in the BGP view and VPN-instance sub-address family view.

Description

Use the **peer group** command to add a peer to an existing peer group.

Use the **undo peer** command to delete a specified peer from the group.

In BGP view and VPN-instance sub-address family view, when adding a peer to an external group out of an AS, you need to specify an AS number. When adding a peer to an internal group or an external group in an AS, the AS number is not needed.

A peer must have been added in a group in BGP view before it can be added to another group in multicast sub-address family view or VPNv4 sub-address family view.

In different address families, one peer can be in different groups and one group may have different peers.

Example

Add the peer with IP address 10.1.1.1 to the peer group test. In this example, the peer group is IBGP peer by default, thus you need not to specify the AS number when adding peers.

```
[3Com-bgp] ipv4-family vpnv4
[3Com-bgp-af-vpn] peer 10.1.1.1 group test
```

peer ip-prefix export

Syntax

peer *group-name* **ip-prefix** *prefixname* **export**

undo peer *group-name* **ip-prefix** *prefixname* **export**

View

VPNv4 sub-address family view, VPN-instance sub-address family view

Parameter

group-name: Name of a neighbor peer group, consisting of 1 to 47 alphanumeric characters.

prefixname: Name of prefix list, a string of one to 19 characters.

Description

Use the **peer ip-prefix export** command to apply the routing filtering policy based on IP prefix list to advertised routing information for peer groups.

Use the **undo peer ip-prefix export** command to cancel the setting.

By default, the peer group does not perform the routing filtering policy.

you can only configure the **peer ip-prefix export** command to the peer group.

Related command: **peer ip-prefix import**.

Example

Configure the peer group group1 to filter the advertised routing information with the IP prefix list list1.

```
[3Com-bgp] ipv4-family vpnv4
[3Com-bgp-af-vpn] peer group1 ip-prefix list1 export
```

peer ip-prefix import

Syntax

peer { *group-name* | *peer-addess* } **ip-prefix** *prefixname* **import**

undo peer { *group-name* | *peer-addess* } **ip-prefix** *prefixname* **import**

View

VPNv4 sub-address family view, VPN-instance sub-address family view

Parameter

group-name: Name of a neighbor peer group, consisting of 1 to 47 alphanumeric characters.

peer-address: Peer IP address in dotted decimal notation.

prefixname: Name of the prefix list, a string of one to 19 characters.

Description

Use the **peer ip-prefix import** command to apply the filtering policy based on IP prefix list to the advertised route for peer groups.

Use the **undo peer ip-prefix import** command to cancel the configuration.

By default, the peer dose not use the routing filtering policy.

The incoming filtering policy configured for peers take precedence over the configuration for peer groups.

Related command: **peer ip-prefix export**.

Example

Configure the peer group group1 to filter the received route with the IP prefix list 1.

```
[3Com-bgp] ipv4-family vpnv4
[3Com-bgp-af-vpn] peer group1 ip-prefix list1 import
```

peer label-route-capability

Syntax

peer *group-name* **label-route-capability**

undo peer *group-name* **label-route-capability**

View

BGP view

Parameter

group-name: Name of a neighbor peer group.

Description

Use the **peer label-route-capability** command to enable a peer group to handle the label-carried IPv4 routes.

Use the **undo peer label-route-capability** command to disable a peer group from handling the label-carried IPv4 routes.

By default, a BGP peer group cannot handle label-carried IPv4 routes.

Example

Enable IBGP peer group and EBGP peer group to handle the label-carried IPv4 routes.

```
[3Com-bgp] group ibgp internal
[3Com-bgp] peer ibgp label-route-capability
[3Com-bgp] group ebgp external
[3Com-bgp] peer ebgp label-route-capability
```

peer next-hop-local

Syntax

peer *group-name* **next-hop-local**

undo peer *group-name* **next-hop-local**

View

VPNv4 sub-address family view, VPN-instance sub-address family view

Parameter

group-name: Name of a neighbor peer group, consisting of 1 to 47 alphanumeric characters.

Description

Use the **peer next-hop-local** command to cancel the processing of the next hop in the routes that BGP advertises to a peer group and configure to use its own address as the next-hop.

Use the **undo peer next-hop-local** command to cancel the existing setting.

Example

Specify the current BGP address as the next-hop in its route advertising to a peer group.

```
[3Com-bgp] ipv4-family vpnv4
[3Com-bgp-af-vpn] peer test next-hop-local
```

peer password

Syntax

peer { *group-name* | *peer-address* } **password** { **cipher** | **simple** } *password*

undo peer { *group-name* | *peer-address* } **password**

View

VPN-instance sub-address family view

Parameter

group-name: Name of a neighbor peer group, consisting of 1 to 47 alphanumeric characters.

peer-address: Peer IP address in dotted decimal notation.

cipher: Displays the password in cipher text.

simple: Displays the password in plain text.

password: Password string. When you provide the **cipher** argument but input the password in plain text, or if you provide the **simple** argument, the password is one to 16 characters in length. When you provide the **cipher** argument and input the password in cipher text, the password must be 24 in length.

Description

Use the **peer password** command to enable BGP to perform the MD5 authentication when establishing a TCP connection.

Use the **undo peer password** command to cancel this function.

By default, BGP does not perform the MD5 authentication when setting up a TCP connection.

When the MD5 authentication is enabled, both parties must have the same authentication mode and password; otherwise, no TCP connection can be established because MD5 authentication fails.

MD5 authentication can be performed on a specific peer only when the group to which the peer belongs is not configured with MD5 authentication. Otherwise, the configuration of the peer group applies.

Example

Assign MD5 authentication to a TCP connection between the local router 10.1.100.1 and the peer 10.1.100.2.

```
[3Com-bgp-af-vpn-instance] peer 10.1.100.2 password simple 3com
```

Perform a similar configuration to the remote end.

```
[3Com-bgp-af-vpn-instance] peer 10.1.100.1 password simple 3com
```

peer public-as-only

Syntax

peer *group-name* **public-as-only**

undo peer *group-name* **public-as-only**

View

VPNv4 sub-address family view, VPN-instance sub-address family view

Parameter

group-name: Name of a neighbor peer group, consisting of 1 to 47 alphanumeric characters.

Description

Use the **peer public-as-only** command to configure BGP not to carry private AS numbers when transmitting update packets.

Use the **undo peer public-as-only** command to configure BGP to carry private AS numbers when transmitting update packets.

By default, private AS numbers are carried when BGP transmits update packets.

Generally, BGP carries AS number (either public or private AS number) when transmitting BGP update packets. BGP can be configured not to carry private AS number so that some egress routers may ignore private AS number when transmitting BGP update packets.

*The **public-as-only** keyword is required for configuring EBGP and alliance, but not for configuring IBGP.*

Example

Send MBGP update packets without carrying private AS numbers.

```
[3Com-bgp] ipv4-family vpnv4
[3Com-bgp-af-vpn] peer 168 public-as-only
```

peer reflect-client

Syntax

peer *group-name* **reflect-client**

undo peer *group-name* **reflect-client**

View

VPNv4 sub-address family view

Parameter

group-name: Name of a neighbor peer group, consisting of 1 to 47 alphanumeric characters.

Description

Use the **peer reflect-client** command to set a specified peer group to be a client of a router reflector.

Use the **undo peer reflect-client** command to cancel this setting.

By default, no router reflector exists in AS.

This configuration only applies to IBGP peer group.

Related command: **reflect between-clients** and **reflect cluster-id**.

Example

Set the peer group test as a client of a router reflector.

```
[3Com-bgp] ipv4-family vpnv4
[3Com-bgp-af-vpn] peer test reflect-client
```

peer route-policy export

Syntax

peer *group-name* **route-policy** *policy-name* **export**

undo peer *group-name* **route-policy** *policy-name* **export**

View

VPNv4 sub-address family view, VPN-instance sub-address family view

Parameter

group-name: Name of a neighbor peer group, consisting of 1 to 47 alphanumeric characters.

policy-name: Name of a routing policy.

Description

Use the **peer route-policy export** command to apply the routing policy to peer group for advertised routing information.

Use the **undo peer route-policy export** command to cancel the configuration.

By default, there is no routing policy.

The **peer route-policy export** command is only used to configure peer groups.

Related command: **peer route-policy import**.

Example

Apply the routing policy test-policy to the outgoing routes of the peer group test.

```
[3Com-bgp] ipv4-family vpnv4
[3Com-bgp-af-vpn] peer test route-policy test-policy export
```

peer route-policy import

Syntax

peer { *group-name* | *peer-address* } **route-policy** *policy-name* **import**

undo peer { *group-name* | *peer-address* } **route-policy** *policy-name* **import**

View

VPNv4 sub-address family view, VPN-instance sub-address family view

Parameter

group-name: Name of a neighbor peer group, consisting of 1 to 47 alphanumeric characters.

peer-address: Peer IP address in dotted decimal notation.

policy-name: Name of the applied routing policy.

Description

Use the **peer route-policy import** command to apply a routing policy to peer for received routing information.

Use the **undo peer route-policy import** command to delete the setting.

By default, there is no routing policy.

The incoming filtering policy configured for peers take precedence over the configuration for peer groups.

Related command: **peer route-policy export**.

Example

Apply the routing policy test-policy to the incoming routes of the peer group test.

```
[3Com-bgp] ipv4-family vpnv4
[3Com-bgp-af-vpn] peer test route-policy test-policy import
```

peer route-update-interval

Syntax

peer *group-name* **route-update-interval** *seconds*

undo peer *group-name* **route-update-interval**

View

VPN-instance sub-address family view

Parameter

group-name: Name of a neighbor peer group, consisting of 1 to 47 alphanumeric characters.

seconds: Update interval in seconds, ranging from 0 to 600.

Description

Use the **peer route-update-interval** command to set the Update interval for peers.

Use the **undo peer route-update-interval** command to restore the default setting.

By default, the Update interval is 5 seconds for IBGP peer group, and for EBGP it is 30 seconds.

Example

Set the minimum interval for sending routing update packet to the BGP peer group group1 to be 10 seconds.

```
[3Com-bgp-af-vpn-instance] peer group1 route-update-interval 10
```

peer timer

Syntax

peer { *group-name* | *peer-address* } **timer keep-alive** *keepalive-interval* **hold** *holdtime-interval*

undo peer { *group-name* | *peer-address* } **timer**

View

VPN-instance sub-address family view

Parameter

group-name: Name of a neighbor peer group, consisting of 1 to 47 alphanumeric characters.

peer-address: Peer IP address in dotted decimal notation.

keepalive-interval: Interval, in seconds, of sending the Keepalive message. It ranges from 1 to 65535 and defaults to 60.

holdtime-interval: Holdtime, in seconds. It ranges from 3 to 65535 and defaults to 180.

Description

Use the **peer timer** command to set the Keepalive interval and holdtime for peers.

Use the **undo peer timer** command to restore the default setting.

The timer set with the **peer timer** command enjoys higher precedence than the timer with the **timer** command.

Related command: **timer keep-alive hold**.

Example

Set the Keepalive interval and holdtime for the peer group test.

```
[3Com-bgp-af-vpn-instance] peer test timer keep-alive 60 hold 180
```

peer upe

Syntax

peer *peer-address* **upe**

undo peer *peer-address* **upe**

View

VPNv4 sub-address family view

Parameter

peer-address: Peer IP address.

Description

Use the **peer upe** command to configure BGP peer as the UPE of hierarchical BGP/MPLS VPN.

Use the **undo peer upe** command to delete this configuration.

Example

Configure BGP peer as the UPE of hierarchical BGP/MPLS VPN.

```
[3Com-bgp] ipv4-family vpnv4
[3Com-bgp-af-vpn] peer 1.1.1.1 upe
```

peer vpn-instance enable

Syntax

peer *group-name* **vpn-instance** *vpn-instance-name* **enable**

undo peer *group-name* **vpn-instance** *vpn-instance-name* **enable**

View

BGP-VPNv4 sub-address family view

Parameter

group-name: Name of a peer group.

vpn-instance-name: Name of the VPN instance the CE peer belongs to.

enable: Enables VPNv4 function for the CE.

Description

Use the **peer vpn-instance enable** command to enable the VPNv4 function for the BGP peer group of a CE.

Use the **undo peer vpn-instance enable** command to disable the function.

By default, the VPNv4 function is disabled.

Example

Enable the VPNv4 function for the peer group of a CE.

```
[3Com-bgp] ipv4-family vpn-instance vrf1
[3Com-bgp-af-vpn-instance] group ebgp external
[3Com-bgp-af-vpn-instance] quit
[3Com-bgp] ipv4-family vpnv4
[3Com-bgp-af-vpn] peer ebgp vpn-instance vrf1 enable
```

peer vpn-instance group

Syntax

peer *peer-address* **vpn-instance** *vpn-instance-name* **group** *group-name*

undo peer *peer-address* **vpn-instance** *vpn-instance-name*

View

BGP-VPNv4 sub-address family view

Parameter

peer-address: IP address of a peer, in dotted decimal notation.

vpn-instance-name: Name of the VPN instance the CE peer belongs to.

group-name: Name of a peer group.

Description

Use the **peer vpn-instance group** command to join a CE neighbor into a BGP peer group.

Use the **undo peer vpn-instance group** command to clear the CE neighbor from the BGP peer group.

By default, a CE neighbor does not belong to any peer group.

Example

Add a CE neighbor to a peer group.

```
[3Com-bgp] ipv4-family vpn-instance vrf1
[3Com-bgp-af-vpn-instance] peer 1.1.1.1 group ebgp as-number 600
[3Com-bgp-af-vpn-instance] quit
[3Com-bgp] ipv4-family vpnv4
[3Com-bgp-af-vpn] peer 1.1.1.1 vpn-instance vrf1 group ebgp
```

peer vpn-instance route-policy import

Syntax

peer { *peer-address* | *group-name* } **vpn-instance** *vpn-instance-name* **route-policy** *policy-name* **import**

undo peer { *peer-address* | *group-name* } **vpn-instance** *vpn-instance-name* **route-policy** *policy-name* **import**

View

BGP-VPNv4 sub-address family view

Parameter

peer-address: IP address of a peer, in dotted decimal.

group-name: Name of a peer group.

vpn-instance-name: Name of the VPN instance the CE peer belongs to.

policy-name: Name of the routing policy to be applied.

Description

Use the **peer vpn-instance route-policy import** command to configure the routing policy applied by the CE peer to VPNv4 routes it received.

Use the **undo peer vpn-instance route-policy import** command to cancel the configuration.

By default, no routing policy is configured.

The ingress routing policy configured for a peer takes precedence over the configuration for the peer group.

Example

Configure the peer group ebgp to apply the routing policy named comtest to the ingress routes.

```
[3Com-bgp-af-vpn] peer ebgp vpn-instance vrf1 route-policy comtest import
```

policy vpn-target

Syntax

policy vpn-target

undo policy vpn-target

View

BGP-VPNv4 sub-address family view

Parameter

None

Description

Use the **policy vpn-target** command to configure to filter the VPN-target extended community attributes of received routing information.

Use the **undo policy vpn-target** command to cancel the setting.

By default, the filtering of VPN-target extended community attribute is conducted.

Example

Filter the VPN-target extended community attributes of the received routing information.

```
[3Com-bgp-af-vpn] policy vpn-target
```

port trunk mpls vlan

Syntax

port trunk mpls vlan from *vlan-id* [**to**] *vlanid*

undo port trunk mpls

View

Ethernet port view

Parameters

vlan-id: *vlan-id* range of MPLS/VPN VLANs allowed to the port. The value ranges from *vlan-id* to *vlan-id*+1023.

Description

Use the **port trunk mpls vlan** command to set the *vlan-id* range of MPLS/VPN VLANs allowed to pass the port.

Use the **undo port trunk mpls** command to restore the default value of *vlan-id*. The default value is 0.

By default, the range of MPLS/VPN VLANs is from 0 to 1023 and the range of vlan-id is from 1 to 3071. The command must be executed on a Trunk port. MPLS/VPN enabled VLANs and VLANs out of the configured range are excluded.

Example

Configure the start *vlan-id* of the Trunk fast Ethernet port 1.

```
<SW8800> system-view
[SW8800]interface Ethernet 3/1/1
[3Com-Ethernet2/1/1] port trunk mpls vlan from 3071
```

port vpn-range share-mode

Syntax

port vpn-range share-mode enable

undo port vpn-range share-mode enable

View

Fast Ethernet port view

Parameter

None

Description

Use the **port vpn-range share-mode** command to set the range of MPLS/VPN VLAN *vlan-id* on the interface to 4K.

Use the **undo port vpn-range share-mode** command to restore the default MPLS/VPN VLAN *vlan-id* range, which is 0 to 1023.

- Ports supporting this function stop supporting the application of ACL rules.
- After you cancel the **port vpn-range share-mode** configuration, the label range does not take effect if the VLAN configuration on the port exceeds 1K. In this case, you need to delete the labels manually.

Example

Enable the range of MPLS/VPN VLAN *vlan-id* on Ethernet3/1/1 as 4K.

```
<SW8800> system-view
[SW8800] interface Ethernet 3/1/1
[3Com-Ethernet3/1/1] port vpn-range share-mode enable
```

preference

Syntax

preference *ebgp-preference ibgp-preference local-preference*

undo preference

View

VPN-instance sub-address family view

Parameter

ebgp-preference: Preference of the routes learned from the EBGP peer, in the range 1 to 256.

ibgp-preference: Preference of the routes learned from the IBGP peer, in the range 1 to 256.

local-preference: Preference of the Local routes, in the range 1 to 256.

Description

Use the **preference** command to set preference value for a BGP route.

Use the **undo preference** command to remove the setting.

Example

Set the preference of the preference of the routes learned from the EBGP peer to 2, the preference of the routes learned from the IBGP peer to 3 and the preference of the local routes to 4.

```
[3Com-bgp-af-vpn-instance] preference 2 3 4
```

reflect between-clients

Syntax

reflect between-clients

undo reflect between-clients

View

VPNv4 sub-address family view

Parameter

None

Description

Use the **reflect between-clients** command to allow the routing reflection between clients.

Use the **undo reflect between-clients** command to forbid routing reflection between clients (PE to PE).

By default, the routing reflection between clients is allowed.

The router reflector reflects one client's route to others after configuration.

Related command: **reflect cluster-id** and **peer reflect-client**.

Example

Disable the routing reflection from client to client.

```
[3Com-bgp-af-vpn] undo reflect between-clients
```

reflector cluster-id

Syntax

reflector cluster-id { *cluster-id* | *address* }

undo reflect cluster-id

View

VPNv4 sub-address family view

Parameter

cluster-id: Router reflector cluster ID in number format, in the range of 1 to 4294967295.

address: Router reflector cluster ID in IP address format.

Description

Use the **reflector cluster-id** command to configure a cluster ID of router reflector.

Use the **undo reflector cluster-id** command to delete the configuration.

By default, each router reflector uses his own ID as a cluster ID.

Usually, one cluster has one router reflector. And it is the router ID of the reflector to identify this cluster. Several router reflectors make the network more stable. If one cluster has several router reflectors, set the same cluster to all the reflectors ID with this command.

Related command: **reflect between-clients** and **peer reflect-client**.

Example

The local router is one of the reflectors in the cluster and identifies this cluster with the cluster ID.

```
[3Com-bgp-af-vpn] reflect cluster-id 80
[3Com-bgp-af-vpn] peer 11.128.160.10 reflect-client
```

route-distinguisher

Syntax

route-distinguisher *route-distinguisher*

View

VPN-instance view

Parameter

route-distinguisher: Configures a VPN IPv4 prefix by adding an 8-byte value to a VPN IPv4 prefix.

Description

Use the **route-distinguisher** command to configure RD for an MPLS VPN instance. A VPN-instance cannot run until it is configured with an RD.

A route distinguisher (RD) creates route and forwarding list for a VPN and specifies the default route identifier. Add an RD to the beginning of a specific IPv4 prefix to make it a globally unique VPN IPv4 prefix.

If an RD is associated with an autonomous system number (ASN), it is composed of the ASN and an arbitrary number; if the RD is associated with an IP address, it is a combination of the IP address and an arbitrary number.

RD has the following formats:

16-bit ASN (can be 0 here): A custom 32-bit number, for example, 101:3.

32-bit IP address (can be 0.0.0.0 here): A custom 16-bit number, for example, 192.168.122.15:1.

Example

Configure RD for an MPLS VPN instance.

```
[SW8800] ip vpn-instance vpn-instance_blue
[3Com-vpn-vpn-instance_blue] route-distinguisher 100:3
[SW8800] ip vpn-instance vpn-instance_red
[3Com-vpn-vpn-instance_red] route-distinguisher 173.13.0.12:200
```

route-tag

Syntax

route-tag *tag-number*

undo route-tag

View

OSPF protocol view

Parameter

tag-number: Tag value to identify VPN import route, in the range of 0 to 4294967295. By default, its first two bytes are fixed to 0xD000, while the last two bytes are the ASN of local BGP. For example, if the local BGP ASN is 100, then the default tag value in decimal is 3489661028. The value is an integer from 0 to 4294967295.

Description

Use the **route-tag** command to specify a tag value to identify VPN import route.

Use the **undo route-tag** command to restore the default value.

If a VPN Site is linked to multiple PEs, when a route learned from MPLS/BGP is advertised by a PE router via its type-5 or type-7 LSA to the VPN Site, the route may be received by another PE router. This will result in routing loop. To avoid routing loop, you should configure Route-tag and you are recommended to configure the same route-tag for the PEs in the same VPN domain. The Route-tag is included in the type-5/-7 LSA. It is not transmitted in the extended community attributes of BGP, and thus it is limited in the local area. Therefore, it can only be configured and function on the PE router which receives BGP routes and generates OSPF LSA.

Configure Route-tag in OSPF protocol view. Different processes can be configured with a same Route-tag. You can configure the same Route-tag using different commands, but they are different in priority.

- Those configured with the **import-route** command are of the highest priority.
- Those configured with the **route-tag** command are in the second place in terms of priority.
- Those configure with the **default tag** command are of the lowest priority.

If the Tag included in the type-5/-7 LSA is identical with its existing Tag, the LSA received will be neglected in route calculation.

CAUTION: *The Route-tag configured will not be validated until the* ***reset ospf*** *command is executed.*

Related command: **import-route** and **default**.

Example

Configure Route-tag 100 to OSPF process 100.

```
[3Com-ospf-100] route-tag 100
 OSPF: Process 100's route tag has been changed
```

```
OSPF: Reboot the system or use the 'reset ospf ID' command for this to take
      effect
```

timer

Syntax

timer keep-alive *keepalive-interval* **hold** *holdtime-interval*

undo timer

View

VPN-instance sub-address family view

Parameter

keepalive-interval: Time interval, in seconds, of sending Keepalive messages. It ranges from 1 to 65535 and defaults to 60.

holdtime-interval: Hold time, in seconds. It ranges from 3 to 65535 and defaults to 180.

Description

Use the **timer** command to specify the time interval and hold time for sending Keepalive messages.

Use the **undo timer** command to restore the default value.

The timer defined with the **peer timer** command takes preference over that with the **timer** command.

Related command: **peer timer**.

Example

Set the time interval and hold time for sending Keepalive messages.

```
[3Com-bgp-af-vpn-instance] timer keep-alive 60 hold 180
```

traffic-redirect

Syntax

traffic-redirect inbound { **link-group** { *acl-number* | *acl-name* } [**rule** *rule* [**system-index** *index*]] | **ip-group** { *acl-number* | *acl-name* } [**rule** *rule* [**system-index** *index*]] } **interface** { *interface-name* | *interface-type interface-number* } *destination-vlan* **l3-vpn**

undo traffic-redirect inbound { **link-group** { *acl-number* | *acl-name* } [**rule** *rule*] | **ip-group** { *acl-number* | *acl-name* } [**rule** *rule*] }

View

Ethernet port view

Parameter

link-group { *acl-number* | *acl-name* } [**rule** *rule*]: Specifies a Layer 2 ACL, *acl-number* is in the range of 4000 to 4999. *acl-name* is a string beginning with English letters (a to z and A to Z) with no spaces or quotation marks between. **rule** *rule*: Optional, ACL matching statement, in the range of 0 to 127. All matching statements will be selected if you skip this keyword.

ip-group { *acl-number* | *acl-name* } [**rule** *rule*]: Specifies a basic or advanced ACL. *acl-number* is in the range of 2000 to 3999. *acl-name* is a string beginning with English letters (a to z and A to Z) with no spaces or quotation marks between. **rule** *rule*: Optional, ACL matching statement, in the range of 0 to 127. All matching statements will be selected if you skip this keyword.

interface { *interface-name* | *interface-type interface-number* }: Specifies to redirect a packet to a specified Ethernet port. *interface-type* can be GigabitEthernet and Ethernet. *interface-number* suggests a complete port name with *interface*-type.

system-index *index*: Specifies an intra-system index of the rule, in the range of 0 to 4294967295. The system assigns automatically an index to it when delivering an ACL rule, for later retrieval. You can also assign a system index to it when delivering an ACL rule with this command. However, generally you are not recommended to do so.

Description

Use the **traffic-redirect** command to redirect the data flow at the port of the EX card to the port of the MX card and make the port on the EX card act as an MPLS VPN CE side interface.

Use the **undo traffic-redirect** command to cancel this configuration.

Example

Redirect the data flow at the Ethernet3/1/4 of the EX card to the MX card and set the port belong to VLAN 24.

```
[3Com-Ethernet3/1/4] traffic-redirect inbound ip-group 2000 rule 0
system-index 1 interface Ethernet5/1/4 24 l3-vpn
```

Cancel the redirection configuration.

```
[3Com-Ethernet5/1/4] undo traffic-redirect inbound ip-group 2000 rule 0
```

routing-table limit

Syntax

routing-table limit *integer* { *alarm-integer* | **syslog-alert** }

undo routing-table limit

View

VPN-instance view

Parameter

integer: The Maximum routes allowed for a VPN-instance, ranging from 1 to 65536.

alarm-integer: Route threshold for alarming.

syslog-alert: When the route maximum specified for a VPN-instance exceeds the threshold, routes can be added and only a SYSLOG error message is sent out.

Description

Use the **routing-table limit** command to limit the route maximum in a VPN-instance.

Use the **undo routing-table limit** command to cancel the limitation.

It is necessary to enter a VPN-instance sub-view before using the **routing-table** command. Create a VPN-instance routing table in this view and allocate a route distinguisher (RD) in either of the following formats:

16-bit ASN: A 32-bit user-defined number, for example, 100:1.

32-bit IP address: A 16-bit user-defined number, for example, 172.1.1.1:1.

Create a VPN-target extended community for a VPN-instance and specify ingress or egress interface or both of them for the **vpn-target** command. These parameters can be used to configure ingress/egress routing information of the VPN-target extended community for a router.

Example

Configure the maximum routes in VPN instance vpn1 to 1000.

```
[SW8800] ip vpn-instance vpn1
[3Com-vpn-vpn1] route-distinguisher 100:1
[3Com-vpn-vpn1] vpn-target 100:1 import-extcommunity
[3Com-vpn-vpn1] routing-table limit 1000 syslog-alert
```

sham-link

Syntax

sham-link *source-addr destination-addr* [**cost** *cost-value*] [**dead** *seconds*] [**hello** *seconds*] [**md5** *keyid key seconds*] [**retransimit** *seconds*] [**simple** *passwor*] [**trans-delay** *seconds*]

undo sham-link *source-addr destination-addr*

View

OSPF area view

Parameter

source-addr: Source address of a Sham-link, a Loopback interface address with a 32-bit mask.

destination-addr: Destination address of a Sham-link, a Loopback interface address with a 32-bit mask.

cost-value: Cost at Sham-link, in the range of 1 to 65535. By default, it is 1.

password: Authentication in plain text on the interface, 8 characters at most. It must be consistent with the authentication of a Sham-link peer.

keyid: MD5 authentication identifier on the interface. The *keyed* is in the range of 1 to 255. It must be consistent with the authentication string of Sham-link peer.

key: Authentication on the interface. *keyid* is from 1 to 255 and *key* is a string up to 16 characters. It must be consistent with the authentication of a Sham-link peer. When the **display current-configuration** command is executed, the system displays the 24-character MD5 authentication in cipher text. You can also input a 24-character authentication in cipher text.

dead *seconds*: Specifies the interval, in seconds, for the dead timer. This value ranges from 1 to 8192 and defaults 40. It must be consistent with the value of **dead** *seconds* for a Sham-link peer router.

hello *seconds*: Specifies the interval, in seconds, between Hello message transmission through the interface. This value ranges from 1 to 8192 and defaults to 10. It must be consistent with the value of **hello** *seconds* for a Sham-link peer router.

retransmit *seconds*: Specifies the internal, in seconds, for LSA packet retransmission through the interface. This value ranges from 1 to 8192 and defaults to 5.

trans-delay *seconds*: Specifies the delay period, in seconds, for LSA packet transmission through the interface. This value ranges from 1 to 8192 and defaults to 1.

Description

Use the **sham-link** command to configure a Sham-link.

Use the **undo sham-link** command to delete a Sham-link.

In the OSPF PE-CE connection, suppose that in an OSPF area there are two sites which belong to the same VPN. They are connected to different PE routers and there is an intra-domain OSPF link (Backdoor) between them. Though there may be other routes connecting the two sites via PE routers, these routes are intra-domain routes, and OSPF will first select those routes through the Backdoor link. Sometimes, users desire to first select the routes through VPN Backbone. Hence it is required to establish Sham-links between PE routers. In this case, the routes through VPN Backbone are of the highest priority within the OSPF area.

If a Backdoor link (an OSPF link that does not pass the MPLS backbone) exists between two PE routers and you want the data to be transported over the MPLS backbone, you need to configure a Sham-link between the two PE routers. The sham link between VPN PE routers is taken as a link within the OSPF area. When configuring the Sham-link command, the optional parameters are not mutually exclusive. You can only choose in the undo command those parameters which are selected in the corresponding **sham-link** command.

CAUTION:

- The source and destination addresses of a sham link are both Loopback interface addresses with a 32-bit mask, which must be bound to a VPN instance and imported into BGP through a direct-connect route.
- In an OSPF processes of VPN, the Loopback interface routes used by the Sham-link cannot be imported directly (so the **import direct** command cannot be used in the OSPF processes of VPN). OSPF can only advertise the route by importing a BGP route.

- The source and destination addresses of a sham link cannot be the same.
- The same sham link cannot be configured for different OSPF processes.
- 50 sham links can be configured for an OSPF process at most.

Example

Configure a Sham-link, with its source address 1.1.1.1 and destination address 2.2.2.2.

```
[3Com-ospf-100-area-0.0.0.1] sham-link 1.1.1.1 2.2.2.2 cost 100
```

summary

Syntax

summary

undo summary

View

VPN-instance sub-address family view

Parameter

None

Description

Use the **summary** command to enable BGP to perform auto summary of subnet routes.

Use the **undo summary** command to cancel this summary.

By default, BGP does not perform the auto summary of subnet routes.

After auto summary is enabled, BGP cannot receive the subnet routes imported from IGP. Using this feature reduces the amount of routing information.

Example

Perform auto summary of subnet routes.

```
[3Com-bgp-af-vpn-instance] summary
```

vlan vpn-range

Syntax

vlan vpn-range slot *slot-number* **enable**

undo vlan vpn-range slot *slot-number* **enable**

View

System view

Parameter

slot-number: Slot number of interface card.

Description

Use the **vlan vpn-range** command to set the MPLS label range on the interface on the card.

Use the **undo vlan vpn-range** command to restore the default MPLS label range for the card.

After **vpn-range** is enabled on the card, the range of MPLS/VPN VLAN *vlan-id* that can be configured on the 12 interfaces on the card is 4K, but not the default value of 1K.

Related command: **port trunk mpls vlan**.

- This command is actually effective for only the first 12 ports on the card. When you configure MPLS/VPN VLAN vlan-id on subsequent ports, only the MPLS/VPN VLAN range enabled for one VLAN will take effect. If you remove MPLS/VPN configuration from an active port, no subsequent port will take effect automatically either, and you have to reconfigure the ports to update their states.
- Restart the card after issuing a command or its corresponding undo command to ensure that the configuration takes effect.
- After the configuration on the card is canceled, if the VLAN configured on a port exceeds 1K, which is the default value, the configuration will be deleted automatically.
- In aggregation mode, VPN-range configuration will not be synchronized automatically and you can manually make/remove the configuration on an individual port.

Example

Configure the range of MPLS/VPN VLAN *vlan-id* on slot 5 as 4K.

```
<SW8800> system-view
[SW8800] vlan vpn-range slot 5 enable
```

vpn-instance-capability simple

Syntax

vpn-instance-capability simple

undo vpn-instance-capability

View

OSPF protocol view

Parameter

None

Description

Use the **vpn-instance-capability simple** command to configure a router as Multi-VPN-Instance CE.

Use the **undo vpn-instance-capability** command to cancel the configuration.

OSPF multi-VPN-instance is often run at a PE router. Therefore, a CE router, on which OSPF multi-VPN-instance runs, is called Multi-VPN-Instance CE. Though

they both support multi-VPN-instance, Multi-VPN-Instance CE does not necessarily support BGP/OSPF interoperability.

When an OSPF process is bound to a VPN instance, the default OSPF router is PE router. This command will remove the default setting and change a router into a Multi-VPN-Instance CE. . After the configuration, OSPF processes will reestablish all its neighbors. DN bits and Route-tag will not be checked in routing calculation. To prevent route loss, routing loop test is disabled on PE routes. MGP/OSPF interoperability is also disabled to save system resources.

After the **display ospf brief** command is executed successfully, the system prompts the following information:

```
Multi-VPN-Instance enable on CE router.
```

CAUTION: *OSPF processes will set up all its neighbors again after this command is executed.*

Example

Configure OSPF process 100 as Multi-VPN-Instance CE.

```
[3Com-ospf-100] vpn-instance-capability simple
```

Restore the OSPF process 100 as PE.

```
[3Com-ospf-100] undo vpn-instance-capability
```

vpn-target

Syntax

vpn-target *vpn-target-ext-community* [**import-extcommunity** | **export-extcommunity** | **both**]

undo vpn-target *vpn-target-ext-community* [**import-extcommunity** | **export-extcommunity** | **both**]

View

VPN-instance view

Parameter

import-extcommunity: Specifies ingress route information from the extended community of target VPN.

export-extcommunity: Specifies egress route information to the extended community of target VPN.

both: Imports both ingress and egress route information to the extended community of target VPN.

vpn-target-ext-community: VPN-target extended community attributes to be added to the ingress and egress of VPN-instance or the VPN-target extended community list of ingress and egress.

Description

Use the **vpn-target** command to create a VPN-target extended community for VPN-instance.

Use the **undo vpn-target** command to remove the VPN-target extended community attributes.

By default, the default value is **both**.

Use the **vpn-target** command to create ingress and egress route target extended community lists for a specified VPN-instance. Execute this command once for each target community. Import the received routing information carrying the specific VPN-target extended community to all VPN-instances, for which an extended community is configured as ingress VPN-target. VPN-target specifies a target VPN extended community. The same as RD, an extended community is either composed of an ASN and an arbitrary number, or composed of an IP address and an arbitrary number.

RD is in either of the following formats:

16-bit ASN (can be 0 here): A custom 32-bit number, for example, 101:3.

32-bit IP address (can be 0.0.0.0 here): A custom 16-bit number, for example, 192.168.122.15:1.

Example

Create a VPN-target extended community for the VPN-instance.

```
[SW8800] ip vpn-instance vpn-instance_blue
[3Com-vpn-vpn-instance_blue] vpn-target 1000:1 both
[3Com-vpn-vpn-instance_blue] vpn-target 1000:2 export-extcommunity
[3Com-vpn-vpn-instance_blue] vpn-target 173.27.0.130:2
import-extcommunity
```

41 MPLS VLL CONFIGURATION COMMANDS

L2VPN mentioned below refers to VLL L2VPN.

CCC Configuration Commands

ccc

Syntax

ccc *ccc-connection-name* **interface vlan-interface** *vlan-id* { **transmit-lsp** *transmit-lsp-name* **receive-lsp** *receive-lsp-name* | **out-interface** *outinterface-type outinterface-number* }

undo ccc *ccc-connection-name*

View

System view

Parameter

ccc-connection-name: Name of the CCC (circuit cross connect) connection, which is used to uniquely identify the CCC connection in the PE (provider edge). This argument is 1 to 20 characters in length.

vlan-id: ID of the VLAN whose interface is used to establish the connection. It must be the ID of an existing VLAN.

transmit-lsp-name: Name of transmitting LSP (the ingress LSP).

receive-lsp-name: Name of receiving LSP (the egress LSP).

outinterface-type outinterface-number: Name of the interface connecting to the second CE (custom edge).

Description

Use the **ccc** *ccc-connection-name* **interface vlan-interface** *vlan-id* **transmit-lsp receive-lsp** command to create a remote CCC connection.

Use the **ccc** *ccc-connection-name* **interface vlan-interface** *vlan-id* **out-interface** command to create a local CCC connection.

Use the **undo ccc** command to remove a local/remote CCC connection.

When the interface is a VLAN interface, a CCC connection encapsulates data as Ethernet packets by default.

Example

Create a remote CCC connection, with the name of clink, the transmitting LSP of tlsp, and the receiving LSP of rlsp.

```
[SW8800] ccc clink interface vlan-interface 201 transmit-lsp tlsp
receive-lsp rlsp
```

Create a local CCC connection, with the name of clink, and the interfaces connecting to the two CEs being the interfaces of VLAN 201 and VLAN 301 respectively.

```
[SW8800] ccc clink interface vlan-interface 201 out-interface
interface vlan-interface 301
```

debugging mpls l2vpn

Syntax

debugging mpls l2vpn { **all** | **advertisement** | **error** | **event** | **connections** [**interface vlan-interface** *vlan-id*] }

undo debugging mpls l2vpn { **all** | **advertisement** | **error** | **event** | **connections** [**interface vlan-interface** *vlan-id*] }

View

User view

Parameter

all: Enables/Disables all types of L2VPN Debugging.

advertisement: Enables/Disables Debugging for L2VPN BGP/LDP advertisement messages.

error: Enables/Disables Debugging for L2VPN error messages.

event: Enables/Disables Debugging for L2VPN event messages.

connections: Enables/Disables Debugging for connection messages.

vlan-id: ID of the VLAN whose interface is used to establish the connection.

Description

Use the **debugging mpls l2vpn** command to enable specific type of L2VPN debugging.

Use the **undo debugging mpls l2vpn** command to disable specific type of L2VPN debugging.

Example

Enable all types of L2VPN Debugging.

```
<SW8800> debugging mpls l2vpn all
```

display ccc

Syntax

display ccc [*ccc-name* | **type** [**local** | **remote**]]

View

Any view

Parameter

ccc-name: Name of the CCC connection whose information is to be displayed.

type local: Displays information about the local CCC connections only.

type remote: Displays information about the remote CCC connections only.

Description

Use the **display ccc** command to display the information about specified CCC connections.

Example

Display information about the CCC connection named c-link.

```
<SW8800> display ccc c-link
name: c-link, type: remote, state: down,
intf: Vlan-interface1003 (down), tran-lsp: ccc2 (up), rcv-lsp: ccc1 (up)
```

static-lsp egress l2vpn

Syntax

static-lsp egress *lsp-name* **l2vpn incoming-interface vlan-interface** *vlan-id* **in-label** *in-label*

undo static-lsp egress *lsp-name*

View

MPLS view

Parameter

lsp-name: Name of the label switching path (LSP).

vlan-id: ID of the VLAN whose interface is to be used to create the LSP.

in-label-value: Value of the in-label, ranging from 16 to 1,023.

Description

Use the **static-lsp egress l2vpn** command to create a static L2VPN LSP for the egress label switching router (LSR).

Use the **undo static-lsp egress** command to remove a L2VPN LSP created for the egress LSR.

You need to create two LSPs (for transmitting and receiving) before creating a remote CCC connection.

Related command: **static-lsp ingress l2vpn**, **static-lsp transit l2vpn**, **debugging mpls**.

Example

Create a static LSP named bj-sh on the egress LSR.

```
[3Com-mpls] static-lsp egress bj-sh l2vpn incoming-interface vlan-
interface 201 in-label 233
```

static-lsp ingress

Syntax

static-lsp ingress *lsp-name* **l2vpn nexthop** *next-hop-addr* **out-label** *out-label*

undo static-lsp ingress *lsp-name*

View

MPLS view

Parameter

lsp-name: Name of the LSP.

next-hop-addr: Address of the next hop.

out-label: Value of the out-label, ranging from 16 to 1,023.

Description

Use the **static-lsp ingress l2vpn** command to create a static L2VPN LSP for the ingress LSR.

Use the **undo static-lsp** command to remove a static L2VPN LSP.

You need to create two LSPs (for transmitting and receiving) before creating a remote CCC connection.

Related command: **static-lsp egress l2vpn**, **static-lsp transit**, **debugging mpls**.

Example

Create a static LSP with the destination IP address of 202.25.38.1 for the ingress LSR.

```
[3Com-mpls] static-lsp ingress bj-sh l2vpn nexthop 1.1.1.1 out-label 100
```

static-lsp transit l2vpn

Syntax

static-lsp transit *lsp-name* **l2vpn incoming-interface vlan-interface** *vlan-id* **in-label** *in-label* **nexthop** *next-hop-addr* **out-label** *out-label*

undo static-lsp transit *lsp-name*

View

MPLS view

Parameter

lsp-name: Name of the LSP.

vlan-id: ID of the VLAN whose interface is to be used to create the LSP.

next-hop-addr: Address of the next hop.

in-label: Value of the in-label, ranging from 16 to 1,023.

out-label: Value of the out-label, ranging from 16 to 1,023.

Description

Use the **static-lsp transit** command to create a static L2VPN LSP for the midway transmitting LSR.

Use the **undo static-lsp transit** command to remove the static L2VPN LSP created for the midway transmitting LSR.

You need to create two LSPs (for transmitting and receiving) before creating a remote CCC connection. You also need to enable the two LSPs to traverse through each of the midway LSRs.

Related command: **static-lsp egress l2vpn**, **static-lsp ingress l2vpn**.

Example

Create a static L2VPN LSP for the interface of VLAN 201 on the midway transmitting LSR, with the in-label of 123 and the out-label of 253.

```
[3Com-mpls] static-lsp transit bj-sh l2vpn incoming-interface vlan-
interface 201 in-label 123 nexthop 202.34.114.7 out-label 253
```

Martini MPLS L2VPN Configuration Commands

display mpls l2vc

Syntax

display mpls l2vc [**interface vlan-interface** *vlan-id* | **verbose**]

View

Any view

Parameter

vlan-id: ID of the VLAN whose interface is used to create the virtual circuit.

verbose: Displays the detailed information.

Description

Use the **display mpls l2vc** command to display the VC information of Martini VLL.

Example

Display detailed VC information.

```
<SW8800> display mpls l2vc verbose
Interface: Vlan-interface1000State: down, Encapsulation: ethernet,
Service: VLL

 VC-ID: 4294967295, VC State: down, Destination: 3.3.3.3
  Group ID: Local 0, Remote 0, VC Label: Local 32770, Remote 0,
  Tunnel Type: LSP, Tunnel Index: 25
```

```
Interface: Vlan-interface1001State: down, Encapsulation: ethernet,
Service: VLL

 VC-ID: 10001, VC State: down, Destination: 1.1.1.1
  Group ID: Local 0, Remote 0, VC Label: Local 32771, Remote 0,
  Tunnel Type: LSP, Tunnel Index: 23
```

mpls l2vc

Syntax

mpls l2vc *ip-address vc-id*

undo mpls l2vc

View

VLAN interface view

Parameter

ip-address: IP address of LSR-ID on the peer PE.

vc-id: ID of the VC, ranging from 1 to 4,294,967,295.

Description

Use the **mpls l2vc** command to create a Martini MPLS L2VPN virtual connection.

Use the **undo mpls l2vc** command to remove a Martini MPLS L2VPN virtual connection.

You need to enable MPLS L2VPN before using the command.

Related command: **mpls l2vpn**, **display mpls l2vc**.

Example

Create a virtual connection with the ID of 23.

```
[3Com-Vlan-interface201] mpls l2vc 10.0.0.11 23
```

Kompella MPLS L2VPN Configuration Commands

ce

Syntax

ce *name* [**id** *id* [**range** *range* | **default-offset** *offset*]

undo ce *name*

View

MPLS L2VPN view

Parameter

name: Name of the CE, which must be unique in the current VPN of the PE. This argument is 1 to 20 characters in length.

id: CE ID, which is used to uniquely identify a CE in the VPN. This argument ranges from 0 to 499.

offset: Specifies the default original CE offset.

range: CE Range, the maximum number of CEs that can be connected to the CE. This argument ranges from 1 to 500.

Description

Use the **ce** command to create a CE or modify the CE Range.

Use the **undo ce** command to remove a CE.

The corresponding CE view is created when you create a CE. All the CE connections are configured in CE view.

For VPN capacity expansion, you can set the *range* argument to a value lager than the currently required number of CEs to be connected. However, this may result in the waste of tags as the system allocates tag blocks for CEs according to the value of the *range* argument. You can also change the CE Range to a larger number when expanding the VPN (if the previously set CE range is not large enough). For example, if the desired CE number is 20 after the expansion, but the current CE Range is 10, you can change the CE range to 20.

Related command: **mpls l2vpn encapsulation**, **ccc**.

Example

Create a CE for VPNA named "beijing", with the CE ID of 1. Use the default range (10).

```
[SW8800] mpls l2vpn
[SW8800] mpls l2vpn vpna encapsulation ethernet
[3Com-mpls-l2vpn-vpna] ce beijing id 1
[3Com-mpls-l2vpn-ce-vpna-beijing]
```

connection

Syntax

connection [**ce-offset** *offset*] { **interface vlan-interface** *vlan-id* }

undo connection [**ce-offset** *offset*] { **interface vlan-interface** *vlan-id* }

View

MPLS L2VPN CE view

Parameter

offset: Specifies the ID of the remote CE of the L2VPN connection to create a remote CE connection.

vlan-id: ID of the VLAN whose interface is used to establish the connection.

Description

Use the **connection** command to create a connection for the CE.

Use the **undo connection** command to remove the specified CE connection.

You need to configure the route distinguisher (RD) for the MPLS L2VPN before creating a CE connection.

Related command: **mpls l2vpn encapsulation**.

Example

Create a CE connection.

```
[SW8800] mpls l2vpn vpna
[3Com-l2vpn-vpna] ce ce-a id 1 range 4
[3Com-l2vpn-vpna-ce-ce-a] connection interface vlan-interface 201
```

display bgp l2vpn

Syntax

display bgp l2vpn { **all** | **peer** | **route-distinguisher** *ASN* }

View

Any view

Parameter

all: Displays all the L2VPN information about the address family.

peer: Displays the information about a specified BGP Peer in brief.

route-distinguisher: Displays the information about a specified VPN RD.

ASN: Route identifier.

Description

Use the **display bgp l2vpn** command to display the information about Kompella L2VPN.

Example

Display all the L2VPN information.

```
<SW8800> display bgp l2vpn all
BGP local router ID is 172.16.1.5 ,   Origin codes: i - IGP, e - EGP, ? -
incomplete
bgp.l2vpn: 3 destinations
CE ID   Label Offset        Label Base  nexthop     pref        as-path

Route Distinguisher: 100:1
2           1           800000      1.1.1.1     100     I   200 600
3           1           500000      1.1.1.1         100     I   200 600

Route Distinguisher: 100:2
1           1           700000      1.1.1.1     100     I   200 600
```

display mpls l2vpn

Syntax

display mpls l2vpn [*vsi-name* [**local-ce** | **remote-ce**] | **connection** [*vsi-name* [**down** | **remote-ce** | **up** | **verbose**] | **brief** | **interface Vlan-interface** *vlan-id*] | **forwarding-info** { *vc-label* | **interface** *interface-type* }]

View

Any view

Parameter

vsi-name: Name of the VPN instance.

local-ce: Displays the state and configuration of the local CE of a specified VPN instance.

remote-ce: Displays the state and configuration of the remote CE of a specified VPN instance.

down: Displays the information about L2VPN whose CE interfaces are Down.

remote-ce: Displays the state and configuration of the remote CE.

up: Displays the information L2VPN whose CE interfaces are Up.

verbose: Displays detailed information about the CE interfaces.

brief: Displays the summary information about a specified connection.

Interface: Displays information about a specified CE interface.

vlan-id: ID of the VLAN whose interface is used to create the connection.

vc-label: VC label.

interface-type: Type of the interface, which can be Aux, Ethernet, LoopBack, M-Ethernet, NULL, Vlan-interface, GigabitEthernet, or 10-GigabitEthernet.

Description

Use the **display mpls l2vpn** command to display the MPLS L2VPN information. The command can display the state and configuration of the local/remote CE of a specified VPN instance, and the L2VPN information about a specified CE interface.

Example

Display the L2VPN information about a specified interface.

```
[DEV-UP]dis mpls l2vpn forwarding-info 10241 interface Vlan-interface 300
VCLABEL  TUNNELTYPE   ENTRYTYPE   OUTINTERFACE   OUTSLOT    TOKEN       CTRLWORD
-------------------------------------------------------------------------------
10241       LSP        SEND        Vlan-interface100   0          0           FA
LSE
   1   Record(s) Found.
[DEV-UP]dis mpls l2vpn connection interface Vlan-interface 300
conn-type: remote, local vc state: up, remote vc state: up,
     Local ce-id: 1, local ce name: ce1, remote ce-id: 2,
     intf(state,encap): Vlan-interface300(up,ethernet),
     peer id: 2.2.2.2, route-distinguisher: 100:1,
     local vc label: 10242, remote vc label: 10241,
     tunnel type: LSP, tunnel val: 0
```

l2vpn-family

Syntax

l2vpn-family

undo l2vpn-family

View

BGP view

Parameter

None

Description

Use the **l2vpn-family** command to create L2VPN address family view.

Use the **undo l2vpn-family** command to remove L2VPN address family view.

Example

Create L2VPN address family view.

```
[SW8800] bgp 100
[3Com-bgp] l2vpn-family
[3Com-bgp-af-l2vpn]
```

mpls l2vpn

Syntax

mpls l2vpn

undo mpls l2vpn

View

System view

Parameter

None

Description

Use the **mpls l2vpn** command to enable L2VPN.

Use the **undo mpls l2vpn** command to disable L2VPN.

To execute the command, you need to enable MPLS first.

Related command: **mpls**, **mpls lsr-id**.

Example

Configure LSR ID and enable MPLS.

```
[SW8800] mpls lsr-id 10.0.0.1
[SW8800] mpls
```

Enable L2VPN.

```
[SW8800] mpls l2vpn
```

mpls l2vpn encapsulation

Syntax

mpls l2vpn *vpn-name* [**encapsulation** { **ethernet** | **vlan** }]

undo mpls l2vpn *vpn-name*

View

System view

Parameter

vpn-name: Name of the VPN, which must be unique in the PE. This argument is 1 to 20 characters in length.

encapsulation: User access encapsulation type. Two types are supported currently: Ethernet access and VLAN access.

Description

Use the **mpls l2vpn encapsulation** command to create a Kompella MPLS L2VPN, specify the encapsulation type, and enter MPLS L2VPN view.

Use the **undo mpls l2vpn** command to remove a Kompella MPLS L2VPN.

Related command: **ce**, **mtu**.

You can create a Kompella MPLS L2VPN only after you enable MPLS L2VPN. All L2VPN parameters are configured in L2VPN view.

Example

Create a Kompella MPLS L2VPN, with the name of 3Com, the encapsulation type of Ethernet.

```
[SW8800] mpls l2vpn 3com encapsulation ethernet
[3Com-mpls-l2vpn-3com]
```

mtu

Syntax

mtu *mtu*

View

MPLS L2VPN view

Parameter

mtu: Layer 2 MTU (maximum transmission unit) of the VPN. This argument ranges from 0 to 10,200 and the default value is 1,500.

Description

Use the **mtu** command to set the MTU for the Kompella MPLS L2VPN.

The same MTU value must be configured for all the PE devices of the same VPN to make sure that the configuration is valid.

Related command: **mpls l2vpn encapsulation**.

Example

Set the MTU of the VPN named vpna to 1,000.

```
[SW8800] mpls l2vpn vpna encapsulation vlan
[3Com-mpls-l2vpn-vpna] mtu 1000
```

peer enable

Syntax

peer { *group-name* | *peer-address* } **enable**

undo peer { *group-name* | *peer-address* } **enable**

View

L2VPN address family view

Parameter

group-name: Name of the peer group. This argument specifies the entire peer group.

peer-address: IP address of a peer. This argument specifies a specific peer.

Description

Use the **peer enable** command to activate a specified peer or peer group in L2VPN address family view.

Use the **undo peer enable** command to deactivate a specified peer or peer group in L2VPN address family view.

By default, the unicast peers or peer groups of IPv4 address family are active. Whereas other types of peers or peer groups are inactive.

Example

Activate peer 192 or peer group 192 in L2VPN address family view.

```
[3Com-bgp] group 192 internal
[3Com-bgp] peer 192.1.1.1 group 192
[3Com-bgp] l2vpn-family
[3Com-bgp-af-l2vpn] peer 192
 enable
```

42 VPLS CONFIGURATION COMMANDS

The VPLS commands require the 3C17548 VPLS Application Module.

VPLS Configuration Commands

bandwidth

Syntax

bandwidth *bw-limit*

View

VSI view

Parameter

bw-limit: Limit on Virtual Switching Instance (VSI) rate, which is in kbit/s. The system automatically takes the smallest number that can be exactly divided by 64. By default, VSI rate is limited at 102,400 kbit/s..

Description

Use the **bandwidth** command to configure a limit on VSI bandwidth.

Note that the rate actually supported ranges from 64 kbps to 2,097,152 kbps. If the rate you set is above 2,097,152 kbps, no rate limitation is performed, and the part of traffic that is under the VSI and exceeding this bandwidth restriction is discarded by the system.

Example

Configure the bandwidth of VSI 3Com as 20 Mbps.

```
<SW8800> system-view
[SW8800] vsi 3Com static
[3Com-vsi-3Com] bandwidth 20480
```

broadcast-restrain

Syntax

broadcast-restrain *percent*

View

VSI view

Parameter

percent: Percentage of VSI broadcast suppression. It ranges from 1 to 100 and defaults to 5, which means the percentage is 5%.

Description

Use the **broadcast-restrain** command to configure the percentage of VSI broadcast suppression. In the VSI, the part of broadcast traffic (including broadcast, multicast, unknown unicast) beyond the suppression percentage is discarded.

Example

Set the broadcast suppression percentage of VSI 3Com to 10%.

```
<SW8800> system-view
[SW8800] vsi 3Com static
[3Com-vsi-3Com] broadcast-restrain 10
```

cos

Syntax

cos { *cos-value* | **user-define-table** *p p p p p p p p* }

View

VSI view

Parameter

cos-value: Specifies Class of Service (CoS). CoS ranges from 1 to 8 and defaults to 1.

p p p p p p p p: User-defined CoS mapping table.

Description

Use the **cos** command to map user priority 802.1Q COS to PSN COS (PSN: Public Switching Network; COS: Class Of Service). When you specify a COS mapping relationship, use the mapping table recommended by the protocol. The protocol recommends the following COS mapping table.

Table 97 IEEE 802.1Q COS service mapping table

	Available classes of service							
User Priority	1	2	3	4	5	6	7	8
0 Best Effort (Default)	0	0	0	1	1	1	1	2
1 Background	0	0	0	0	0	0	0	0
2 Spare	0	0	0	0	0	0	0	1
3 Excellent Effort	0	0	0	1	1	2	2	3
4 Controlled Load	0	1	1	2	2	3	3	4
5 Interactive Multimedia	0	1	1	2	3	4	4	5
6 Interactive Voice	0	1	2	3	4	5	5	6
7 Network Control	0	1	2	3	4	5	6	7

With this mapping table, the **cos** command specifies available classes of service from 1 to 8 and the CoS and the user priority specified combine to determine the COS of user data transmitted over PSN.

You can also customize the mapping relationship between user priority and PSN COS and directly specify the COS for user data transmitted over PSN for each of the user priorities 0 to 7 by configuring *p-p-p-p-p-p-p-p*.

Example

Set the COS of VSI 3Com to 8.

```
<SW8800> system-view
[SW8800] vsi 3com static
[3Com-vsi-3com] cos 8
```

description

Syntax

description *text*

undo description

View

VSI view

Parameter

text: Description text for the VSI, an alphanumeric character string of up to 80 characters.

Description

Use the **description** command to set the description of current VSI.

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

Example

Set the description of VSI 3Com to 3Com Corporation Co., Ltd.

```
<SW8800> system-view
[SW8800] vsi 3Com static
[3Com-vsi-3Com] description 3Com Corporation Co., Ltd.
```

debugging mpls l2vpn

Syntax

debugging mpls l2vpn { **advertisement** | **all** | **connections** | **error** | **event** | **loadshare** }

undo debugging mpls l2vpn { **advertisement** | **all** | **connections** | **error** | **event** | **loadshare** }

View

User view

Parameter

advertisement: Enables debugging for L2VPN signaling protocol.

all: Enables all types of debugging concerning L2VPN module.

connections: Enables debugging for MPLS layer 2 VC connections.

error: Enables debugging for L2VPN errors.

event: Enables debugging for event notification among modules.

Loadshare: Enables debugging for load sharing.

Description

Use the **debugging mpls l2vpn** command to enable individual kinds of L2VPN debugging.

Use the **undo debugging mpls l2vpn** command to disable the corresponding debugging.

By default, all L2VPN debugging is disabled.

Example

Enable debugging for L2VPN errors.

```
<SW8800> debugging mpls l2vpn error
```

display mac-address vsi

Syntax

display mac-address vsi [*vsi-name*] [**peer** *peer-address* | **local** | **vlan-interface** *vlan-interface-number*]] [**dynamic** | **static**] [**count**]

View

Any view

Parameter

peer: Specifies the peer IP address.

peer-address: Peer IP address.

local: All local MAC addresses.

vlan-interface: Specifies the VLAN interface whose MAC address corresponds with the locally bound VSI.

vlan-interface-number: VLAN interface number.

vsi: Specifies the VSI to be displayed.

vsi-name: VSI Name.

dynamic: Displays only dynamic VSI MAC forwarding entries.

static: Displays only static VSI MAC forwarding entries.

count: Displays only the number of VSI MAC forwarding entries.

Description

Use the **display mac-address vsi** command to display VSI MAC forwarding information.. You can display the MAC forwarding entries of either all VSIs or a specific VSI.

Related command: **vsi**, **mac-address static**.

Example

Display the MAC forwarding entries of VSI 3Com.

```
<SW8800> display mac-address vsi  3Com
MAC ADDR        STATE          VPN ID    PEER                    AGING TIME
0004-0000-005b  dynamic        150       Vlan-interface10        AGING
 ---  1 mac address(es) found  ---
```

display vpls connection

Syntax

display vpls connection [**vsi** *vsi-name*] [**peer** *peer-ip*] [**up** | **down** | **block**] [**verbose** | **statistics**]

View

Any view

Parameter

vsi: Specifies a VSI.

vsi-name: VSI name.

peer: Specifies a peer PE.

peer-ip: IP address of the peer PE.

up: Displays only the information of the Pseudowires (PWs) in Up state.

down: Displays only the information of the Pseudowires in Down state.

block: Displays only the information of the Pseudowires in Block state.

verbose: Displays the details of Pseudowires.

statistics: Displays the statistics of Pseudowires.

Description

Use the **display vpls connection** command to display the Pseudowire information of the VSI. You can query the information of statistics of Pseudowires by any combination of VSI name, peer IP address, and Pseudowire state.

Example

Display the VC information of VSI 3Com.

```
<SW8800> display vpls connection vsi 3com
VSI name : 3com
MTU      : 2000
Status   : open
VCID EncapType PeerAddr  state     Lcl-Label/Rmt-Label TnlType/TnlID
200  vlan      2.2.2.2   down      131514/0            LSP/1
100  ethernet 3.3.3.3    down      131515/0            LSP/2

2 total connection(s):0 up, 0 block, 2 down
```

Table 98 Brief description on the fields of a VC

Field	Description
VSI name	VSI name

Table 98 Brief description on the fields of a VC

Field	Description
MTU	Specifies the MTU of the VSI
Status	VSI service status: open (enabled) or shutdown (closed)
VCID	Virtual circuit ID
EncapType	Encapsulation type
PeerAddr	IP address of peer PE
Lcl-Label	Local label, namely, label that the local device assigns the peer PE.
Rmt-Label	Remote label, namely, label that the remote PE assigns the local device.
TnlType	Tunnel type, such as LSP
TnlID	Tunnel ID

display vsi

Syntax

display vsi *vsi-name*

View

Any view

Parameter

vsi-name: VSI name.

Description

Use the **display vsi** command to display the information of one specific or all VSIs.

Related command: **vsi**.

Example

Display the configuration of VSI 3Com.

```
<SW8800> display vsi 3Com
VPLS-Instance : 3Com
  VSI service status : Open
  Vsi ID : 1000
  Vpn ID : 54
  MTU : 900
  Description : 3Com Corporation Co., Ltd.
  VPLS Peers : 2
    3.3.3.3          1000        npe
    4.4.4.4          1000        npe
  Interface :
    Vlan-interface1000
  Bandwidth: 20480kbps
  Broadcast-restrain: 10%
  CoS : 8
  CoS-table : [2 0 1 3 4 5 6 7]
  Mac-table limit : 128
```

Table 99 Detailed description on the fields of a VC

Field	Description
npe	The peer PE is an NPE (network side PE).
Interface	Interface bound to the VSI

Table 99 Detailed description on the fields of a VC

Field	Description
Bandwidth	VSI bandwidth limit
Broadcast-restrain	Percentage of VSI broadcast suppression
CoS	Class of Service
CoS-table	Service registration mapping table of user priority on the PSN
Mac-table limit	Limit on the number of MAC forwarding entries of the VSI

encapsulation

Command

encapsulation { **vlan** | **ethernet** }

View

VSI view

Parameter

encapsulation: Specifies the VC encapsulation type of the VSI.

vlan: Sets the encapsulation type of the VC to Ethernet Tagged mode.

ethernet: Sets the encapsulation type of the VC to Ethernet Raw mode. By default, it is in Ethernet mode.

Description

Use the **encapsulation** command to specify the VC encapsulation type of the VSI. By default, the VC encapsulation type in the VSI takes this value.

Example

Specify the encapsulation type of VSI 3Com as VLAN.

```
<SW8800> system-view view
[SW8800] vsi 3Com static
[3Com-vsi-3Com] encapsulation vlan
```

label-range

Syntax

label-range *label-range-id*

View

VSI view

Parameter

label-range-id: Specifies label range ID.

Description

Use the **label-range** command to manually configure the label range ID corresponding to the VSI.

After label range redirection is configured, you can change the direction of VSI flow by changing the label range corresponding to the VSI, namely, redirect the new label range to the VPLS module for VSI flow processing so that the load on the VPLS module is shared.

Example

Configure the label range ID corresponding to the VSI as 2.

```
<SW8800> system-view view
[SW8800] vsi 3Com static
[3Com-vsi-3Com] label-range 2
```

l2 binding vsi

Syntax

l2 binding vsi *vsi-name* [**access-mode** { **vlan** | **ethernet** }]

undo l2 binding vsi *vsi-name* [**encapsulation** { **vlan** | **ethernet** }]

View

VLAN interface view

Parameter

vsi-name: VSI name.

access-mode: Specifies the user access encapsulation type. The default access encapsulation type is Ethernet.

ethernet: Specifies the user access encapsulation mode as Ethernet.

vlan: Specifies the user access encapsulation mode as VLAN.

Description

Use the **l2 binding vsi** command to bind a VSI to a VLAN interface. The services provided by the VLAN will be regarded as the VPN internal services of the specified VSI.

Use the **undo l2 binding vsi** command to remove the binding relation between a VLAN and a VSI.

You can specify the access type of VPLS. The default access type is Ethernet access. The port configuration on a VLAN interface differs depending on user access modes. If user gets access by Ethernet, you must enable VLAN-VPN on the access port of the VLAN. If user makes H-VPLS access by VLAN, or user's convergence multi-tenant unit (MTU) makes H-VPLS access by VLAN-VPN, you need not enable VLAN-VPN on the access port; instead, you must configure the port as Trunk; in this case, the VLAN Tag (VLAN ID currently configured for the user) carried in uplink packets must be consistent with that of the VLAN bound with the Trunk. If convergence UPE makes H-VPLS access by LSP, you can bind a VPLS instance to a VLAN containing no port.

Related command: **vsi**, **peer**.

Example

Bind VSI 3Com to VLAN 100 in VLAN view. Enabled VLAN VPN on the port of the VLAN indicates the VSI can be accessed through Ethernet.

```
<SW8800> system-view view
[SW8800] interface GigabitEthernet3/1/4
[3Com-GigabitEthernet3/1/4] vlan-vpn enable
[3Com-GigabitEthernet3/1/4] port access vlan 100
```

```
[3Com-GigabitEthernet3/1/4] interface vlan-interface 100
[3Com-Vlan-interface100] undo ip address
[3Com-Vlan-interface100] L2 binding vsi 3Com
```

CAUTION:

- If you have enabled GVRP, STP or 802.1x protocol for a port, you are prohibited from enabling VLAN VPN feature for the port.
- If you have enabled IGMP Snooping or IGMP for the VLAN which the port belongs to, you are prohibited to enable VLAN VPN feature for the port. Similarly, if you have enabled VLAN VPN feature for the port, you are prohibited from enabling IGMP Snooping or IGMP for the VLAN which the port belongs to.
- If you want to add the ports with VLAN VPN enabled to a VLAN, you cannot enable IGMP Snooping in the VLAN and enable IGMP for the VLAN interface.
- You cannot configure an IP address for a VLAN interface with a VSI bound to it. Similarly, you cannot bind a VSI to a VLAN interface with an IP address configured.
- You can bind one VSI to up to eight VLANs.
- You cannot bind any VSI to Vlan-interface1.

mac-address

Syntax

mac-address { **static** *H-H-H* } **vsi** *vsi-name* { **peer** *peer-ip* | **vlan-interface** *vlan-interface-number* }

undo mac-address { **static** *H-H-H* } **vsi** *vsi-name*

View

System view

Parameter

static: Specifies a static MAC address. Only static VSI MAC addresses are allowed at present.

H-H-H: Value of the static MAC address.

vsi: Specifies a VSI name.

vsi-name: VSI name.

peer: Specifies the remote peer corresponding to the static MAC address.

peer-ip: Specifies the IP address of the remote peer corresponding to the static MAC address.

vlan-interface: Specifies the VLAN interface of the local peer corresponding to the static MAC address.

vlan-interface-number: Number of the specified VLAN interface

Description

Use the **mac-address** command to configure a static MAC address for a VSI. The address you configured can be either a MAC address on a local VSI or a MAC address on a remote peer.

Use the **undo mac-address** command to disable the configuration.

Note that when you configure a MAC address for a remote peer with the **peer** keyword provided, if you specify the VLAN-interface, the command configures the MAC address for a local peer.

Related command: **vsi**, **display mac-address vsi**.

Example

Configure to bind the static MAC entries of VLAN interface 10 and the remote peer to the local peer of VSI 3Com.

```
<SW8800> system-view view
[SW8800] mac-address static 0000-fc39-a9b5 vsi 3Com vlan-interface 1
0
[SW8800] mac-address static 0000-fc39-a9b4 vsi  3Com peer 2.2.2.2
```

mac-table limit

Syntax

mac-table limit *mac-limit*

View

VSI view

Parameter

mac-limit: Maximum number of the MAC addresses of a specific VSI.

Description

Use the **mac-table limit** command to configure the maximum number of the MAC addresses in the VSI. This number ranges from 0 to 65,535 and defaults to 128. When the total number of the MAC addresses of the VSI exceeds this number, the system no longer learns any new source MAC address; instead, it directly broadcasts the packet in the VSI.

Example

Set the maximum number of MAC addresses of the VSI 3Com to 1,024.

```
<SW8800> system-view view
[SW8800] vsi 3Com static
[3Com-vsi-3Com] mac-table limit 1024
```

mtu

Syntax

mtu *mtu*

undo mtu

View

VSI view

Parameter

mtu: Value of the access maximum transmission unit (MTU) of a VSI, in the range of 128 bytes to 8,192 bytes. By default, MTU is 1,500 bytes.

Description

Use the **mtu** command to specify the MTU value for user access packets of this VSI. This mtu value is also that for PW.

MTU value is an integral characteristic of a VSI, and all MTU values of the peer PEs of the instance must be consistent.

Use the **undo mtu** command to restore the default MTU value.

Example

Set the MTU for VSI 3Com to 1,400 bytes.

```
<SW8800> system-view view
[SW8800] vsi 3Com static
[3Com-vsi-3Com] mtu 1400
```

peer

Syntax

peer *peer-ip* [**vc-id** *vc-id*] [**upe** | **dual-npe**] [**encapsulation** { **ethernet** | **vlan** }]

undo peer *peer-ip* [**vc-id** *vc-id*]

View

VSI-LDP View

Parameter

peer: Specifies the IP address of the peer PE of the VSI.

peer-ip: IP address of a VSI remote peer PE.

vc-id: Specifies the ID of the VC between the VSI and the peer PE. It defaults to VSI-ID.

vc-id: VSI VC ID.

upe: Specifies the peer PE as the user convergence node UPE in the H-VPLS model.

dual-npe: Specifies the peer PE as an NPE in the H-VPLS model. You can specify up to two NPEs.

encapsulation: Specifies the VC encapsulation type.

ethernet: Specifies the VC encapsulation type as Ethernet Raw mode. By default, the Raw mode is used.

vlan: Specifies the VC encapsulation type as Ethernet Tagged mode.

Description

Use the **peer** command to create a VPLS peer PE contained in an instance. When you create a VPLS peer PE, you must specify an IP address and peer type for the peer PE.

Use the **undo peer** command to remove the specified VPLS peer PE. Note that, for the **undo peer** command, if there are multiple peers for the same PE in an instance, you must specify the corresponding VC-ID when you remove a peer; if there is only one peer, you do not need to specify a VC-ID.

By default, the peer type is NPE. When you specify UPE as the peer type, it indicates the peer is a user convergence node UPE in hierarchical VPLS architecture. You can also specify an ID for a VC to the peer, and the ID must be consistent with that of the remote. Multipoint-to-multipoint connections are needed among specified multiple remote peer NPEs, but not needed between UPEs and NPEs.

By default, VC-ID is VSI-ID.

Related command: **vsi**, **vsi-id**.

Example

In VPLS-LDP view, create a user convergence node UPE whose IP address is 4.4.4.4 in hierarchical architecture and set the VC ID for the UPE to 200.

```
<SW8800> system-view view
[SW8800] vsi 3Com static
[3Com-vsi-3Com] pwsignal ldp
[3Com-vsi-3Com-ldp] vsi-id 1000
[3Com-vsi-3Com-ldp] peer 4.4.4.4 vc-id 200 upe
```

For H-VPLS networking, specify two PEs, 4.4.4.4 and 5.5.5.5, as peer PEs (up to two) that serve as primary/backup links so that when the primary link is unavailable, the backup link is switched on.

```
<SW8800> system-view
[SW8800] vsi 3com static
[3Com-vsi-3com] pwsignal ldp
[3Com-vsi-3com-ldp] vsi-id 200
[3Com-vsi-3com-ldp] peer 4.4.4.4 dual-npe
[3Com-vsi-3com-ldp] peer 5.5.5.5 dual-npe
```

rule permit mpls l2label-range

Syntax

rule [*rule-id*] **permit mpls l2label-range** [*range-id*] **ingress any egress any**

View

Link ACL view

Parameter

rule-id: ACL rule ID.

range-id: Label range.

Description

Use the **rule permit mpls l2label-range** command to add a rule for the Link ACL. The MPLS label range ID corresponding to the rule is *range-id*. In this case, the corresponding label range is 128K + *range-id* Đó 16K ~ 128K + (*range-id* + 1) Đó 16K - 1. If no *range-id* is provided, by default, the label range corresponding to the rule is 128K ~ 256K - 1.

Example

Create a rule of the Link ACL. The label range corresponding to the rule is 128K ~ 256K - 1.

```
<SW8800> system-view
[SW8800]acl number 4000
[3Com-acl-link-4000] rule 0 permit mpls l2label-range
```

vpls-load-share

Syntax

vpls-load-share enable

vpls-load-share disable

View

System view

Parameter

None

Description

Use the **vpls-load-share enable** command to enable VPLS load sharing and allow VPLS module switchover upon failure.

Use the **vpls-load-share disable** command to disable VPLS load sharing and prohibit VPLS module switchover upon failure.

By default, VPLS load sharing is enabled; that is, switchover upon failure is allowed. If the service on a VPLS module has been switched over to another module, you cannot prohibit switchover upon failure.

Example

Enables VPLS load sharing.

```
<SW8800> system-view
[SW8800] vpls-load-share enable
```

pwsignal

Syntax

pwsignal [**ldp**]

View

VSI view

Parameter

ldp: Configures the VSI to use LDP as the PW signaling protocol.

Description

Use the **pwsignal** command to specify a PW signaling protocol for a VSI and enter VSI-LDP view.

Specifying LDP as the PW signaling protocol for the VSI takes you to the VSI-LDP view.

By default, the VSI uses LDP as the PW signaling protocol.

Example

Set LDP as the PW signaling protocol for VSI 3Com and enter the VSI-LDP view.

```
<SW8800> system-view
[SW8800] vsi 3com static
[3Com-vsi-3com] pwsignal ldp
```

reset mac-address vsi

Syntax

reset mac-address vsi [*vsi-name* [**peer** *peer-ip* | **vlan-interface** *vlan-num*]] { **static** | **dynamic** | **all** }

View

User view

Parameter

vsi-name: Refer to the configuration of related commands for VSI.

vlan-id: VLAN interface ID.

static: Specifies static MAC addresses.

dynamic: Specifies dynamic MAC addresses.

Description

Use the **reset mac-address vsi** command to batch remove VPLS MAC addresses. The **reset mac-address vsi** command performs the same function as the **undo mac-address vsi** command does.

Related command: **undo mac-address vsi**.

Example

Remove all dynamic VPLS MAC addresses on Vlan-interface10 in VSI VPN1.

```
<SW8800> reset mac-address vsi vpn1 vlan-interface 10 dynamic
```

shutdown

Syntax

shutdown

undo shutdown

View

VSI view

Parameter

None

Description

Use the **shutdown** command to shut down the service of the VSI. When the service of the VSI is shut down, the system does not process any traffic for this VSI.

Use the **undo shutdown** command to restore the service for the VSI.

Example

Shut down the service of VSI 3Com.

```
<SW8800> system-view
[SW8800] vsi 3com static
[3Com-vsi-3Com] shutdown
```

Restore the service of VSI 3Com.

```
<SW8800> system-view
[SW8800] vsi 3com static
3Com-vsi-3Com] undo shutdown
```

undo mac-address vsi

Syntax

undo mac-address vsi [*vsi-name* [**peer** *peer-ip* | **vlan-interface** *vlan-id*]] [**static** | **dynamic**]

View

System view

Parameter

vsi-name: VSI name.

vlan-id: VLAN interface ID.

static: Specifies static MAC addresses.

dynamic: Specifies dynamic MAC addresses.

Description

Use the **undo mac-address vsi** command to batch remove VPLS MAC addresses.

Related command: **display mac-address vsi** and **reset mac-address vsi**.

Example

Remove all dynamic VPLS MAC addresses on Vlan-interface10 in VSI VPN1.

```
<SW8800> system-view
[SW8800] undo mac-address vsi vpn1 vlan-interface 10 dynamic
```

vsi

Syntax

vsi *vsi-name* [**static**]

undo vsi *vsi-name*

View

System view

Parameter

vsi: Creates a VSI or enter the VSI view.

vsi-name: VSI name, a locally unique string of 1 to 20 alphanumeric characters.

static: Indicates that the peer discovery mechanism is static manual configuration. When you create a VSI, you must specify to manually configure the mechanism, but you do not need to specify the configuration mode after the VSI is created and you are in the VSI view.

Description

Use the **vsi** command to create a VSI or enter the VSI view. When you create an instance, you must specify the mechanism for discovering VSIs and the peers. At present, you can only configure the mechanism statically and manually and must specify the configuration mode explicitly.

Use the **undo vsi** command to delete a VSI.

Related command: **display vsi**.

Example

Create a VSI named 3Com and specify to manually configure the mechanism for discovering the peers of the VSI.

```
<SW8800> system-view
[SW8800] vsi 3com static
```

vsi-id

Syntax

vsi-id *vsi-id*

View

VSI-LDP view

Parameter

vsi-id: VSI ID. The value of *vsi-id* is locally unique and ranges from 1 to 4294967295. For a VC in the current VSI, by default, VC ID defaults to *vsi-id*.

Description

Use the **vsi-id** command to configure the ID of the current VSI. If you do not specify a VC-ID when configuring Peer, VC-ID takes the value of VSI-ID.

Example

Configure the VSI-ID of VSI "3Com" as 100.

```
<SW8800> system-view
[SW8800] vsi 3com static
[3Com-vsi-3com] pwsignal ldp
[3Com-vsi-3com-ldp] vsi-id 100
```

43 VRRP CONFIGURATION COMMANDS

VRRP Configuration Commands

debugging vrrp

Syntax

debugging vrrp { **state** | **packet** | **error** }

undo debugging vrrp { **state** | **packet** | **error** }

View

User view

Parameter

state: Debugs VRRP state.

packet: Debugs VRRP packets.

error: Debugs VRRP errors.

Description

Use the **debugging vrrp** command to enable the VRRP debugging.

Use the **undo debugging vrrp** command to disable the VRRP debugging.

By default, the VRRP debugging is disabled.

Example

Enable VRRP state debugging.

```
<SW8800> debugging vrrp state
```

display vrrp

Syntax

display vrrp [**interface vlan-interface** *interface-number* [*virtual-router-ID*]]

View

Any view

Parameter

interface: Displays the VRRP state of a specified VLAN interface.

vlan-interface *interface-number*: VLAN interface name.

virtual-router-ID: VRRP virtual router ID, ranging from 1 to 255.

Description

Use the **display vrrp** command to view the information about the VRRP state.

If the interface name and virtual router ID are not specified, the state information about all the virtual routers on the switch will be displayed. If only the interface name is specified, the state information about all the virtual routers on the interface will be displayed. If the interface name and virtual router ID are specified, the state information about the specified virtual router on the interface will be displayed.

Example

Display the VRRP state information on VLAN-interface 1.

```
[3Com-Vlan-interface1] display vrrp interface vlan-interface 1
Run Method : VIRTUAL-MAC
 Virtual Ip Ping : Disable
 Interface       : Vlan-interface1
 VRID            : 1                    Adver. Timer    : 1
 Admin Status    : UP                   State           : Initialize
 Config Pri      : 100                  Run Pri         : 90
 Preempt Mode    : YES                  Delay Time      : 0
 Auth Type       : NONE
 Track IF        : Vlan-interface2      Pri Reduced     : 10
 Virtual IP      : 1.1.1.1
 Master IP       : 0.0.0.0
```

Table 100 Description on the fields of the display vrrp command

Field	Description
Run Method	Run method: real or virtual MAC method
Virtual IP ping	Whether to enable to ping through virtual IP
Interface	Interface in which virtual router resides
VRID	ID of virtual router
Adver.Timer	Interval for sending vrrp packets
Admin Status	Control status of virtual router
State	Running state of virtual router
Config Pri	Configured priority
Run Pri	Run priority
Preempt Mode	Preempt mode
Delay Time	Delay time
Auth Type	Authentication type
Virtual IP	Virtual IP address list of virtual router
Master IP	IP address of the master device in virtual router

display vrrp ifm

Syntax

display vrrp ifm

View

Any view

Parameter

None

Description

Use the **display vrrp ifm** command to display the configuration information of the VRRP-enabled IFM device.

Example

Display the configuration information of the VRRP-enabled IFM device.

```
<SW8800> display vrrp ifm
 Interface                     : Vlan-interface1000
 VRID                          : 1
 Track IFM increased value     : 20
 IFM Connecting Status         :

 CPU ID          State
 ==========      ================
 1               Master
 2               Backup
```

display vrrp statistics

Syntax

display vrrp statistics [**vlan-interface** *interface-number* [*virtual-router-ID*]]

View

Any view

Parameter

vlan-interface *interface-number*: Specifies the name of the VLAN interface to which the virtual router belongs.

virtual-router-ID: VRRP virtual router ID, ranging from 1 to 255.

Description

Use the **display vrrp statistics** command to view the information about the VRRP statistics.

If the interface name and virtual router ID are not specified, the statistics information about all the virtual routers on the switch will be displayed. If only the interface name is specified, the statistics information about all the virtual routers on the interface will be displayed. If the interface name and virtual router ID are specified, the statistics information about the specified virtual router on the interface will be displayed.

Example

Display the VRRP statistics information on VLAN-interface 2.

```
<SW8800> display vrrp statistics vlan-interface 2
Interface              : Vlan-interface2
 VRID                  : 1
 CheckSum Errors       : 0          Version Errors                : 0
 VRID Errors           : 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         : 0          Invalid Type Pkts Rcvd         : 0
```

display vrrp summary

Syntax

display vrrp summary

View

Any view

Parameter

None

Description

Use the **display vrrp summary** command to view the VRRP summary information on the switch.

Example

Display the VRRP summary information on the switch.

```
<SW8800> display vrrp summary
 Run Method      : VIRTUAL-MAC
 Virtual Ip Ping : Disable
 The total number of the vitual routers:  64
  VLANID  VRID  State          Run       Adver.  Auth     Virtual
                               Pri       Time    Type     IP
------------------------------------------------------------------------------
  2       2     Initialize     100       1       NONE     2.2.2.192
  3       3     Initialize     100       1       NONE     3.3.3.192
  4       4     Initialize     100       1       NONE     4.4.4.192
  5       5     Initialize     100       1       NONE     5.5.5.192
  6       6     Initialize     100       1       NONE     6.6.6.192
  7       7     Initialize     100       1       NONE     7.7.7.192
  8       8     Initialize     100       1       NONE     8.8.8.192
  9       9     Initialize     100       1       NONE     9.9.9.192
  10      10    Initialize     100       1       NONE     10.10.10.192
  11      11    Initialize     100       1       NONE     11.11.11.192
  12      12    Initialize     100       1       NONE     12.12.12.192
  13      13    Initialize     100       1       NONE     13.13.13.192
  14      14    Initialize     100       1       NONE     14.14.14.192
  15      15    Initialize     100       1       NONE     15.15.15.192
  16      16    Initialize     100       1       NONE     16.16.16.192
  17      17    Initialize     100       1       NONE     17.17.17.192
```

Table 101 Description on the fields of the display vrrp summary command

Field	Description
Run Method	Run method: real or virtual MAC method
Virtual IP ping	Whether to enable to ping through virtual IP address
VRID	ID of virtual router
Adver.Timer	Interval for sending vrrp packets
State	Running state of virtual router
Run Pri	Run priority
Adver.Timer	Interval of sending VRRP packets
Auth Type	Authentication type
Virtual IP	Virtual IP address list of virtual router

reset vrrp statistics

Syntax

reset vrrp statistics [**vlan-interface** *interface-number* [*virtual-router-ID*]]

View

User view

Parameter

statistics: VRRP statistics.

vlan-interface *interface-number*: Interface name.

virtual-router-ID: VRRP virtual router ID, ranging from 1 to 255.

Description

Use the **reset vrrp statistics** command to clear the statistics information about VRRP.

If the interface name and virtual router ID are not specified, the statistics information about all the virtual routers on the switch will be cleared. If only the interface name is specified, the statistics information about all the virtual routers on the interface will be cleared. If the interface name and virtual router ID are specified, the statistics information about the specified virtual router on the interface will be cleared.

Example

Clear the VRRP statistics on the switch.

```
<SW8800> reset vrrp statistics
```

vrrp authentication-mode

Syntax

vrrp authentication-mode *authentication-type authentication-key*

undo vrrp authentication-mode

View

VLAN interface view

Parameter

authentication-type: Authentication type. There are following types:

- **simple**: Indicates to perform simple character authentication.
- **md5**: Indicates to perform the AH authentication with MD5 algorithm.

authentication-key: The key cannot exceed 8 characters.

Description

Use the **vrrp authentication-mode** command to configure the authentication type and key of a specified VRRP virtual router.

Use the **undo vrrp authentication-mode** command to reset the authentication type and key of a specified VRRP virtual router.

If the **simple** or **md5** authentication is configured, it is required to set the authentication key.

This command is used to configure the authentication type and key for all the VRRP virtual routers on an interface. As defined in the protocol, all the virtual routers on an interface shall use the same authentication type and key. And all the members joining the same virtual router shall also use the same authentication type and key.

Note that the authentication key is case sensitive.

Example

Specify the authentication type and key for a VRRP virtual router.

```
[3Com-vlan-interface2] vrrp authentication-mode simple 3com
```

vrrp log-state

Syntax

vrrp log-state

undo vrrp log-state

View

System view

Parameter

None

Description

Use the **vrrp log-state** command to enable debugging of state transition logs of the VRRP virtual router.

Use the **undo vrrp log-state** command to disable debugging of state transition logs of the VRRP virtual router.

Note that if you enable VRRP debugging after executing the **vrrp log-state** command, the system does not output the state transition log of the VRRP virtual router because the information is the same as the debugging information.

By default, debugging of state transition logs of the VRRP virtual router is disabled.

Example

Enable debugging of VRRP state transition logs.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] vrrp log-state
```

vrrp method“vrrp log-state”

Syntax

vrrp method { **real-mac** | **virtual-mac** }

undo vrrp method

View

System view

Parameter

real-mac: Uses the real MAC address of the interface to match the virtual IP address of the virtual router in VRRP backup.

virtual-mac: Uses the virtual MAC address of the interface to match the virtual IP address of the virtual router in VRRP backup.

Description

Use **vrrp method** command to set correspondence between the MAC address and the virtual IP address of the virtual router: matching the real MAC address or the virtual address with the virtual IP address.

Use the **undo vrrp method** command to reset the correspondence to the default value.

By default, the switch matches the virtual MAC address with the IP address of the virtual router.

Due to the chips installed, some switches support matching one IP address to multiple MAC addresses. Then you may configure correspondence between the virtual IP address of the virtual router and the real/virtual MAC address.

You should set correspondence between the IP address of the virtual router and the MAC address before configuring the virtual router. Otherwise, you cannot configure the correspondence.

If you set correspondence between the IP address of the virtual router and the real MAC address, then you can configure only one virtual router on VLAN interface.

Example

Set the real MAC address of the interface match the virtual IP address of the virtual router.

```
[SW8800] vrrp method real-mac
```

vrrp ping-enable

Syntax

vrrp ping-enable

undo vrrp ping-enable

View

System view

Parameter

None

Description

Use **vrrp ping-enable** command to enable the function to ping the virtual IP address of the virtual router.

Use the **undo vrrp ping-enable** command to disable the function.

By default, the ping function is enabled.

You can only use the commands before configuring any virtual router. If a virtual router is already established on the switch, it is not allowed to use the **vrrp ping-enable** command the **undo vrrp ping-enable** command to modify the configuration any more.

Example

Enable to ping the virtual IP address of the virtual router.

```
[SW8800] vrrp ping-enable
```

vrrp un-check ttl

Syntax

vrrp un-check ttl

undo vrrp un-check ttl

View

VLAN interface view

Parameter

None

Description

Use the **vrrp un-check ttl** command to disable the check of TTL value of VRRP packet. Use the **undo vrrp un-check ttl** command to enable the check of TTL value of VRRP packet.

The TTL value must be 225. If the Backup switch finds TTL is not 225 when receiving VRRP packet, the packet will be discarded.

By default, the switch checks TTL value of VRRP packets.

Example

Disable to check TTL value of VRRP packet.

```
[3Com-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**

View

VLAN interface view

Parameter

virtual-router-ID: VRRP virtual router ID, ranging from 1 to 255.

delay-value: Delay in seconds, ranging from 0 to 255.

Description

Use the **vrrp vrid preempt-mode** command to configure the preemption and delay of the virtual router.

Use the **undo vrrp vrid preempt-mode** command to cancel the preemption.

By default, virtual router is in preempt mode and *delay-value* is 0 second.

If a higher-priority switch is required to preempt the Master, you need to configure it as preemption. You can also set a delay for the preemption. If you configure it not to preempt, the delay will be set to 0 automatically.

Example

Configure the switch to preempt.

```
[3Com-vlan-interface2] vrrp vrid 1 preempt-mode
```

Set a delay.

```
[3Com-vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5
```

Configure the switch not to preempt.

```
[3Com-vlan-interface2] undo vrrp vrid 1 preempt-mode
```

vrrp vrid priority

Syntax

vrrp vrid *virtual-router-ID* **priority** *priority*

undo vrrp vrid *virtual-router-ID* **priority**

View

VLAN interface view

Parameter

virtual-router-ID: VRRP virtual router ID, ranging from 1 to 255.

priority: Priority value, ranging from 1 to 254; By default, the priority value is 100.

Description

Use the **vrrp vrid priority** command to configure the virtual router priority.

Use the **undo vrrp vrid priority** command to remove the virtual router priority.

The priority decides the status of a switch in the virtual router. A higher-priority switch is more likely to be a Master. Priority 0 is reserved for some special purpose. 255 is reserved for the IP address owner. The priority of the IP address owner is always 255 and cannot be modified.

Example

Set the virtual router priority on VLAN-interface2.

```
[3Com-vlan-interface2] vrrp vrid 1 priority 120
```

vrrp vrid timer

Syntax

vrrp vrid *virtual-router-ID* **timer advertise** *adver-interval*

undo vrrp vrid *virtual-router-ID* **timer advertise**

View

VLAN interface view

Parameter

virtual-router-ID: VRRP virtual router ID, ranging from 1 to 255.

adver-interval: VRRP packet interval of the Master in the virtual router in seconds, ranging from 1 to 255; By default, the value is 1s.

Description

Use the **vrrp vrid timer** command to set the time interval for the Master in the virtual router to send VRRP packets.

Use the **undo vrrp vrid timer advertise** command to restore the default value.

You are supposed to set the identical timer value for the switches in the same virtual router to avoid wrong configuration.

Example

Configure the Master to transmit VRRP packets every 15 seconds.

```
[3Com-vlan-interface2] vrrp vrid 1 timer advertise 15
```

vrrp vrid track

Syntax

vrrp vrid *virtual-router-ID* **track** { **ifm** [**increased** *value-increased*] | **vlan-interface** *interface-number* [**reduced** *value-reduced*] }

undo vrrp vrid *virtual-router-ID* **track** [**ifm | vlan-interface** *interface-number*]

View

VLAN interface view

Parameter

virtual-router-ID: VRRP virtual router ID, ranging from 1 to 255.

ifm: Tracks the IFM device.

increased: Increases the priority of the virtual router.

value-increased: Value of the increased priority, ranging from 1 to 254. The default value is 2.

vlan-interface *interface-number*: Interface which is to be tracked.

Reduced: Reduces the priority of the virtual router.

value-reduced: Reduced value of priority, ranging from 1 to 255; By default, the reduced value of priority is 10.

Description

Use the **vrrp vrid track** command to configure the switch to track the interface.

Use the **undo vrrp vrid track** command to stop tracking the interface.

VRRP interface track expends the backup function, which thereby can be implemented not only when the switch fails, but also when the state of a network interface is Down. The user can use this command to track or stop tracking an interface or all the interfaces. After the command is configured, the priority of the switch will be reduced, if the state of the tracked interface goes Down. Accordingly, some other switch in the virtual router will have the comparatively highest priority and become the new Master, thereby implementing the backup function. The IP address owner does not allow the configuration of interface tracking.

Each virtual router can track up to 8 interfaces.

Example

Set to track vlan-interface1 on vlan-interface2, and lower the priority of virtual router 1 on vlan-interface2 by 50 when the state of vlan-interface1 goes Down.

```
[3Com-vlan-interface2] vrrp vrid 1 track vlan-interface 1 reduced 50
```

vrrp vrid virtual-ip

Syntax

vrrp vrid *virtual-router-ID* **virtual-ip** *ip-address*

undo vrrp vrid *virtual-router-ID* [**virtual-ip** *virtual-address*]

View

VLAN interface view

Parameter

virtual-router-ID: VRRP virtual router ID, ranging from 1 to 255.

ip-address: Virtual IP address.

Description

Use the **vrrp vrid virtual-ip** command to create a virtual router or add a virtual IP address to an existing virtual router.

Use the **undo vrrp vrid virtual-ip** command to cancel an existing virtual router or an address from the virtual router.

You can add up to 16 virtual IP addresses to one virtual router.

If all of the addresses in a virtual router are deleted, the system will delete the virtual router automatically.

Example

Create a virtual router.

```
[3Com-vlan-interface2] vrrp vrid 1 virtual-ip 10.10.10.10
```

Add a virtual IP address to an existing virtual router.

```
[3Com-vlan-interface2] vrrp vrid 1 virtual-ip 10.10.10.11
```

Delete a virtual IP address.

```
[3Com-vlan-interface2] undo vrrp vrid 1 virtual-ip 10.10.10.10
```

Delete a virtual router.

```
[3Com-vlan-interface2] undo vrrp vrid 1
```

44 HA CONFIGURATION COMMANDS_HA_CONFIGURATION

HA Configuration Commands

debugging ha

Syntax

debugging ha { **all** | **event** | **message | state** }

undo debugging ha { **all** | **event** | **message | state** }

View

User view

Parameter

all: All HA debugging switches.

event: HA batch backup or tamed event debugging switch.

message: Debugging switch for messages received or sent by HA.

state: HA state machine state information debugging switch.

Description

Use the **debugging ha** command to enable HA debugging.

Use the **undo debugging ha** command to disable HA debugging.

By default, HA debugging is disabled.

Example

Enable all the HA debugging.

```
<SW8800> debugging ha all
```

display switchover state

Syntax

display switchover state [*slot-id*]

View

Any view

Parameter

slot-id: Slot number of master or slave fabric.

Description

Use the **display switchover state** command to view the switchover state of master or slave fabric.

This command is used to display the switchover state of the master or slave fabric according to the specified slot number. If *slot-id* is not specified, the status of the fabric will be displayed.

Example

Display the switchover state of master fabric.

```
<SW8800> display switchover state
HA FSM State(master): Slave is absent.
```

display xbar

Syntax

display xbar

View

System view

Parameter

None

Description

Use the **display xbar** command to view the load mode of master and slave fabrics, which includes the configured system Xbar load mode and the active system Xbar load mode.

Note that the configured system Xbar load mode is not always the same as the active system Xbar load mode. Only when the slave fabric is in position or is started, can the system operate in the configured load mode.

Example

Display the load mode of the master/slave fabric.

```
<SW8800> display xbar
The configured system HA Xbar Load Mode is BALANCE
The active system HA Xbar Load Mode is SINGLE
```

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 automatic synchronization between the master and slave systems.

Use the **undo slave auto-update config** command to disable automatic synchronization between the master and slave systems.

By default, automatic synchronization is enabled.

Related command: **slave update config**.

Example

Enable automatic synchronous switch between master/slave systems.

```
[SW8800] slave auto-update config
```

slave restart

Syntax

slave restart

View

User view

Parameter

None

Description

Use the **slave restart** command to restart slave fabric.

When the slave system works abnormally, and needs to be reloaded, you can use this command to restart the slave fabric.

Example

Implement the restart of the slave system.

```
<SW8800> slave restart
The slave will reset! Continue?[Y/N]:y
```

slave switchover

Syntax

slave switchover

View

User view

Parameter

None

Description

Use the **slave switchover** command to start the master-slave switchover manually.

In the environment in which the slave fabric is available and master in real-time backup state, the user can inform the slave fabric of a master-slave switchover by

using a command if he expects the slave fabric to operate in place of the master fabric. After the switchover, the slave fabric will control the system and the original master fabric will be forced to reset.

Example

Enable master-slave switchover manually.

```
<SW8800> slave switchover
Caution!!! Confirm switch slave to master[Y/N]?y
Starting.....
RAM Line....OK
```

slave update configuration

Syntax

slave update configuration

View

User view

Parameter

None

Description

Use the **slave update configuration** command to manually synchronize the configuration file between the master and slave fabrics.

Related command: **slave auto-update config**.

Example

Synchronize the configuration file between the master and slave fabrics.

```
<SW8800> slave update configuration
```

xbar

Syntax

xbar [**load-balance** | **load-single**]

View

System view

Parameter

load-balance: Sets Xbar load balance mode.

load-single: Sets Xbar load single mode.

Description

Use the **xbar** command to configure the load mode of the master/slave fabric.

By default, the master and slave fabrics are both in load single mode.

CAUTION: *When a single fabric is in position, the load-balance mode is not effective and the fabric changes to the load-single mode automatically.*

Example

Configure the system Xbar load mode.

```
[SW8800] xbar load-balance
```

45 ARP CONFIGURATION COMMANDS

ARP Configuration Commands

arp non-flooding

Syntax

arp non-flooding enable

undo arp non-flooding enable

View

Ethernet port view

Parameter

None

Description

Use the **arp non-flooding enable** command to enable the feature that the ARP packets of a port are not broadcast in the VLAN where this port lies.

Use the **undo arp non-flooding** command to disable this feature.

By default, ARP request packets are broadcast in the VLAN where the port lies.

Example

Enable the feature that ARP request packets of Ethernet 2/1/1 are not broadcast in the VLAN where Ethernet 2/1/1 lies.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface ethernet2/1/1
[3Com-Ethernet2/1/1] arp non-flooding enable
```

Disable the feature above, namely, ARP request packets of Ethernet 2/1/1 are broadcast in the VLAN where Ethernet 2/1/1 lies.

```
[3Com-Ethernet2/1/1] undo arp non-flooding
```

arp proxy enable

Syntax

arp proxy enable

undo arp proxy enable

View

VLAN view

Parameter

None

Description

Use the **arp proxy enable** command to enable ARP proxy function.

Use the **undo arp proxy enable** command to disable ARP proxy function.

By default, ARP proxy function is disabled.

You can configure these commands for a VLAN and sub-VLAN. If you enable ARP proxy for a VLAN, the device with ARP proxy function directly forwards received ARP requests in the VLAN. If you enable ARP proxy for a sub-VLAN, the device with ARP proxy function directly forwards received ARP requests in other sub-VLANs which belong to the same super-VLAN and also have the ARP proxy function enabled.

Related command: **display arp proxy**.

Example

Enable ARP proxy function for VLAN 2.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] vlan 2
[3Com-vlan2] arp proxy enable
```

arp static

Syntax

arp static *ip-address* [*mac-address* [*vlan-id* { *interface-type interface-number* }] [vpn-instance *vpn-instance-name*]

undo arp *ip-address*

View

System view

Parameter

ip-address: IP address of the ARP mapping entry.

mac-address: MAC address of the ARP mapping entry, whose format is H-H-H (H indicates a hexadecimal number).

vlan-id: VLAN to which the static ARP entry belongs, in the range of 1 to 4094.

interface-type interface-number: The type and number of the port to which the static ARP entry belongs. For the specific parameter values, refer to the description on the **interface** command in *Ethernet Port Command Manual*.

vpn-instance *vpn-instance-name*: VPN instance name in MPLS VPN.

Description

Use the **arp static** command to configure the static ARP mapping entries in an ARP mapping table.

Use the **undo arp static** command to delete a static ARP mapping entry from the ARP table.

By default, the mapping table of the system ARP is empty and the switch can obtain its address mapping by means of dynamic ARP.

The **arp static** command can be used to configure auto filling of ARP entries. When configuring an ARP entry, if you input on the IP address, the switch will automatically set the MAC address to 0. Such a mapping entry is auto-fill ARP mapping entry. When an auto-fill ARP entry is resolved, the switch can automatically fill it with the learned MAC address as the MAC address corresponding to the IP address in this mapping entry.

Note that:

- When the switch works normally, its static ARP mapping entries remain valid and work unless you perform operations that invalidate ARP entries, such as changing or removing VLAN interfaces, removing a VLAN, or removing an port from a VLAN. These operations will cause the corresponding ARP mapping entries to be automatically removed.
- The argument *vlan-id* must be the ID of an existing VLAN, and the Ethernet port specified behind this parameter must belong to the VLAN.
- The argument *vpn-instance-name* must be the VPN-instance name of an existing MPLS VPN.
- ARP mapping entries with port parameters can be configured on manually aggregated ports or static aggregated ports, but cannot be configured on LACP-enabled dynamic aggregated ports.
- If the *mac-address* of an ARP entry is a multicast MAC address, the system will assume this ARP entry to be multicast ARP entry.
- The MAC address auto filling function is enabled only when the IP address protection function is enabled on the interface.
- Once after the initial auto filling, the auto-fill ARP entry becomes a normal static ARP entry and cannot be filled again.
- Long static ARP can be configured only on manually aggregated ports, but not on static aggregated ported or dynamic aggregated ports.

Related command: **reset arp**, **display arp**, and **debugging arp**.

Example

Configure the MAC address corresponding to the IP address 202.38.10.2 to 00e0-fc01-0000. This static ARP mapping entry is on Ethernet port Ethernet 2/1/1, which belongs to VLAN1.

```
[SW8800] arp static 202.38.0.10 00e0-fc01-0000 1 ethernet2/1/1
```

arp static multi-port

Syntax

arp static *ip-address mac-address vlan-id* **multi-port** *interface-type interface-number* [**vpn-instance** *vpn-instance-name*]]

undo arp *ip-address* **multi-port** *interface-type interface-number* [**vpn-instance** *vpn-instance-name*]

View

System view

Parameter

ip-address: IP address of the ARP mapping entry.

mac-address: MAC address of the ARP mapping entry, in the format of H-H-H. For a multiple-outgoing-port ARP entry, this is a multicast MAC address.

vlan-id: ID of the VLAN of the static ARP entry, in the range of 1 to 4094.

interface-type: Port type.

interface-number: Port number.

For details about the above two parameters, refer to the **interface** command in *port command* manual.

vpn-instance-name: The VPN instance name of the VPN which the IP address belongs to.

Description

Use the **arp static multi-port** command to add a multicast ARP port. When you add the first port, the system generates a multicast ARP entry.

Use the **undo arp multi-port** command to remove a multicast ARP port. When you remove the last port, the system removes the multicast ARP entry.

The multicast ARP feature allows you to associate a common unicast route to a Layer 2 multicast group, that is, add multiple outgoing ports for an outgoing ARP packet so that the packet can be sent to multiple ports. As a result, a static multicast ARP entry is generated. In brief, a multicast ARP entry is a static ARP entry with a multicast MAC address, which may correspond to multiple ports.

According to the **multi-port** keyword in this command, the switch decides that the port to be added is for a multicast ARP entry. Only one port can be added every time the command is executed. If the multicast ARP entry does not exist, a new multicast ARP entry is generated. If the multicast ARP entries exist with the same egress, the switch will not add a multicast ARP port.

Note that:

- You cannot configure multicast ARP for aggregation ports. Otherwise, the system will prompt error message.
- At present, the outgoing ports in the same multicast ARP entry cannot be in different modules.

You can add multiple ports one by one by setting the multicast static ARP entry. To view the configuration, use the **display arp multi-port** command.

Related commands: **reset arp**, **display arp**, **debugging arp**, **arp static**.

Example

In an ARP entry, the IP address is 10.10.10.98, and the MAC address is 0150-0098-0098. Add the outgoing ports Ethernet 6/1/1, Ethernet 6/1/2 and Ethernet 6/1/3 to the ARP entry.

```
[SW8800] arp static 10.10.10.98 0150-0098-0098 20 multi-port Ethernet 6/1/1
[SW8800] arp static 10.10.10.98 0150-0098-0098 20 multi-port Ethernet 6/1/2
[SW8800] arp static 10.10.10.98 0150-0098-0098 20 multi-port Ethernet 6/1/3
```

arp timer aging

Syntax

arp timer aging *aging-time*

undo arp timer aging

View

System view

Parameter

aging-time: Aging time of dynamic ARP aging timer, which is in the range of 1 to 1440 minutes. By default, the aging time is 20 minutes.

Description

Use the **arp timer aging** command to configure the dynamic ARP aging timer.

Use the **undo arp timer aging** command to restore the default dynamic ARP aging timer.

Related command: **display arp timer aging**.

Example

Configure the dynamic ARP aging timer to 10 minutes.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] arp timer aging 10
```

debugging arp

Syntax

debugging arp { **error** | **info** | **packet** }

undo debugging arp { **error** | **info** | **packet** }

View

User view

Parameter

error: ARP error debugging.

info: ARP mapping table and information management debugging.

packet: ARP packet debugging.

Description

Use the **debugging arp** command to enable ARP debugging.

Use the **undo debugging arp** command to disable the corresponding ARP debugging.

By default, no ARP debugging is enabled.

Related command: **arp static**, **display arp**.

Example

Enable ARP packet debugging.

```
<SW8800> debugging arp packet
*0.771346-ARP-8-S1-arp_send:Send an ARP Packet, operation : 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
*0.771584-ARP-8-S1-arp_rcv:Receive an ARP Packet, operation : 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 102 Description on the fields of the debugging arp command

Field	Description
operation	Kind of ARP packets: 1 ARP request packet; 2 ARP reply packet
sender_eth_addr	Ethernet address of the sender
sender_ip_addr	IP address of the sender
target_eth_addr	Target Ethernet address. If the packet is a ARP request packet, the target IP address will be 0. It changes to the correct address when the target responds.
target_ip_addr	Target IP address

debugging arp packet

Syntax

debugging arp packet [**sip** *sip-address* | **dip** *dip-address* | **smac** *smac-address* | **dmac** *dmac-address*] *

undo debugging arp packet

View

User view

Parameter

sip-address: Source IP address of all the permitted ARP packets, expressed in dotted decimal format. It can be combined with other restrictive conditions at discretion. If it is set to all zeros, ARP packets of all source IP addresses are permitted by default.

dip-address: Destination IP address of all the permitted ARP packets, expressed in dotted decimal format. It can be combined with other restrictive conditions at discretion. If it is set to all zeros, ARP packets of all destination IP addresses are permitted by default.

smac-address: Source MAC address of all the permitted ARP packets, expressed in dotted decimal format. It can be combined with other restrictive conditions at discretion. If it is set to all zeros, ARP packets of all source MAC addresses are permitted by default.

dmac-address: Destination MAC address of all the permitted ARP packets, expressed in dotted decimal format. It can be combined with other restrictive conditions at discretion. If it is set to all zeros, ARP packets of all destination MAC addresses are permitted by default.

Description

Use the **debugging arp packet** command to enable the debugging for the permitted ARP packets.

Use the **undo debugging arp packet** command to disable the debugging output.

Example

Display and print the ARP packets whose source IP address is 8.8.8.1, destination address is 8.8.8.26 and source MAC address is 000a-ebf2-51a8.

```
<SW8800> debugging arp packet dip 8.8.8.26 sip 8.8.8.1 smac 000a-ebf
2-51a8 dmac 0-0-0
```

Disable the debugging output.

```
<SW8800> undo debugging arp packet
```

display arp

Syntax

display arp [*ip-address* | [**dynamic** | **static**] [| { **begin** | **include** | **exclude** } *text*]]

View

Any view

Parameter

dynamic: Displays the dynamic ARP entries in ARP mapping table.

static: Displays the static ARP entries in ARP mapping table.

ip-address: Displays ARP mapping entries according to specified IP address.

begin: Starts displaying from the first ARP entry that contains the specified character string "text".

include: Displays only the ARP entries that contain the specified character string "text".

exclude: Displays only the ARP entries that do not contain the specified character string "text".

text: Character string. The ARP entries that are related with this character string are displayed.

Description

Use the **display arp** command to view the ARP mapping table.

Related command: **arp static**, **reset arp**, **debugging arp**.

Example

Display all the ARP entries.

```
<SW8800> display arp | inc 2.2.1
           Type: S-Static   D-Dynamic
IP Address  MAC Address VLAN ID Port Name   Aging   Type
2.2.2.231      0001-0001-0001    N/A        N/A             N/A   S
2.2.1.2        0002-0002-0002    N/A        N/A             N/A   S
--   2 entries found   ---
```

Character of "." in a regular expression is a wildcard. So, as for "2.2.2.231", "2.2.1" matches its sub-string "2.231" and thus the ARP mapping entry with an IP address of 2.2.2.231 is displayed as a matched entry.

Table 103 Description on the fields of the display arp command

Field	Description
IP Address	IP address of the ARP mapping entry
MAC Address	MAC address of the ARP mapping entry
VLAN ID	ID of the VLAN to which the static ARP entry belongs
Port Name	Name of the port to which the static ARP entry belongs
Aging	Aging time of dynamic ARP entry in minutes
Type	Type of ARP entry

display arp multi-port

Syntax

display arp multi-port [*ip-address*]

View

Any view

Parameter

ip-address: IP address of an ARP mapping entry.

Description

Use the **display arp multi-port** command to display configuration information about multicast ARP. The multicast ARP (that is, multiple-port ARP) feature allows one ARP entry to correspond to multiple outgoing ports; it is used to send one packet to multiple ports simultaneously.

Related command: **arp static**.

Example

Display configuration information about the multicast ARP entry with the IP address of 10.10.10.98.

```
<SW8800> display arp multi-port 10.10.10.98
IP Address   :10.10.10.98
Mac Address :0150-0098-0098
```

```
VLAN  ID    :20
ARP Port-List :
Ethernet6/1/2      Ethernet6/1/3
Ethernet6/1/4     *Ethernet6/1/5
Ethernet6/1/6      Ethernet6/1/7
Ethernet6/1/8      Ethernet6/1/9
Ethernet6/1/1
VPN-Name   :Public-ARP
```

When a "*" precedes a port, the port is in the Up state; otherwise, the port is in the Down state.

display arp proxy

Syntax

display arp proxy [**vlan** *vlan-id*]

View

Any view

Parameter

vlan-id: Specifies the VLAN ID.

Description

Use the **display arp proxy** command to display the state of the ARP proxy of a specified VLAN. An ARP proxy can be in enabled or disabled state.

Related command: **arp proxy enable**.

Example

Display the state of the ARP proxy of VLAN 3.

```
<SW8800> display arp proxy vlan 3
vlan 3
Proxy ARP status: disabled
```

display arp timer aging

Syntax

display arp timer aging

View

Any view

Parameter

None

Description

Use the **display arp timer aging** command to view the current setting of the dynamic ARP aging timer.

Related command: **arp timer aging**.

Example

Display the current setting of the ARP aging timer.

```
<SW8800> display arp timer aging
Current ARP aging time is 10 minute(s)
```

You can see that the ARP aging time is 10 minutes.

display debugging arp

Syntax

display debugging arp

View

Any view

Parameter

None

Description

Use the **display debugging arp** command to display the ARP packet debugging information.

Example

Display the ARP packet debugging information.

```
<SW8800> display debugging arp
ARP packet debugging switch is on, Source IP Address is 8.8.8.1, Destination
IP Address is 8.8.8.26, Source MAC Address is 000a-ebf2-51a8
```

Table 104 Description on the fields of the display debugging arp command

Field	Description
ARP packet debugging switch	State of the switch for ARP packet debugging
Source IP Address	Source IP address of an ARP packet
Destination IP Address	Destination IP address of an ARP packet
Source MAC Address	Source MAC address of an ARP packet

gratuitous-arp-learning enable

Syntax

gratuitous-arp-learning enable

undo gratuitous-arp-learning enable

View

System view

Parameter

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 gratuitous ARP packet learning function.

By default, the gratuitous ARP packet learning function is enabled.

By sending gratuitous ARP packets, a network device can:

- Determine whether or not IP address conflicts exist between it and other network devices.
- Trigger other network devices to update its hardware address stored in their caches.

Example

Enable the gratuitous ARP packet learning function on the switch.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] gratuitous-arp-learning enable
```

reset arp

Syntax

reset arp [**dynamic** | **static** | **interface** { *interface-type interface-number* } | **all**]

View

User view

Parameter

dynamic: Clears the dynamic ARP mapping entries.

static: Clears the static ARP mapping entries

interface-type is port type and *interface-number* is port number. For details, refer to the description of **interface** command in the *Port Command Manual*.

all: Clears all the ARP mapping entries.

Description

Use the **reset arp** command to reset the ARP mapping entries.

Related command: **arp static, display arp**.

Example

Reset the static ARP entries.

```
<SW8800> reset arp static
```

46 ARP TABLE SIZE CONFIGURATION COMMANDS

ARP Table Size Configuration Commands

arp max-entry

Syntax

arp max-entry *slot-num max-num*

undo arp max-entry *slot-num*

View

System view

Parameter

slot-num: Slot number of the card.

max-num: Maximum number of ARP entries that can be supported by the specified card. This argument counts in K (1K = 1024) and ranges from 4K to 8K.

Description

Use the **arp max-entry** command to configure the maximum number of ARP entries that can be supported by a specified card in the system.

Use the **undo arp max-entry** command to cancel the configuration.

By default, each card supports up to 4K ARP entries.

You can configure the maximum number of ARP entries to be 4K, 5K, 6K, 7K or 8K modules 3C17525, 3C1757, 3C17530, and 3C17531. For all other modules, the maximum number of ARP entries is 4K.

Example

Configure the maximum number of ARP entries that can be supported by the interface card in slot 12 to 8K.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800]arp max-entry 12 8
The configuration won't be enabled until the system is rebooted.
```

arp max-aggregation-entry

Syntax

arp max-aggregation-entry *max-aggnum*

undo arp max-aggregation-entry

View

System view

Parameter

max-aggnum: Maximum number of ARP entries for aggregation port (that is, aggregation ARP entries) supported by each card. This argument counts in K (1K = 1024).

Description

Use the **arp max-aggregation-entry** command to configure the maximum number of aggregation ARP entries that can be supported by each card of the switch.

Use the **undo arp max-aggregation-entry** command to restore the default maximum number of aggregation ARP entries supported by each card.

You can configure the maximum number of ARP entries to be 4K, 5K, 6K, 7K or 8K modules 3C17525, 3C1757, 3C17530, and 3C17531. For all other modules, the maximum number of ARP entries is 4K.

By default, each card supports up to 1K aggregation ARP entries.

Example

Configure the maximum number of aggregation ARP entries that can be supported by each card of the switch to 8K.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800]arp max-aggregation-entry 8
The configuration won't be enables until the system is rebooted.
```

arp enable size

Syntax

arp enable size { **4** | **64** }

undo arp enable size

View

System view

Parameter

4: Configures the maximum number of ARP entries of the whole switch to 4K (1K = 1024).

64: Configure the maximum number of ARP entries of the whole switch to 64K.

Description

Use the **arp enable size** command to configure the maximum number of ARP entries that can be supported by the whole switch.

Use the **undo arp enable size** command to restore the default maximum number of ARP entries supported by the whole switch.

By default, the whole switch supports up to 4K ARP entries, each card supports up to 4K ARP entries, and each card supports up to 1K aggregation ARP entries.

Example

Configure the maximum number of ARP entries of the whole switch to 64K.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] arp enable size 64
The configuration won't be enabled until the system is rebooted.
```

CAUTION:

- You must restart the system for each of the three configurations to take effect.
- Do not remove a card or change the place of a card from one slot to another before restarting the system. Otherwise, the configuration may fail to take effect.
- After the configurations, do not perform active/standby switchover before restarting the system. Otherwise, the configurations will not take effect even if you restart the system.

display arp max-entry

Syntax

display arp max-entry

View

Any view

Parameter

None

Description

Use the **display arp max-entry** command to display the current maximum numbers of ARP entries and the intending counterparts that will take effect after the switch restarts next time.

Example

Display the current maximum numbers of ARP entries and the intending counterparts that will take effect after the switch restarts next time.

```
<SW8800> display arp max-entry
The current max arp entry config information:
  max arp entry config(Main module): 65536
  max link aggregation arp entry config: 0
  max arp entry config of slot 0: 8192
  ..............
  max arp entry config of slot 13: 8192
The next max arp entry config information:
  max arp entry config(Main module): 65536
  max link aggregation arp entry config: 8192
  max arp entry config of slot 0: 8192
```

```
  ............
max arp entry config of slot 13: 8192
```

47 DHCP CONFIGURATION COMMANDS

General DHCP Configuration Commands

dhcp enable

Syntax

dhcp enable

undo dhcp enable

View

System view

Parameter

None

Description

Use the **dhcp enable** command to enable DHCP service.

Use the **undo dhcp enable** command to disable the DHCP service.

For both DHCP server and DHCP relay, you must enable DHCP service first before performing other DHCP configurations. The other related DHCP configurations take effect only after DHCP service is enabled.

Example

Enable DHCP service.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] dhcp enable
```

dhcp select

Syntax

In VLAN interface view:

dhcp select { **global** | **interface** | **relay** }

undo dhcp select

In system view:

dhcp select { **global** | **interface** | **relay** } { **interface vlan-interface** *vlan-id* [**to vlan-interface** *vlan-id*] | **all** }

undo dhcp select { **interface vlan-interface** *vlan-id* [**to vlan-interface** *vlan-id*] | **all** }

View

VLAN interface view, system view

Parameter

global: Specifies to forward DHCP packets to local DHCP server and let the local server assign IP addresses in global address pools to DHCP clients.

interface: Specifies to forward DHCP packets to local DHCP server and let the local server assign IP addresses in VLAN interface address pool to DHCP clients.

relay: Specifies to forward DHCP packets to remote DHCP servers and let remote servers assign IP addresses to DHCP clients. In this case, the current switch operates as a DHCP relay.

interface vlan-interface *vlan-id* [**to vlan-interface** *vlan-id*]: Specifies a VLAN interface or a range of VLAN interfaces.

all: Specifies all the VLAN interfaces.

CAUTION: *The **dhcp select interface** command cannot be used together with the **ip relay address** or **dhcp relay security address-check enable** command. Otherwise, the **ip relay address** command or the **dhcp relay security address-check enable** command will not take effect.*

Description

Use the **dhcp select** command to specify a method used by the switch to process the DHCP packets it received. You can use this command in VLAN interface view to specify a processing method of DHCP packets for current VLAN interface, or in system view to specify a processing method for multiple VLAN interfaces.

Use the **undo dhcp select** command to revert to the default processing mode of DHCP packets.

By default, the switch forwards the DHCP packets it received to the local DHCP server and let the local server assign IP addresses in global address pools to DHCP clients. (That is, the switch processes the DHCP packets in the **global** method.)

Example

Specify to forward DHCP packets to the local DHCP server and let the local server assign IP addresses in global address pools to DHCP clients.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface vlan-interface 1
[3Com-Vlan-interface1] dhcp select global
```

dhcp server detect

Syntax

dhcp server detect

undo dhcp server detect

View

System view

Parameter

None

Description

Use the **dhcp server detect** command to enable fake DHCP server detection.

Use the **undo dhcp server detect** command to disable fake DHCP server detection.

Fake DHCP server detection is disabled by default.

Example

Enable fake DHCP server detection.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] dhcp server detect
```

DHCP Server Configuration Commands

debugging dhcp server

Syntax

debugging dhcp server { **all** | **error** | **event** | **packet** }

undo debugging dhcp server { **all** | **error** | **event** | **packet** }

View

User view

Parameter

all: Used to enable/disable all types of debugging for DHCP server.

error: Used to enable/disable error debugging for DHCP server errors, including those occur when a DHCP server processes DHCP packets or assigns IP addresses.

event: Used to enable/disable debugging for DHCP server events, including the assigning of IP addresses and timing out of ping packets.

packet: Specifies debugging for packets received/sent by DHCP servers, including DHCP packets and ping packets.

Description

Use the **debugging dhcp server** command to enable debugging for DHCP server.

Use the **undo debugging dhcp server** command to disable debugging for DHCP server.

Each type of debugging concerning DHCP servers is disabled by default.

Example

Enable debugging for DHCP server events.

```
<SW8800> debugging dhcp server event
```

display dhcp server forbidden-ip

Syntax

display dhcp server forbidden-ip

View

Any view

Parameter

None

Description

Use the **display dhcp server forbidden-ip** command to display forbidden IP addresses in the DHCP address pool.

Example

Display forbidden IP addresses in the DHCP address pool.

```
<SW8800> display dhcp server forbidden-ip
Forbidden IP Range from 3.3.3.1              to  3.3.3.1
Forbidden IP Range from 3.3.3.4              to  3.3.3.99
Forbidden IP Range from 3.3.3.101            to  3.3.3.254
Forbidden IP Range from 17.9.0.1             to  17.9.0.1
Forbidden IP Range from 17.9.0.3             to  17.9.0.5
Forbidden IP Range from 17.9.0.8             to  17.9.255.254
```

dhcp server dns-list

Syntax

In VLAN interface view:

dhcp server dns-list *ip-address* [*ip-address*]

undo dhcp server dns-list { *ip-address* | **all** }

In system view:

dhcp server dns-list *ip-address* [*ip-address*] { **interface vlan-interface** *vlan-id* [**to vlan-interface** *vlan-id*] | **all** }

undo dhcp server dns-list { *ip-address* | **all** } { **interface vlan-interface** *vlan-id* [**to vlan-interface** *vlan-id*] | **all** }

View

VLAN interface view, system view

Parameter

ip-address: IP address of a DHCP server. You can specify up to eight IP addresses (separated by spaces) in one command.

interface vlan-interface *vlan-id* [**to vlan-interface** *vlan-id*]: Specifies one VLAN interface, or a range of VLAN interfaces.

all: Specifies all VLAN interfaces or all configured IP addresses.

Description

Use the **dhcp server dns-list** command to configure one or more DNS server addresses for the DHCP address pool of current VLAN interface, or for the DHCP address pool(s) of the specified VLAN interface(s).

Use the **undo dhcp server dns-list** command to remove one or more DNS server addresses configured for the DHCP address pool of current VLAN interface, or for the DHCP address pool(s) of the specified VLAN interface(s).

By default, no DNS server address is configured.

With eight DNS server addresses already configured, if you add a new DNS server address by executing the **dhcp server dns-list** command, the newly configured one overwrites the oldest one.

Related command: **dns-list**.

Example

Configure the DNS server address 1.1.1.254 for the DHCP address pool of VLAN interface 1.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface Vlan-interface 1
[3Com-Vlan-interface1] dhcp server dns-list 1.1.1.254
```

dhcp server domain-name

Syntax

In VLAN interface view:

dhcp server domain-name *domain-name*

undo dhcp server domain-name

In system view:

dhcp server domain-name *domain-name* { **interface vlan-interface** *vlan-id* [**to vlan-interface** *vlan-id*] | **all** }

undo dhcp server domain-name *domain-name* { **interface vlan-interface** *vlan-id* [**to vlan-interface** *vlan-id*] | **all** }

View

DHCP address pool view, VLAN interface view, system view

Parameter

domain-name: DHCP client domain name for DHCP address pool of specified VLAN interface, a string that is of 3 to 50 characters in length.

interface vlan-interface *vlan-id* [**to vlan-interface** *vlan-id*]: Specifies one VLAN interface, or a range of VLAN interfaces.

all: Specifies all VLAN interfaces.

Description

Use the **dhcp server domain-name** command to configure a DHCP client domain name for the DHCP address pool of the current VLAN interface, or for the DHCP address pool(s) of the specified VLAN interface(s).

Use the **undo dhcp server domain-name** command to remove the DHCP client domain name configured for the DHCP address pool of the current VLAN interface, or for the DHCP address pool(s) of the specified VLAN interface(s).

No DHCP client domain name is configured by default.

Related command: **domain-name**.

Example

Configure the DHCP client domain name of the DHCP address pool of the current VLAN interface to vlan-interface1.com.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface vlan-interface 1
[3Com-Vlan-interface1] dhcp server domain-name vlan-interface1.com
```

dhcp server expired

Syntax

In VLAN interface view:

dhcp server expired { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** }

undo dhcp server expired

In system view:

dhcp server expired { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** } { **interface vlan-interface** *vlan-id* [**to vlan-interface** *vlan-id*] | **all** }

undo dhcp server expired { **interface vlan-interface** *vlan-id* [**to vlan-interface** *vlan-id*] | **all** }

View

VLAN interface view, system view

Parameter

day *day*: Sets the number of days. The *day* argument ranges from 0 to 365.

hour *hour*: Sets the number of hours. The *hour* argument ranges from 0 to 23.

minute *minute*: Sets the number of minutes. The *minute* argument ranges from 0 to 59.

unlimited: Sets an unlimited lease time.

interface vlan-interface *vlan-id* [**to vlan-interface** *vlan-id*]: Specifies one VLAN interface, or a range of VLAN interfaces.

all: Specifies all VLAN interfaces.

Description

Use the **dhcp server expired** command to set the IP address lease time for the DHCP address pool of current VLAN interface, or for the DHCP address pool(s) of the specified VLAN interface(s).

Use the **undo dhcp server expired** command to revert to the default IP address lease time for the DHCP address pool of current VLAN interface, or for the DHCP address pool(s) of the specified VLAN interface(s).

The default lease time is one day.

Related command: **expired**.

Example

Set the IP address lease time of the DHCP address pool of VLAN interface 1 to unlimited.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface vlan-interface 1
[3Com-Vlan-interface1] dhcp server expired unlimited
```

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

Parameter

low-ip-address: Minimum IP address in the forbidden IP address range.

high-ip-address: The highest IP address in the forbidden IP address range. Note that the value of this argument must be larger than (or equal to) that of the *low-ip-address* argument. If you do not provide this argument, then the forbidden IP address range contains only the IP address specified by the *low-ip-address* argument.

Description

Use the **dhcp server forbidden-ip** command to forbid a range of IP addresses to be automatically assigned to DHCP clients.

Use the **undo dhcp server forbidden-ip** command to cancel the forbiddance.

All IP addresses in a DHCP address pool can be automatically assigned by default.

Related command: **dhcp server ip-pool**, **network**, **static-bind ip-address**, and **dhcp server static-bind**.

Example

Forbid the IP addresses from 10.110.1.1 to 10.110.1.63 to be automatically assigned.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] 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

Parameter

pool-name: Name of the address pool, a string that is of 1 to 64 characters in length. An address pool name uniquely identifies an address pool.

Description

Use the **dhcp server ip-pool** command to create a global DHCP address pool and enter the corresponding DHCP address pool view.

Use the **undo dhcp server ip-pool** command to remove a specified global DHCP address pool.

No global DHCP address pool is created by default.

Related command: **dhcp enable**.

Example

Create a global DHCP address pool with a name of 0.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] dhcp server ip-pool 0
[3Com-dhcp-0]
```

dhcp server nbns-list

Syntax

In VLAN interface view:

dhcp server nbns-list *ip-address* [*ip-address*]

undo dhcp server nbns-list { *ip-address* | **all** }

In system view:

dhcp server nbns-list *ip-address* [*ip-address*] { **interface vlan-interface** *vlan-id* [**to vlan-interface** *vlan-id*] | **all** }

undo dhcp server nbns-list { *ip-address* | **all** } { **interface vlan-interface** *vlan-id* [**to vlan-interface** *vlan-id*] | **all** }

View

VLAN interface view, system view

Parameter

ip-address: NetBIOS server IP address. You can specify up to eight IP addresses (separated by spaces) in one command.

interface vlan-interface *vlan-id* [**to vlan-interface** *vlan-id*]: Specifies one VLAN interface, or a range of VLAN interfaces.

all: Specifies all VLAN interfaces or all configured IP addresses.

Description

Use the **dhcp server nbns-list** command to configure one or more NetBIOS server IP addresses for the DHCP address pool of current VLAN interface, or for the DHCP address pool(s) of the specified VLAN interface(s).

Use the **undo dhcp server nbns-list** command to remove one or all NetBIOS server IP addresses configured for the DHCP address pool of current VLAN interface, or for the DHCP address pool(s) of the specified VLAN interface(s).

By default, no NetBIOS server IP address is configured.

With eight NetBIOS server addresses already configured, if you add a new one by executing the **dhcp server nbns-list** command, the newly configured one overwrites the oldest one.

Related command: **nbns-list**, **dhcp server netbios-type**.

Example

Configure the NetBIOS server with an IP address of 10.12.1.99 for the DHCP address pool of VLAN interface 1.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface vlan-interface 1
[3Com-Vlan-interface1] dhcp server nbns-list 10.12.1.99
```

dhcp server netbios-type

Syntax

In VLAN interface view:

dhcp server netbios-type { **b-node** | **h-node** | **m-node** | **p-node** }

undo dhcp server netbios-type

In system view:

dhcp server netbios-type { **b-node** | **h-node** | **m-node** | **p-node** } { **interface vlan-interface** *vlan-id* [**to vlan-interface** *vlan-id*] | **all** }

undo dhcp server netbios-type { **interface vlan-interface** *vlan-id* [**to vlan-interface** *vlan-id*] | **all** }

View

VLAN interface view, system view

Parameter

b-node: Specifies b-node to be the NetBIOS node type. DHCP clients of this node type establish host name-to-IP address mapping by broadcasting. (b stands for broadcast.)

p-node: Specifies p-node to be the NetBIOS node type. DHCP clients of this node type establish host name-to-IP address mapping by communicating with NetBIOS server. (p stands for peer-to-peer.)

m-node: Specifies m-node to be the NetBIOS node type. DHCP clients of this node type are p nodes which take some broadcast features. (m stands for mixed.)

h-node: Specifies h-node to be the NetBIOS node type. DHCP clients of this node type are b nodes which take peer-to-peer mechanism. (h stands for hybrid.)

Description

Use the **dhcp server netbios-type** command to configure the NetBIOS node type for DHCP clients of DHCP address pool of current or specified VLAN interface.

Use the **undo dhcp server netbios-type** command to remove the NetBIOS node type configured for DHCP clients of DHCP address pool of current or specified VLAN interface.

The default DHCP client NetBIOS node type is h-node.

Related command: **netbios-type**, **dhcp server nbns-list**.

Example

Configure p-node as the NetBIOS node type for DHCP clients of the DHCP address pool of VLAN interface 1.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface vlan-interface 1
[3Com-Vlan-interface1] dhcp server netbios-type p-node
```

dhcp server option

Syntax

In VLAN interface view:

dhcp server option *code* { **ascii** *ascii-string* | **hex** *hex-string* | **ip-address** *ip-address* [*ip-address*] }

undo dhcp server option *code*

In system view:

dhcp server option *code* { **ascii** *ascii-string* | **hex** *hex-string* | **ip-address** *ip-address* [*ip-address*] } { **interface vlan-interface** *vlan-id* [**to vlan-interface** *vlan-id*] | **all** }

undo dhcp server option *code* { **interface vlan-interface** *vlan-id* [**to vlan-interface** *vlan-id*] | **all** }

View

VLAN interface view, system view

Parameter

code: Option code customized by user. This argument ranges from 2 to 254.

ascii *ascii-string*: Specifies a string comprising ASCII characters. The string can be of 1 to 63 characters in length.

hex *hex-string*: Specifies a numeric string containing 2 or 4 hexadecimal digits (hh or hhhh).

ip-address *ip-address* [*ip-address*]: Specifies one or more IP addresses. You can specify up to eight IP addresses (separated by spaces) in one command.

interface vlan-interface *vlan-id* [**to vlan-interface** *vlan-id*]: Specifies one or more VLAN interfaces.

all: Specifies all VLAN interfaces.

Description

Use the **dhcp server option** command to configure a custom DHCP option for the DHCP address pool of current VLAN interface, or for the DHCP address pool(s) of the specified VLAN interface(s).

Use the **undo dhcp server option** command to remove a custom DHCP option configured for the DHCP address pool of current VLAN interface, or for the DHCP address pool(s) of the specified VLAN interface(s).

If you execute the **dhcp server option** command multiple times, the new configurations overwrite the corresponding old ones.

Related command: **option**.

Example

Configure a custom DHCP option for the DHCP address pool of VLAN interface 1, with the *code* argument of 100 and the *hex-string* argument of 0x11 and 0x22.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface vlan-interface 1
[3Com-Vlan-interface1] dhcp server option 100 hex 11 22
```

dhcp server ping

Syntax

dhcp server ping { **packets** *number* | **timeout** *milliseconds* }

undo dhcp server ping { **packets** | **timeout** }

View

System view

Parameter

packets *number*: Sets the maximum times to send ping packets. The *number* argument ranges from 0 to 10 and defaults to 2. Value of 0 specifies not to send any ping packet.

timeout *milliseconds*: Sets the maximum time to wait for a response to a ping packet. The *milliseconds* argument is in the unit of milliseconds; it ranges from 0 to 10000 and defaults to 500.

Description

Use the **dhcp server ping** command to set the maximum times to send ping packets or the maximum time for the DHCP server to wait for a response after sending a ping packet.

Use the **undo dhcp server ping** command to revert to the corresponding default setting.

CAUTION: *The host's interval of sending discover packets is in the range of 15 seconds to 30 seconds. When the* ***ping*** *command is used for collision detection, the host will fail to apply for IP addresses if the server's time to wait for a response to a ping packet is longer than the host's interval of sending discover packets. So you had better satisfy the condition that the server's time to wait for a response to a ping packet must be shorter than 15 seconds when the* ***ping*** *command is used for collision detection.*

Example

Set the maximum times to send ping packets to 10.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] dhcp server ping packets 10
```

Set the maximum time to wait for a response to a ping packet to 600 milliseconds.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] dhcp server ping timeout 600
```

dhcp server static-bind

Syntax

dhcp server static-bind ip-address *ip-address* **mac-address** *mac-address*

undo dhcp server static-bind { **ip-address** *ip-address* | **mac-address** *mac-address* }

View

VLAN interface view

Parameter

ip-address: IP address to be bound statically. Note that the IP address must be a valid IP address in the address pool of the current VLAN interface.

mac-address: MAC address for the IP address to be bound to.

Description

Use the **dhcp server static-bind** command to statically bind an IP address in the address pool of the current VLAN interface to a MAC address.

Use the **undo dhcp server static-bind** command to remove a statically bound IP address entry.

IP addresses in the address pool of a VLAN interface are not statically bound by default.

VLAN interface address pool only supports one-to-one MAC-IP binding.

Example

Statically bind the IP address 10.1.1.1 to the MAC address 0000-e03f-0305.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface vlan-interface 1
[3Com-Vlan-interface1] dhcp server static-bind ip-address 10.1.1.1 m
ac-address 0000-e03f-0305
```

display dhcp server conflict

Syntax

display dhcp server conflict { **all** | **ip** *ip-address* }

View

Any view

Parameter

all: Specifies all IP addresses.

ip *ip-address*: Specifies an IP address.

Description

Use the **display dhcp server conflict** command to display the statistics about DHCP address conflicts.

Related command: **reset dhcp server conflict**.

Example

Display the statistics about DHCP address conflicts.

```
<SW8800> display dhcp server conflict all
Address             Discover Time
10.110.1.2         Jan 11 2003 11:57: 7 PM
```

Table 105 Description on the fields of the display dhcp server conflict command

Field	Description
Address	The IP address that causes the conflict
Discover Time	The time when the conflict is discovered

display dhcp server expired

Syntax

display dhcp server expired { **ip** *ip-address* | **pool** [*pool-name*] | **interface** [**vlan-interface** *vlan-id*] | **all** }

View

Any view

Parameter

ip *ip-address*: Specifies an IP address.

pool [*pool-name*]: Specifies a global address pool. If you do not input a *pool-name*, all global address pools are included.

interface [**vlan-interface** *vlan-id*]: Specifies a VLAN interface address pool. If you do not input a *vlan-id*, all VLAN interface address pools are included.

all: Specifies all DHCP address pools.

Description

Use the **display dhcp server expired** command to display information about lease-expired addresses. If no available IP address exists in a DHCP address pool, the DHCP server assigns the lease-expired IP addresses in the pool to DHCP clients as needed.

Example

Display information about lease-expired addresses.

```
<SW8800> display dhcp server expired all
Global pool:
 IP address     Hardware address    Lease expiration          Type
Interface pool:
 IP address     Hardware address    Lease expiration          Type
```

Table 106 Description on the fields of the display dhcp server expired command

Field	Description
Global pool	The information followed is about expired IP addresses in global address pool(s)
Interface pool	The information followed is about lease-expired IP addresses in VLAN interface address pool(s)
IP address	Bound IP addresses
Hardware address	Bound MAC addresses
Lease expiration	The time when an IP address expires
Type	Binding type

display dhcp server free-ip

Syntax

display dhcp server free-ip

View

Any view

Parameter

None

Description

Use the **display dhcp server free-ip** command to display the ranges of available (unassigned) IP addresses in DHCP address pools.

Example

Display the ranges of available (unassigned) IP addresses in DHCP address pools.

```
<SW8800> display dhcp server free-ip
IP Range from 1.0.0.0              to  2.2.2.1
IP Range from 2.2.2.3              to  2.255.255.255
IP Range from 4.0.0.0              to  4.255.255.255
IP Range from 5.5.5.0              to  5.5.5.0
IP Range from 5.5.5.2              to  5.5.5.255
```

display dhcp server ip-in-use

Syntax

display dhcp server ip-in-use { **ip** *ip-address* | **pool** [*pool-name*] | **interface** [**vlan-interface** *vlan-id*] | **all** }

View

Any view

Parameter

ip *ip-address*: Specifies an IP address.

pool [*pool-name*]: Specifies a global address pool. If you do not input a *pool-name*, all global address pools are included.

interface [**vlan-interface** *vlan-id*]: Specifies a VLAN interface address pool. If you do not input a *vlan-id*, all VLAN interface address pools are included.

all: Specifies all DHCP address pools.

Description

Use the **display dhcp server ip-in-use** command to display information about IP address binding in DHCP address pool(s).

Related command: **reset dhcp server ip-in-use**.

Example

Display information about IP address binding in all DHCP address pools.

```
<SW8800> display dhcp server ip-in-use all
Global pool:
 IP address     Hardware address     Lease expiration     Type
```

```
 2.2.2.2     44444-4444-4444     NOT Used     Manual

Interface pool:
 IP address     Hardware address     Lease expiration     Type
 5.5.5.1     0050-ba28-930a     Jun 5 2003 10:56: 7 AM     Auto:COMMITED
```

Table 107 Description on the fields of the display dhcp server ip-in-use command

Fields	Description
Global pool	The information followed is about bound IP addresses in global address pool(s)
Interface pool	The information followed is about bound IP addresses in VLAN interface address pool(s)
IP address	Bound IP addresses
Hardware address	Bound MAC addresses
Lease expiration	The time when an IP address expires
Type	Binding type

display dhcp server statistics

Syntax

display dhcp server statistics

View

Any view

Parameter

None

Description

Use the **display dhcp server statistics** command to display statistics information about the DHCP server.

Related command: **reset dhcp server statistics**.

Example

Display statistics information about the DHCP server.

```
<SW8800> display dhcp server statistics
    Global Pool:
     Pool Number:             5
     Binding
      Auto:                   0
      Manual:                 1
      Expire:                 0
    Interface Pool:
     Pool Number:             1
     Binding
      Auto:                   1
      Manual:                 0
      Expire:                 0
    Boot Request:             6
     Dhcp Discover:           1
     Dhcp Request:            4
     Dhcp Decline:            0
     Dhcp Release:            1
```

```
     Dhcp Inform:              0
    Boot Reply:                4
     Dhcp Offer:               1
     Dhcp Ack:                 3
     Dhcp Nak:                 0
Bad Messages:             0
```

Table 108 Description on the fields of the display dhcp server statistics command

Field	Description
Global Pool	The information followed is about the statistics of the global address pools
Interface Pool	The information followed is about the statistics of the address pools of VLAN interfaces
Pool Number	Number of address pools
Auto	Number of automatically bound IP addresses
Manual	Number of manually bound IP addresses
Expire	Number of expired IP addresses
Boot Request: 6 Dhcp Discover: 1 Dhcp Request: 4 Dhcp Decline: 0 Dhcp Release: 1 Dhcp Inform: 0	Total and categorized DHCP packets received by the DHCP server
Boot Reply: 4 Dhcp Offer: 1 Dhcp Ack: 3 Dhcp Nak: 0	Total and categorized DHCP packets sent by the DHCP server
Bad Messages	Number of bad DHCP packets

display dhcp server tree

Syntax

display dhcp server tree { **pool** [*pool-name*] | **interface** [**vlan-interface** *vlan-id*] | **all** }

View

Any view

Parameter

pool [*pool-name*]: Specifies a global address pool. If you do not specify a global address pool, all global address pools are included.

interface [**vlan-interface** *vlan-id*]: Specifies the address pool of a VLAN interface. If you do not specify a VALN interface, address pools of all VLAN interfaces are included.

all: Specifies all addresses pools.

Description

Use the **display dhcp server tree** command to display information about DHCP address pool hierarchy.

Example

Display information about DHCP address pool hierarchy.

```
<SW8800> display dhcp server tree all
Global pool:
Pool name: 5
network 10.10.1.0 mask 255.255.255.0
Child node:6
Sibling node:7
  option 1 ip-address 255.0.0.0
  expired 1 0 0
  option 58 hex 00 00 A8 C0
  option 59 hex 00 00 00 3C
Pool name: 6
  static-bind ip-address 10.10.1.2 mask 255.0.0.0
  static-bind mac-address 00e0-00fc-0001
Parent node:5
  option 1 ip-address 255.255.0.
  expired 1 0 0
  option 58 hex 00 00 A8 C0
  option 59 hex 00 00 00 3C

Pool name: 7
network 10.10.1.64 mask 255.255.255.192
PrevSibling node:5
  option 1 ip-address 255.0.0.0
  gateway-list 2.2.2.2
  dns-list 1.1.1.1
  domain-name 444444
  nbns-list 3.3.3.3
  expired 1 0 0
  option 58 hex 00 00 A8 C0
  option 59 hex 00 00 00 3C
```

Table 109 Description on the fields of the display dhcp server tree command

Field	Description
Global pool	The information followed is about global address pools
Interface pool	The information followed is about VLAN interface address pools
Pool Name	The name of an address pool
Network	Range of addresses available for assigning
static-bind ip-address 10.10.1.2 mask 255.0.0.0 static-bind mac-address 00e0-00fc-0001	An IP address and the corresponding MAC address statically bound to it

Table 109 Description on the fields of the display dhcp server tree command

Field	Description
child node:6	The address pool named 6 is a child node of the one named 5 Based on the node position of the address pool named 5, the node type displayed here includes the following: Child node: Indicates the node to which the address pool named 6 corresponds is a child node of that of the address pool named 5. In this case, node 6 stands for a subnet of the network node 5 stands for Parent node: Indicates the node to which the address pool named 6 corresponds is the parent node of that of the address pool named 5. In this case, node 6 stands for the network segment Sibling node: Indicates the node to which the address pool named 6 corresponds is the next sibling node of that of the address pool named 5. Information about these address pools is displayed in the order they are established PrevSibling node: Indicates the node to which the address pool named 6 corresponds is the previous sibling node of that of the address pool named 5
Option	Customized DHCP options
expired	The valid period of the leased IP addresses in the address pool, including number of days, hours and minutes
gateway-list	The list of outbound gateways configured for the DHCP clients
dns-list	The list of DNS servers configured for the DHCP clients
domain-name	The domain name configured for the DHCP clients
nbns-list	The NetBIOS server configured for the DHCP clients

dns-list

Syntax

dns-list *ip-address* [*ip-address*]

undo dns-list { *ip-address* | **all** }

View

DHCP address pool view

Parameter

ip-address: IP address of a DNS server. You can specify up to eight IP addresses (separated by spaces) in one command.

all: Specifies all configured DNS server IP addresses.

Description

Use the **dns-list** command to configure one or more DNS server IP addresses for a global DHCP address pool.

Use the **undo dns-list** command to remove one or all DNS server IP addresses configured for a global DHCP address pool.

By default, no DNS server IP address is configured for a global DHCP address pool.

With eight DNS server addresses already configured, if you add a new one by executing the **dns-list** command, the new one overwrites the oldest one.

Related command: **dhcp server dns-list**, **dhcp server ip-pool**.

Example

Configure a DNS server with an IP address of 1.1.1.254 for the global DHCP address pool 0.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] dhcp server ip-pool 0
[3Com-dhcp-0] dns-list 1.1.1.254
```

domain-name

Syntax

domain-name *domain-name*

undo domain-name

View

DHCP address pool view

Parameter

domain-name: Domain name, a string that is of 3 to 50 characters in length.

Description

Use the **domain-name** command to configure a domain name for the DHCP clients of a global DHCP address pool.

Use the **undo domain-name** command to remove the domain name configured for the DHCP clients of a global DHCP address pool.

By default, no domain name is configured for the DHCP clients of a global DHCP address pool.

Related command: **dhcp server ip-pool**, **dhcp server domain-name**.

Example

Configure a domain name (mydomain.com) for the DHCP clients of the global DHCP address pool 0.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] dhcp server ip-pool 0
[3Com-dhcp-0] domain-name mydomain.com
```

expired

Syntax

expired { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** }

undo expired

View

DHCP address pool view

Parameter

day *day*: Specifies the number of days. The *day* argument ranges from 0 to 365.

hour *hour*: Specifies the number of hours. The *hour* argument ranges from 0 to 23.

minute *minute*: Specifies the number of minutes. The *minute* argument ranges from 0 to 59.

unlimited: Specifies an unlimited lease time.

Description

Use the **expired** command to set the valid period for a global DHCP address pool.

Use the **undo expired** command to revert to the default valid period.

The default valid period is 1 day.

Related command: **dhcp server ip-pool**, **dhcp server expired**.

Example

Set the IP address lease time of the global DHCP address pool 0 to one day plus two hours and three minutes.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] dhcp server ip-pool 0
[3Com-dhcp-0] expired day 1 hour 2 minute 3
```

gateway-list

Syntax

gateway-list *ip-address* [*ip-address*]

undo gateway-list { *ip-address* | **all** }

View

DHCP address pool view

Parameter

ip-address: IP address of an outbound gateway. You can specify up to eight IP addresses (separated by spaces) in one command.

all: Specifies all outbound gateway IP addresses.

Description

Use the **gateway-list** command to configure one or more outbound gateway addresses for DHCP clients.

Use the **undo gateway-list** command to remove one or all outbound gateway addresses configured for DHCP clients.

By default, no outbound gateway address is configured for DHCP clients.

With eight outbound gateway addresses already configured, if you add a new outbound gateway address by executing the **gateway-list** command, the new one overwrites the oldest one.

Example

Configure an outbound gateway with an IP address of 10.110.1.99 for DHCP clients of global DHCP address pool 0.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] dhcp server ip-pool 0
[3Com-dhcp-0] gateway-list 10.110.1.99
```

nbns-list

Syntax

nbns-list *ip-address* [*ip-address*]

undo nbns-list { *ip-address* | **all** }

View

DHCP address pool view

Parameter

ip-address: IP address of a NetBIOS server. You can specify up to eight IP addresses (separated by spaces) in one command.

all: Specifies all configured NetBIOS server IP addresses.

Description

Use the **nbns-list** command to configure one or more NetBIOS server addresses for a global DHCP address pool.

Use the **undo nbns-list** command to remove one or all NetBIOS server addresses configured for a global DHCP address pool.

By default, no NetBIOS server address is configured for a global DHCP address pool.

With eight NetBIOS server addresses already configured, if you add a new NetBIOS server address by executing the **nbns-list** command, the new one overwrites the oldest one.

Related command: **dhcp server ip-pool**, **dhcp server nbns-list**, **netbios-type**.

Example

Configure a NetBIOS server with an IP address of 10.12.1.99 for the global DHCP address pool named 0.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] dhcp server ip-pool 0
[3Com-dhcp-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

Parameter

b-node: Specifies the NetBIOS node type of DHCP clients to be b-node (b stands for broadcast). Nodes of this type establish their host name-to-IP address mappings by broadcasting.

p-node: Specifies the NetBIOS node type of DHCP clients to be p-node (p stands for peer-to-peer). Nodes of this type establish their host name-to-IP address mappings by communicating with NetBIOS server.

m-node: Specifies the NetBIOS node type of DHCP clients to be m-node (m stands for mixed). Nodes of this type are p nodes which take some broadcast features.

h-node: Specifies the NetBIOS node type of DHCP clients to be h-node (h stands for hybrid). Nodes of this type are b nodes which take peer-to-peer mechanism.

Description

Use the **netbios-type** command to configure the NetBIOS node type for DHCP clients of a global DHCP address pool.

Use the **undo netbios-type** command to remove NetBIOS node type configuration of a global DHCP address pool.

By default, the DHCP clients are of h-node type.

Related command: **dhcp server ip-pool**, **dhcp server netbios-byte**, **nbns-list**.

Example

Configure the NetBIOS node type of DHCP clients of the global DHCP address pool 0 to b-node.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] dhcp server ip-pool 0
[3Com-dhcp-0] netbios-type b-node
```

network

Syntax

network *ip-address* [**mask** *netmask* | *mask-length*]

undo network

View

DHCP address pool view

Parameter

ip-address: Address range for dynamic IP address assigning.

mask *netmask*: Specifies the subnet mask of the address pool. If you do not provide this argument, the default subnet mask is used.

mask-length: Length of the network mask of an IP address pool. It is an integer in the range of 0 to 32.

Description

Use the **network** command to configure an address range for dynamic IP address assignment.

Use the **undo network** command to remove the address range configured for dynamic IP address assignment.

By default, no IP address range is configured for dynamic IP address assignment.

Each DHCP address pool can be configured with only one address range. If you execute the **network** command multiple times, then only the last configured address range works.

Related command: **dhcp server ip-pool**, **dhcp server forbidden-ip**.

Example

Configure 192.168.8.0/24 as the address range for the global DHCP address pool 0.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] dhcp server ip-pool 0
[3Com-dhcp-0] network 192.168.8.0 mask 255.255.255.0
```

option

Syntax

option *code* { **ascii** *ascii-string* | **hex** *hex-string* | **ip-address** *ip-address* [*ip-address*] }

undo option *code*

View

DHCP address pool view

Parameter

code: Customized option value, a number ranging from 2 to 254.

ascii *ascii-string*: Specifies an ASCII string. The *ascii-string* argument is a string that is of 1 to 63 characters in length.

hex *hex-string*: Specifies a numeric string containing two or four hexadecimal digits (hh or hhhh).

ip-address *ip-address* [*ip-address*]: Specifies one or more IP addresses. You can specify up to eight IP addresses (separated by spaces) in one command.

Description

Use the **option** command to configure a custom DHCP option for a global DHCP address pool.

Use the **undo option** command to remove a custom DHCP option configured for the global DHCP address pool.

If you execute the **option** command multiple times, the new configurations overwrite the corresponding old ones

Related command: **dhcp server ip-pool**, **dhcp server option**.

Example

Configure a custom option for the global DHCP address pool, with an option value of 100 and two hexadecimal numbers of 0x11 and 0x22.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] dhcp server ip-pool 0
[3Com-dhcp-0] option 100 hex 11 22
```

reset dhcp server conflict

Syntax

reset dhcp server conflict { **ip** *ip-address* | **all** }

View

User view

Parameter

ip-address: Clears statistics about the specified IP address conflicts.

all: Clears all statistics about address conflicts.

Description

Use the **reset dhcp server conflict** command to clear statistics information about DHCP address conflicts.

Related command: **display dhcp server conflict**.

Example

Clear all statistics information about DHCP address conflicts.

```
<SW8800> reset dhcp server conflict all
```

reset dhcp server ip-in-use

Syntax

reset dhcp server ip-in-use{ **all** | **interface** [**vlan-interface** *vlan-id*] | **ip** *ip-address* | **pool** [*pool-name*] }

View

User view

Parameter

all: Specifies all binding entries.

ip-address: Specifies the binding entry that contains the specified IP address.

pool-name: Specifies a global DHCP address pool. If you do not provide this argument, then all global DHCP address pools are included.

vlan-id: Specifies a VLAN interface DHCP address pool. If you do not provide this argument, then all VLAN interface DHCP address pools are included.

Description

Use the **reset dhcp server ip-in-use** command to clear configuration about dynamically bound DHCP addresses.

Related command: **display dhcp server ip-in-use**.

Example

Clear the binding entries that contain the IP address of 10.110.1.1.

```
<SW8800> reset dhcp server ip-in-use ip 10.110.1.1
```

reset dhcp server statistics

Syntax

reset dhcp server statistics

View

User view

Parameter

None

Description

Use the **reset dhcp server statistics** command to clear statistics information about the DHCP servers, such as the number of DHCP address pools, the number of automatically bound, manually bound IP addresses and expired IP addresses, and the number of unrecognized packets, DHCP_Request packets and DHCP_ACK packets.

Related command: **display dhcp server statistics**.

Example

Clear statistics information about the DHCP servers.

```
<SW8800> reset dhcp server statistics
```

static-bind ip-address

Syntax

static-bind ip-address *ip-address* [**mask** *netmask*]

undo static-bind ip-address

View

DHCP address pool view

Parameter

ip-address: IP address to be bound.

mask *netmask*: Specifies the subnet mask of the IP address to be bound. If you do not provide the argument, the default subnet mask is used.

Description

Use the **static-bind ip-address** command to specify the IP address to be statically bound.

Use the **undo static-bind ip-address** command to free a statically bound IP address.

By default, no IP address is statically bound.

The **static-bind ip-address** command and the **static-bind mac-address** command must be coupled when you configure statically bound entries to specify the corresponding IP address bound to the MAC address specified by the **static-bind mac-address** command.

Related command: **dhcp server ip-pool**, **static-bind mac-address**.

Example

Bind the PC with a MAC address of 0000-e03f-0305 to 10.1.1.1, whose subnet mask is 255.255.255.0.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] dhcp server ip-pool 0
[3Com-dhcp-0] static-bind ip-address 10.1.1.1 mask 255.255.255.0
[3Com-dhcp-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

Parameter

mac-address: MAC address to be bound.

Description

Use the **static-bind mac-address** command to specify the MAC address to be statically bound.

Use the **undo static-bind mac-address** command to free a statically bound MAC address.

By default, no MAC address is statically bound.

The **static-bind mac-address** command and the **static-bind ip-address** command must be coupled when you configure statically bound entries to specify the corresponding MAC address bound to the IP address specified by the **static-bind ip-address** command.

Related command: **dhcp server ip-pool** and **static-bind ip-address**.

Example

Bind the PC with a MAC address of 0000-e03f-0305 to 10.1.1.1, whose subnet mask is 255.255.255.0.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] dhcp server ip-pool 0
[3Com-dhcp-0] static-bind ip-address 10.1.1.1 mask 255.255.255.0
[3Com-dhcp-0] static-bind mac-address 0000-e03f-0305
```

DHCP Relay Configuration Commands

debugging dhcp relay

Syntax

debugging dhcp relay { **all**| **packet** | **error** | **even**t }

undo debugging dhcp relay { **all**| **packet** | **error** | **event** }

View

User view

Parameter

all: Enables all types of debugging concerning DHCP Relay.

packet: Enables debugging for packets.

error: Enables debugging for error messages.

event: Enables debugging for events.

Description

Use the **debugging dhcp-relay** command to enable debugging for DHCP Relay.

Use the **undo debugging dhcp-relay** command to disable specified type of debugging concerning DHCP Relay.

Debugging for DHCP Relay is disabled by default.

Example

Enable debugging for DHCP Relay.

```
<SW8800> debugging dhcp relay
*0.7200205-DHCP-8-dhcp_debug:
From client to server:
Interface: VLAN-Interface 1
Type: dhcp-request
ClientHardAddress: 0010-dc19-695d
          ServerIpAddress: 192.168.1.2

*0.7200230-DHCP-8-dhcp_debug:
```

```
From server to client:
Interface: VLAN-Interface 1
ServerGroupNo: 0
Type: dhcp-ack
ClientHardAddress: 0010-dc19-695d
         your ip address: 10.1.1.1

*0.7200580-DHCP-8-largehop:
Discard DHCP request packet because of too large hop count!

*0.7200725-DHCP-8-invalidpkt:
Wrong DHCP packet!
```

Table 110 Description on the fields of the debugging dhcp-relay command

Field	Description
Interface	The VLAN interface that forwards DHCP packets
Type	Type of the forwarded DHCP packet
ClientHardAddress	The MAC address of the DHCP client
ServerIpAddress	The IP address of the DHCP server
your ip address	The IP address assigned to the DHCP client

dhcp relay security

Syntax

dhcp relay security *ip-address mac-address* **static**

undo dhcp relay security *ip-address*

View

System view, VLAN interface view

Parameter

ip-address: IP address the user uses.

mac-address: MAC address the user owns.

static: Specifies the user address entry is static.

Description

Use the **dhcp relay security** command to add a user address entry for the DHCP server.

Use the **undo dhcp relay security** command to remove a user address entry configured for the DHCP server.

Before adding/removing a user address entry, you can check user address entries configured for the DHCP server using the **display dhcprelay-security** command.

Example

Configure a user address entry for a DHCP server, with an IP address of 1.1.1.1 and a MAC address of 0005-5D02-F2B3.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] dhcp relay security 1.1.1.1 0005-5D02-F2B3 static
```

dhcp relay security address-check

Syntax

dhcp relay security address-check { **enable** | **disable** }

View

VLAN interface view

Parameter

None

Description

Use the **dhcp relay security address-check enable** command to enable security address checking on a VLAN interface.

Use the **dhcp relay security address-check disable** command to disable security address checking on a VLAN interface.

The DHCP security feature is disabled on the VLAN interface by default. .

Example

Enable security address checking on VLAN interface 1.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800]interface vlan-interface 1
[3Com-Vlan-interface1] dhcp relay security address-check enable
```

dhcp-server detect

Syntax

dhcp server detect

undo dhcp server detect

View

System view

Parameter

None

Description

Use the **dhcp server detect** command to enable fake DHCP server detecting.

Use the **undo dhcp server detect** command to disable fake DHCP server detecting.

A private DHCP server in a network also answers IP address request packets and issues IP addresses to DHCP clients. However, the IP addresses they issued always bring addresses conflicts and cause users cannot access networks. This kind of DHCP servers are known as fake DHCP servers.

Example

Enable fake DHCP server detecting.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] dhcp server detect
```

display dhcp relay address

Syntax

display dhcp relay address { **interface vlan-interface** *vlan-id* | **all** }

View

Any view

Parameter

vlan-id: VLAN number.

interface vlan-interface: Specifies to display information about the DHCP servers configured for the VLAN interface.

all: Specifies to display information about the DHCP servers configured for all VLAN interfaces.

Description

Use the **display dhcp relay address** command to display information about DHCP servers configured for a VLAN interface.

Example

Display information about DHCP servers configured for all VLAN interfaces.

```
<SW8800> display dhcp relay address all
    **  Vlan-interface192 DHCP Relay Address  **
    Relay Address [0] :    193.193.1.1
    Relay Address [1] :    1.1.1.1
```

Display information about DHCP servers configured for VLAN interface 192.

```
<SW8800> display dhcp relay address interface vlan 192
    **  Vlan-interface192 DHCP Relay Address  **
    Relay Address [0] :    193.193.1.1
    Relay Address [1] :    1.1.1.1
```

display dhcprelay-security

Syntax

display dhcprelay-security [*ip-address*]

View

Any view

Parameter

ip-address: User IP address.

Description

Use the **display dhcprelay-security** command to display information about specific or all user address entries that the DHCP server maintains.

Example

Display information about all user address entries that the DHCP server maintains.

```
<SW8800> display dhcprelay-security
IP Address          MAC Address IP Address Type
2.2.2.2 0005-5d02-f2b2  Static
3.3.3.3 0005-5d02-f2b3  Dynamic
---   2 dhcp-security item(s) found   ---
```

Table 111 Description on the fields of the display dhcp-security command

Field	Description
IP Address	User IP address
MAC Address	User MAC address
IP Address Type	Type of the user address entry, which can be static or dynamic

ip relay address

Syntax

ip relay address *ip-address*

undo ip relay address { *ip-address* | **all** }

View

VLAN interface view

Parameter

ip-address: IP address of the DHCP server to which the DHCP packets received by this VLAN interface are forwarded.

all: Specifies all DHCP servers configured for the VLAN interface to forward DHCP packets to.

Description

Use the **ip relay address** command to specify the VLAN interface to operate in DHCP Relay mode and to specify the DHCP server to which the DHCP packets received by this VLAN interface are forwarded.

Use the **undo ip relay address** command to remove the DHCP server configured for the VLAN interface to forward DHCP packets.

No DHCP server is configured for a VLAN interface by default.

CAUTION: *The IP address of the intended DHCP server for the Dhcp relay feature cannot be the IP address of the VLAN interface corresponding to the DHCP Relay. Otherwise, the system gives the information such as "Error. The DHCP relay address you entered overlaps with local ip!".*

Example

Specify users belonging to VLAN interface 1 to acquire their IP addresses from a specified DHCP server.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
```

```
[SW8800]interface vlan1
[3Com-Vlan-interface1] ip relay address 10.9.0.3
```

DHCP Option 82 Configuration Commands

dhcp relay information enable

Syntax

To enable the option 82 function on a VLAN interface in its VLAN interface view:

dhcp relay information enable

undo dhcp relay information enable

To enable the option 82 function on multiple VLAN interfaces in system view:

dhcp relay information enable { **interface vlan-interface** *vlan-id* [**to vlan-interface** *vlan-id*] | **all** }

undo dhcp relay information enable { **interface vlan-interface** *vlan-id* [**to vlan-interface** *vlan-id*] | **all** }

View

VLAN interface view, System view

Parameter

vlan-id: ID of the specific VLAN interface.

all: All VLAN interfaces.

Description

Use the **dhcp relay information enable** command to enable the function of Option 82 support on DHCP relay.

Use the **undo dhcp relay information enable** command to disable the function of Option 82 support on DHCP relay.

By default, this function is disabled.

Related command: **dhcp server relay information enable**.

Example

Enable Option 82 support on DHCP relay so that the relay on VLAN interface 1 adds Option 82 into the request packets from the DHCP clients before it sends these packets to a DHCP server.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z
[SW8800] interface vlan 1
[3Com-Vlan-interface] dhcp relay information enable
```

Disable Option 82 support on DHCP relay

```
[SW8800] interface vlan1
[3Com-Vlan-interface1] undo dhcp raly information enable
```

dhcp relay information format

Syntax

dhcp relay information format { **normal | verbose** }

undo dhcp relay information format

View

VLAN interface view

Parameter

normal: Normal mode of DHCP relay option 82.

verbose: 3Com fixed network mode of DHCP relay option 82.

Description

Use the **dhcp relay information format** command to configure the mode of the DHCP Relay option 82.

Use the **undo dhcp relay information format** command to restore the default mode of DHCP Relay option 82.

The **normal** mode is adopted by default.

Example

Configure the mode of the relay option 82 on VLAN interface 1 as 3Com fixed network mode.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z
[SW8800]interface vlan1
[3Com-Vlan-interface1] dhcp relay information format verbose
```

Restore the default mode of the relay option 82 on VLAN interface 1.

```
[3Com-Vlan-interface1] undo dhcp relay information format
```

dhcp relay information strategy

Syntax

dhcp relay information strategy { **drop** | **keep** | **replace** }

undo dhcp relay information strategy

View

VLAN interface view

Parameter

drop: Indicates that the DHCP relay will drop the packets carrying Option 82.

keep: Indicates that the DHCP relay DHCP relay does not change the packets carrying Option 82.

replace: Indicates that the DHCP relay replaces Option 82 carried by the packets with its own Option 82.

Description

Use the **dhcp relay information strategy** command to configure the strategy for the DHCP relay to process the packets carrying Option 82.

Use the **undo dhcp relay information strategy** command to restore the default strategy.

By default, the **replace** strategy is adopted.

Example

Configure the DHCP relay on VLAN interface 1 to drop the request packets carrying Option 82.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z
[SW8800] interface vlan1
[3Com-Vlan-interface1] dhcp relay information strategy  drop
```

Restore the default strategy for the DHCP relay on VLAN interface 1 to process the request packets.

```
[3Com-Vlan-interface1]undo dhcp relay information strategy
```

dhcp relay information format verbose node-identifier

Syntax

dhcp relay information format verbose node-identifier { **mac | sysname | user-defined** *string<1-50>* }

undo dhcp relay information format verbose node-identifier

View

VLAN interface view

Parameter

mac: Sets the bridge MAC as the node identifier of the Option 82 of a relay.

sysname: Sets the system name as the node identifier of the Option 82 of a relay.

user-defined *string<1-50>*: Sets the bridge-user-defined strings as the node identifier of the Option 82 of the relay.

Description

Use the **dhcp relay information format verbose node-identifier** command to set the node identifier of the Option 82 of a relay.

Use the **undo dhcp relay information format verbose node-identifier** command to restore the node identifier of the Option 82 of a relay to the default value.

The system sets bridge MAC as the default node identifier of the Option 82 of the relay.

Example

Set the system name as the node identifier when the mode of the relay option 82 on VLAN interface 1 is 3Com fixed network mode.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z
[SW8800]interface vlan1
[3Com-Vlan-interface1] dhcp relay information format verbose
node-identifier sysname
```

Restore the default node identifier of the user when the mode of relay option 82 on VLAN interface 1 is 3Com fixed network mode.

```
[3Com-Vlan-interface1] undo dhcp relay information format verbose
node-identifier
```

dhcp server relay information enable

Syntax

dhcp server relay information enable

undo dhcp server relay information enable

View

System view

Parameter

None

Description

Use the **dhcp server relay information enable** command to enable the function of Option 82 support on DHCP server.

Use the **undo dhcp server relay information enable** command to disable the function of Option 82 support on DHCP server.

When a client connected to a DHCP relay broadcasts a DHCP request packet, the DHCP relay is responsible for forwarding the packet to a DHCP server. After Option 82 support is enabled on the DHCP server, if the request packet forwarded by the DHCP relay to the DHCP server carries Option 82, the response packet sent by the DHCP server will carry a response Option 82.

After receiving the response packet from the DHCP server to the DHCP client, the DHCP relay check whether Option 82 exists in the packet. If yes, it strips Option 82. That is, the response packet sent to the client does not carry Option 82.

By default, the function is enabled. That is, the DHCP server will return Option 82 carried in the request packet to the DHCP relay.

Related command: **dhcp relay information enable**.

Example

Enable the DHCP server to return Option 82 carried in the request packets to the DHCP relay.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z
[SW8800] dhcp server relay information enable
```

Disable the DHCP server from returning Option 82 carried in the request packets to the DHCP relay.

```
[SW8800] undo dhcp server relay information enable
```

48

DNS CONFIGURATION COMMANDS

Static DNS Configuration Commands

ip host

Syntax

ip host *hostname ip-address*

undo ip host *hostname* [*ip-address*]

View

System view

Parameter

hostname: Name of the host. It is a character string that consists of 1 to 20 characters, including letters, numbers, "_" or ",", and it must contain at least one letter.

ip-address: Host IP address (the corresponding IP address to the host name) in dotted decimal notation.

Description

Use the **ip host** command to configure the host name and the host IP address.

Use the **undo ip host** command to cancel the host name and the host IP address.

By default, Host name and corresponding IP address are null.

Related command: **display ip host**.

Example

Set swtich1's IP address to be 10.110.0.1.

```
[SW8800] ip host switch1 10.110.0.1
```

display ip host

Syntax

display ip host

View

Any view

Parameter

None

Description

Use the **display ip host** command to view all the host names and the corresponding IP addresses.

Example

Display all host names and the corresponding IP addresses of the hosts.

```
<3Com< display ip host
Host             Age     Flags       Address
My           0       static      1.1.1.1
Aa           0       static      2.2.2.4
```

Table 112 Description on the fields of the display ip host command

Field	Description
Host	Host name
Age	Valid period
Flags	Flags
Address	Host IP address

Dynamic DNS Configuration Commands

debugging dns

Syntax

debugging dns

undo debugging dns

View

User view

Parameter

None

Description

Use the **debugging dns** command to enable DNS debugging.

Use the **undo debugging dns** command to disable DNS debugging.

By default, DNS debugging is disabled.

Example

Enable DNS debugging

```
<3Com< debugging dns
make DNS packet for name adcd.com succeed
```

The information above indicates that the query packet for the domain name "abcd.com" is generated.

```
send the packet to 172.16.1.1 DNS server for 1 time
```

The information above indicates that the first query is performed to the domain name with the IP address of "172.16.1.1".

```
receive a right answer from server 0xAC100101
```

The information above indicates that a correct answer packet is received from the server.

```
query timeout
```

The information above indicates that the query for a domain name from a server times out because no answer is received.

display dns domain

Syntax

display dns domain

View

Any view

Parameter

None

Description

Use the **display dns domain** command to view the domain name suffix list.

Related command: **dns domain**.

Example

View domain name suffix list.

```
<3Com< display dns domain
No          Domain-name
0           abcd.com
```

Table 113 Description on the fields of the display dns domain command

Field	Description
No	Sequence number
Domain-name	Domain name suffix name

display dns dynamic-host

Syntax

display dns dynamic-host

View

Any view

Parameter

None

Description

Use the **display dns dynamic-host** command to view the dynamic domain name buffer.

Example

View the dynamic domain name buffer.

```
<3Com< display dns dynamic-host
No  Domain-name             Ipaddress            RR-TTL(S)     Alias
0   www.baidu.com           202.108.249.134      63000
1   www.yahoo.akadns.net    66.94.230.39         24
2   www.hotmail.com         207.68.172.239       3585
3   www.eyou.com            61.136.62.70         3591
```

Table 114 Description on the fields of the display dns dynamic-host command

Field	Description
No	Sequence number
Domain-name	Domain name
Ipaddress	Corresponding IP name of the domain name
RR-TTL(S)	Time to live, that is, the time for an entry to be stored, in seconds.
Alias	Alias of the domain name. There can be four of them at the most.

display dns server

Syntax

display dns server

View

Any view

Parameter

None

Description

Use the **display dns server** command to view the related information of the domain name server.

Related command: **dns server**.

Example

View the related information of the domain name server.

```
<3Com< display dns server
Domain-server               Ipaddress
0                           172.16.1.1
1                           172.16.1.2
```

Table 115 Description on the fields of the display dns server command

Field	Description
Domain-server	Domain name server
Ipaddress	Corresponding IP address of the domain name server

dns domain

Syntax

dns domain *domain-name*

undo dns domain [*domain-name*]

View

System view

Parameter

domain-name: Domain name suffix.

Description

Use the **dns domain** command to add the domain name suffix.

Use the **undo dns domain** command to delete the domain name suffix.

The system supports up to 10 domain name suffixes. To delete the domain name suffix, input the suffix name, and the specific suffix is deleted. Otherwise, all of the suffixes are deleted.

Related command: **display dns domain**.

Example

Configure a domain name suffix "com".

```
<3Com< system-view
System View: return to User View with Ctrl+Z.
[SW8800] dns domain com
```

dns resolve

Syntax

dns resolve

undo dns resolve

View

System view

Parameter

None

Description

Use the **dns resolve** command to enable the dynamic domain name resolution function.

Use the **undo dns resolve** command to disable the dynamic domain name resolution function.

By default, the dynamic domain name resolution function is disabled.

Example

Enable dynamic domain name resolution.

```
<3Com< system-view
System View: return to User View with Ctrl+Z.
[SW8800] dns resolve
```

dns server

Syntax

dns server *ip-address*

undo dns server [*ip-address*]

View

System view

Parameter

ip-address: IP address of the domain name server.

Description

Use the **dns server** command to configure the IP address of a domain name server.

Use the **undo dns server** command to delete the IP address of a domain name server.

The system supports up to six domain name server. To delete the domain name server, input the IP address, and the specific server is deleted. Otherwise, all of the servers are deleted.

Related command: **display dns server**.

Example

Configure a domain name server, with an IP address of 172.16.1.1.

```
<3Com< system-view
System View: return to User View with Ctrl+Z.
[SW8800] dns server 172.16.1.1
```

reset dns dynamic-host

Syntax

reset dns dynamic-host

View

User view

Parameter

None

Description

Use the **reset dns dynamic-host** command to clear the dynamic domain name buffer.

Related command: **display dns dynamic-host**.

Example

Clear the dynamic domain name buffer.

```
<3Com< reset dns dynamic-host
```

49 NETSTREAM CONFIGURATION COMMANDS

Netstream Configuration Commands

display ip netstream cache

Syntax

display ip netstream cache slot *slot-no*

View

Any view

Parameter

slot-no: Number of the slot where the NMM Application Module resides.

Description

Use the **display netstream cache** command to query the configuration and status information about the Netstream cache on the NMM Application Module.

Example

Query the information about the Netstream cache.

<SW8800> display ip Netstream cache slot 4

```
IP netstream cache information in slot 4
  Stream active timeout(minute)      : 5
  Stream inactive timeout(second)    : 60
  Active IP stream entry             : 0
  Active MPLS stream entry           : 0
  IP Stream entry been statistics    : 382858
  MPLS Stream entry been statistics  : 0
  Last statistics reset time         : 09:52:40 2005/12/01

 Protocol           Total   Packets   Stream   Packets
                  Streams     /Sec     /Sec   /stream
 ------------------------------------------------------
 TCP-other         382858       22       21         1
 Total             382858       22       21         1
```

Table 116 Description on the fields of the display Netstream cache command

Field	Description
Stream active timeout(minute) : 5	The current active aging time is 5 minutes
Stream inactive timeout(second) : 60	The current inactive aging time is 60 seconds

Table 116 Description on the fields of the display Netstream cache command

Field	Description
Active IP stream entry : 0	0 active IP stream entry is in the Netstream cache
Active MPLS stream entry : 0	0 active MPLS stream entry is in the Netstream cache
IP Stream entry been statistics : 0	0 IP stream entry has been aged by Netstream
MPLS Stream entry been statistics: 0	0 MPLS stream entry has been aged by Netstream
Last statistics reset time : 09:52:40 2005/12/01	The time when statistics was cleared last time

display ip netstream export

Syntax

display ip netstream export slot *slot-no*

View

Any view

Parameter

slot-no: Number of the slot where the NMM Application Module resides.

Description

Use the **display ip netstream export** command to query various information about the Netstream statistics export packets on the NMM Application Module on the specified slot.

Example

Query the Netstream statistics export information.

```
<SW8800> display ip netstream export slot 2
Version 5 export information
  Stream source address                       : 192.168.1.5
  Stream destination IP(UDP)                  : 192.168.1.2(9991)
   Exported stream number                     : 16
   Exported UDP datagram number(failed number): 16(0)

 Version 9 MPLS export information
  Stream source address                       : 0
  Stream destination IP(UDP)                  : 192.168.1.2(9991)
   Exported stream number                     : 0
   Exported UDP datagram number(failed number): 0(0)

 Version 8 tos-source-prefix export information
  Stream source address                       : 0
  Stream destination IP(UDP)                  : 192.168.1.2(9991)
   Exported stream number                     : 2
   Exported UDP datagram number(failed number): 2(0)
```

Table 117 Description on the fields of the display ip Netstream export command

Field	Description
Version 5 export information	Version 5 statistics export information
Stream source address	Source address of the export packet

Table 117 Description on the fields of the display ip Netstream export command

Field	Description
Stream destination IP(UDP)	Destination address and destination port number of the export packet
Exported stream number	Number of exported streams
Exported UDP datagram number(failed number)	Number of exported UDP packets (times of sending failures)
Version 9 MPLS export information	Version 9 MPLS stream statistics export information
Version 8 tos-source-prefix export information	Version 8 statistics export information which has enabled the ToS-source-prefix aggregation (the disabled aggregation function is not displayed)

enable

Syntax

enable

undo enable

View

Netstream aggregation view

Parameter

None

Description

Use the **enable** command to enable the aggregation mode corresponding to the current aggregation view.

Use the **undo enable** command to disable this aggregation mode.

Aggregation mode is not enabled by default.

Related command: **ip netstream aggregation**.

Example

Enable the autonomous system (AS) aggregation mode of Netstream.

```
<SW8800> system-view
[SW8800] ip netstream aggregation as
[3Com-aggregation-as] enable
```

ip netstream enable

Syntax

ip netstream enable slot *slot-no*

undo ip netstream enable *slot-no*

View

System view

Parameter

slot-no: Number of the slot where the NMM Application Module resides.

Description

Use the **ip netstream enable** command to enable the Netstream statistics function.

Use the **undo ip netstream enable** command to disable the Netstream statistics function.

The Netstream statistics function is disabled by default

Example

Mirror the inbound packets of GigabitEthernet6/1/2 to the NMM module on slot 2, and enable the Netstream statistics function.

```
<SW8800> system-view
[SW8800] mirror-group 1 inbound GigabitEthernet6/1/2 mirror-to slot
2
[SW8800] ip netstream enable slot 2
```

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 which classifies the stream according to the Netstream's source AS number, destination AS number and the outbound interface index keywords.

destination-prefix: Destination prefix aggregation which classifies the stream according to the Netstream's destination AS number, destination mask length, the destination prefix and the outbound interface index keywords.

prefix: Source and destination prefix aggregation which classifies the stream according to the Netstream's source AS number, destination AS number, source mask length, destination mask length, source prefix, destination prefix and the outbound interface index keywords.

prefix-port: Prefix port aggregation which classifies the stream according to the Netstream's source prefix, destination prefix, source port, outbound interface index and ToS value keywords.

protocol-port: Protocol port aggregation which classifies the stream according to the Netstream's protocol number, source port and destination port keywords.

source-prefix: Source prefix aggregation which classifies the stream according to the Netstream's source AS number, source mask length and the source prefix keywords.

tos: ToS-AS aggregation which classifies the stream according to the Netstream's ToS, source AS number, destination AS number, source interface and the outbound interface index keywords.

tos-destination-prefix: ToS-destination-prefix aggregation which classifies the stream according to the Netstream's destination AS number, destination mask length, destination prefix and outbound interface index keywords.

tos-prefix: ToS-prefix aggregation which classifies the stream according to the Netstream's ToS, source AS number, source prefix, source mask length, destination AS number, destination mask length and destination prefix keywords.

tos-protocol-port: Tos-protocol-port aggregation which classifies the stream according to the Netstream's ToS, protocol type, source port and destination port keywords.

tos-source-prefix: ToS-source-prefix aggregation which classifies the stream according to the Netstream's ToS, source prefix, source mask length and source interface index keywords.

Description

Use the **ip netstream aggregation** command to enter Netstream aggregation view.

In aggregation view, you can enable/disable the aggregation function, and set the source interface, destination IP address and destination port number of the version 8 UDP packet.

Related command: **enable**, **ip netstream export host**, and **ip netstream export source**.

Example

Enter Netstream AS aggregation view.

```
<SW8800> system-view
[SW8800] ip netstream aggregation as
[3Com-aggregation-as]
```

ip netstream export host

Syntax

ip netstream export host *ipaddress udpport*

undo ip netstream export host *ipaddress*

View

System view, aggregation view

Parameter

ip-address: IP address of the destination host of Netstream statistics export packets, expressed in dotted decimal.

udpport: UDP port number of the destination host of Netstream statistics export packets.

Description

Use the **ip netstream export host** command to configure the destination host IP address and UDP port number of the Netstream statistics export packet.

Use the **undo ip netstream export host** command to disable the configured destination host IP address of the Netstream statistics export packet. If the destination host IP address is not configured currently, the default setting is adopted.

By default, the destination address and destination port number are 0 in system view, and in aggregation view the destination address and destination port number are what they are set in system view.

Related command: **ip netstream aggregation** and **ip netstream export source**.

You can configure different destination host IP addresses and port numbers in different aggregation modes.

A packet can be sent to two different destination hosts at the same time.

Example

Set the destination IP address and UDP port number of the Netstream statistics export packet to 192.168.1.2 and 9991 respectively.

```
<SW8800> system-view
[SW8800] ip netstream export host 192.168.1.2 9991
```

ip netstream export source

Syntax

ip netstream export source *ipaddress*

undo ip netstream export source

View

System view, aggregation view

Parameter

ip-address: Source IP address of the Netstream statistics export packet, expressed in dotted decimal.

Description

Use the **ip netstream export source** command to configure the source IP address of the Netstream statistics export packet. This IP address will serve as the source address of the UDP packet.

Use the **undo ip netstream export source** command to restore the default setting.

The source IP address is 0 by default.

Related command: **ip netstream aggregation** and **ip netstream export host**.

You can configure different source IP addresses in different aggregation modes.

Example

Set the source interface IP address of the Netstream statistics export packet to 192.168.1.5.

```
<SW8800> system-view
[SW8800] ip netstream export source 192.168.1.5
```

ip netstream export version

Syntax

ip netstream export version *versionNo* [**origin-as** | **peer-as**]

undo ip netstream export version

View

System view

Parameter

versionNo: Version number of the Netstream statistics export packets. Version 5 and version 9 are currently supported.

To use version 8, use the following command: ip netstream aggregation. See the section entitled "ip netstream aggregation"

origin-as: Uses the original AS number as the AS number of the specified IP address.

peer-as: Uses the peer AS number as the AS number of the specified IP address.

Description

Use the **ip netstream export version** command to configure the version number and AS options of the Netstream statistics export packet.

Use the **undo ip netstream export version** command to restore the default setting.

By default, the AS option is **peer-as**, the version number of MPLS packets is 9, the version number of aggregation statistics packets is 8, and the version number of other packets is 5.

Example

Set the version number of Netstream statistics export packets to 5 and use the original AS number as the AS number of the specified IP address.

```
<SW8800> system-view
[SW8800] 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: Active aging time of Netstream in minutes.

Description

Use the **ip netstream timeout active** command to configure the active aging time of the streams on all the NMM modules in the system.

Use the **undo ip netstream timeout active** command to restore the default value of the active aging time of the streams on all the NMM modules in the system.

By default, the active aging time of the stream is 30 minutes.

When the active time of a stream (from the set-up time to now) exceeds the set limit, it will be aged.

Related command: **ip netstream timeout inactive**.

Example

Set the active aging time of Netstream to 60 minutes.

```
<SW8800> system-view
[SW8800] 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: Inactive aging time of Netstream in seconds.

Description

Use the **ip netstream timeout inactive** command to configure the inactive aging time of Netstream.

Use the **undo ip netstream timeout inactive** command to restore the default setting.

By default, the inactive aging time of Netstream is 60 seconds.

When the inactive time of a stream (from the time when the last packet of this stream flows by to now) exceeds the set limit, it will be aged.

Related command: **ip netstream timeout active**.

Example

Set the inactive aging time of Netstream to 150 seconds.

```
<SW8800> system-view
[SW8800] ip netstream timeout inactive 150
```

reset ip netstream statistics

Syntax

reset ip netstream statistics slot *slot-no*

View

User view

Parameter

slot-no: Number of the slot where the NMM Application Module resides.

Description

Use the **reset ip netstream statistics** command to clear the Netstream statistics information and export statistics information of the specified NMM Application Module and age all the streams in the stream cache.

Example

Clear the Netstream statistics information of the NMM moduleon slot 2 and age all the streams in the stream cache.

```
<SW8800> reset ip netstream statistics slot 2
```

ip netstream template refresh

Syntax

ip netstream template refresh *packets*

undo ip netstream template refresh

View

System view

Parameter

packets: Packet refresh rate of the template.

Description

Use the **ip stream template refresh** command to set the packet refresh rate of the template.

Use the **undo ip stream template refresh** command to restore the packet refresh rate of the template to the default value.

The packet refresh rate of the template is 20 by default.

Example

Set the packet refresh rate of the template to 100.

```
<SW8800> system-view
[SW8800] ip netstream template refresh 100
```

ip netstream template timeout

Syntax

ip netstream template timeout *minutes*

undo ip netstream template timeout

View

System view

Parameter

minutes: Aging time of the template in minutes.

Description

Use the **ip stream template timeout** command to set the aging time of the template.

Use the **undo ip stream template timeout** command to restore the aging time of the template to the default value.

By default, the aging time of the template is 30 minutes.

Example

Set the aging time of the template to 60 minutes.

```
<SW8800> system-view
[SW8800] ip netstream template timeout 60
```

50 PoE Configuration Commands

PoE Configuration Commands

display poe interface

Syntax

display poe interface [*interface-type interface-num*]

View

Any view

Parameter

interface-type interface-num: Port type and port number; refer to *Command Manual - Port* for details.

Description

Use the **display poe interface** *interface-type interface-num* command to display the PoE status of a specific port on the switch.

Use the **display poe interface** command without any option to display the PoE status of all the PoE-capable ports on the switch.

Example

Display the PoE status of the port GigabitEthernet3/1/1.

```
<SW8800> display poe interface GigabitEthernet3/1/1
Port power status            :delivering
Port power mode              :signal
Port PD class                :2
port power priority          :high
Port max power               :16800 mW
Port current power           :552 mW
Port remaining power         :16248 mW
Port average power           :717 mW
Port peak power              :1196 mW
Port current                 :13 mA
Port voltage                 :53.7 V
```

Table 118 Description on the fields of the display poe interface command

Field	Description
Port power status	PoE status of the port: **1** disabled: PoE is disabled on the port. **2** searching: the port is searching for a PD. **3** delivering: the port is supplying power to the PD. **4** PD disconnected: the port is not connected with a PD. **5** testing: the port is in testing. **6** fault: the port detected an nonstandard or fault PD.
Port power mode	PoE mode of the port: **1** auto: the system automatically selects the PoE mode. **2** signal **3** spare
Port PD class	The class of the power the port supplies to the PD
Port power priority	Port priority: **1** critical (the highest) **2** high **3** low
Port max power	Maximum power on the port
Port current power	Present power on the port
Port average power	Average power on the port
Port peak power	Peak power on the port
Port current	Present current on the port
Port voltage	Present voltage on the port
Port remaining power	Remaining power on the port

- The sampling cycle of the power, current and voltage of ports is 1 second;
- The sampling cycle of the peak power and average power of ports is 5 minutes

display poe interface power

Syntax

display poe interface power [*interface-type interface-num*]

View

Any view

Parameter

interface-type interface-num: Port type and port number; refer to C*ommand Manual - Port* for details.

Description

Use the **display poe interface power** *interface-type interface-num* command to display the PoE power information of the specified port on the switch. If you enter

the **display poe interface power** command without any argument, the PoE power information about all PoE-capable ports on the switch will be displayed.

Example

Display the power information of the port GigabitEthernet3/1/1.

```
<SW8800> display poe interface power GigabitEthernet3/1/1
Port power                    :700 mW
```

display poe pse

Syntax

display poe pse

View

Any view

Parameter

None

Description

Use the **display poe pse** command to display the parameters of all the PoE cards in the switch that serve as a power sourcing equipment (PSE).

Example

Display the parameters of all the PoE cards in the switch.

```
<SW8800> display poe pse
PSE Information of slot 6:
  Power Current Value     :67 W
  Power Remaining Value   :738 W
  Power Max Value         :806 W
  Power Peak Value        :1 W
  Power Average Value     :0 W
  Software Version        :290
  Hardware Version        :000
  CPLD Version            :021
```

Table 119 Description on the fields of the display poe pse command

Field	Description
Power Current Value	Current power of the card
Power Remaining Value	Remaining power of the card
Power Max Value	Maximum power of the card
Power Peak Value	Peak power of the card
Power Average Value	Average power of the card
Software Version	PSE software version
Hardware Version	PSE hardware version

The sampling cycle of the current power of the interface card is 1 minute, and the sampling cycle of the peak power and average power is 5 minutes.

display poe slot

Syntax

display poe slot *slotnum*

View

Any view

Parameter

slotnum: Slot number of a PoE card

Description

Use the **display poe slot** *slotnum* command to display the information of a PoE card in the switch.

Example

Display the information of the PoE card in slot 8 of the switch.

```
[SW8800] display poe slot 8
PSE Information of slot 8:
  Power Current Value     :33 W
  Power Remaining Value :772 W
  Power Max Value         :806 W
  Power Peak Value        :34 W
  Power Average Value     :33 W
  Software Version        :290
  Hardware Version        :000
```

poe enable

Syntax

poe enable

undo poe enable

View

Ethernet port view

Parameter

None

Description

Use the **poe enable** command to enable the PoE feature on a port.

Use the **undo poe enable** command to disable the PoE feature on a port.

By default, PoE is disabled on port.

Example

Enable PoE on current port.

```
[3Com-GigabitEthernet3/1/1] poe enable
```

Disable PoE on current port.

```
[3Com-GigabitEthernet3/1/1] undo poe enable
```

poe enable slot

Syntax

poe enable slot *slot-num*

undo poe enable slot *slot-num*

View

System view

Parameter

slot-num: Number of the slot where the module resides.

Description

Use the **poe enable slot** command to enable PoE on a module.

Use the **undo poe enable slot** command to disable PoE on a module.

By default, PoE is disabled on a module.

The switch checks that the total power of the current system is sufficient before allowing you to enable PoE on the module by using this command.

Example

Enable PoE on the module in slot 2.

```
[SW8800]poe enable slot 2
```

Disable PoE on the module in slot 2.

```
[SW8800]undo poe enable slot 2
```

poe legacy enable slot

Syntax

poe legacy enable slot *slot-num*

undo poe legacy enable slot *slot-num*

View

System view

Parameter

slot-num: Number of the slot where the module resides.

Description

Use the **poe legacy enable slot** command to enable the module to detect the compatibility of the PD connected to it.

Use the **undo poe legacy enable slot** command so that the module does not detect the compatibility of the PD connected to it.

When detecting the compatibility of PDs, the module can detect and power the PDs incompatible with the 802.3af standard.

By default, the module does not detect the compatibility of the PD connected to it.

CAUTION: *Detecting an incompatible device slows down the detection and decreases system performance; therefore, you are not recommended to enable compatibility detection if the device connected is 802.3af-compliant.*

Example

Enable the module in slot 2 to detect the compatibility of the PD connected to it.

```
[SW8800] poe legacy enable slot 2
```

Disable the detection of the compatibility of the PD connected to the module in slot 2.

```
[SW8800] undo poe legacy enable slot 2
```

poe max-power

Syntax

poe max-power *max-power*

undo poe max-power

View

Ethernet port view

Parameter

max-power: Maximum power distributed to the port, ranging from 3000 mW to 16800 mW.

Description

Use the **poe max-power** command to set the maximum PoE power on the current port.

Use the **undo poe max-power** command to restore the default PoE power on current port.

By default, the maximum PoE power on a port is 16800 mW.

Example

Set the maximum PoE power on the current port GigabitEthernet3/1/1 to 12,000 mW.

```
[3Com-GigabitEthernet3/1/1] poe max-power 12000
```

Restore the default maximum PoE power on the current port GigabitEthernet3/1/1.

```
[3Com-GigabitEthernet3/1/1] undo poe max-power
```

poe max-power slot

Syntax

poe max-power *max-power* **slot** *slot-num*

undo poe max-power slot *slot-num*

View

System view

Parameter

max-power: Maximum power distributed to the card, ranging from 37 W to 806 W.

slot-num: Slot number of a card.

Description

Use the **poe max-power** command to set the maximum power on a card.

Use the **undo poe max-power** command to restore the default maximum power on the card.

By default, the maximum power on a card is 806 W.

Example

Set the maximum power on the card in slot 3 to 400 W.

```
[SW8800] poe max-power 400 slot 3
```

Restore the default maximum power on the card.

```
[SW8800] undo poe max-power slot 3
```

poe mode

Syntax

poe mode { **signal** | **spare** | **auto** }

undo poe mode

View

Ethernet port view

Parameter

signal: The port supplies power through signal lines.

spare: The port supplies power through spare lines.

auto: The port supplies power in automatically selected mode.

Description

Use the **poe mode** command to configure the PoE mode on the current port.

Use the **undo poe mode** command to restore the default PoE mode on current port.

By default, the port adopts signal lines to supply power.

CAUTION: *3Com Switch 8800 Family series routing switches currently do not support the spare mode. If a PD only supports the spare mode, a conversion will be needed.*

Example

Configure the PoE mode on current port to signal.

```
[3Com-GigabitEthernet3/1/1] poe mode signal
```

poe power-management

Syntax

poe power-management { **auto** | **manual** } **slot** *slot-num*

View

System view

Parameter

slot-num: Number of the slot where the module resides.

auto: The switch automatically manages the PoE mode on a module.

manual: You need to manually manage the PoE mode on a module on the switch.

Description

Use the **poe power-management** command to configure the PoE power management mode for a module on the switch.

By default, you need to manually manage PoE on the module on the switch.

Before the power supply is almost fully loaded, the system powers all ports. Working together with the command for configuring PoE priority on a port, this command takes effect when the external power supply by the switch is almost fully loaded.

The following section describes PoE in auto mode and in manual mode:

- Auto mode: Priority management mode. If new PDs are connected to the switch when the external power supply is almost fully loaded, the switch first powers the PD connected to the port whose PoE priority is the highest. For example, assume that the PoE priority on port A is set to **critical**. If a new PD is connected to port A when the external power supply by the switch is almost fully loaded, the switch stops powering the PD connected to the port whose PoE priority is the lowest and begins to power the PD connected to port A.
- Manual mode: If new PDs are connected to the switch when the external power supply is almost fully loaded, the switch disregards the PoE priority of the port but notifies you that a new device is connected, without changing the original PoE status. For example, assume that the PoE priority on port A is set to **critical**. If a new PD is connected to port A when the external power supply by the switch is fully loaded, the switch notifies you that a new device is connected but will not power the device connected to port A.

Related command: **poe priority**.

Example

Configure the switch to automatically power the PD connected to the module in slot 2.

```
[SW8800]poe power-management auto slot 2
```

Restore the mode in which the switch powers the PD connected to the module in slot 2 to manual.

```
[SW8800] poe power-management manual slot 2
```

poe power max-value

Syntax

poe power max-value *max-value*

undo poe power max-value

View

System view

Parameter

max-value: Configures the maximum power of the switch, in Watts.

Description

Use the **poe power max-value** command to configure the maximum PoE power of switch.

By default, the maximum PoE power of the switch is 4,500 W.

Example

Configure the maximum PoE power of the switch as 2,300 W.

```
[SW8800]poe power max-value 2300
```

Restore the default PoE power of switch.

```
[SW8800] undo poe power max-value
```

poe priority

Syntax

poe priority { **critical** | **high** | **low** }

undo poe priority

View

Ethernet port view

Parameter

critical: Sets the port priority to critical (the highest).

high: Sets the port priority to high.

low: Sets the port priority to low.

Description

Use the **poe priority** command to set the PoE priority on a port.

Use the **undo poe priority** command to restore the default priority.

By default, the PoE priority on each port is low.

CAUTION: *When the PoE power of the switch is not enough to support all the port, the switch supplies power to ports with higher priority, and powers down some ports with lower priority.*

Example

Set the PoE priority of current port to critical.

```
[3Com-GigabitEthernet3/1/1] poe priority critical
```

Restore the default priority.

```
[3Com-GigabitEthernet3/1/1] undo poe priority
```

51 PoE PSU Supervision Commands

PoE PSU Supervision Display Commands

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 AC input state of each power supply unit (PSU).

Example

Display the AC input state of each PSU.

```
<SW8800> display poe-power ac-input state
PSU 1 AC Input State : Lack Phase
PSU 2 AC Input State : Normal
PSU 3 AC Input State : Lack Phase
```

Table 120 Description on the fields of the display poe-power ac-input state command

Field	Description
NORMAL	The AC input is normal.
Under Limit	The AC input is below the lower threshold.
Upper Limit	The AC input is above the upper threshold.
Lack Phase	The AC input is lack of phase.
Fuse Broken	The fuse is blown.
Switch Off	The switch is off.

display poe-power alarm

Syntax

display poe-power alarm

View

Any view

Parameter

None

Description

Use the **display poe-power alarm** command to display detailed alarm information about the PoE PSUs.

Example

Display detailed alarm information about the PoE PSUs.

```
<SW8800> display poe-power alarm
 PSU alarm detail, PSU number : 2
 PSU 1 alarm : NORMAL
 PSU 2 alarm : NOTLINK      Controller/Rectifier communication  Fail
/Rectifier not in present
```

Table 121 Description on the fields of the display poe-power alarm command

Field	Description
NORMAL	Normal
NOTLINK	The PSU is disconnected. That is, the controller was able to communicate with the PSU; but it cannot now. Power-cycling the unit or re-inserting a new PSU can resolve this problem.
INERROR	The PSU input is in trouble. Restoring the AC input can resolve this problem.
OUTERROR	The PSU output is in trouble, the PSU cannot output normal DC voltage.
HIGHVOL	The PSU is over-voltage. The PSU is shut down because the output voltage is too high.
HIGHTEP	It is overheated in the PSU.
FANERROR	The PSU fan is in trouble.
CLOSE	The PSU is shut down remotely.
CURLIMIT	The PSU is current limited.

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 current DC output state of the PoE PSUs.

Example

Display the current DC output state.

```
<SW8800> display poe-power dc-output state
DC Output State : Normal
```

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 DC output voltage/current value of the PoE PSUs.

Example

Display the DC output voltage/current value of the PoE PSUs.

```
<SW8800> display poe-power dc-output value
DC Output Voltage : 53.997 V
DC Output Current : 0.000 A
```

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 number and current state of the AC power distribution switches of the PSUs.

Example

Display the number and current state of the AC power distribution switches.

```
<SW8800>display poe-power switch state
 Switch Number : 0
```

Table 122 Description on the fields of the display poe-power switch state command

Field	Description
On	The switch is on.
Off	The switch is off.
High Volt Input	The input is high voltage.
Low Volt Input	The input is low voltage.

display supervision-module information

Syntax

display supervision-module information

View

Any view

Parameter

None

Description

Use the **display supervision-module information** command to display the name of the supervision module, power supply model, specifications and output power, and other information.

Example

Display current information about the power system

```
<SW8800> display supervision-module information
Supervision Module Version  : 2.0
 Supervision Module Name  :Spring Pms
 Power Type  :PSE4500-A
 Power Rating Value          : 2250 W (220V)/1125 W(110V)
 Power Current Value         : 53 W
 Power Remaining Value : 2197 W
 Power Peak Value            : 0 W
 Power Average Value         : 0 W
 PSU Number                  : 2
 PSU 1
      Rating Output Power    : 2500 W
      Hard Version Info  :NP 2500
 PSU 2
Rating Output Power    : 2500 W
Hard Version Info  :NP 2500
```

Table 123 Description on the fields of the display supervision-module information command

Field	Description
Supervision Module Version	Software version of the supervision module
Supervision Module Name	Name of the supervision module
Power Type	Power type
Power Rating Value	Rated power of the power system
Power Current Value	Current consumption power of the power system
Power Remaining Value	Current remaining power of the power system
Power Peak Value	Peak power of the power system
Power Average Value	Average power of the power system
Rating Output Power	Rated output power. When one or two PSUs are available, it is 2250 W for 220 VAC input and 1125 W for 110 VAC input. When three PSUs are available, it is 4500 W for 220 VAC input and 2250 W for 110 VAC input.

PoE PSU Supervision Configuration Commands

poe-power input-thresh lower

Syntax

poe-power input-thresh lower *string*

View

System view

Parameter

string: Undervoltage alarm threshold. It ranges from 90.00 V to 264.00 V in the format of X.X and within the accuracy of the second decimal.

Description

Use the **poe-power input-thresh lower** command to set the undervoltage alarm threshold of AC input for the PoE PSUs (lower threshold):

- For 220 VAC input, it is recommended to set the threshold to 181.0 V.
- For 110 VAC input, it is recommended to set the threshold to 90.0 V.

Example

Set the undervoltage alarm threshold of AC input to 181.0 V.

```
[SW8800] poe-power input-thresh lower 181.0
Set lower input-threshold power successfully!
```

poe-power input-thresh upper

Syntax

poe-power input-thresh upper *string*

View

System view

Parameter

string: Overvoltage alarm threshold. It ranges from 90 V to 264 V in the format of X.X.

Description

Use the **poe-power input-thresh upper** command to set overvoltage alarm threshold of AC input (upper threshold):

- For 220 VAC input, it is recommended to set the threshold to 264.0 V.
- For 110 VAC input, it is recommended to set the threshold to 132.0 V.

Example

Set the overvoltage alarm threshold of AC input to 264.0 V.

```
[SW8800] poe-power input upper 264.0
Set upper input-threshold power successfully!
```

poe-power output-thresh lower

Syntax

poe-power output-thresh lower *string*

View

System view

Parameter

string: Undervoltage alarm threshold. It ranges from 45.00 V to 47.00 V in the format of x.x.

Description

Use the **poe-power output-thresh lower** command to set the undervoltage alarm threshold of DC output (lower threshold):

For both 220 VAC and 110 VAC input, it is recommended to set the threshold to 45.00 V.

Example

Set the undervoltage alarm threshold of DC output to 45.00 V.

```
[SW8800] poe-power output-thresh upper 57.0
Set lower output-threshold power successfully!
```

poe-power output-thresh upper

Syntax

poe-power output-thresh upper *string*

View

System view

Parameter

string: Overvoltage alarm threshold. It ranges from 55.00 V to 57.00 V in the format of X.X.

Description

Use the **poe-power output-thresh upper** command to set the overvoltage alarm threshold of DC output (upper threshold):

For both 220 VAC and 110 VAC input, it is recommended to set the threshold to 57.00 V.

Example

Set the overvoltage alarm threshold of DC output to 57.00V.

```
[SW8800] poe-power output upper 57.00
Set upper output-threshold power successfully!
```

52 UDP HELPER CONFIGURATION COMMANDS

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.

Example

Enable packet debugging for UDP Helper.

```
<SW8800> debugging udp-helper packet
```

display udp-helper

Syntax

display udp-helper { server [**interface vlan-interface** *vlan-id*] | port }

View

Any view

Parameter

vlan-id: ID of a VLAN.

Description

Use the **display udp-helper server** command to display the information of the destination server corresponding to the VLAN interface.

Use the **display udp-helper port** command to display the configuration of the global UDP ports.

Example

Display the information of the destination server corresponding to VLAN interface 1.

```
<SW8800> 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 VLAN interface 1 is 192.1.1.2, and no packets have been forwarded.

Display the configuration of the global UDP ports.

```
<SW8800> display udp-helper port
Now, the following config udp-helper port exist(s):
 37(time), 49(tacacs), 53(dns), 34, 89, 456, 10000-10005
```

The information above shows the configuration of the global UDP ports (including the default port 37, 49, 53 and the configured ports) when UDP helper is enabled.

udp-helper enable

Syntax

udp-helper enable

udp-helper enable

View

System view

Parameter

None

Description

Use the **udp-helper enable** command to enable the function of forwarding UDP broadcast packets.

Use the **undo udp-helper enable** command to disable the function.

By default, the function of forwarding UDP broadcast packets is disabled.

Example

Enable the function of forwarding UDP broadcast packets.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] udp-helper enable
```

udp-helper port

Syntax

udp-helper port { *port* | **dns** | **netbios-ds** | **netbios-ns** | **tacacs** | **tftp** | **time** }

undo udp-helper port { *port* | **dns** | **netbios-ds** | **netbios-ns** | **tacacs** | **tftp** | **time** }

View

System view

Parameter

port: Number of the port whose UDP packets are to be forwarded, in the range 1 to 65,535. Up to 250 ports are supported besides the default ports. Port 67 and port 68 are the ports of known protocols, so they cannot be specifies as UDP ports.

dns: Refers to domain name system (DNS), whose UDP port number is 53.

netbios-ds: Refers to netBIOS datagram service (netbios-ds), whose UDP port number is 138.

netbios-ns: Refers to netBIOS name service (netbios-ns), whose UDP port number is 137.

tacacs: Refers to terminal access controller access control system (TACACS), whose UDP port number is 49.

tftp: Refers to trivial transfer protocol (TFTP), whose UDP port number is 69.

time: Refers to time service, whose UDP port number is 37.

Description

Use the **udp-helper port** command to specify the port whose UDP packets are to be forwarded.

Use the **undo udp-helper port** command to remove the configuration.

Example

Specify the port corresponding to the DNS protocol as an UDP port.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] udp-helper port dns
```

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, in dotted decimal notation. This argument can be the address of a host or the broadcast address of a subnet. Up to 20 destination servers can be configured on a VLAN virtual interface.

Description

Use the **udp-helper server** command to specify the destination server for the UDP packets to be forwarded.

No destination server is configured by default.

Related command: **display udp-helper server**.

Example

Specify to forward UDP packets to the server whose IP address is 192.1.1.2.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800]interface Vlan-interface 1
[3Com-Vlan-interface1] udp-helper server 192.1.1.2
```

53 SNMP CONFIGURATION COMMANDS

SNMP Configuration Commands

display snmp-agent

Syntax

display snmp-agent local-engineid

View

Any view

Parameter

local-engineid: Local engine ID.

remote-engineid: Remote engine ID.

Description

Use the **display snmp-agent** command to view engine ID of current device.

SNMP engine is the core of SNMP entity. It performs the function of sending, receiving and authenticating SNMP message, extracting PDU, packet encapsulation and the communication with SNMP application, and so on.

Example

Display the engine ID of current device.

```
<SW8800> display snmp-agent local-engineid
SNMP local EngineID: 800007DB00E0FC0000FF6877
```

The above displayed information "SNMP local engine ID" represents local SNMP engine ID.

display snmp-agent community

Syntax

display snmp-agent community [**read** | **write**]

View

Any view

Parameter

read: Displays read-only community information.

write: Displays read-write community information.

Description

Use the **display snmp-agent community** command to view the currently configured community names.

Example

Display the currently configured community names.

```
<SW8800> display snmp-agent community
Community name:public
       Group name:public
       Storage-type: nonVolatile

   Community name:private
       Group name:private
       Storage-type: nonVolatile
```

Table 124 Description on the fields of the display snmp-agent community command

Field	Description
community name	Community name
Group name	Group name
storage-type	Storage mode

display snmp-agent group

Syntax

display snmp-agent group [*group-name*]

View

Any view

Parameter

groupname: Group name.

Description

Use the **display snmp-agent group** command to view group name, security mode, state of various views and storage modes.

Example

Display SNMP group name and safe mode.

```
<SW8800> display snmp-agent group
       Group name: 3com
       Security model: v2c noAuthnoPriv
       Readview: ViewDefault
       Writeview: <no specified>
       Notifyview :<no specified>
       Storage-type: nonVolatile
```

The following table describes the output fields.

Table 125 Description on the fields of the display snmp-agent group command

Field	Description
groupname	SNMP Group name

Table 125 Description on the fields of the display snmp-agent group command

Field	Description
Security model	The security mode adopted by SNMP
readview	Read-only MIB view name corresponding to that group
writeview	Writable MIB view corresponding to that group
notifyview	The name of the notify MIB view corresponding to that group
storage-type	Storage mode

display snmp-agent mib-view

Syntax

display snmp-agent mib-view [**exclude** | **include** | { **viewname** *mib-view* }]

View

Any view

Parameter

exclude: Displays the SNMP MIB view excluded.

Include: Displays the SNMP MIB view included.

viewname: Displays the SNMP MIB view according to the mib view name.

mib-view: Specifies the MIB view name.

Description

Use the **display snmp-agent mib-view** command to view the MIB view configuration information of the switch.

Example

Display the information about the currently configured MIB view.

```
<SW8800> display snmp-agent mib-view
View name:ViewDefault
       MIB Subtree:internet
       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
```

The following table describes the output fields.

Table 126 Description on the fields of the display snmp-agent mib-view command

Field	Description
View name	View name
MIB Subtree	MIB subtree
Subtree mask	Subtree mask
storage-type	Storage type
View Type	Permit or forbid access to an MIB object
View status	Indicate the line state in the table

CAUTION: *If the SNMP Agent is disabled, "Snmp Agent disabled" will be displayed after you execute the above* ***display*** *commands.*

display snmp-agent statistics

Syntax

display snmp-agent statistics

View

Any view

Parameter

None

Description

Use the **display snmp-agent statistics** command to view current state of SNMP communication.

This command provides a counter for SNMP operations.

Example

Display the current state of SNMP communication.

```
<SW8800> 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
  9 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 2000)
  9 MIB objects retrieved successfully
  0 MIB objects altered successfully
  0 GetRequest-PDU accepted and processed
  9 GetNextRequest-PDU accepted and processed
  0 GetBulkRequest-PDU accepted and processed
9 GetResponse-PDU accepted and processed
  0 SetRequest-PDU accepted and processed
  0 Trap PDUs accepted and processed
  0 Alternate Response Class PDUs droped silently
  0 Forwarded Confirmed Class PDUs droped silently
```

The following table describes the output fields.

Table 127 Description on the fields of the display snmp-agent statistics command

Field	Description
9 Get-next PDUs accepted and processed	Total number of the input SNMP packets
0 GetBulkRequest-PDU accepted and processed	Number of packets with version information error
0 GetResponse PDUs accepted and processed	Number of packets with community name error
0 Set-request PDU accepted and processed	Number of packets with authority error corresponding to the community name
0 Trap PDUs accepted and processed	Number of SNMP packets with encoding error
0 Alternate Response Class PDUs droped silently	Number of SNMP data packets output
0 Forwarded Confirmed Class PDUs droped silently	Number of SNMP packets with erroneous values
9 Get-next PDUs accepted and processed	Number of SNMP packets with general error
0 GetBulkRequest-PDU accepted and processed	Number or packets request for nonexistent MIB objects
0 GetResponse PDUs accepted and processed	Number of too long SNMP packets
0 Set-request PDU accepted and processed	Number of variables requested by NMS
0 Trap PDUs accepted and processed	Number of variables sent by NMS
0 Alternate Response Class PDUs droped silently	Number of the received packets requested by get
0 Forwarded Confirmed Class PDUs droped silently	Number of the received packets requested by get-next
9 Get-next PDUs accepted and processed	Number of the received packets requested by getBulk
0 GetBulkRequest-PDU accepted and processed	Number of the response packets sent
0 GetResponse PDUs accepted and processed	Number of the Trap packets sent
0 Set-request PDU accepted and processed	Number of the response packets dropped
0 Trap PDUs accepted and processed	Number of the Trap packets dropped

display snmp-agent sys-info

Syntax

display snmp-agent sys-info [**contact** | **location** | **version**]*

View

Any view

Parameter

None

Description

Use the **display snmp-agent sys-info** command to view the character string sysContact (system contact), character string describing the system location and the version information about the running SMNMP in the system.

Example

Display the character string sysContact.

```
<SW8800> display snmp-agent sys-info contact
The contact person for this managed node:
           R&D Beijing, 3Com Corporation co.,Ltd.
```

The above information represents that the contact person for this machine is R&D Beijing, 3Com Corporation co.,Ltd

Display the character string describing the system location.

```
<SW8800> display snmp-agent sys-info location
The physical location of this node:
 BeiJing China
```

The above information represents that the physical location of this machine is: BeiJing China.

Display the version information of running SNMP

```
<SW8800> display snmp-agent sys-info version
SNMP version running in the system:
           SNMPv3
```

The above information represents that the SNMP version running in the system is: SNMPv3.

display snmp-agent usm-user

Syntax

display snmp-agent usm-user [**engineid** *engineid* | **group** *groupname* | **username** *username*]*

View

Any view

Parameter

engineid: Displays user information with specified engine ID.

username: Displays user information with specified user name.

groupname: Displays user information of specified group.

Description

Use the **display snmp-agent usm-user** command to view information of all the SNMP usernames in the group username list.

SNMP user is the remote user executing SNMP administrative operation. You can use the **snmp-agent usm-user** command to specify the SNMP user.

Example

Display the information of all the current users.

```
<SW8800> display snmp-agent usm-user
User name: NotifyV3
   Group name: NotifyGroup
       Authencation Mode: sha
       Privacy Mode: des
       Engine ID: 800007DB00E0FC2085026877 active

   User name: publicV3
   Group name: groupV3
       Authencation Mode: no
       Privacy Mode: no
       Engine ID: 800007DB00E0FC2085026877 active
       Acl:2000
```

The following table describes the output fields.

Table 128 Description on the fields of the display snmp-agent usm-user command

Field	Description
User name	Character string identifying the SNMP user
Group name	Character string identifying the group the user belongs to
Authencation Mode	Authentication code
Privacy Mode	Personal code
Engine ID	Character string identifying the SNMP device
Acl	Character string identifying the access control list

enable snmp trap

Syntax

enable snmp trap updown

undo enable snmp trap updown

View

Ethernet port view / VLAN interface view

Parameter

None

Description

Use the **enable snmp trap updown** command to enable current port or VLAN interface to transmit the LINK UP and LINK DOWN trap messages.

Use the **undo enable snmp trap updown** command to disable current port or VLAN interface to transmit the LINK UP and LINK DOWN trap messages.

The **enable snmp trap** command should be used in cooperation with the **snmp-agent trap enable** and the **snmp-agent target-host** commands. The **snmp-agent target-host** command is used to specify which hosts can receive the trap messages. To enable the transmitting of trap messages, you must execute the **snmp-agent target-host** command at least once.

Example

Enable current port Ethernet6/1/1 to transmit the LINK UP and LINK DOWN trap information with the community name public

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[3Com-Ethernet6/1/1] snmp trap updown enable
[SW8800] snmp-agent target-host trap address udp-domain 10.1.1.1
params securityname public
[SW8800] interface ethernet6/1/1
[3Com-Ethernet6/1/1] enable snmp trap updown
```

snmp-agent community

Syntax

snmp-agent community { **read** | **write** } *community-name* [[**mib-view** *view-name*] [**acl** *acl-list*]]

undo snmp-agent community *community-name*

View

System view

Parameter

read: Indicates that MIB object can only be read.

write: Indicates that MIB object can be read and written.

community-name: Community name character string.

view-name: MIB view name.

acl *acl-list*: sets access control list for specified community.

Description

Use the **snmp-agent community** command to configure community access name and enable the access to SNMP.

Use the **undo snmp-agent community** command to cancel the settings of community access name.

Example

Configure community name as comaccess and permits read-only access by this community name.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] snmp-agent community read comaccess
```

Configure community name as mgr and permits read-write access.

```
[SW8800] snmp-agent community write mgr
```

Delete the community name comaccess.

```
[SW8800] undo snmp-agent community comaccess
```

snmp-agent group

Syntax

snmp-agent group { **v1** | **v2c** } *group-name* [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*] [**acl** *acl-list*]

undo snmp-agent group { **v1** | **v2c** } *group-name*

snmp-agent group v3 *group-name* [**authentication** | **privacy**] [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*] [**acl** *acl-list*]

undo snmp-agent group v3 *group-name* [**authentication** | **privacy**]

View

System view

Parameter

v1: V1 security mode.

v2c: V2C security mode.

v3: V3 security mode.

group-name: Group name, ranging from 1 to 32 bytes.

authentication: Configures to authenticate the packet without encryption.

privacy: Configures to authenticate and encrypt the packet.

read-view: Configures to allow read-only view settings.

read-view: Read-only view name, ranging from 1 to 32 bytes.

write-view: Configures to allow read-write view settings.

write-view: Name of read-write view, ranging from 1 to 32 bytes.

notify-view: Configures to allow notify view settings.

notify-view: Specifies the notify view name, ranging from 1 to 32 bytes.

acl Sets access control list for this group name.

acl-list: access control list

Description

Use the **snmp-agent group** command to configure a new SNMP group, that is, to map SNMP user to SNMP view.

Use the **undo snmp-agent group** command to cancel a specified SNMP group.

By default, the SNMP group configured using the **snmp-agent group v3** command is in none authentication mode.

Related command: **snmp-agent mib-view** and **snmp-agent usm-user**.

Example

Create an SNMP group named test.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] snmp-agent group v3 test.
```

snmp-agent local-engineid

Syntax

snmp-agent local-engineid *engineid*

undo snmp-agent local-engineid

View

System view

Parameter

engineid: Specifies the engine ID with a character string, only composed of hexadecimal numbers between 5 and 32 including.

Description

Use the **snmp-agent local-engineid** command to configure a name for a local or remote SNMP engine on the switch.

Use the command to Using **undo snmp-agent local-engineid** command, you can restore the default setting of engine ID.

By default, the engine ID is corporation number + device information. Device information is determined according to different products. It can be IP address, MAC address or user defined text. However, you must use numbers in hexadecimal form.

Example

Configure the ID of a local or remote device as 1234512345.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] snmp-agent local-engineid 1234512345
```

snmp-agent mib-view

Syntax

snmp-agent mib-view { **included** | **excluded** } *view-name oid-tree*

undo snmp-agent mib-view *view-name*

View

System view

Parameter

included: Includes this MIB subtree.

excluded: Excludes this MIB subtree.

view-name: Specifies the view name, with a character string, ranging from 1 to 32 characters.

oid-tree: MIB object subtree. It can be a character string of the variable OID, or a variable name, ranging from 1 to 255 characters. By default, OID is 1.3.6.1.

Description

Use the **snmp-agent mib-view** command to create or update the view information.

Use the **undo snmp-agent mib-view** command to cancel the view information

By default, the view name is ViewDefault. OID is 1.3.6.1.

This command supports the parameter input of both OID and node name.

Related command: **snmp-agent group**.

Example

Create a view that consists of all the objects of MIB-II.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] snmp-agent mib-view included mib2 1.3.6.1.2.1
```

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: Specifies the size of SNMP packet (measured in bytes), ranging from 484 to 17940. By default, the size is 2000 bytes.

Description

Use the **snmp-agent packet max-size** command to configure the size of SNMP packet that the Agent can send/receive.

Use the **undo snmp-agent packet max-size** command to restore the default size of SNMP packet.

The sizes of the SNMP packets received/sent by the Agent are different in different network environment.

Example

Set the size of SNMP packet to 1042 bytes.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] snmp-agent packet max-size 1042
```

snmp-agent sys-info

Syntax

snmp-agent sys-info { **contact** *sysContact* | **location** *syslocation* | **version** { { **v1** | **v2c** | **v3** } * | **all** } }

undo snmp-agent sys-info { { **contact** | **location** }* | **version** { { **v1** | **v2c** | **v3** } * | **all** } }

View

System view

Parameter

contact: The contact information for system maintenance.

sysContact: Characters describe the contact information for system maintenance.

location: Sets the geographical location of the device.

sysLocation: Geographical location of the device.

version: version of running SNMP.

v1: SNMP V1.

v2c: SNMP V2C.

v3: SNMP V3.

*: Indicates that you can select more than one item from the three options **v1**, **v2c**, and **v3**. Here, you must select at least one option, and you can select all the three options.

all: all SNMP version (includes SNMP V1, SNMP V2C, SNMP V3).

Description

Use the **snmp-agent sys-info** command to configure system information such as geographical location of the device, contact information for system maintenance and version information of running SNMP.

Use the **undo snmp-agent sys-info location** command to restore the default value.

By default, the contact information for system maintenance is "R&D Hangzhou,3Com3Com Technology Co.,Ltd.", the system information about geographical location is "Hangzhou China", and the version information is " SNMPv1, SNMPv2c, and SNMPv3".

Related command: **display snmp-agent sys-info**.

Example

Set the system maintenance information to "Dial System Operator at beeper # 27345".

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] snmp-agent sys-info contact Dial System Operator at beeper # 27345
```

snmp-agent target-host

Syntax

snmp-agent target-host trap address udp-domain *host-addr* [**udp-port** *udp-port-number*] **params securityname** *securityname* [**v1** | **v2c** | **v3** [**authentication** | **privacy**]]

undo snmp-agent target-host *host-addr* **securityname** *securityname*

View

System view

Parameter

address: Specifies the address of the host which receives SNMP messages.

host-addr: IP address of the host.

udp-port *udp-port-number*: Specifies the UDP port number of the host to receive the SNMP notification.

v1: Represent the version of SNMPV1.

v2c: Represent the version of SNMPV2C.

v3: Represent the version of SNMPV3.

securityname: Specifies the community name, ranging 1 to 32 bytes. It can be the community name of SNMPv1/v2c or the user name of SNMPv3.

authentication: Configures to authenticate the packet without encryption.

privacy: Configures to authenticate and encrypt the packet.

Description

Use the **snmp-agent target-host** command to configure destination of SNMP notification.

Use the **undo snmp-agent target-host** command to cancel the host that receives SNMP notification.

The **snmp-agent target-host** command and the **snmp-agent trap enable** command should be used at the same time. Use the **snmp-agent trap enable** command to enable the device to transmit Trap packets. The **snmp-agent trap enable** command and **snmp-agent target-host** command should be used at the same time on the host to enable notify message sending.

If the version of SNMP message is v3, the packet authentication encryption mode specified by the command must be consistent with configuration for SNMP group to which the securityname belongs.

Related command: **snmp-agent trap enable**, **snmp-agent trap source** and **snmp-agent trap life**, **snmp-agent group**, **snmp-agent usm-user**.

Example

Enable sending Trap message to 10.1.1.1 with community name public.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] snmp-agent trap enable
[SW8800] snmp-agent target-host trap address udp-domain 10.1.1.1 par
ams securityname public
```

snmp-agent trap enable

Syntax

snmp-agent trap enable [**bgp** [**backwardtransition** | **established**]* | **configuration** | **flash** | **ospf** [*process-id*] [*ospf-trap-list*] | **ldp** | **lsp** | **standard** [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**]* | **system** | **vrrp** [**authfailure** | **newmaster**]]

undo snmp-agent trap enable [**bgp** [**backwardtransition** | **established**]* | **configuration** | **flash** | **ospf** [*process-id*] [*ospf-trap-list*] | **ldp** | **lsp** | **standard** [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**]* | **system** | **vrrp** [**authfailure** | **newmaster**]]

View

System view

Parameter

standard [**authentication**] [**coldstart**] [**linkdown**] [**linkup**]: Enables the sending of standard Trap messages.

authentication: Enables the sending of SNMP authentication Trap messages.

coldstart: Enables the sending of SNMP cold start Trap messages.

linkdown: Enables the sending of SNMP link down Trap messages.

linkup: Enables the sending of SNMP link up Trap messages.

warmstart: Enables the sending of SNMP hot start Trap messages.

bgp [**backwardtransition**] [**established**] : Enables the sending of BGP Trap messages.

configuration: Enables the sending of configuration management Trap messages.

flash: Enables the sending of FLASH Trap messages.

System: Enables the sending of system management MIB Trap messages.

vrrp [**authfailure** | **newmaster**]: Enables the sending of VRRP Trap messages.

ldp: Enables the sending of LDP Trap messages.

lsp: Enables the sending of LSP Trap messages.

Description

Use the **snmp-agent trap enable** command to enable the sending of Trap messages.

Use the **undo snmp-agent trap enable** command to disable the sending of Trap messages.

By default, Trap message sending is disabled.

The **snmp-agent trap enable** command and **snmp-agent target-host** command should be used at the same time. The **snmp-agent target-host** command specifies which hosts can receive Trap message. However, to send Trap message, at least one the **snmp-agent target-host** command should be configured.

Example

Enable to send the trap packet of SNMP authentication failure to 10.1.1.1. The community name is public.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] snmp-agent trap enable standard authentication
[SW8800] snmp-agent target-host trap address udp-domain 10.1.1.1
params securityname public
```

snmp-agent trap life

Syntax

snmp-agent trap life *seconds*

undo snmp-agent trap life

View

System view

Parameter

seconds: Specifies the timeouts, ranging from 1 to 2,592,000 seconds; By default, the timeout interval is 120 seconds.

Description

Use the **snmp-agent trap life** command to configure the timeout of Trap packets.

Use the **undo snmp-agent trap life** command to restore the default value.

The set timeout of Trap packet is represented by *seconds*. If time exceeds *seconds*, this Trap packet will be discarded.

Related command: **snmp-agent trap enable, snmp-agent target-host** .

Example

Configure the timeout interval of Trap packet as 60 seconds.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] snmp-agent trap life 60
```

snmp-agent trap queue-size

Syntax

snmp-agent trap queue-size *length*

undo snmp-agent trap queue-size

View

System view

Parameter

length: Length of queue, ranging from 1 to 1,000. By default, the length is 100.

Description

Use the **snmp-agent trap queue-size** command to configure the information queue length of Trap packet sent to Destination Host.

Use the **undo snmp-agent trap queue-size** command to restore the default value.

Related command: **snmp-agent trap enable, snmp-agent target-host, snmp-agent trap life**.

Example

Configure the queue length to 200.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] snmp-agent trap queue-size 200
```

snmp-agent trap source

Syntax

snmp-agent trap source vlan-interface *vlan-id*

undo snmp-agent trap source

View

System view

Parameter

vlan-id: Specifies the VLAN interface ID, ranging from 1 to 4094.

Description

Use the **snmp-agent trap source** command to configure the source address for sending Trap.

Use the **undo snmp-agent trap source** command to cancel the source address for sending Trap.

You can use this command to configure to track specific event by using the trap address.

Example

Configure the IP address of the VLAN interface 1 as the source address for transmitting the Trap packets.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] snmp-agent trap source vlan-interface 1
```

snmp-agent usm-user

Syntax

snmp-agent usm-user { **v1** | **v2c** } *username groupname* [**acl** *acl-list*]

undo snmp-agent usm-user { **v1** | **v2c** } *username groupname*

snmp-agent usm-user v3 *username groupname* [**authentication-mode** { **md5** | **sha** } *authpassstring* [**privacy-mode** { **des56** *privpassstring* }]] [**acl** *acl-list*]

undo snmp-agent usm-user v3 *username groupname* { **local** | **engineid** *engine-id* }

View

System view

Parameter

v1: Configures to use V1 safe mode.

v2c: Configures to use V2c safe mode.

v3: Configures to use V3 safe mode.

username: Specifies the user name, ranging from 1 to 32 bytes.

groupname: Specifies the group name corresponding to that user, a character string at the length ranging from 1 to 32 bytes.

authentication-mode: Specifies the safety level as authentication required.

md5: MD5 algorithm is adopted in authentication. MD5 authentication uses the 128-digit password. Computation speed of MD5 is faster than that of SHA

sha: SHA algorithm is adopted in authentication. SHA authentication uses the 160-digit password. Computation speed of SHA is slower than that of MD5, but with higher security.

authpasstring: Specifies the authentication password with a character string, ranging from 1 to 64 bytes.

privacy-mode: Specifies the safety level as encrypted.

des56: Specifies the authentication protocol as DES.

privpassword: Specifies the encryption password with a character string, ranging from 1 to 64 bytes.

acl *acl-list*: Sets access control list for this user based on USM name

engineid *engine-id*: SNMP engineID.

Description

Use the **snmp-agent usm-user** command to add a new user to an SNMP group.

Use the **undo snmp-agent usm-user** command to cancel a user from SNMP group.

SNMP engineID (for authentication) is required when configuring remote user for an agent. This command will not be effective without engineID configured.

For V1 and V2C, this command will add a new community name. For V3, it will add a new user for an SNMP group.

Example

Add a user wang for 3com (an SNMP group), configures to authenticate with MD5 and sets authentication password as pass.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] snmp-agent usm-user v3 wang 3com authentication-mode md5 pass
```

undo snmp-agent

Syntax

undo snmp-agent

View

System view

Parameter

None

Description

Use the **undo snmp-agent** command to disable all versions of SNMP running on the server.

Perform any command of **snmp-agent** will enable SNMP Agent.

Example

Disable the running SNMP agents of all SNMP versions.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] undo snmp-agent
```

54 RMON CONFIGURATION COMMANDS

RMON Configuration Commands

display rmon alarm

Syntax

display rmon alarm [*alarm-table-entry*]

View

Any view

Parameter

alarm-table-entry: Alarm table entry index.

Description

Use the **display rmon alarm** command to view RMON alarm information.

Related command: **rmon alarm**.

Example

Display the RMON alarm information.

```
<SW8800> display rmon alarm
Alarm table 1 owned by monitor is VALID.
  Samples type          : delta
  Variable formula      : 1.3.6.1.2.1.16.1.1.1.3.1<etherStatsDropEvents.1>
  Description           : Ethernet5/1/1
  Sampling interval     : 10(sec)
  Rising threshold      : 10(linked with event 1)
  Falling threshold     : 2(linked with event 1)
  When startup enables  : risingOrFallingAlarm
  Latest value          : 0
```

Table 129 Description on the fields of the display rmon alarm command

Field	Description
Alarm table 1	Index 1 in alarm table
monitor	Owner
VALID	The alarm entry corresponding to this index is valid.
Samples type	Type of sampling
Variable formula	Variable parameters
Description	Description information
Sampling interval	Time interval for sampling
Rising threshold is 1000	The rising threshold is 1000.
Falling threshold is 100	The falling threshold is 100.

Table 129 Description on the fields of the display rmon alarm command

Field	Description
startup	First triggering
When startup enables : risingOrFallingAlarm	Type of the first alarm. The startup may trigger rising threshold alarm, falling threshold alarm, or both.
Latest value	Last sample value

display rmon event

Syntax

display rmon event [*event-table-entry*]

View

Any view

Parameter

event-table-entry: Entry index of event table.

Description

Use the **display rmon event** command to view RMON events.

The display includes event index in event table, owner of the event, description to the event, action caused by event (log or alarm information), and occurrence time of the latest event (counted on system initiate/boot time in centiseconds).

Related command: **rmon event**.

Example

Show the RMON event.

```
<SW8800> display rmon event
Event table 1 owned by null is VALID.
  Description: null.
  Will cause log-trap when triggered, last triggered at 0days 00h:02m:27s.
```

Table 130 Description on the fields of the display rmon event command

Field	Description
Event table 1	Index in event table
VALID	The entry corresponding to the index is valid
Description	Event description
Cause log-trap when triggered,	When the event is triggered, it will cause the log-trap.
Last triggered at 0days 00h:02m:27s	The last triggered time is 00h:02m:27s

display rmon eventlog

Syntax

display rmon eventlog [*event-number*]

View

Any view

Parameter

event-number: Entry index of event table.

Description

Use the **display rmon eventlog** command to view RMON event log.

The display includes event index in the event table, the status of the event, the time at which the event log is generated (this time starts from the system initialization or booting and counted in milliseconds), and event description.

Example

Show event log of RMON.

```
<SW8800> display rmon eventlog 1
Event table 1 owned by null 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 131 Description on the fields of the display rmon eventlog command

Field	Description
Event table 1	Index 1 in event table
VALID	The entry corresponding to the index is valid
Description	Event description
less than(or =) 100 with alarm value 0	The alarm sample value is less than or equal to 100
Alarm sample type is absolute	The type of alarm sampling is absolute
Generates eventLog 1.2 at 0days 00h:02m:27s	The eventlog corresponding to the index 1.2 is generated at 0days 00h:02m:27s.

display rmon history

Syntax

display rmon history [*port-num*]

View

Any view

Parameter

port-num: Ethernet port name.

Description

Use the **display rmon history** command to view latest RMON history sampling information (including utility, error number and total packet number).

Related command: **rmon history**.

Example

Show the RMON history information.

```
<SW8800> display rmon history ethernet 2/1/1
History control entry 1 owned by null 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 132 Description on the fields of the display rmon history command

Field	Description
Samples interface	The sampled interface
History control entry	Index number in history control table
VALID	The entry corresponding to the index is valid
Sampling interval	Sampling interval
buckets	Records in history control table
Latest sampled values	The latest sample information
dropevents	Dropping packet events
octets	Sent/Received octets in sampling time
packets	Packets sent/received in sampling time
broadcast packets	Number of broadcast packets
multicast packets	Number of multicast packets
CRC alignment errors	Number of CRC error packets
undersized packets	Number of undersized packets
oversized packets	Number of oversized packets
fragments	Number of undersized and CRC error packets
jabbers	Number of oversized and CRC error packets
collisions	Number of collision packets
utilization	Utilization

display rmon prialarm

Syntax

display rmon prialarm [*prialarm-table-entry*]

View

Any view

Parameter

prialarm-table-entry: Entry index of extended RMON alarm table.

Description

Use the **display rmon prialarm** command to view information about extended RMON alarm table.

Related command: **rmon prialarm**.

Example

Display the information about extended RMON alarm table.

```
<SW8800> display rmon prialarm
Prialarm table 1 owned by monitor is UNDERCREATION.
  Samples type          : changeratio
  Variable formula      : (.1.3.6.1.2.1.2.2.1.10.201326601+.1.3.6.1.2.1.2.2.1.16
```

```
.201326601)*8*100/.1.3.6.1.2.1.2.2.1.5.201326601
  Description           : ifUtilization.Ethernet5/1/1
  Sampling interval     : 10(sec)
  Rising threshold      : 50(linked with event 1)
  Falling threshold     : 5(linked with event 1)
  When startup enables  : risingOrFallingAlarm
  This entry will exist : forever.
  Latest value          : 0
```

Table 133 Description on the fields of the display rmon prialarm command

Field	Description
Prialarm table 1	Index of extended alarm entry.
owned by monitor	Creator of the extended alarm entry.
UNDERCREATION	Status of expansion alarms
Samples type	Type of sampling
Variable formula	Formula for expansion alarms
Description	Description information
Sampling interval : 10(sec)	Sampling interval
Rising threshold	Rising threshold. When sampling value rises from normal value to this threshold, rising threshold alarm will be triggered.
Falling threshold	Falling threshold. When sampling value decreases from normal value to this threshold, falling threshold alarm will be triggered.
linked with event 1	Corresponding event index of ring and falling threshold alarm.
When startup enables: risingOrFallingAlarm	Kind of first alarm. It may trigger rising threshold alarm or falling threshold alarm or both.
This entry will exist forever	The lifespan of this alarm entry which can be forever or a specified period of time.
Latest value : 0	The value of the latest sampling.

display rmon statistics

Syntax

display rmon statistics [*port-num*]

View

Any view

Parameter

port-num: Ethernet port number.

Description

Use the **display rmon statistics** command to view RMON statistics.

The displayed information includes collision, CRC (Cyclic Redundancy Check) and queue, undersized or oversized packet, timeout, fragment, broadcast, multicast, unicast, and bandwidth utility.

Related command: **rmon statistics**.

Example

Show RMON statistics.

```
<SW8800> display rmon statistics Ethernet 2/1/1
Statistics entry 1 owned by aaa is VALID.
  Interface : Ethernet2/1/1<ifIndex.872418178>
  etherStatsOctets         : 756       , etherStatsPkts          : 9
  etherStatsBroadcastPkts  : 9         , etherStatsMulticastPkts : 0
  etherStatsUndersizePkts  : 0         , etherStatsOversizePkts  : 0
  etherStatsFragments      : 0         , etherStatsJabbers       : 0
  etherStatsCRCAlignErrors : 0         , etherStatsCollisions    : 0
  etherStatsDropEvents (insufficient resources): 0
  Packets received according to length (etherStatsPktsXXXtoYYYOctets):
  64     : 0         ,  65-127  : 444       ,  128-255  : 0
  256-511: 0         ,  512-1023: 0         ,  1024-max : 0
```

rmon alarm

Syntax

rmon alarm *entry-number alarm-variable sampling-time* { **delta** | **absolute** } **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: Number of the entry to be added/deleted, ranging from 1 to 65535.

alarm-variable: Specifies the alarm variable with a character string, ranging from 1 to 256, in the OID dotted format, like 1.3.6.1.2.1.2.1.10.1 (or ifInOctets.1).

sampling-time: Specifies the sampling interval, ranging from 5 to 65535 (measured in seconds).

delta: Sampling type is delta.

absolute: Sampling type is absolute.

rising-threshold *threshold-value1*: Rising threshold, ranging from 0 to 2147483647.

event-entry1: Event number corresponding to the upper limit of threshold, ranging from 0 to 65535.

falling-threshold *threshold-value2*: Falling threshold, ranging from 0 to 2147483647.

event-entry2: Event number corresponding to the falling threshold, ranging from 0 to 65535.

owner *text*: Specifies the creator of the alarm. Length of the character string ranges from 1 to 127.

Description

Use the **rmon alarm** command to add an entry to the alarm table.

Use the **undo rmon alarm** command to cancel an entry from this table.

In this way, the alarm event can be triggered in the abnormal situations and then decides to log and send trap to the NM station.

*Before adding an alarm entry, you need first to define the event to be referenced in the alarm entry using the **rmon event** command.*

The system takes these actions on the defined alarm entries:

- Sampling the defined alarm variables at a specified time interval.
- Comparing the sample values against the predefined threshold and take further actions (see Table 134).

Table 134 Handling alarm entries

Item	Handling
The sample value is greater than the upper limit *threshold-value1*.	Triggers the defined event *event-entry1*
The sample value is less than the lower limit *threshold-value2*.	Triggers the defined event *event-entry2*

Example

Create alarm group

- Configure an event before configuring "alarm" and "prialarm".

```
[SW8800]rmon event 1 log  owner 3com-rmon
```

- View configuration information.

```
[SW8800]display rmon event 1
Event table 1 owned by 3com-rmon is VALID.
  Description: null.
  Will cause log when triggered, last triggered at 1days 01h:42m:09s.
```

- Configure alarm group.

Add the first line in the alarm table. Sample the nodes 1.3.6.1.2.1.16.1.1.1.4.1 every 10 seconds. Trigger event 1 when the sampling value exceeds the upper threshold 50, and trigger event 2 when the sampling value gets below the lower threshold 5. The owner is user1.

```
<SW8800> system-view
[SW8800]rmon alarm 1 1.3.6.1.2.1.16.1.1.1.4.1 10 absolute rising_
threshold 50 1 falling_threshold 5 2 owner user1
```

Delete the information of entry 15 from the alarm table.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] undo rmon alarm 15
```

rmon event

Syntax

rmon event *event-entry* [**description** *string*] { **log** | **trap** *trap-community* | **log-trap** *log-trapcommunity* | **none** } [**owner** *text*]

undo rmon event *event-entry*

View

System view

Parameter

event-entry: Number of the entry to be added/deleted, ranging from 1 to 65535.

description *string*: Event description. Length of the character string ranges from 1 to 127.

log-trap *log-trapcommunity*: Defines the event as log and trap event, and specifies the community name of the NMS which receives the messages triggered by the event.

log: Log event.

trap *trap-community*: Defines the event as trap event, and specifies the community name of the NMS which receives the messages triggered by the event.

none: Neither log nor trap event.

owner *text*: Creator for this entry. The length of the character string ranges from 1 to 127.

Description

Use the **rmon event** command to add an entry to the event table.

Use the **undo rmon event** command to cancel an entry from this table.

RMON event management defines the event ID and the handling of the event.

You can handle the event in the following ways:

- Keeping logs
- Sending the trap messages to NMS
- Keeping logs and sending the trap messages to NMS

Example

Add the entry 10 to the event table and marks it as log event.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] rmon event 10 log
```

rmon history

Syntax

rmon history *entry-number* **buckets** *number* **interval** *sampling-interval* [**owner** *text-string*]

undo rmon history *entry-number*

View

Ethernet port view

Parameter

entry-number: Number of the entry to be added/deleted, ranging from 1 to 65,535.

buckets *number*: Capacity of the history table corresponding to the control line.

interval *sampling-interval*: Sampling interval, ranging from 5 to 3600 (measured in seconds).

owner *text-string*: Creator of this entry. Length of the character string ranges from 1 to127.

Description

Use the **rmon history** command to add an entry to the history control table.

Use the **undo rmon history** command to cancel an entry from history control table.

Perform this command to sample, set sample parameter (sample time interval) and storage amounts for a port. RMON will periodically perform data collection and save for query on this port. Sample information includes utility, error number and total packet number.

Related command: **display rmon history**.

Example

Create a history control table entry with the index number of 15, capacity of 100 and sampling interval of 10 seconds. The owner is tester.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800]interface Ethernet 2/1/1
[3Com-Ethernet2/1/1] rmon history 15 buckets 100 interval 10 owner tester
```

rmon prialarm

Syntax

rmon prialarm *entry-number prialarm-formula prialarm-des sampling-timer* { **delta** | **absolute** | **changeratio** } **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: Specifies the entry number, ranging from 1 to 65535.

prialarm-formula: Variables in the formula must be represented by OID, for example, (1.3.6.1.2.1.2.1.10.1)*8. The operation results are in long integers. Every operation result must be within the range of the long integer; otherwise, errors may be prompted.

prialarm-des : Specifies the alarm description with a length ranging from 1 to 256;

sampling-timer: Sets the sampling interval, ranging from 10 to 65535 and measured in seconds.

delta | **absolute** | **changeratio**: Specifies the sampling type as delta ratio, absolute ratio or change ratio.

threshold-value1: Rising threshold value, specified with a number greater than 0.

event-entry1: Corresponding event number to the upper limit threshold value, ranging from 0 to 65535.

threshold-value2: Falling threshold value, specified with a number greater than 0.

event-entry2: Event number corresponding to the falling threshold, ranging from 0 to 65535.

forever | **cycle** *cycle-period*: Specifies the type of the alarm instance line.

cycle-period specifies the functional cycle of the instance.

owner *text*: Creator of this entry. Length of the character string ranges from 1 to 127.

Description

Use the **rmon prialarm** command to add an entry to the extended RMON alarm table.

Use the **undo rmon prialarm** command to cancel an entry from the extended RMON alarm table.

The number of instances can be created in the table depends on the hardware resource of the product.

*Before adding an extended alarm entry, you need first to define the event to be referenced in the extended alarm entry using the **rmon event** command.*

You can define up to 50 prialarm entries.

The system takes these actions on the extended alarm entries you defined:

- Sampling the alarm variables in the defined extended alarm formula at a specified time interval.
- Calculating the sample value using the defined extended alarm formula.
- Comparing the sample values against the predefined threshold and take further actions (see Table 135).

Table 135 Handling extended alarm entries

Item	Handling
The calculated sample value is greater than the upper limit *threshold-value1*.	Triggers the defined event *event-entry1*
The calculated sample value is less than the lower limit *threshold-value2*.	Triggers the defined event *event-entry2*

Example

Add an extended alarm entry in the fifth line of the extended alarm table. Perform operation on the corresponding variant by means of the formular ((.1.3.6.1.4.1.43.45.1.6.1.2.1.1.2.1-.1.3.6.1.4.1.43.45.1.6.1.2.1.1.3.1)*100/.1.3.6.1.4.1.43.45.1.6.1.2.1.1.2.1) to get the port utilization of Gigabit Ethernet interface 1/1/1. Monitor the operation results at the sampling interval of 10 seconds. When the variation rate exceeds the upper threshold 50, trigger event 1; when the variation rate gets below the lower threshold 2, trigger event 2. Set the alarm instance sampling type to "forever", and set the owner of the extended alarm table to "user1".

```
<SW8800> system-view
[SW8800] rmon prialarm 5 ((.1.3.6.1.4.1.43.45.1.6.1.2.1.1.2.1-.1.3.6
.1.4.1.43.45.1.6.1.2.1.1.3.1)*100/.1.3.6.1.4.1.43.45.1.6.1.2.1.1.2.1
) ifUtilization.GigabitEthernet1/1/1 10 changeratio rising_threshold
 50 1 falling_threshold 5 2 entrytype forever owner user1
```

Delete line 10 from the extended RMON alarm table.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] undo rmon prialarm 10
```

rmon statistics

Syntax

rmon statistics *entry-number* [**owner** *text-string*]

undo rmon statistics *entry-number*

View

Ethernet port view

Parameter

entry-number: Number of the entry to be added/deleted, ranging from 1 to 65535.

owner *text-string*: Creator of this entry. Length of the character string ranges from 1 to127.

Description

Use the **rmon statistics** command to add an entry to the statistic table.

Use the **undo rmon statistics** command to cancel an entry from statistic table.

RMON statistic management concerns the statistics and monitoring of the usage and error on a port. Statistics includes collision, undersized or oversized packet, timeout, fragment, broadcast, multicast, unicast, and bandwidth utility.

You can use the **display rmon statistics** command to view information about statistics table entry.

Example

Add statistics of Ethernet2/1/1 to the entry 20.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800]interface Ethernet 2/1/1
[3Com-Ethernet2/1/1] rmon statistic 20
```

55 NTP CONFIGURATION COMMANDS

NTP Configuration Commands

debugging ntp-service

Syntax

debugging ntp-service { **access** | **adjustment** | **authentication** | **event** | **filter** | **packet** | **parameter** | **refclock** | **selection** | **synchronization** | **validity** | **all** }

undo debugging ntp-service { **access** | **adjustment** | **authentication** | **event** | **filter** | **packet** | **parameter** | **refclock** | **selection** | **synchronization** | **validity** | **all** }

View

User view

Parameter

access: Enables NTP access control debugging.

adjustment: Enables NTP clock adjustment debugging.

all: Enables all NTP debugging functions.

authentication: Enables NTP authentication debugging.

event: Enables NTP event debugging.

filter: Enables NTP filter information debugging.

packet: Enables NTP packet debugging.

parameter: Enables NTP clock parameter debugging.

refclock: Enables NTP reference clock debugging.

selection: Enables NTP clock selection information debugging.

synchronization: Enables NTP clock synchronization information debugging.

validity: Enables NTP remote host validity debugging.

Description

Use the **debugging ntp-service** command to debug different NTP services.

Use the **undo debugging ntp-service** command to disable corresponding debugging function.

By default, no debugging function is enabled.

Example

Enable NTP access control debugging.

```
<SW8800> debugging ntp-service access
```

display ntp-service sessions

Syntax

display ntp-service sessions [**verbose**]

View

Any view

Parameter

verbose: Specifies to display the detail information about the SESSIONS.

Description

Use the **display ntp-service sessions** command to display the status of all the SESSIONS maintained by NTP service provided by the local equipment.

By default, the status of all the SESSIONS maintained by NTP service provided by the local equipment will be displayed.

- When you configure this command without the **verbose** argument, the switch will display the brief information about all the SESSIONS it maintains.
- With the **verbose** argument configured, the switch will display the detail information about all the SESSIONS it maintains.

Example

Display status of all SESSIONS maintained by the local device NTP service.

```
<SW8800> display ntp-service sessions
source  reference   stra reach poll  now offset  delay disper
**************************************************************
[12345]127.127.1.0  LOCAL(0)    7    377   64   16    0.0    0.0    0.9
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
```

display ntp-service status

Syntax

display ntp-service status

View

Any view

Parameter

None

Description

Use the **display ntp-service status** command to display the NTP service status.

Example

Display the NTP service status.

```
<SW8800> display ntp-service status
Clock status: synchronized
 Clock stratum: 8
 Reference clock ID: 127.127.1.0
 Nominal frequency: 100.0000 Hz
 Actual frequency: 100.0000 Hz
 Clock precision: 2^18
 Clock offset: 0.0000 ms
 Root delay: 0.00 ms
 Root dispersion: 0.00 ms
 Peer dispersion: 10.00 ms
 Reference time: 09:13:32.953 UTC Feb 13 2006(C79ACC3C.F405F6BA)
```

The following table describes the outputs:

Table 136 Description on the fields of the display ntp-service status command

Field	Description
clock status: unsynchronized	Local clock status: do not synchronize to any remote NTP server.
clock stratum: 16	Indicates the NTP stratum of local clock.
reference clock ID	Indicates the address of a remote server of the reference ID, in the case that the local system has been synchronized by a remote NTP server or the ID of some clock source.
nominal frequency	Nominal frequency of the local system hardware clock
actual frequency	Actual frequency of the local system hardware clock
clock precision	Precision of local system clock
clock offset	Offset of the local clock to the NTP server clock
root delay	Root delay from local equipment to the master reference clock.
root dispersion	Dispersion of the local clock relative to the NTP server clock
peer dispersion	Dispersion of the remote NTP server
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 to display the brief information about every NTP server on the way from the local device to the reference clock source.

With this command, the system synchronizes the NTP server link from the local device along time till the reference clock source, and displays brief information about every NTP server.

Example

Display brief information about every NTP server on the way from the local device to the reference clock source.

```
<SW8800> display ntp-service trace
server 127.0.0.1,stratum 8, offset 0.000000, synch distance 0.00000
 refid 127.127.1.0
```

ntp-service access

Syntax

ntp-service access { **query** | **synchronization** | **server** | **peer** } *acl-number*

undo ntp-service access { **query** | **synchronization** | **server** | **peer** }

View

System view

Parameter

query: Allows to control query authority.

synchronization: Only allows the server to access.

server: Allows query to server and access.

peer: Full access authority.

acl-number: IP address list number.

Description

Use the **ntp-service access** command to set the authority to access the local equipment.

Use the **undo ntp-service access** command to cancel the access authority settings.

By default, there is no limit to the access.

Set authority to access the NTP services on a local Ethernet Switch. This is a basic and brief security measure, compared to authentication. An access request will be matched with **peer**, **server**, **synchronization**, and **query** in an ascending order of the limitation. The first matched authority will be given.

Example

Give the authority of time request, query control and synchronization with the local equipment to the peer in ACL 2000.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] ntp-service access peer 2000
```

Give the authority of time request and query control of the local equipment to the peer in ACL 2000.

```
[SW8800] ntp-service access synchronization 2000
```

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 the NTP-service authentication function.

Use the **undo ntp-service authentication enable** command to disable this function.

By default, the authentication is disabled.

Example

Enable NTP authentication function.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] ntp-service authentication enable
```

ntp-service authentication-keyid

Syntax

ntp-service authentication-keyid *number* **authentication-mode md5** *value*

undo ntp-service authentication-keyid *number*

View

System view

Parameter

number: Key number, ranging from 1 to 4,294,967,295.

value: Value of the key with 1 to 16 ASCII characters.

Description

Use the **ntp-service authentication-keyid** command to set NTP authentication key.

Use the **undo ntp-service authentication-keyid** command to cancel the NTP authentication key.

By default, there is no authentication key.

Only MD5 authentication is supported for the NTP authentication key settings.

Example

Set MD5 authentication key 10 as 3com.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] ntp-service authentication-keyid 10 authentication-mode md5 3com
```

ntp-service broadcast-client

Syntax

ntp-service broadcast-client

undo ntp-service broadcast-client

View

VLAN interface view

Parameter

None

Description

Use the **ntp-service broadcast-client** command to configure NTP broadcast client mode.

Use the **undo ntp-service broadcast-client** command to disable the NTP broadcast client mode.

By default, the NTP broadcast client mode is disabled.

Designate an interface on the local Ethernet Switch to receive NTP broadcast messages and operate in broadcast client mode. The local Ethernet Switch listens to the broadcast from the server. When it receives the first broadcast packet, it starts a brief Client/Server mode to switch messages with a remote server for estimating the network delay. Thereafter, the local Ethernet Switch enters Broadcast Client mode and continues listening to the broadcast and synchronizes the local clock according to the arrived broadcast message.

Example

Configure to receive NTP broadcast packets through Vlan-Interface1.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface vlan-interface1
[3Com-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

VLAN interface view

Parameter

authentication-keyid: Specifies the authentication key.

keyid: Key ID used in broadcast, ranging from 0 to 4294967295.

version: Defines NTP version number.

number: NTP version number, ranging from 1 to 3.

Description

Use the **ntp-service broadcast-server** command to configure NTP broadcast server mode.

Use the **undo ntp-service broadcast-server** command to disable the NTP broadcast server mode.

By default, the broadcast service is disabled and *number* defaults to 3.

Designate an interface on the local equipment to broadcast NTP packets. The local equipment runs in broadcast-server mode and regularly broadcasts packets to its clients.

Example

Configure to broadcast NTP packets through Vlan-Interface1, encrypt them with Key 4, and set the NTP version number as 3.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface vlan-interface1
[3Com-Vlan-interface1] ntp-service broadcast-server authentication-
key 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 SESSIONS that can be created locally, ranging from 0 to 100.

Description

Use the **ntp-service max-dynamic-sessions** command to set how many SESSIONS can be created locally.

Use the **undo ntp-service max-dynamic-sessions** command to resume the default maximum SESSIONS number

By default, a local device allows up to 100 SESSIONS.

Example

Set the local equipment to allow up to 50 SESSIONS.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] 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

VLAN interface view

Parameter

ip-address: Multicast IP address of Class D. By default, the *ip-address* argument is set to 224.0.1.1. Actually, for the Switch 8800 Family series, you can set 224.0.1.1 as the multicast IP address only.

Description

Use the **ntp-service multicast-client** command to configure the NTP multicast client mode.

Use the **undo ntp-service multicast-client** command to disable the NTP multicast client mode.

By default, the multicast client service is disabled. *ip-address* defaults to 224.0.1.1.

Designate an interface on the local Ethernet Switch to receive NTP multicast messages and operate in Multicast Client mode. The local Ethernet Switch listens to the multicast packets from the server. When it receives the first multicast packet, it starts a brief Client/Server mode to switch messages with a remote server for estimating the network delay. Thereafter, the local Ethernet Switch enters Multicast Client mode and continues listening to the multicast packets and synchronizes the local clock according to the arrived multicast packets.

Example

Configure to receive NTP multicast packet through Vlan-Interface1 and the multicast group corresponding to these packets located at 224.0.1.1.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface vlan-interface 1
[3Com-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

VLAN interface view

Parameter

ip-address: Multicast IP address of Class D. It defaults to 224.0.1.1. Actually, for the Switch 8800 Family series, you can set 224.0.1.1 as the multicast IP address only.

authentication-keyid: Specifies authentication key.

keyid: Key ID used in multicast, ranging from 1 to 4294967295.

ttl: Time to live of a multicast packet.

ttl-number: ttl of a multicast packet, ranging from 1 to 255.

version: Specifies the NTP version number.

number: NTP version number and range from 1 to 3.

Description

Use the **ntp-service multicast-server** command to configure NTP multicast server mode, if no IP address is specified, switch automatically choice the 224.0.1.1 as the multicast IP address.

Use the **undo ntp-service multicast-server** command to disable NTP multicast server mode, if no IP address is specified, the switch will disable the configuration of the multicast IP address 224.0.1.1.

By default, the multicast service is disabled. IP address defaults to 224.0.1.1 and the version number defaults to 3.

Designate an interface on the local equipment to transmit NTP multicast packet. The local equipment operates in multicast-server mode and multicasts packets regularly to its clients.

Example

Configure to transmit NTP multicast packets encrypted with Key 4 through Vlan-Interface1 at 224.0.1.1 and use NTP version 3.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] interface vlan-interface 1
[3Com-Vlan-interface1] ntp-service multicast-server 224.0.1.1
authentication-keyid 4 version 3
```

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: Specifies the reference clock IP address as 127.127.u, where u ranges from 0 to 3.

stratum: Specifies which stratum the local clock is located at and range from 1 to 15.

Description

Use the **ntp-service refclock-master** command to configure an external reference clock or the local clock as an NTP master clock.

Use the **undo ntp-service refclock-master** command to cancel the NTP master clock settings.

By default, *ip-address* is 127.127.1.0 and *stratum* defaults to 8.

You can use this command to designate an NTP external reference clock or the local clock as an NTP master clock to provide synchronized time for other equipment. *ip-address* specifies the IP address of an external clock as 127.127.u. If no IP address is specified, the local clock is set as the NTP master clock by default. You can also specify the stratum of the NTP master clock.

Example

Set the local clock as the NTP master clock to provide synchronized time for its peers and locate it at stratum 3.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] ntp-service refclock-master 3
```

ntp-service reliable authentication-keyid

Syntax

ntp-service reliable authentication-keyid *number*

undo ntp-service reliable authentication-keyid *number*

View

System view

Parameter

number: Key number, ranging from 1 to 4294967295.

Description

Use the **ntp-service reliable authentication-keyid** command to configure the key as reliable.

Use the **undo ntp-service reliable authentication-keyid** command to cancel the current setting.

By default, no key is configured as reliable.

When you enable the authentication, you can use this command to configure one or more than one keys as reliable. In this case, a Client will only get synchronized by a server whichever can provide a reliable key.

Example

Enable NTP authentication, adopt MD5 encryption, and designate Key 37 BetterKey and configure it as reliable.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] ntp-service authentication enable
[SW8800] ntp-service authentication-keyid 37 authentication-mode
md5 BetterKey
[SW8800] 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: Specifies the interface type and determine an interface with the *interface-number* argument.

interface-number: Specifies the interface number and determine an interface with the *interface-type* argument.

Description

Use the **ntp-service source-interface** command to designate an interface to transmit NTP message.

Use the **undo ntp-service source-interface** command to cancel the current setting.

By default, the source address specifies where the packets are transmitted from.

You can use this command to designate an interface to transmit all the NTP packets and take the source address of these packets from its IP address. If you do not want any other interface to receive the acknowledgement packets, use this command to specify one interface to send all the NTP packets.

Example

Configure all the outgoing NTP packets to use the IP address of Vlan-Interface1 as their source IP address.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] ntp-service source-interface Vlan-Interface 1
```

ntp-service unicast-peer

Syntax

ntp-service unicast-peer *ip-address* [**version** *number*] [**authentication-keyid** *keyid*] [**source-interface** *interface-type interface-number*] [**priority**]*

undo ntp-service unicast-peer *ip-address*

View

System view

Parameter

ip-address: IP address of a remote server.

version: Defines NTP version number.

number: NTP version number, ranging from 1 to 3.

authentication-keyid: Defines authentication key.

keyid: Key ID used for transmitting messages to a remote server, ranging from 1 to 4294967295.

source-interface: Specifies the name of an interface, the interface can be VLAN interface and Loopback interface currently.

interface-type: Specifies the interface type and determine an interface together with the *interface-number* argument.

interface-number: Specifies the interface number and determine an interface together with the *interface-type* argument.

interface-type interface-number specifies from which interface to obtain the source IP address carried in the packet sent by the local switch to the peer. Currently, only VLAN interfaces and Loopback interfaces are supported.

priority: Designates a server as the first choice.

Description

Use the **ntp-service unicast-peer** command to configure NTP peer mode.

Use the **undo ntp-service unicast-peer** command to cancel NTP peer mode.

By default, version number *number* defaults to 3, the authentication is disabled, and the local server is not the first choice.

This command sets the remote server at *ip-address* as a peer of the local equipment, which operates in symmetric active mode. *ip-address* specifies a host address other than an IP address of broadcast, multicast, or reference clock. By operating in this mode, a local device can synchronize and be synchronized by a remote server.

Example

Configure the local equipment to synchronize or synchronized by a peer at 128.108.22.44. Set the NTP version to 3. The IP address of the NTP packets are taken from that of Vlan-Interface1.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] ntp-service unicast-peer 131.108.22.33 version 3 source-
interface Vlan-Interface 1
```

ntp-service unicast-server

Syntax

ntp-service unicast-server *ip-address* [**version** *number*] [**authentication-keyid** *keyid*] [**source-interface** *interface-type interface-number*] [**priority**]*

undo ntp-service unicast-server *ip-address*

View

System view

Parameter

ip-address: IP address of a remote server.

version: Defines NTP version number.

number: NTP version number, ranging from 1 to 3.

authentication-keyid: Defines authentication key.

keyid: Key ID used for transmitting messages to a remote server, ranging from 1 to 4294967295.

source-interface: Specifies the name of an interface, the interface can be VLAN interface and Loopback interface.

interface-type: Specifies the interface type and determine an interface together with the *interface-number* argument.

interface-number: Specifies the interface number and determine an interface together with the *interface-type* argument.

When the local switch sends an NTP packet to the timer server, the source IP address carried in the packet is obtained from the interface. Currently, only VLAN interfaces and Loopback interfaces are supported.

priority: Designates a server as the first choice.

Description

Use the **ntp-service unicast-server** command to configure NTP server mode.

Use the **undo ntp-service unicast-server** command to disable NTP server mode.

By default, version number *number* defaults to 3, the authentication is disabled, and the local server is not the first choice.

The command announces to use the remote server at *ip-address* as the local time server. *ip-address* specifies a host address other than an IP address of broadcast, multicast, or reference clock. By operating in client mode, a local device can be synchronized by a remote server, but not synchronize any remote server.

Example

Designate the server at 128.108.22.44 to synchronize the local device and use NTP version 3.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] ntp-service unicast-server 128.108.22.44 version 3
```

56 SSH TERMINAL SERVICE CONFIGURATION COMMANDS

SSH Server Configuration Commands

debugging ssh server

Syntax

debugging ssh server { **VTY** *index* | **all** }

undo debugging ssh server { **VTY** *index* | **all** }

View

User view

Parameter

index: SSH channel to be debugged, whose value is dictated by VTY numbers. The default VTY numbers are 0 to 4.

all: Specifies all the SSH channels.

Description

Use the **debugging ssh server** command to send information regulated by the SSH2.0 protocol, such as the negotiation procedure, to the information center in the format of Debugging information. You can also use it to debug a user interface individually.

Use the **undo debugging ssh server** command to disable the debugging.

By default, the debugging is disabled.

Logs related to the SSH server are recorded into the log file or log buffer only if debugging is enabled.

Related command: **ssh server authentication-retries**, **ssh server rekey-interval**, **ssh server timeout**.

Example

Print the Debugging information when the SSH is running.

```
<SW8800> debugging ssh server vty 0
*0.1426091 8505A SSH/8/debugging_msg_send:SSH_VERSION_SEND message
sent on VTY 0
*0.1426188 8505A SSH/8/SSH2 debug:debug info:The server's ssh
version sent SSH-1
.99-Comware-3.3
```

```
*0.1426299 8505A SSH/8/msg_rcv_vty:SSH_VERSION_RECEIVE message
received on VTY 0
*0.1426995 8505A SSH/8/SSH2 debug:debug info:Now the server
version is ssh2
*0.1427088 8505A SSH/8/SSH2 debug:debug info: The algorithm
negotiation begins
*0.1427190 8505A SSH/8/SSH2 debug:debug info:SSH2_MSG_KEXINIT sent
*0.1427269 8505A SSH/8/SSH2 debug:debug info: SSH2_MSG_KEXINIT
received
*0.1427360 8505A SSH/8/SSH2 debug:debug info:kex: client->server
des-cbc hmac-sh
a1
*0.1427461 8505A SSH/8/SSH2 debug:debug info:kex: server->client
des-cbc hmac-sh
a1
*0.1427562 8505A SSH/8/SSH2 debug:debug info:The key exchange
algorithm is diffi
e-hellman-group1-sha1
*0.1427695 8505A SSH/8/SSH2 debug:debug info: The algorithm choose
is done
*0.1427784 8505A SSH/8/SSH2 debug:debug info:SSH2_MSG_KEXDH_INIT
received
*0.1427875 8505A SSH/8/SSH2 debug:debug info:SSH2_MSG_KEXDH_REPLY
sent
*0.1427966 8505A SSH/8/SSH2 debug:debug info:SSH2_MSG_NEWKEYS  sent
*0.1428047 8505A SSH/8/SSH2 debug:debug info:SSH2_MSG_NEWKEYS
received
*0.1428138 8505A SSH/8/SSH2 debug:debug info:The key exchange is
done
*0.1428229 8505A SSH/8/SSH2 debug:debug info:User authentication
begins
*0.1428320 8505A SSH/8/SSH2 debug:debug info:SSH2_MSG_SERVICE_
REQUEST received
*0.1428421 8505A SSH/8/SSH2 debug:debug info:SSH2_MSG_SERVICE_
ACCEPT sent
*0.1428513 8505A SSH/8/SSH2 debug:debug info:SSH2_MSG_USERAUTH_
REQUEST received
with user:admin,service:ssh-connection,metho
d:none
```

display rsa local-key-pair public

Syntax

display rsa local-key-pair public

View

Any view

Parameter

None

Description

Use the **display rsa local-key-pair public** command to display the public key of the server's host key pair and server key pair.

Related command: **rsa local-key-pair create**.

Example

Display the public key of the server's host key pair and server key pair.

```
<SW8800> display rsa local-key-pair public
% Key pair was generated at: 12:26:33 UTC 2002/4/4
 Key name: rtvrp_Host
 Usage: Encryption Key
 Key Data:
30470240 AF7DB1D0 DA78944F 53B7B59B 40D425D0 DC9C57D2 A60916C2
1F165807 08B84DDB 5F4DB8E7 A115B74E 2D41D96C AC61D276 AA027E41
DD48DE64 696E0934 EB872805 02030100 01
% Key pair was generated at: 12:26:45 UTC 2002/4/4
 Key name: rtvrp_Server
 Usage: Encryption Key
 Key Data:
30670260 C05280D9 BA0D56C8 7BE43379 8634CDE7 83ABA9A2 3F36280E
25995487 4FF6AD7A 0E57871C 761E6D92 9914D8C5 CC577388 5B580B94
C2172C8F 36039EED 160A0478 651DED3A 9CCF1AAD D800AAF2 DF7FBEC4
A13ADA59 9E738319 AF366B8B 519D39F5 02030100 01
```

display rsa peer-public-key

Syntax

display rsa peer-public-key [**brief** | **name** *keyname*]

View

Any view

Parameter

brief: Displays the brief information about all client public keys.

keyname: Public key name of the client to be displayed. The key name is a consecutive string whose length ranges from 1 to 64 characters.

Description

Use the **display rsa peer-public-key** command to display the public key of RSA key pair specified by the client. If you do not specify the *keyname* argument, all public keys will be displayed.

Related command: **rsa local-key-pair create**.

Example

Display the public key of the specified RSA key pair of the client.

```
<SW8800> display rsa peer-public-key brief
Address        Bits   Name
               1023   abcd
               1024   hq
               1024   wn1
               1024   hq_all
```

Display the public key of the specified RSA key pair named abcd of the client.

```
<SW8800> display rsa peer-public-key name 127.0.0.1
=====================================
    Key name: 127.0.0.1
    Key address:
```

```
=====================================
Key Code:
308188
  028180
    CFC6A68B 39F742A2 76E55B07 39D60B73 D7B4040D 515B2516 17CE9380
53829FF5
    C0489BD9 559CC425 CAF37E6F E6417337 693DF5CD 02F12469 420BBD5C
38741295
    D74B2336 A5F28FE8 00E0429F FCF47A7F AEF0A1B9 740FC2BE 99F26F35
39C8867D
    FAE8C2A1 EAC4CB42 A64982C9 4BA1DD63 49619762 E46F17DF ED1C1ACC
DFAB8CB5
  0203
    010001
```

display ssh server

Syntax

display ssh server { **status** | **session** }

View

Any view

Parameter

status: Displays the SSH status information.

session: Displays the SSH session information.

Description

Use the **display ssh server** command to display the status information or session information of an SSH server.

Related command: **ssh server authentication-retries**, **ssh server rekey-interval**, **ssh server timeout**.

Example

Display the status information of the SSH server.

```
<SW8800> display ssh server status
SSH - version 2.0
SSH connection timeout: 60 seconds
SSH Authentication retries: 3 times
SFTP Server: Disable
```

Display the session information of the SSH server.

```
[SW8800] display ssh server session
Connection Version Encryption     State              Username
VTY0         2.0       3DES    Session started         3Com
VTY3         1.5       DES     Session started         switch
```

display ssh user-information

Syntax

display ssh user-information [*username*]

View

Any view

Parameter

username: Valid SSH username.

Description

Use the **display ssh user-information** command to display information about the current SSH user, including username, peer key name, authentication mode and the types of authorized services. If you specify the argument *username* in the command, the user information about the specified username will be displayed.

Related command: **ssh user username assign rsa-key**, **ssh user username authentication-type**, **ssh user username service-type**, **display local-user**, **display rsa peer-public-key**.

Example

Display the current SSH user information.

```
<SW8800> display ssh user-information
Username            Authentication-type  User-public-key-name  Service-type
 sshuser2            rsa                  sshuser2              stelnet
 sshuser1            password             sshuser1              stelnet
```

If the Username and User-key-name are too long, the result of the **dispaly ssh user-information** is displayed with wildcard " **...**". An example is given below:

Display current SSH user information.

```
<SW8800> display ssh user-information
Username            Authentication-type  User-public-key-name  Service-type
admin               password             aaaaaaaaaabbbbbbb...  sftp
aaaaaaaaaabbbbbb... all                  aaaaaaaaaabbbbbbb...  stelnet
fxdfxdfxdfxdfxdf... null                 null                  stelnet|sftp
```

You can use the **display local-user** command and the **display rsa peer-public-key** command respectively to view Username and User-public-key-name which are too long.

peer-public-key end

Syntax

peer-public-key end

View

Public key view

Parameter

None

Description

Use the **peer-public-key end** command to exit the public key view and return to the system view.

Related command: **rsa peer-public-key**, **public-key-code begin**.

Example

Exit the public key view and save the configuration.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] rsa peer-public-key sw8800003
RSA public key view: return to System View with "peer-public-key end".
[3Com-rsa-public-key] peer-public-key end
[SW8800]
```

protocol inbound

Syntax

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

View

VTY user interface view

Parameter

all: Supports all protocols, including Telnet and SSH.

ssh: Supports the SSH protocol only, and does not support the Telnet protocol.

telnet: Supports the Telnet protocol only, and does not support the SSH protocol.

Description

Use the **protocol inbound** command to specify the protocol supported by the current user interface.

By default, all protocols are supported.

This configuration takes effect at the next login. Note that after enabling SSH by this command, you still cannot log in through SSH if the client RSA key is not configured.

CAUTION:

- If the supported protocol configured in the user interface is SSH, make sure to configure the corresponding authentication mode to **authentication-mode scheme** (using AAA authentication mode).
- If the authentication mode is configured as **authentication-mode password** or **authentication-mode none**, the configuration of **protocol inbound ssh** will fail; contrarily, if a user interface is configured to support the SSH protocol, you will fail to configure **authentication-mode password** and **authentication-mode none**.

Related command: **user-interface vty**.

Example

Set VTY 0 to 4 to support the SSH protocol only.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] user-interface vty 0 4
[3Com-ui-vty0-4] protocol inbound ssh
```

Disable the Telnet function of VTY 0 and make it support SSH only.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] user-interface vty 0
[3Com-ui-vty0] protocol inbound ssh
```

public-key-code begin

Syntax

public-key-code begin

View

Public key view

Parameter

None

Description

Use the **public-key-code begin** command to enter the public key edit view and input the public key of the client. Note that you must use the **rsa peer-public-key** command to specify a client key name before performing this command.

When inputting the public key, you may type spaces between the characters (the system will delete the spaces automatically), or press <Enter> and then continue to input the key. Note that the public key must be a hexadecimal string coded in the public key format and is randomly generated by the SSH 2.0-enabled client software or the client switch.

Related command: **rsa peer-public-key**, **public-key-code end**.

Example

Enter the public key edit view and input the key.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] rsa peer-public-key sw8800003
[3Com-rsa-public-key] public-key-code begin
RSA key code view: return to last view with "public-key-code end".
[3Com-key-code] 308186028180739A291ABDA704F5D93DC8FDF84C427463
[3Com-key-code] 1991C164B0DF178C55FA833591C7D47D5381D09CE82913
[3Com-key-code] D7EDF9C08511D83CA4ED2B30B809808EB0D1F52D045DE4
[3Com-key-code] 0861B74A0E135523CCD74CAC61F8E58C452B2F3F2DA0DC
[3Com-key-code] C48E3306367FE187BDD944018B3B69F3CBB0A573202C16
[3Com-key-code] BB2FC1ACF3EC8F828D55A36F1CDDC4BB45504F020125
[3Com-key-code] public-key-code end
[3Com-rsa-public-key]
```

public-key-code end

Syntax

public-key-code end

View

Public key edit view

Parameter

None

Description

Use the **public-key-code end** command to return from the public key edit view to the public key view and save the public key entered.

After this command is performed to end the public key edit procedure, the system will check the validity of the key before saving the input public key. If the public key string contains any illegal character, the system will prompt the failure of the configuration and the configured key will be discarded; otherwise, the key is valid and will be saved to the user public keys in the system.

Related command: **rsa peer-public-key**, **public-key-code begin**.

Example

Exit the public key edit view and save the configured public key.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] rsa peer-public-key sw8800003
[3Com-rsa-public-key] public-key-code begin
RSA key code view: return to last view with "public-key-code end".
[3Com-rsa-key-code] public-key-code end
[3Com-rsa-public-key]
```

rsa local-key-pair create

Syntax

rsa local-key-pair create

View

System view

Parameter

None

Description

Use the **rsa local-key-pair create** command to generate the RSA key pair (including the host key and server key) of the server. The naming conventions for the keys are *switch name* + *host* and *switch name* + *server* respectively, for example, 3Com_host, 3Com_server.

When configuring by this command, if the RSA key pair already exists, you will get a warning asking if you want to replace the existing one. Note that the host key and the server key must have a difference of 128 bits at least, and that the minimum and maximum lengths for the host key and the server key are 512 bits and 2048 bits .

Generating the RSA key pair of the server is the first step to perform after SSH login. It needs to be performed only once; you need not re-perform it after rebooting the switch.

CAUTION: *When you log in through SSH user, the key generated by the server must be longer than 768 bits. The RSA key genetated by the server is 1,024 bits by default.*

Related command: **rsa local-key-pair destroy**.

Example

Generate the local RSA key pair.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] rsa local-key-pair create
The name for the keys will be: rtvrp_Host
% You already have RSA keys defined for rtvrp_Host
% Do you really want to replace them? [yes/no]:y
Choose the size of the key modulus in the range of 512 to 2048 for your Keys.
Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus [512]:512
Generating keys...
.....++++++++++++
.....++++++++++++
.........++++++++
.........++++++++
```

rsa local-key-pair destroy

Syntax

rsa local-key-pair destroy

View

System view

Parameter

None

Description

Use the **rsa local-key-pair destroy** command to destroy all the RSA key pairs of the server, including the host keys and server keys.

Related command: **rsa local-key-pair create**.

Example

Destroy all the RSA keys of the server.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] rsa local-key-pair destroy
% Keys to be removed are named rtvrp_Host .
% Do you really want to remove these keys? [yes/no]:y
```

rsa peer-public-key

Syntax

rsa peer-public-key *key-name*

View

System view

Parameter

key-name: Name of the public key of the client. It is a consecutive string whose length ranges from 1 to 64 characters.

Description

Use the **rsa peer-public-key** command to enter the public key view.

Performing this command, you can enter the public key view. Then you can use the **public-key-code begin** command to configure the client public key on the server. The client public key is generated randomly by the SSH 2.0-enabled client software.

Related command: **public-key-code begin**, **public-key-code end**.

Example

Enter the public key view named sw8800002.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] rsa peer-public-key sw8800002
[3Com-rsa-public-key]
```

ssh server authentication-retries

Syntax

ssh server authentication-retries *times*

undo ssh server authentication-retries

View

System view

Parameter

times: Number of authentication retries, in the range from 1 to 5. By default, the value is 3.

Description

Use the **ssh server authentication-retries** command to set the number of SSH connection authentication retries.

Use the **ssh server authentication-retries** command to restore the default number of SSH connection authentication retries.

Related command: **display ssh server**.

Example

Specify the number of login authentication retries as 4.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] ssh server authentication-retries 4
```

ssh server compatible_ssh1x enable

Syntax

ssh server compatible_ssh1x enable

undo ssh server compatible_ssh1x

View

System view

Parameter

None

Description

Use the **ssh server compatible_ssh1x enable** command to make the server compatible with the SSH 1.x client.

Use the **undo ssh server compatible_ssh1x** command to make the server not compatible with an SSH 1.x client.

By default, the server is compatible with the SSH 1.x client.

Example

Set the server to be compatible with the SSH 1.x client.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] ssh server compatible_ssh1x enable
```

ssh server rekey-interval

Syntax

ssh server rekey-interval *hours*

undo ssh server rekey-interval

View

System view

Parameter

hours: Update interval of the server key, in range of 1 to 24 (hours). It cannot be 0.

Description

Use the **ssh server rekey-interval** command to set update interval of the server key.

Use the **undo ssh server rekey-interval** command to remove the configuration.

By default, the system does not update the server key.

Related command: **display ssh server**

Example

Set to update the server key every three hours.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] ssh server rekey-interval 3
```

ssh server timeout

Syntax

ssh server timeout *seconds*

undo ssh server timeout

View

System view

Parameter

seconds: Login timeout (in seconds), in the range from 1 to 120. By default, the value is 60.

Description

Use the **ssh server timeout** command to set the authentication timeout of SSH connections.

Use the **undo ssh server timeout** command to restore the default SSH authentication timeout.

The configuration takes effect at the next login.

Related command: **display ssh server**.

Example

Set the login timeout to 80 seconds.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] ssh server timeout 80
```

ssh user assign rsa-key

Syntax

ssh user *username* **assign rsa-key** *keyname*

undo ssh user *username* **assign rsa-key**

View

System view

Parameter

keyname: Name of the client public key. It is a consecutive string whose length ranges from 1 to 64 characters.

username: Valid SSH username. It is a consecutive string whose length ranges from 1 to 80 characters.

Description

Use the **ssh user assign rsa-key** command to assign an existing public key for the specified SSH user.

Use the **undo ssh user assign rsa-key** command to cancel the corresponding relationship between the user and the public key.

The new public key takes effect at the next login.

If a public key already exists before this command is performed, the newly configured key takes effect.

Related command: **display ssh user-information**.

Example

Assign public key1 for user zhangsan.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] ssh user zhangsan 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**

View

System view

Parameter

password: Forces the user's authentication mode to password authentication.

rsa: Forces the user's authentication mode to RSA public key authentication.

password-publickey: Forces the user's authentication mode to password authentication plus RSA public key authentication.

all: Specifies that the user's authentication mode can be either password authentication or public authentication.

Description

Use the **ssh user authentication-type** command to specify an authentication mode for a user.

Use the **undo ssh user authentication-type** command to restore the user authentication mode to NULL, namely, the unable-to-login mode.

The new authentication mode takes effect at the next login.

By default, no login authentication mode is specified, that is, SSH users are unable to login.

For a new user, you must specify an authentication mode; otherwise, the new user will not be able to log in.

Related command: **display ssh user-information**.

Example

Specify the authentication mode of user zhangsan to password authentication.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] ssh user zhangsan authentication-type password
```

ssh authentication-type default

Syntax

ssh authentication-type default { **password** | **rsa** | **all** | **password-publickey** }

undo ssh authentication-type default

View

System view

Parameter

password: Configures the default user authentication mode as password authentication.

rsa: Configures the default user authentication mode as RSA public key authentication.

all: Specifies that the default user authentication mode can be either password authentication or public key authentication.

password-publickey: Configures the default user authentication mode as a combination of password authentication and public key authentication.

Description

Use the **ssh authentication-type default** command to configure the default authentication mode for SSH users.

Use the **undo ssh authentication-type default** command to cancel the default authentication mode for SSH users.

The default authentication mode is NULL, which means that an authentication mode needs to be configured for each SSH user.

Example

Configure the default user authentication mode as password authentication.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] ssh authentication-type default password
```

SSH Client Configuration Commands

display ssh server-info

Syntax

display ssh server-info

View

Any view

Parameter

None

Description

Use the **display ssh server-info** command to view the corresponding relationship between the client's servers and public keys.

Example

Display the corresponding relationship between the client's servers and public keys.

```
<SW8800> display ssh server-info
ServerIP  public-key-name
192.168.0.1    3com_key01
192.168.0.2    3com_key02
```

quit

Syntax

quit

View

User view

Parameter

None

Description

Use the **quit** command to terminate the connection with the remote SSH server.

Example

Terminate the connection with the remote SSH server.

```
<SW8800> quit
```

ssh client assign rsa-key

Syntax

ssh client *server-ip* **assign rsa-key** *keyname*

undo ssh client *server-ip* **assign rsa-key**

View

System view

Parameter

server-ip: IP address of the server.

keyname: Public key name of the client.

Description

Use the **ssh client assign rsa-key** command to specify the IP address and the corresponding public key name of the server on the client.

Use the **undo ssh client assign rsa-key** command to cancel the configuration.

Example

Specify the public key of a server with IP address 192.168.0.1 on the client as serverkey01.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] ssh client 192.168.0.1 assign rsa-key serverkey01
```

ssh client first-time enable

Syntax

ssh client first-time enable

undo client ssh first-time

View

System view

Parameter

None

Description

Use the **ssh client first-time enable** command to set the SSH client to perform the first-time authentication of the SSH server to be accessed.

Use the **undo ssh client first-time** command to cancel the first-time authentication.

The first-time authentication means that when the SSH client accesses the server for the first time in the case that there is no local copy of the server's public key, the user can proceed to access the server and save a local copy of the server's public key; when the client accesses the server next time, it uses the saved public key to authenticate the server.

If the first-time authentication is not supported, when there is no local copy of the public key of the connected server, the client assumes that the server is illegal and will refuse to access the server. The user can save a copy of the server's public key locally by other means beforehand.

By default, the client does not perform the first-time authentication.

Example

Set the SSH client to perform the first-time authentication of the SSH server to be accessed.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] ssh client first-time enable
```

ssh2

Syntax

ssh2 { *host-ip* | *host-name* } [*port-num*] [**prefer_kex** { **dh_group1** | **dh_exchange_group** }] [**prefer_ctos_cipher** { **des** | **3des** | **aes128** }] [**prefer_stoc_cipher** { **des** | **3des** | **aes128** }] [**prefer_ctos_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }] [**prefer_stoc_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }]

View

System view

Parameter

host-ip: IP address of the server.

host-name: Server name, a string with 1 to 30 characters.

port-num: Server port number, ranges from 0 to 65535, and defaults to 22.

prefer_kex: Preferred key exchange algorithm, which can be one of the two algorithms.

dh_group1: Key exchange algorithm diffie-hellman-group1-sha1, which is the default algorithm.

dh_exchange_group: Key exchange algorithm diffie-hellman-group-exchange-sha1.

prefer_ctos_cipher: Preferred encryption algorithm from the client to the server. The default algorithm is aes128.

prefer_stoc_cipher: Preferred encryption algorithm from the server to the client. The default algorithm is aes128.

des: Encryption algorithm des_cbc.

3des: Encryption algorithm 3des_cbc.

aes128: Encryption algorithm aes_128.

prefer_ctos_hmac: Preferred HMAC algorithm from the client to the server. The default algorithm is sha1_96.

prefer_stoc_hmac: Preferred HMAC algorithm from the server to the client. The default algorithm is sha1_96.

sha1: HMAC algorithm hmac-sha1.

sha1_96: HMAC algorithm hmac-sha1-96.

md5: HMAC algorithm hmac-md5.

md5_96: HMAC algorithm hmac-md5-96.

Description

Use the **ssh2** command to enable the connection between the SSH client and the server, and specify the preferred key exchange algorithm, encryption algorithm and HMAC algorithm of the client and the server.

Example

Log in to remote SSH2 server with IP address 10.214.50.51, and configure encryption algorithms as follows:

- Preferred key exchange algorithm: dh_exchange_group
- Preferred encryption algorithm from the client to the server: 3DES-CBC
- Preferred HMAC algorithm from the client to the server: HMAC-MD5
- Preferred encryption algorithm from the server to the client: AES-128
- Preferred HMAC algorithm from the server to the client: HMAC-SHA1-96

The command is as follows:

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] ssh2 10.214.50.51 prefer_kex dh_exchange_group prefer_ctos_
cipher 3des prefer_ctos_hmac md5
```

SFTP Server Configuration Commands

sftp server enable

Syntax

sftp server enable

undo sftp server

View

System view

Parameter

None

Description

Use the **sftp server enable** command to start the SFTP server.

Use the **undo sftp server enable** command to shutdown the SFTP server.

By default, the SFTP server is shutdown.

Example

Start the SFTP server.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] sftp server enable
```

Shutdown the SFTP server.

```
[SW8800] undo sftp server
```

ssh service-type default

Syntax

ssh service-type default { **all** [**sftp-directory** *directory*] | **sftp** [**sftp-directory** *directory*] | **stelnet** }

undo ssh service-type default

View

System view

Parameter

all: Specifies that the default service type can be either Stelnet or SFTP.

sftp: Configures the default service type as SFTP.

stelnet: Configures the default service type as Stelnet.

sftp-directory *directory*: Configures the default directory an SFTP user logs in to.

Description

Use the **ssh service-type default** command to configure the default service type and the default directory for SFTP users.

Use the **undo ssh service-type default** command to cancel the default service type and the default directory for SFTP users.

The default service type is NULL and the default directory for SFTP users is NULL.

Example

Configure the default service type as SFTP and specify cf: as the default directory.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] ssh service-type default sftp sftp-directory cf:
```

ssh user service-type

Syntax

ssh service-type default { **all** [**sftp-directory** *directory*] | **sftp** [**sftp-directory** *directory*] | **stelnet** }

undo ssh service-type default

View

System view

Parameter

all: Specifies that the default service type can be either Stelnet or SFTP.

sftp: Configures the default service type as SFTP.

stelnet: Configures the default service type as Stelnet.

sftp-directory *directory*: Configures the default directory an SFTP user logs in to.

Description

Use the **ssh service-type default** command to configure the default service type and the default directory for SFTP users.

Use the **undo ssh service-type default** command to cancel the default service type and the default directory for SFTP users.

The default service type is NULL and the default directory for SFTP users is NULL.

Example

Configure the default service type as SFTP and specifies cf: as the default directory.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] ssh service-type default sftp sftp-directory cf:
```

SFTP Client Configuration Commands

bye

Syntax

bye

View

SFTP Client view

Parameter

None

Description

Use the **bye** command to terminate the connection with the remote SFTP server and return to the user view.

This command has the same functionality as the **exit** and **quit** commands.

Example

Terminate the connection with the remote SFTP server.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
sftp-client> bye
<SW8800>
```

cd

Syntax

cd [*remote-path*]

View

SFTP Client view

Parameter

remote-path: Name of a path on the server.

Description

Use the **cd** command to change the current path on the SFTP server. If you do not specify the *remote-path* argument, the current path will be displayed.

Example

Change the current path to d:/temp.

```
sftp-client> cd d:/temp
```

cdup

Syntax

cdup

View

SFTP Client view

Parameter

None

Description

Use the **cdup** command to change the current path to its upper directory.

Example

Change the current path to its upper directory.

```
sftp-client> cdup
```

delete

Syntax

delete *remote-file*

View

SFTP Client view

Parameter

remote-file: Name of a file on the server.

Description

Use the **delete** command to delete the specified file from the server.

This command has the same functionality as the **remove** command.

Example

Delete file temp.c from the server.

```
sftp-client> delete temp.c
```

dir

Syntax

dir [*remote-path*]

View

SFTP Client view

Parameter

remote-path: Name of the directory to view.

Description

Use the **dir** command to view the files in the specified directory.

If the *remote-path* argument is not specified, the files in the current directory will be displayed.

This command has the same functionality as the **ls** command.

Example

View directory flash:/

```
sftp-client> dir flash:/
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 vrpcfg.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

Syntax

exit

View

SFTP Client view

Parameter

None

Description

Use the **exit** command to terminate the connection with the remote SFTP server and return to the user view.

This command has the same functionality as the **bye** and **quit** commands.

Example

Terminate the connection with the remote SFTP server.

```
sftp-client> exit
<SW8800>
```

get

Syntax

get *remote-file* [*local-file*]

View

SFTP Client view

Parameter

remote-file: Name of a file on the remote SFTP server.

local-file: Name of a local file.

Description

Use the **get** command to download a file from the remote server and save it locally.

By default, if no local file name is specified, it is assumed that the local file has the same name as the file on the SFTP server.

Example

Download file temp1.c and save it with name temp.c.

```
sftp-client> get temp1.c temp.c
```

help **Syntax**

help [*command*]

View

SFTP Client view

Parameter

command: Name of a command.

Description

Use the **help** command to view the help information for SFTP client commands.

If the *command* argument is not specified, all command names will be displayed.

Example

View the help information for the **get** command.

```
sftp-client> help get
get remote-path [local-path]  Download file
Default local-path is the same with remote-path
```

ls **Syntax**

ls [*remote-path*]

View

SFTP Client view

Parameter

remote-path: Name of the directory to view.

Description

Use the **ls** command to view the files in the specified directory.

If the *remote-path* argument is not specified, the files in the current directory will be displayed.

This command has the same functionality as the **dir** command.

Example

View directory flash:/.

```
sftp-client> ls flash:/
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 vrpcfg.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

Syntax

mkdir *remote-path*

View

SFTP Client view

Parameter

remote-path: Name of a directory on the remote SFTP server.

Description

Use the **mkdir** command to create a directory on the remote SFTP server.

Example

Create directory test on the remote SFTP server.

```
sftp-client> mkdir test
```

put

Syntax

put *local-file* [*remote-file*]

View

SFTP Client view

Parameter

local-file: Name of a local file.

remote-file: Name of a file on the remote SFTP server.

Description

Use the **put** command to upload a local file to the remote SFTP server.

By default, if no name of the file on the remote server is specified, it is assumed that the file on the remote server has the same name as the local file.

Example

Upload local file temp.c to the remote SFTP server and save it with the name temp1.c.

```
sftp-client> put temp.c temp1.c
```

pwd

Syntax

pwd

View

SFTP Client view

Parameter

None

Description

Use the **pwd** command to display the current directory on the SFTP server.

Example

Display the current directory on the SFTP server.

```
sftp-client> pwd
flash:
```

quit **Syntax**

quit

View

SFTP Client view

Parameter

None

Description

Use the **quit** command to terminate the connection with the remote SFTP server and return to the user view.

This command has the same functionality as the **bye** and **exit** commands.

Example

Terminate the connection with the remote SFTP server.

```
sftp-client> quit
<SW8800>
```

remove **Syntax**

remove *remote-file*

View

SFTP Client view

Parameter

remote-file: Name of a file on the server.

Description

Use the **remove** command to delete the specified file from the server.

This command has the same functionality as the **delete** command.

Example

Delete the file temp.c from the server.

```
sftp-client> delete temp.c
```

rename **Syntax**

rename *oldname newname*

View

SFTP Client view

Parameter

oldname: Original file name.

newname: New file name.

Description

Use the **rename** command to change the name of the specified file on the SFTP server.

Example

Change the name of the file temp1 on the SFTP server to temp2.

```
sftp-client> rename temp1 temp2
```

rmdir

Syntax

rmdir *remote-path*

View

SFTP Client view

Parameter

remote-path: Name of a directory on the remote SFTP server.

Description

Use the **rmdir** command to delete the specified directory from the SFTP server.

Example

Delete the directory D:/temp1 from the SFTP server.

```
sftp-client> rmdir D:/temp1
```

sftp

Syntax

sftp *ipaddr* [**prefer_kex** { **dh_group1** | **dh_exchange_group** }] [**prefer_ctos_cipher** { **des** | **3des** | **aes128** }] [**prefer_stoc_cipher** { **des** | **3des** | **aes128** }] [**prefer_ctos_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }] [**prefer_stoc_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }]

View

System view

Parameter

ipaddr: IP address of the server.

prefer_key: Preferred key exchange algorithm, which can be either diffie-hellman-group1-sha1 or diffie-hellman-group-exchange-sha1.

dh_group1: Key exchange algorithm diffie-hellman-group1-sha1, which is default algorithm.

dh_exchange_group: Key exchange algorithm diffie-hellman-group-exchange-sha1.

prefer_ctos_cipher: Preferred encryption algorithm from the client to the server. The default algorithm is aes128.

prefer_stoc_cipher: Preferred encryption algorithm from the server to the client. The default algorithm is aes128.

des: Encryption algorithm des_cbc.

3des: Encryption algorithm 3des_cbc.

aes128: Encryption algorithm aes_128.

prefer_ctos_hmac: Preferred HMAC algorithm from the client to the server. The default algorithm is sha1_96.

prefer_stoc_hmac: Preferred HMAC algorithm from the server to the client. The default algorithm is sha1_96.

sha1: HMAC algorithm hmac-sha1.

sha1_96: HMAC algorithm hmac-sha1-96.

md5: HMAC algorithm hmac-md5.

md5_96: HMAC algorithm hmac-md5-96.

Description

Use the **sftp** command to establish the connection with the remote SFTP server and enter the SFTP Client view.

Example

Connect to the SFTP server with IP address 10.214.49.126 using the default encryption algorithm.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] sftp 10.214.49.126
```

57 FILE SYSTEM MANAGEMENT COMMANDS

File System

The limitation on the names of directories and files on switch are as follows:

- It is recommended that the name of a directory or file should not contain more than 64 characters; otherwise you will not be able to delete such a directory or file, even though the system supports directory or file names containing more than 64 characters.
- The total number of characters including device, single directory and file names can be up to 136 characters long.

cd

Syntax

cd *directory*

View

User view

Parameter

directory: Destination directory; By default, the directory is the working path configured by the user when the system starts.

Description

Use the **cd** command to change the current user configuration path on the Switch.

The default directory is the user startup configuration path.

Example

Change the current working directory of the switch to flash.

```
<SW8800> cd flash:
<SW8800> pwd
flash:
```

copy

Syntax

copy *fileurl-source fileurl-dest*

View

User view

Parameter

fileurl-source: Source file name.

fileurl-dest: Destination file name.

Description

Use the **copy** command to copy a file.

You can use this command to copy a file from current directory to another directory, or vise versa. Where, the source filename must be the name of a file that has already existed in the specified directory, and the destination filename can be changed as required. When the destination filename is the same as that of an existing file, the system will ask whether to overwrite it.

Example

Copy the file test.txt and saves it as test.bak.

```
<SW8800> copy test.txt test.bak
Copy flash:/test/test.txt to flash:/test/test.bak ? [Y/N]:
% Copyed file flash:/test/test.txt flash:/test/test.bak
```

delete

Syntax

delete [**/unreserved**] *file-url*

View

User view

Parameter

/unreserved: Delete the file completely.

file-url: Path and name of the file you want to delete.

Description

Use the **delete** command to cancel a specified file from the storage device of the switch.

This command supports wildcard characters. The deleted files are kept in the recycle bin and will not be displayed when you use the **dir** command. However they will be displayed, using the **dir /all** command. The files deleted by the **delete** command can be recovered with the **undelete** command or deleted permanently from the recycle bin, using the **reset recycle-bin** command.

Note that, if two files with the same name in a directory are deleted, only the latest deleted file will be kept in the recycle bin.

Example

Delete the file flash:/test/test.txt

```
<SW8800> delete flash:/test/test.txt
Delete flash:/test/test.txt?[Y/N]:
```

dir

Syntax

dir [**/all**] [*file-url*]

View

User view

Parameter

/all: Display all the files (including the deleted ones).

file-url: File or directory name to be displayed. The *file-url* parameter supports "*" matching. For example, using **dir *.**txt will display all the files with the extension txt in the current directory.

Description

Use the **dir** command to view the information about the specified file or directory in the storage device of the switch. This command supports "*" wildcard characters.

Example

Display the information about the file flash:/test/test.txt

```
<SW8800> dir flash:/test/test.txt
Directory of flash:/test/
-rwxrwxrwx   1 noone    nogroup       971  Sep 20 2003 14:28:52   test.txt
7932928 bytes total (4966400 bytes free)
```

Display the information about all the files (including the deleted ones) in the flash:/test/ directory.

```
<SW8800> dir /all flash:/test/
Directory of flash:/test/
-rwxrwxrwx   1 noone    nogroup       971  Sep 20 2003 14:28:52   test.txt
   1   -rw-         4  Apr 04 2005 20:13:47   [snmpboots]

31877 KB total (2182 KB free)
```

The files that have already been deleted and kept in the recycle bin are displayed with the [ ] prompt.

Display the information about all the files (including the deleted ones) in the flash:/test/ directory whose names start with the t character.

```
<SW8800> dir /all flash:/test/t*
Directory of flash:/test/
0 -rw-   1 noone    nogroup       971  Sep 20 2003 14:28:52   test.txt
7932928 bytes total (4966400 bytes free)
```

execute

Syntax

execute *filename*

View

System view

Parameter

filename: Name of the batch file, ranging from 1 to 256, with a suffix of ".bat".

Description

Use the **execute** command to execute the specified batch file.

The batch command executes the command lines in the batch file one by one. There should be no invisible character in the batch file. If invisible characters are found, the batch command will quit the current execution without back off operation. The batch command does not guarantee the execution of each command, nor does it perform hot backup itself. The forms and contents of the commands are not restricted in the batch file.

Example

Execute the batch file "test.bat" in the directory of "flash:/".

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] execute test.bat
```

file prompt

Syntax

file prompt { **alert** | **quiet** }

View

System view

Parameter

alert: Performs interactive confirmation on dangerous file operations.

quiet: Does not prompt for the file operations.

Description

Use the **file prompt** command to change the prompt modes of the file operation on the switch.

By default, the prompt mode of the file operation is **alert**, which performs interactive confirmation on dangerous file operations.

If the prompt mode is set as **quiet**, that is, no prompt for file operations, some non-recoverable operations may lead to system damage.

Example

Configure the prompt mode of file operation as **quiet.**

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] file prompt quiet
```

fixdisk

Syntax

fixdisk *device*

View

User view

Parameter

device: Device name.

Description

Use the **fixdisk** command to restore the space of a storage device.

Some of the space of a storage device may be unavailable due to some reason (such as abnormal operations). In this case, you can use this command to restore the space.

Currently, the switch does not support this command on the compact flash (CF) card.

Example

Restore the space of the storage device flash.

```
<SW8800> fixdisk flash:
```

format

Syntax

format *filesystem*

View

User view

Parameter

filesystem: Device name.

Description

Use the **format** command to format the storage device.

Format operation will cause non-recoverable loss of all the files on the device. Specially, configuration files will be lost after formatting the flash memory.

Example

Format flash.

```
<SW8800> format flash:
All data on Flash will be lost , proceed with format ? [Y/N] y
% Now begin to format flash, please wait for a while...
Format winc: completed
```

mkdir

Syntax

mkdir *directory*

View

User view

Parameter

directory: Directory name, in the range 1 to 136 characters.

Description

Use the **mkdir** command to create directory in the specified directory on the storage device.

The directory to be created cannot have the same name as that of other directory or file in the specified directory.

Example

Create the directory dd.

```
<SW8800> mkdir dd
Created dir flash:/dd
```

more

Syntax

more *file-url*

View

User view

Parameter

file-url: File name.

Description

Use the **more** command to view the contents of a specific file.

At present, the file system can display files in text format. This command can be used to display the contents of the files with .txt suffix or .cfg (configuration) suffix.

Example

Display the contents of file test.txt.

```
<SW8800> 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
files that make up your test application.
Test.dsp
This file (the project file) contains information at the project
level and is used to build a single project or subproject. Other use
rs can share the project (.dsp) file, but they should export the
makefiles locally.
```

move

Syntax

move *fileurl-source fileurl-dest*

View

User view

Parameter

fileurl-source: Source file name.

fileurl-dest: Destination file name.

Description

Use the **move** command to move files.

When the destination filename is the same as that of an existing file, the system will ask whether to overwrite it.

Example

Move flash:/test/sample.txt to flash:/sample.txt.

```
<SW8800> 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
```

The switch has the following limitation on directory name and filename:

- The maximum length of a directory name or filename is 64 characters.
- The maximum length of a full-path filename (including the device name, directory name, and filename) is 136 characters.
- The **move** command can be successfully executed only when the source file and the destination file are on the same device.

pwd

Syntax

pwd

View

User view

Parameter

None

Description

Use the **pwd** command to view the current path.

Error may occur without setting the current path.

Example

Display the current path.

```
<SW8800> pwd
flash:
```

rename

Syntax

rename *fileurl-source fileurl-dest*

View

User view

Parameter

fileurl-source: Source file name.

fileurl-dest: Destination file name.

Description

Use the **rename** command to rename a file.

If the destination file name is identical with that of an already existent directory or file, the rename operation fails and the system prompts that name has already been used or the file is being used.

Example

Rename the file sample.txt to sample.bak.

```
<SW8800> 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

Syntax

reset recycle-bin [*file-url*]

View

User view

Parameter

file-url: Name of the file to be deleted.

Description

Use the **reset recycle-bin** command to permanently delete files from the recycle bin.

The *file-url* supports the wildcard character "*".The **delete** command only puts the file into the recycle bin, but **reset recycle-bin** command will delete this file permanently.

Example

Delete the file from the recycle bin.

```
<SW8800> reset recycle-bin flash:/ vrpcfg.vrrp
Squeeze flash:/ vrpcgf.vrrp ? [Y/N]:
```

rmdir

Syntax

rmdir *directory*

View

User view

Parameter

directory: Directory name.

Description

Use the **rmdir** command to cancel a directory.

The directory to be deleted must be empty, that is, all the files under the directory should be removed first.

*When you delete a directory using the **rmdir** command, the files that originally belonged to this direction, now in the Recycle Bin, will also be deleted.*

Example

Delete the directory 3com.

```
<SW8800> rmdir 3com
Rmdir 3com?[Y/N]:y
% Removed directory 3com
```

umount

Syntax

umount *device*

View

User view

Parameter

device: Device name. Now, it can only be CF.

Description

Use the **umount** command to unload the CF card from the file system.

Example

Unload the CF card from the file system.

```
<SW8800> umount cf:
```

undelete

Syntax

undelete *file-url*

View

User view

Parameter

file-url: Name of the file to be recovered.

Description

Use the **undelete** command to recover the file that has not been deleted completely.

The file name to be recovered cannot be the same as an existing directory name. If the destination file name is the same as an existing file name, prompt whether to overwrite.

Example

Recover the deleted file sample.bak.

```
<SW8800> undelete sample.bak
Undelete flash:/sample.bak ?[Y/N]:y
%Undeleted file flash:/sample.bak
```

58 DEVICE MANAGEMENT COMMANDS

boot boot-loader

Syntax

boot boot-loader { **primary** | **backup** } *file-url* [**slot** *slot-number*]

View

User view

Parameter

file-url: ARP program path + program name

slot-number: Slot number of the active or standby SRPC.

primary: Specifies this program to be the primary bootstrap program.

backup: Specifies this program to be the backup bootstrap program.

Description

Use the **boot boot-loader primary** command to set a specified program as the primary bootstrap program.

Use the **boot boot-loader backup** command to set a specified program as the backup bootstrap program.

If the switch cannot be started through specified bootstrap program, a program will be selected from the Flash or CF card as bootstrap program. If the switch still cannot be started normally, the switch fails to boot up.

An Switch 8800 Family series routing switch supports system switchover, both its active and standby SRPCs have an application program system. You can operate on the programs on both SRPCs. But when you specify a bootstrap program on the standby SRPC, the URL of the program must begin with "slot[No.]#[flash: | cf:]/", where, [No.] is the slot number of the standby SRPC and [flash: | cf:] is the name of the equipment, flash card or CF card. For example, if the slot number of the standby SRPC is 1, the URL of the 8500.app program under the root directory on the standby SRPC must be "slot1#flash:/8500.app".

Example

Specify flash:/s8500-vrp310-r1262.app as the current primary bootstrap program of the active SRPC.

```
<SW8800> boot boot-loader primary flash:/s8500-vrp310-r1262.app
The specified file will be booted next time!.
```

Specify slot1#flash:/s8500-vrp310-r1262.app as the current primary bootstrap program on the standby SRPC in slot 1.

```
<SW8800> boot boot-loader primary slot1#flash:/s8500-vrp310-r1262.app slot 1
The specified file will be booted next time!.
```

boot bootrom

Syntax

boot bootrom *file-url* **slot** *slot-num-list*

View

User view

Parameter

file-url: Path and name of Bootrom file in the storage device.

slot *slot-num-list*: Specifies the slot number list of switch. The formula is *slot-num-list*={ *slot-num* [to *slot-num*] }&<1-n>. &<1-n> indicates that the prior parameter can be input for n times. For Switch 8807, n is 7; for Switch 8814, n is 14.

Description

Use the **boot bootrom** command to upgrade Bootrom.

Example

Upgrade bootrom of No.1slot.

```
<SW8800> boot bootrom PLATV100R002B09D002.app slot 1
```

display boot-loader

Syntax

display boot-loader

View

Any view

Parameter

None

Description

Use the **display boot-loader** command to view APP file used this time and next time.

Example

```
<SW8800> display boot-loader
The primary app to boot of slot 0 at the next time is: flash:/switch.app
The backup app to boot of slot 0 at the next  time is: flash:/switch.app
The app to boot of slot 0 at this time is: flash:/switch.app
```

Table 137 Description on the fields of the display boot-loader command

Field	Description
The app to boot of `slot` 0 at the next time is: flash:/Switch.app	Startup file used on startup next time
The app to boot of `slot` 0 at this time is: flash:/PLAT.APP	Startup file used on startup this time

display cpu

Syntax

display cpu [**slot** *slot-no*]

View

Any view

Parameter

slot *slot-no*: Specifies the module number.

Description

Use the **display cpu** command to display CPU occupancy.

Example

Display CPU occupancy on slot 0.

```
<SW8800> display cpu slot 0
slot 0 CPU busy status:
     6% in last 5 seconds
     7% in last 1 minute
    12% in last 5 minutes
```

Table 138 Description on the fields of the display cpu command

Field	Description
slot 0 CPU busy status:	CPU usage of switch
6% in last 5 seconds	CPU usage in last 5 seconds is 6%.
7% in last 1 minute	CPU usage in last 1 minute is 7%.
12% in last 5 minutes	CPU usage in last 5 minutes is 12%.

display device

Syntax

display device [**detail** | [**shelf** *shelf-no*] [**frame** *frame-no*] [**slot** *slot-no*]]

View

Any view

Parameter

detail: displays all slot detail information.

shelf-no: Shelf number.

frame-no: Frame number.

slot-no: Slot number.

Description

Use the **display device** command to display the module type and working status information of a card, including physical card number, physical daughter card number, PCB version number, hardware version number, FPGA version number, version number of BOOTROM software, application version number, address learning mode, interface card type and interface card type description, and so on.

Example

Show device information.

```
<SW8800> display device
Slot No.   Brd Type  Brd Status   Subslot Num    Sft Ver
 0         3C17539  Master       0              8500-0004
 1         NONE      Absent       Absent         None
 2         NONE      Absent       Absent         None
 3         NONE      Absent       Absent         None
 4         NONE      Absent       Absent         None
 5         NONE      Absent       Absent         None
 6         NONE      Absent       Absent         None
 7         NONE      Absent       Absent         None
```

display environment

Syntax

display environment

View

Any view

Parameter

None

Description

Use the **display environment** command to view environment information.

Example

Display the environment information.

```
<SW8800> display environment
System temperature information (degree centigrade):
------------------------------------------------------
Slot    Temperature         Lower limit      Upper limit
 0        33                  10               45
 2        35                  10               65
 4        34                  10               65
```

display fan

Syntax

display fan [*fan-id*]

View

Any view

Parameter

fan-id: the fan ID.

Description

Use the **display fan** command to view the working state of the built-in fans. User can perform this command to see if they work normally.

Example

Display the working state of the fans.

```
<SW8800> display fan
 Fan  1 State: Normal
```

display memory

Syntax

display memory [**slot** *slot-no*]

View

Any view

Parameter

slot-no: Specifies slot number

Description

Use the **display memory** command to display memory situation.

Example

Display memory situation.

```
<SW8800> display memory slot 0
System Total Memory(bytes): 197932416
Total Used Memory(bytes): 65234704
Used Rate: 32%
```

Table 139 Description on the fields of the display memory command

Field	Description
System Total Memory(bytes)	The Total Memory of switch, unit in byte
Total Used Memory(bytes)	The Total used Memory of switch, unit in byte
Used Rate	The memory used rate

display power

Syntax

display power [*power-ID*]

View

Any view

Parameter

power-ID: Power ID.

Description

Use the **display power** command to view the working state of the built-in power supply.

Example

Show power state.

```
<SW8800> display power
Power   1 State: Absent
Power   2 State: Normal
Power   3 State: Absent
```

display schedule reboot

Syntax

display schedule reboot

View

Any view

Parameter

None

Description

Use the **display schedule reboot** command to check the configuration of related parameters of the switch **schedule reboot** terminal service.

Related command: **reboot**, **schedule reboot at**.

Example

Display the configuration of the **schedule reboot** terminal service parameters of the current switch.

```
<SW8800> display schedule reboot
System will reboot at 16:00:00 2004/11/1 (in 2 hours and 5 minutes).
```

reboot

Syntax

reboot [**slot** *slot-no*]

View

User view

Parameter

slot *slot-no*: Specifies the physical card number.

Description

Use the **reboot** command to reboot to restart the switch or the specified card.
Example

Reset the switch.

```
<SW8800> reboot
```

schedule reboot at

Syntax

schedule reboot at *hh:mm* [*yyyy/mm/dd*]

undo schedule reboot

View

User view

Parameter

hh:mm: Reboot time of the switch, in the format of "hour: minute" The *hh* ranges from 0 to 23, and the *mm* ranges from 0 to 59.

yyyy/mm/dd: Reboot date of the switch, in the format of "year/month/day. The *yyyy* ranges from 2000 to 2099, the *mm* ranges from 1 to 12, and the value of *dd* is related to the specific month.

Description

Use the **schedule reboot at** command to enable the timing reboot function of the switch and set the specific reboot time and date.

Use the **undo schedule reboot** command to disable the timing reboot function.

By default, the timing reboot switch function is disabled.

The precision of switch timer is 1 minute. The switch will reboot in one minute when time comes to the specified rebooting point.

If the **schedule reboot at** command sets specified date parameters, which represents a data in the future, the switch will be restarted in specified time, with error not more than 1 minute.

If no specified date parameters are configured, two cases are involved: If the configured time is after the current time, the switch will be restarted at the time point of that day; if the configured time is before the current time, the switch will be restarted at the time point of the next day.

It should be noted that the configured date should not exceed the current date more than 30 days. In addition, after the command is configured, the system will prompt you to input confirmation information. Only after the "*Y*" or the "*y*" is entered can the configuration be valid. If there is related configuration before, it will be covered directly.

Moreover, after the **schedule reboot at** command is configured and the system time is adjusted by the **clock** command, the former configured **schedule reboot at** parameter will go invalid.

Related command: **reboot**, **display schedule reboot**.

Example

Set the switch to be restarted at 22:00 that night (the current time is 15:50).

```
<SW8800> schedule reboot at 22:00
Reboot system at 22:00:00 UTC 2003/11/18 (in 6 hours and 10 minutes)
confirm?[Y/N]:y
aux0: schedule reboot parameters at 15:50:00 UTC 2003/11/18. And system will
 reboot at 22:00:00 UTC 2003/11/18
Proceed with reboot? [Y/N]:y
```

schedule reboot delay

Syntax

schedule reboot delay { *hhh:mm* | *mmm* }

undo schedule reboot

View

User view

Parameter

hhh:mm: Waiting time for rebooting a switch, in the format of "hour: minute" The *hhh* ranges from 0 to 720, and the *mm* ranges from 0 to 59.

mmm: Waiting delay for rebooting a switch, in the format of "absolute minutes" . Ranging from 0 to 43200,

Description

Use the **schedule reboot delay** command to enable the timing reboot switch function and set the waiting time.

Use the **undo schedule reboot** command to disable the timing reboot function.

By default, the timing reboot switch function is disabled.

The precision of switch timer is 1 minute. The switch will reboot in one minute when time comes to the specified rebooting point.

Two formats can be used to set the waiting delay of timing reboot switch, namely the format of "hour: minute" and the format of "absolute minutes". But the total minutes should be no more than 30Đó24Đó60 minutes, or 30 days.

After this command is configured, the system will prompt you to input confirmation information. Only after the "*Y*" or the "*y*" is entered can the configuration be valid. If there is related configuration before, it will be covered directly.

Moreover, after the **schedule reboot at** command is configured, and the system time is adjusted by the **clock** command, the original **schedule reboot at** parameter will become invalid.

Related command: **reboot**, **schedule reboot at**, **undo schedule reboot**, **display schedule reboot**.

Example

Configure the switch to be restarted after 88 minutes (the current time is 21:32).

```
<SW8800> schedule reboot delay 88
Reboot system for 23:00:00 UTC 2002/11/1 (in 1 hours and 28 minutes)
Confirm? [Y/N]:y
```

temperature-limit

Syntax

temperature-limit *slot-no down-value up-value*

undo temperature-limit *slot-no*

View

User view

Parameter

Slot-no: Physical card number.

down-value: Lower temperature limit, in the range 0 to 70 °C.

up-value: Upper temperature limit, in the range 20 to 90 °C.

Description

Use the **temperature-limit** command to configure temperature limit.

Use the **undo temperature-limit** command to restore temperature limit to default value.

Example

Set the lower and upper temperature limit of card 0.

```
<SW8800> temperature-limit 0 10 75
```

update l3plus

Syntax

update l3plus slot *slot-no* **filename** *file-name* **ftpserver** *server-name* **username** *user-name* **password** *password* [**port** *port-num*]

View

System view

Parameter

slot-no: Slot for the service processing module to be updated.

file-name: Name of upgrading file to be downloaded. The file suffix is .app.

server-name: IP address or host name of FTP Server where the file to be updated locates.

user-name: User name for file transfer protocol (FTP) login.

password: User password for FTP login.

port-num: FTP port number, in the range 0 to 65,535. By default, it is 21.

Description

Use the **update l3plus** command to update service processing modules. After the command is executed, the system logs into an FTP Server with the host name, user name and user password provided. The system downloads the host software containing load program of service processing module to the system's synchronous dynamic random access memory (SDRAM), and uses the file to enable service processing modules.

CAUTION:

- When you use the **update l3plus** command to update service processing modules, you must use the switch host APP file which includes the load program of L3PLUS service processing modules.
- The maximum size of L3PLUS update file loaded by the **update l3plus** command is 24 M.

Example

Update the service processing module in slot 2. The file to be downloaded is place in the host with the IP address 192.168.1.100, and its name is L3PLUS.app. The user name and password for FTP login are 654321 and 123456 respectively.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] update l3plus slot 2 filename L3PLUS.app ftpserver 192.168.
1.100 username 654321 password 123456
```

59 FTP&TFTP CONFIGURATION COMMANDS

FTP Client Commands

ascii

Syntax

ascii

View

FTP Client view

Parameter

None

Description

Use the **ascii** command to configure data transmission mode as ASCII mode.

By default, the file transmission mode is ASCII mode.

Perform this command if the user needs to change the file transmission mode to default mode.

Example

Configure to transmit data in the ASCII mode.

```
<SW8800> ftp
[ftp] ascii
200 Type set to A.
```

binary

Syntax

binary

View

FTP Client view

Parameter

None

Description

Use the **binary** command to configure file transmission type as binary mode.

Example

Configure to transmit data in the binary mode.

```
<SW8800>ftp
[ftp] binary
200 Type set to I.
```

bye

Syntax

bye

View

FTP Client view

Parameter

None

Description

Use the **bye** command to disconnect with the remote FTP Server and return to user view.

After performing this command, you can terminate the control connection and data connection with the remote FTP Server.

Example

Terminate connection with the remote FTP Server and return to user view.

```
<SW8800> ftp
[ftp] bye
```

cd

Syntax

cd *pathname*

View

FTP Client view

Parameter

pathname: Path name.

Description

Use the **cd** command to change the working path on the remote FTP Server.

This command is used to access another directory on FTP Server. Note that the user can only access the directories authorized by the FTP server.

Example

Change the working path to flash:/temp

```
<SW8800> ftp
[ftp] cd flash:/temp
```

cdup

Syntax

cdup

View

FTP Client view

Parameter

None

Description

Use the **cdup** command to change working path to the upper level directory.

This command is used to exit the current directory and return to the upper level directory.

Example

Change working path to the upper level directory.

```
<SW8800> ftp
[ftp] cdup
```

close

Syntax

close

View

FTP Client view

Parameter

None

Description

Use the **close** command to disconnect FTP client side from FTP server side without exiting FTP client side view. That is to say, you can terminate the control connection and data connection with the remote FTP Server at the same time.

Example

Terminate connection with the remote FTP Server and stays in FTP Client view.

```
<SW8800> ftp
[ftp] close
```

debugging

Syntax

debugging

undo debugging

View

FTP Client view

Parameter

None

Description

Use the **debugging** command to enable the debugging for FTP Client commands.

Use the **undo debugging** command to disable the debugging for FTP Client commands.

By default, the debugging for FTP Client commands is disabled.

Example

Enable the debugging for FTP Client commands.

```
<SW8800> ftp
[ftp] debugging
```

delete

Syntax

delete *remotefile*

View

FTP Client view

Parameter

remotefile: File name.

Description

Use the **delete** command to cancel the specified file.

Example

Delete the file temp.c

```
<SW8800>ftp
[ftp] delete temp.c
```

dir

Syntax

dir [*filename*] [*localfile*]

View

FTP Client view

Parameter

filename: File name to be queried.

localfile: Saves local file name of the query result.

Description

Use the **dir** command to query a specified file.

If no parameter of this command is specified, then all the files in the directory will be displayed.

Example

Query the file temp.c and saves the results in the file temp1.

```
<SW8800> ftp
[ftp] dir temp.c temp1
```

disconnect

Syntax

disconnect

View

FTP Client view

Parameter

None

Description

Use the **disconnect** command to disconnect FTP Client side from FTP server side without exiting FTP client side view.

This command terminates the control connection and data connection with the remote FTP Server at the same time.

Example

Terminate connection with the remote FTP Server and stays in FTP Client view.

```
<SW8800> ftp
[ftp] disconnect
```

ftp

Syntax

ftp [{ *ipaddress* | *host-name*} [*port*]]

View

User view

Parameter

ipaddress: IP address of the remote FTP Server.

port: Port number of remote FTP Server.

Host-name: Name of the remote FTP Server, a string which is 1 to 30 characters long.

Description

Use the **ftp** command to establish control connection with the remote FTP Server and enter FTP Client view.

Example

Connect to FTP Server at the IP address 1.1.1.1

```
<SW8800> ftp 1.1.1.1
```

get

Syntax

get *remotefile* [*localfile*]

View

FTP Client view

Parameter

localfile: Local file name.

remotefile: Name of a file on the remote FTP Server.

Description

Use the **get** command to download a remote file and save it locally.

If no local file name is specified, it will be considered the same as that on the remote FTP Server.

Example

Download the file temp1.c and saves it as temp.c

```
<SW8800> ftp
[ftp] get temp1.c temp.c
```

lcd

Syntax

lcd

View

FTP Client view

Parameter

None

Description

Use the **lcd** command to view local working path of FTP Client.

Example

Show local working path.

```
<SW8800> ftp
[ftp] lcd
% Local directory now flash:/temp
```

ls

Syntax

ls [*remotefile*] [*localfile*]

View

FTP Client view

Parameter

remotefile: Remote file to be queried.

localfile: Saves local file name of the query result.

Description

Use the **ls** command to query a specified file.

If no parameter is specified, all the files will be shown.

Note that, the **ls** command only displays the file names, while the **dir** command also displays other file-related information such as the file size and creation date.

Example

Query file temp.c

```
<SW8800>ftp
[ftp] ls temp.c
```

mkdir

Syntax

mkdir *pathname*

View

FTP Client view

Parameter

pathname: Directory name.

Description

Use the **mkdir** command to create a directory on the remote FTP Server.

User can perform this operation as long as the remote FTP server has authorized.

Example

Create the directory flash:/lanswitch on the remote FTP Server.

```
<SW8800>ftp
[ftp] mkdir flash:/lanswitch
```

open

Syntax

open *ipaddr* [*port*]

View

FTP Client view

Parameter

ipaddr: IP address of the remote FTP server.

port: Port number of the remote server.

Description

Use the **open** command to set up an FTP connection with a remote FTP server.

Example

Set up a FTP connection with the FTP server with the IP address of 10.110.3.1.

```
<SW8800> ftp
[ftp] open 10.110.3.1
```

passive

Syntax

passive

undo passive

View

FTP Client view

Parameter

None

Description

Use the **passive** command to configure the data transmission mode as passive mode.

Use the **undo passive** command to configure the data transmission mode as active mode.

By default, the data transmission mode is passive mode

Example

Set the data transmission to passive mode.

```
<SW8800> ftp
[ftp] passive
```

put

Syntax

put *localfile* [*remotefile*]

View

FTP Client view

Parameter

localfile: Local file name.

remotefile: File name on the remote FTP Server.

Description

Use the **put** command to upload a local file to the remote FTP Server.

If the user does not specify the filename on the remote server, the system will consider it the same as the local file name by default.

Example

Upload the local file temp.c to the remote FTP Server and saves it as temp1.c.

```
<SW8800> ftp
[ftp] put temp.c temp1.c
```

pwd

Syntax

pwd

View

FTP Client view

Parameter

None

Description

Use the **pwd** command to view the current directory on the remote FTP Server.

Example

Show the current directory on the remote FTP Server.

```
<SW8800> ftp
[ftp] pwd
"flash:/temp" is current directory.
```

quit

Syntax

quit

View

FTP Client view

Parameter

None

Description

Use the **quit** command to terminate the connection with the remote FTP Server and return to user view.

Example

Terminate connection with the remote FTP Server and returns to user view.

```
<SW8800> ftp
[ftp] quit
<SW8800>
```

remotehelp

Syntax

remotehelp [*protocol-command*]

View

FTP Client view

Parameter

protocol-command: FTP protocol command.

Description

Use the **remotehelp** command to view help information about the FTP protocol command. This command takes effects only when the FTP server provides the protocol command help. (Switch 8800 Family series serving as servers provide this help service, but common FTP software do not provide this service).

Example

Show the syntax of the protocol command **user**.

```
<SW8800> ftp
[ftp] remotehelp user
214 Syntax: USER <sp> <username>
```

rmdir

Syntax

rmdir *pathname*

View

FTP Client view

Parameter

pathname: Directory name of remote FTP Server.

Description

Use the **rmdir** command to remove the specified directory from FTP Server. Note that, this command can be successfully executed only when the specified directory contains no files.

Example

Delete the directory flash:/temp1 from FTP Server.

```
<SW8800> ftp
[ftp] rmdir flash:/temp1
```

user

Syntax

user *username* [*password*]

View

FTP Client view

Parameter

username: Logon username.

password: Logon password.

Description

Use the **user** command to register an FTP user.

This command is available when you log in FTP server with a specified user account.

Example

Log in the FTP Server with username tom and password bjhw.

```
<SW8800> ftp
[ftp] user tom bjhw
```

verbose

Syntax

verbose

undo verbose

View

FTP Client view

Parameter

None

Description

Use the **verbose** command to enable the client to display the commands received from/sent to the server.

Use the **undo verbose** command to disable the client from display the commands received from/sent to the server

By default, the VERBOSE is enabled and the client displays the commands received from/sent to the server.

Example

Enable VERBOSE.

```
<SW8800> ftp
[ftp]verbose
```

TFTP Configuration Commands

tftp get

Syntax

tftp *tftp-server* **get** *source-file* [*dest-file*]

View

User view

Parameter

tftp-server: IP address or hostname of the TFTP server. The name of the TFTP server should be a string ranging from 1 to 20 characters.

source-file: Filename of the source file on the TFTP server.

dest-file: Filename of the destination file which will be saved on the switch.

Description

Use the **tftp get** command to download a file from the specified directory of the TFTP server and saving it on the switch.

Related command: **tftp put**.

Example

Download the file LANSwitch.app from the TFTP server at 1.1.3.214 and save it as vxWorks.app on the local switch.

```
<SW8800> tftp 1.1.3.214 get LANSwitch.app vxWorks.app
```

tftp put

Syntax

tftp *tftp-server* **put** *source-file* [*dest-file*]

View

User view

Parameter

tftp-server: IP address or hostname of the TFTP server. The name of the TFTP server should be a string ranging from 1 to 20 characters.

source-file: Filename of the source file which is saved on the switch.

dest-file: Name of the saved-as file uploaded to the specified directory on the TFTP server.

Description

Use the **tftp put** command to upload a file from the switch to the specified directory on the TFTP server.

Related command: **tftp get**.

Example

Upload the vrpcfg.txt to the TFTP server at 1.1.3.214 and save it as temp.txt.

```
<SW8800> tftp 1.1.3.214 put vrpcfg.txt temp.txt
```

60 INFORMATION CENTER

Information Center Configuration Commands

display channel

Syntax

display channel [*channel-number* | *channel-name*]

View

Any view

Parameter

channel-number: Channel number, ranging from 0 to 9, that is, the system has ten channels.

channel-name: Specifies the channel name. the name can be **channel7, channel8, channel9, console, logbuffer, loghost, monitor, snmpagent, trapbuffer, logfile**.

Description

Use the **display channel** command to view the details about the information channel.

Without parameter, the **display channel** command shows the configurations of all the channels.

Example

Show details about the information channel 0.

```
<SW8800> display channel 0
channel number:0, channel name:console
MODU_ID NAME    ENABLE  LOG LEVEL   ENABLE  TRAP LEVEL  ENABLE
DEBUGGING LEVEL
0xffff0000  default Y   warning Y   debugging   Y   debugging
```

display info-center

Syntax

display info-center

View

Any view

Parameter

None

Description

Use the **display info-center** command to view the configuration of system log and the information recorded in the memory buffer.

If the information in the current log/trap buffer is less than the size of buffer, display the actual log/trap information.

Related command: **info-center enable,info-center loghost,info-center logbuffer,info-center console channel,info-center monitor channel**.

Example

Show the system log information.

```
<SW8800> 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:256
         current messages:6, channel number:4, channel name:logbuffer
         dropped messages:0, overwrote messages:0
Trap buffer:
         enabled, max buffer size:1024, current buffer size:256
         current messages:0, channel number:3, channel name:trapbuffer
         dropped messages:0, overwrote messages:0
Log file :
        enabled,max file buffer size 32KB, current file buffer size 7KB,
        channel number : 6, channel name : logfile
        max log file number : 5, max length of each log file : 2MB
        log file directory : cf:/logfile
Information timestamp setting:
         log - date, trap - date, debug - boot
```

Table 140 Description on the fields of the display info-center command

Field	Description
Information Center:	The status of the information center
Log host:	The status of the log host, including its IP address, occupied channel number, channel name, language and the priority level of the log host.
Console:	The status of the console port, including the occupied channel name and channel number.
Monitor:	The status of the monitoring port, including the occupied channel number and channel name.
SNMP Agent:	The status of the SNMP agent, including the occupied channel number and channel name.
Log buffer:	The status of the log buffer, including enable status, maximum size, current size, number of current messages, channel name, channel number, number of dropped messages, number of the overwritten messages.
Trap buffer:	The status of the trap buffer, including enable status, maximum size, current size, number of current messages, channel name, channel number, number of dropped messages, number of the overwritten messages.

Table 140 Description on the fields of the display info-center command

Field	Description
Log file	The status of the log file, including enable status, maximum file buffer size, channel number, channel name, maximum number of log files, maximum size of the log file, storage path of log files.
Information timestamp setting:	Information timestamp settings, including the timestamp type of log messages, trap messages and debugging messages.

display logbuffer

Syntax

display logbuffer [**summary**] [**size** *sizenum* | [**reverse**] | **level** [*levelnum* | **emergencies** | **alerts** | **critical** | **errors** | **warnings** | **notifications** | **informational** | **debugging** }] * [| { **begin** | **include** | **exclude** } *text*]

View

Any view

Parameter

Size *sizenum*: Optional parameter. Number of log information you want to query.

Levelnum: Optional parameter. Level of the log information you want to query.

Summary: Optional parameter, displays the statistics of all logs levels in the log buffer.

Reverse: Optional parameter, searches for the matching log information from the head of the log buffer.

emergencies, **alerts**, **critical**, **debugging**, **errors**, **informational**, **notifications**, **warnings** are the names of the eight log severity levels. You can type the values or names of the desired severity levels, which are equivalent, in commands. Table 141 gives the details.

Table 141 Severity levels defined in the information center

Severity	Value	Description
emergencies	1	Emergent errors
alerts	2	Errors you must correct immediately
critical	3	Critical errors
errors	4	Errors requiring your attention but not critical
warnings	5	Warning, an error may occur
notifications	6	Information requiring your attention
informational	7	General prompt information
debugging	8	Debugging information

size: Configures the size of buffer.

sizenum: Size of buffer (number of messages which can be kept); ranging from 1 to 1024. By default, the size of the buffer is 256.

|: Filters the configuration information to be output by regular expression.

begin: Optioanl parameter, displays all items beginning friom the matching item.

exclude: Optional parameter, only displays the matching items.

include: Optional parameter, only displays the non-matching items..

text: Defines the regular expression.

Table 142 Special characters in the regular expression

Special characters	Description	Restriction
_	Underscore, similar to a wildcard and can stand for these characters: (^|$|[,(){}]) A space, the beginning of the input string, the end of the input string	If the first character in the regular expression is not a underscore, then there is no restriction on the number of the underscore (but it is restricted by the command length) If the first character in the regular expression is an underscore, then there should be less than five consecutive underscores. If the underscores in a command are discrete, on the first group of underscores are filtered for the output information, but not the subsequent underscores.
(	Left parenthesis, push flag in program	It is recommended not to use this character in the regular expression.

Description

Use the **display logbuffer** command to view the attribute of logbuffer and the information recorded in logbuffer.

All log messages are saved in the log buffer. When the log buffer is full, the latest message will overlap the earliest one.

The displaying sequence of all log messages is from the newest message to the oldest one.

When you input **size**, if the size of current configured log messages is bigger than the *logsize*, the system will search for the messages on the following principles.

- If you input **reverse**, the system will search for *logsize* matiching messages from the oldest one(the head of the log buffer), then displays them from the newest message to the oldest one.
- If you do not input **inverse**, the system will search for the *logsize* matiching messages from the newest one(the end of the log buffer), then displays them from the newest message to the oldest one.

Example

Show the system logbuffer attribute and the log information in logbuffer.

```
<SW8800> 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 : 91
```

display logbuffer summary

Syntax

display logbuffer summary [**level** *severity*]

View

Any view

Parameter

level: Information level.

severity: Information level, do not output information below this level. Information at different levels is as the following table:

Table 143 Severity levels defined in the information center

Severity	Value	Description
emergencies	1	Emergent errors
alerts	2	Errors you must correct immediately
critical	3	Critical errors
errors	4	Errors requiring your attention but not critical
warnings	5	Warning, an error may occur
notifications	6	Information requiring your attention
informational	7	General prompt information
debugging	8	Debugging information

Description

Use the **display logbuffer summary** command to view the summary information recorded in logbuffer.

Related command: **info-center enable,info-center loghost,info-center logbuffer,info-center console channel,info-center monitor channel**.

Example

Show the summary information recorded in logbuffer.

```
<SW8800> display logbuffer summary
EMERG ALERT CRIT ERROR WARN NOTIF INFO DEBUG
0     0     0    0     94   0     1    0
```

display trapbuffer

Syntax

display trapbuffer [**summary**] [**level** [*levelnum* | **emergencies** | **alerts** | **critical** | **debugging** | **errors** | **informational** | **notifications** | **warnings**]] [**size** *sizenum*]

View

Any view

Parameter

size: Configures the size of buffer.

summary: Number of statistical logs.

sizenum: Size of buffer (number of messages which can be kept), ranging from 1 to 1024. By default, the size of the buffer is 256.

level: level.

levelnum: Information level value, ranging from 1 to 8.

emergencies, **alerts**, **critical**, **debugging**, **errors**, **informational**, **notifications**, **warnings** are the names of the eight log severity levels. You can type the values or names of the desired severity levels, which are equivalent, in commands. Table 141 gives the details.

Description

Use the **display trapbuffer** command to view the attribute of trapbuffer and the information recorded in trapbuffer.

Example

Show the system trapbuffer attribute and the log information in trapbuffer.

```
<SW8800> 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
overwrote messages : 0
current messages : 6

#Dec 31 14:01:25 2004 3Com DEV/2/LOAD FINISHED:
 Trap 1.3.6.1.4.1.2011.2.23.1.12.1.20: frameIndex is 0, slotIndex 0.4

#Dec 31 14:01:33 2004 3Com DEV/2/SLOT STATE CHANGE TO NORMAL:
 Trap 1.3.6.1.4.1.2011.2.23.1.12.1.11: frameIndex is 0, slotIndex 0.2

#Dec 31 14:01:40 2004 3Com DEV/2/SLOT STATE CHANGE TO NORMAL:
 Trap 1.3.6.1.4.1.2011.2.23.1.12.1.11: frameIndex is 0, slotIndex 0.
```

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: Channel number, ranging from 0 to 9, that is, system has ten channels.

channel-name: Specifies the channel name with a character string not exceeding 30 characters, excluding digit, "-", "/" or " ". .

Description

Use the **info-center channel name** command to rename a channel specified by the *channel-number* as *channel-name*.

Use the **undo info-center channel** command to restore the channel name.

The system assigns a channel in each output direction by default. See the table below.

Table 144 Numbers and names of the channels for log output

Output direction	Channel number	Default channel name
Console	0	console
Monitor	1	monitor
Info-center loghost	2	loghost
Trap buffer	3	trapbuf
Logging buffer	4	logbuf
snmp	5	snmpagent
Log file	6	Logfile

Note that the channel name cannot be duplicated.

Example

Rename the channel 0 as execconsole.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] info-center channel 0 name execconsole
```

info-center console channel

Syntax

info-center console channel { *channel-number* | *channel-name* }

undo info-center console channel

View

System view

Parameter

channel-number: Channel number, ranging from 0 to 9, that is, system has ten channels.

channel-name: Specifies the channel name. The name can be **channel7, channel8, channel9, console, logbuffer, loghost, monitor, snmpagent, trapbuffer, logfile**.

Description

Use the **info-center console channel** command to configure the channel through which the log information is output to the console.

By default, Ethernet switches do not output log information to the console.

This command takes effect only after system logging is started.

Related command: **info-center enable, display info-center**.

Example

Configure to output log information to the console through channel 0.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] 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 the system log function.

Use the **undo info-center enable** command to disable system log function.

By default, system log function is enabled.

Only after the system log function is enabled can the system output the log information to the info-center loghost and console, and so on.

Related command: **info-center loghost, info-center logbuffer, info-center console channel, info-center monitor channel, display info-center**.

Example

Enable the system log function.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] info-center enable
```

info-center logbuffer

Syntax

info-center logbuffer [**channel** { *channel-number* | *channel-name* } | **size** *buffersize*]*

undo info-center logbuffer [**channel** | **size**]

View

System view

Parameter

channel: Configures the channel to output information to buffer.

channel-number: Channel number, ranging from 0 to 9, that is, system has ten channels.

channel-name: Specifies the channel name. The name can be **channel7, channel8, channel9, console, logbuffer, loghost, monitor, snmpagent, trapbuffer, logfile**.

size: Configures the size of buffer.

buffersize: Size of buffer (number of messages which can be kept).

Description

Use the **info-center logbuffer** command to configure to output information to the memory buffer.

Use the **undo info-center logbuffer** command to cancel the information output to buffer.

By default, the switch outputs information to the memory buffer whose size is 512, that is, the memory buffer can hold 512 messages.

This command takes effect only after the system logging is enabled.

Related command: **info-center enable, display info-center**.

Example

Send log information to buffer and sets the size of buffer to 50.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] info-center logbuffer size 50
```

info-center logfile

Syntax

info-center logfile

undo info-center logfile

View

System view

Parameter

None

Description

Use the **info-center logfile** command to configure to output information to the logfile.

Use the **undo info-center logfile** command to cancel the information output to logfile.

This command takes effect only after the system logging is enabled.

Related command: **info-center enable, display info-center**.

Example

Send log information to logfile.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] info-center logfile
```

info-center loghost

Syntax

info-center loghost { **source** *interface-type interface-number* | *host-ip-addr* [**channel** { *channel-number* | *channel-name* } | **facility** *local-number* | **language** { **chinese** | **english** }]*}

undo info-center loghost *host-ip-addr*

View

System view

Parameter

host-ip-addr: IP address of info-center loghost.

channel: Configures information channel of the info-center loghost.

channel-number: Channel number, ranging from 0 to 9, that is, system has ten channels.

channel-name: Specifies the channel name. The name can be **channel7, channel8, channel9, console, logbuffer, loghost, monitor, snmpagent, trapbuffer, logfile**.

Source: Source address of the packet sent to the loghost.

interface-type interface-number: Type and number of interface sending log file.

facility: Configures the recording tool of info-center loghost.

local-number: Record tool of info-center loghost, ranging from local0 to local7.

language: Sets the logging language.

chinese,**english**: Language used in log file.

Description

Use the **info-center loghost** command to configure the system to output information to the log host.

Use the **undo info-center loghost** command to cancel output to info-center loghost.

By default, Ethernet switches do not output information to info-center loghost.

This command takes effect only after the system logging is enabled.

Related command: **info-center enable, display info-center**.

Example

Configure to send log information to the UNIX workstation at 202.38.160.1.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] info-center loghost 202.38.160.1
```

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: Layer 3 interface on the switch.

Description

Use the **info-center loghost source** command to specify source address of the packets sent to loghost as the address of the interface specified by the *interface-name*.

Use the **undo info-center loghost source** command to cancel the specified source address of the packets sent to loghost.

Related command: **info-center enable, display info-center**.

Example

Specify source address of the packets sent to loghost as the address of the VLAN interface 1.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] info-center loghost source vlan-interface 1
```

info-center monitor channel

Syntax

info-center monitor channel { *channel-number* | *channel-name* }

undo info-center monitor channel

View

System view

Parameter

channel-number: Channel number, ranging from 0 to 9, that is, the system has ten channels.

channel-name: Channel name. The name can be **channel7, channel8, channel9, console, logbuffer, loghost, monitor, snmpagent, trapbuffer, logfile**.

Description

Use the **info-center monitor channel** command to configure the channel to output the log information to the user terminal.

Use the **undo info-center monitor channel** command to restore the channel to output the log information to the user terminal to default value.

By default, Ethernet switches do not output log information to user terminal.

This command takes effect only after system logging is started.

Related command: **info-center enable, display info-center**.

Example

Configure channel 0 to output log information to user terminal.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] 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: Channel number, ranging from 0 to 9, that is, the system has ten channels. By default, channel 5 is used.

channel-name: Channel name. The name can be **channel7, channel8, channel9, console, logbuffer, loghost, monitor, snmpagent, trapbuffer, logfile**.

Description

Use the **info-center snmp channel** command to configure new channel for transmitting the SNMP information.

Use the **undo info-center snmp channel** command to restore the default channel for transmitting the SNMP information.

The default channel for transmitting the SNMP information is channel 5.

Related command: **display snmp**.

Example

Configure channel 6 as the SNMP information channel.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] info-center snmp channel 6
```

info-center source

Syntax

info-center source { *modu-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 { *modu-name* | **default** | **all** } **channel** { *channel-number* | *channel-name* }

View

System view

Parameter

modu-name: Module name.

Table 145 gives the details.

Table 145 The module name field

Module name	Description
8021X	802.1X module
ACL	ACL (access control list) module
ADBM	MAC address management module
ARP	ARP (address resolution protocol) module
BGP	BGP (border gateway protocol) module
CFM	Configuration file management module
CMD	Command module
default	Default setting of all modules
DEV	Device management module
DHCP	Dynamic host configuration protocol module
DIAGCLI	Diagnosis module
DNS	Domain name server module
DRVMPLS	MPLS (multiprotocol label switching) drive module
DRV_L2	Layer 2 drive module
DRV_L3	Layer 3 drive module
DRV_L3MC	Layer 3 multicast module
MPLS	MPLS (multiprotocol label switching) drive module
DRVQACL	QACL drive module
DRVVPLS	VPLS (virtual private LAN service) drive module
ETH	Ethernet module
FTPS	FTP server module
HA	High availability module
HABP	HABP (3Com authentication bypass protocol) module
HWCM	3Com configuration management MIB module

Table 145 The module name field

Module name	Description
IFNET	Interface management module
IGSP	IGMP snooping module
IP	IP (internet protocol) module
ISIS	IS-IS (intermediate system-to-intermediate system intradomain routing protocol) module
L2INF	L2 interface management module
L2V	L2 VPN module
LACL	LAN switch ACL module
LDP	LDP (label distribution protocol) module
LINKAGG	LINKAGG module
LQOS	LAN switch QoS module
LS	Local server module
LSPAGENT	LSP (label switched path) agent module
LSPM	LSPM (label switch path management) module
MIX	Dual system management module
MMC	MMC module
MODEM	Modem module
MPLSFW	MPLS forward module
MPM	Multicast port management module
MSDP	MSDP (multicast source discovery protocol) module
MSTP	MSTP (multiple spanning tree protocol) module
NTP	NTP (network time protocol) module
OSPF	OSPF (open shortest path first) module
PHY	Physical sublayer & physical layer module
PPP	PPP module
PSSINIT	PSSINIT module
RDS	RADIUS module
RM	Routing management module
RMON	Remote monitor module
RSA	RSA (Revest, Shamir and Adleman) encryption module
RTPRO	Routing protocol module
SHELL	User interface module
SNMP	SNMP (simple network management protocol) module
SOCKET	Socket module
SSH	Secure Shell module
SYSM	System manage veneer module
SYSMIB	System MIB module
TELNET	Telnet module
VFS	VFS (virtual file system) module
VLAN	VLAN (virtual local area network) module
VRRP	VRRP (virtual router redundancy protocol) module

Table 145 The module name field

Module name	Description
VTY	VTY (virtual type terminal) module

default: All the modules.

log: Log information.

trap: Trap information.

all: Clears all the information filtering configuration on the channelnum channel except the default one.

debugging: Debugging information.

level: Level.

severity: Information level, do not output information below this level.

Table 146 gives detailed severity information:

Table 146 Severity levels defined in the information center

Severity	Value	Description
emergencies	1	Emergent errors
alerts	2	Errors you must correct immediately
critical	3	Critical errors
errors	4	Errors requiring your attention but not critical
warnings	5	Warning, an error may occur
notifications	6	Information requiring your attention
informational	7	General prompt information
debugging	8	Debugging information

By default, the information level of each channel is as follows:

Table 147 Default information level of each channel

channel	Log information level	Trap information level	Debugging information level
Console	warning	debugging	debugging
Terminal	warning	debugging	debugging
Log host	informational	debugging	debugging
Trapbuffer	informational	warning	debugging
Logbuffer	warning	debugging	debugging
SNMPagent	debugging	warning	debugging
Logfile	warning	debugging	debugging
Channel7	debugging	debugging	debugging
Channel8	debugging	debugging	debugging
Channel9	debugging	debugging	debugging

By default, the information switch state of each channel is shown in Table 148:

Table 148 Default information switch state of each channel

Channel	Log information switch	Trap information switch	Debug information switch
Console	Enable	Disable	Enable
Terminal	Enable	Disable	Enable
Log host	Enable	Enable	Disable
Trapbuffer	Disable	Enable	Disable
Logbuffer	Enable	Disable	Disable
SNMPagent	Disable	Enable	Disable
Logfile	Enable	Disable	Disable
Channel7	Enable	Enable	Disable
Channel8	Enable	Enable	Disable
Channel9	Enable	Enable	Disable

If you only specify the level for one/two of the three types of information, the level(s) of the unspecified two/one return(s) to the default. For example, if you only define the level of the log information, then the levels of the trap and debugging information return to the defaults.

channel-number: Channel number to be set.

channel-name: Channel name to be set. The name can be **channel7, channel8, channel9, console, logbuffer, loghost, monitor, snmpagent, trapbuffer, logfile**.

state: Sets the state of the information.

state: Specifies the state as **on** or **off**.

Description

Use the **info-center source** command to add/delete a record to the information channel.

Use the **undo info-center source** command to cancel the contents of the information channel.

Use this command to configure the information of log/trap/debugging type. For example, for the filter of IP module log output, you can configure to output the logs at a level higher than warnings to the log host and output those higher than informational to the log buffer. You can also configure to output the trap information on the IP module to a specified trap host, and so on.

The channels for filtering in all the directions are specified by this configuration command. All the information will be sent to the corresponding directions through the specified channels. You can configure the channels in the output direction, channel filter information, filtering and redirecting of all kinds of information.

At present, the system distributes an information channel in each output direction by default, shown as follows:

Table 149 Default information channel in each output direction

Output direction	Information channel name
Console	console
Monitor	monitor
Info-center loghost	loghost
Log buffer	logbuffer
Trap buffer	trapbuffer
snmp	snmpagent
Log file	logfile

In addition, each information channel has a default record with the module name "default" and module number as 0xffff0000. However, for different information channel, the default log, trap and debugging settings in the records may be different with one another. Use default configuration record if a module does not have any specific configuration record in the channel.

Example

Configure to enable the log information of VLAN module in SNMP channel and allows the output of the information with a level higher than emergencies.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] info-center source vlan channel snmp log level emergencies
```

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: Debugging information.

boot: Time elapsing after system starts. Format: xxxxxx.yyyyyy, xxxxxx is the high 32 bits of the elapsed time (in milliseconds) after system starts, and yyyyyy is the low 32 bits.

date: Current system date and time. It shows as yyyy/mm/dd-hh:mm:ss in Chinese environment and mm dd hh:mm:ss yyyy in Western language environment.

none: No timestamp format.

Description

Use the **info-center timestamp** command to configure the timestamp output format in debugging/trap information.

Use the **undo info-center timestamp** command to disable the output of timestamp field.

By default, date stamp is used.

Example

Configure the debugging information timestamp format as boot.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] info-center timestamp debugging boot
```

info-center trapbuffer

Syntax

info-center trapbuffer [**size** *buffersize* | **channel** { *channel-number* | *channel-name* }]*

undo info-center trapbuffer [**channel** | **size**]

View

System view

Parameter

size: Configures the size of the trap buffer.

buffersize: Size of trap buffer (numbers of messages).

channel: Configures the channel to output information to trap buffer.

channel-number: Channel number, ranging from 0 to 9, that is, the system has ten channels.

channel-name: Channel name which can be the **channel7**, **channel8**, **channel9**, **console**, **logbuffer**, **loghost**, **monitor**, **snmpagent**, **trapbuffer**, **logfile**

Description

Use the **info-center trapbuffer** command to output information to the trap buffer.

Use the **undo info-center trapbuffer** command to cancel output information to trap buffer.

By default, output information is transmitted to trap buffer and size of trap buffer is 256, that is, the trap buffer can hold 256 messages.

This command takes effect only after the system logging is enabled.

The information can be output to the trap buffer by configuring the size of the buffer.

Related command: **info-center enable, display info-center**.

Example

Send information to the trap buffer and sets the size of the buffer to 30.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] info-center trapbuffer size 30
```

reset logbuffer

Syntax

reset logbuffer

View

User view

Parameter

None

Description

Use the **reset logbuffer** command to reset information in log buffer.

Example

Clear information in log buffer.

```
<SW8800> reset logbuffer
```

reset trapbuffer

Syntax

reset trapbuffer

View

User view

Parameter

None

Description

Use the **reset trapbuffer** command to reset information in trap buffer.

Example

Clear information in trap buffer.

```
<SW8800> reset trapbuffer
```

terminal debugging

Syntax

terminal debugging

undo terminal debugging

View

User view

Parameter

None

Description

Use the **terminal debugging** command to configure to display the debugging information on the terminal.

Use the **undo terminal debugging** command to configure not to display the debugging information on the terminal.

By default, the terminal display function of debugging information is disabled.

Related command: **debugging**.

Example

Enable the terminal display debugging.

```
<SW8800> terminal debugging
```

terminal logging

Syntax

terminal logging

undo terminal logging

View

User view

Parameter

None

Description

Use the **terminal logging** command to enable terminal log information display.

Use the **undo terminal logging** command to disable terminal log information display.

By default, the log information display is enabled on the console and disabled on the terminal.

Example

Disable the terminal display function of log information.

```
<SW8800> undo terminal logging
```

terminal monitor

Syntax

terminal monitor

undo terminal monitor

View

User view

Parameter

None

Description

Use the **terminal monitor** command to enable the terminal display functions.

Use the **undo terminal monitor** command to disable the terminal display functions.

By default, the system enables the functions of debugging/log/trap information on the console and disable them on the terminal.

This command only takes effect on the current terminal where the commands are input. The debugging/log/trap information can be output to the current terminal, beginning in user view. When the terminal monitor is shut down, no debugging/log/trap information will be displayed in local terminal, which is equals to having performed **undo terminal debugging, undo terminal logging, undo terminal trapping** commands. When the terminal monitor is enabled, you can use **terminal debugging / undo terminal debugging**, **terminal logging / terminal logging** and **terminal trapping / undo terminal trapping** respectively to enable or disable the corresponding functions.

Example

Disable the terminal monitor.

```
<SW8800> undo terminal monitor
```

terminal trapping

Syntax

terminal trapping

undo terminal trapping

View

User view

Parameter

None

Description

Use the **terminal trapping** command to enable terminal display function of trap information.

Use the **undo terminal trapping** command to disable this function.

By default, this function is enabled.

Example

Enable the terminal display function of trap information.

```
<SW8800> terminal trapping
```

61 System Maintenance Commands

Basic System Configuration and Management Commands

clock datetime

Syntax

clock datetime *HH:MM:SS YYYY/MM/DD*

View

User view

Parameter

HH:MM:SS: Current time. *HH* ranges from 0 to 23. *MM* and *SS* range from 0 to 59.

YYYY/MM/DD: Year, month and date. *YYYY* ranges from 2000 to 2100. *MM* ranges from 1 to 12 and *DD* ranges from 1 to 31.

Description

Use the **clock datetime** command to configure the current date and clock of the switch.

By default, the date and clock of the switch is set to 0:0:0, 2000/1/1.

The current date and clock of the switch must be set by this command where absolute time is strictly required.

Related command: **display clock**.

Example

Set the current date of the switch to 0:0:0, 2001/01/01.

```
<SW8800> clock datetime 0:0:0 2001/01/01
```

clock summer-time

Syntax

clock summer-time *zone-name* { **one-off** | **repeating** } *start-time start-date end-time end-date offset-time*

undo clock summer-time

View

User view

Parameter

zone-name: Name of the summer time, which is a string of 1 to 32 characters.

one-off: Sets the summer time of a certain year.

repeating: Sets the summer time of every year starting from a certain year.

start-time: Sets start time of the summer time, in the form of *HH:MM:SS* (hour/minute/second).

start-date: Sets start date of the summer time, in the form of *YYYY/MM/DD* (year/month/day).

end-time: Sets end time of the summer time, in the form of *HH:MM:SS* (hour/minute/second).

end-date: Sets end date of the summer time, in the form of *YYYY/MM/DD* (year/month/day).

offset-time: Sets the offset relative to the summer time, in the form of *HH:MM:SS* (hour/minute/second).

Description

Use the **clock summer-time** command to set the name, start and end time of the summer time.

Use the **undo clock summer-time** command to restore the local time to the default UTC time.

After the configuration takes effect, the **display clock** command can be used to check it. Besides, the time of the log or debugging information uses the local time after the adjustment of the time zone and summer time.

Related command: **clock timezone**.

Example

Set the summer time for z2 that starts at 06:00:00 on 08/06/2002 and ends at 06:00:00 on 01/09/2002 with the time adding 1 hour.

```
<SW8800> clock summer-time z2 one-off 06:00:00 2002/06/08 06:00:00
2002/09/01 01:00:00
```

Set the summer time for z2 that starts at 06:00:00 on 08/06 and ends at 06:00:00 on 01/09 in each year from 2002 on with the time adding 1 hour.

```
<SW8800> clock summer-time z2 repeating 06:00:00 2002/06/08 06:00:00

2002/09/01 01:00:00
```

clock timezone

Syntax

clock timezone *zone-name* { **add** | **minus** } *HH:MM:SS*

undo clock timezone

View

User view

Parameter

zone-name: Name of the time zone, which is a character with the length ranging from 1 to 32.

add: Tme is adding compared with the UTC.

minus: Time is minus compared with the UTC.

HH:MM:SS: Time (hour/minute/second).

Description

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

Use the **undo clock timezone** command to restore to the default Universal Time Coordinated (UTC) time zone.

After the configuration takes effect, the **display clock** command can be used to check it. Besides, the time of the log or debug information uses the local time after the adjustment of the time zone and summer time.

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

Example

Set the name of the local time zone to Z5 with five hours adhead compared with the UTC time.

```
<SW8800> clock timezone z5 add 05:00:00
```

quick-ping enable

Syntax

quick-ping enable

undo quick-ping enable

View

System view

Parameter

None

Description

Use the quick-**ping enable** command to enable the PING distribution function.

Use the **undo quick-ping enable** command to disable the PING distribution function.

By default, the PING distribution function is enabled.

Example

Enable the ping distribution function.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] quick-ping enable
```

sysname

Syntax

sysname *sys-name*

undo sysname

View

System view

Parameter

sys-name: Hostname of the switch. A string of 1 to 30 characters. The default hostname of the switch is 3Com.

Description

Use the **sysname** command to configure the system name of the switch.

Changing the hostname name of the switch will affect the prompt of command line interface. For example, if the system name of the switch is 3Com, and the prompt in user view is <SW8800>.

Use the **undo sysname** command to restore the system name of the switch to the default value.

Example

Set the system name of the switch to 3ComLANSwitch.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] sysname 3ComLANSwitch
[3ComLANSwitch]
```

System Status and System Information Query Commands

display clock

Syntax

display clock

View

Any view

Parameter

None

Description

Use the **display clock** command to display the system date and time information, so that you make timely changes if the system time is incorrect.

The maximum time value supported by this command is 23:59:59 9999/12/31.

Related command: **clock datetime**.

Example

View the current system date and time.

```
<SW8800> display clock
18:36:31 beijing Sat 2002/02/02
Time Zone : beijing add 01:00:00
Summer-Time : bj one-off 01:00:00 2003/01/01 01:00:00 2003/08/08 01:00:00
```

Table 150 Description on the fields of the display clock command

Field	Description
18:36:31 beijing Sat 2002/02/02	Current system time
Time Zone : beijing add 01:00:00	Configured time zone information
Summer-Time : bj one-off 01:00:00 2003/01/01 01:00:00 2003/08/08 01:00:00	Configured summer time information

display debugging

Syntax

display debugging [**interface** *interface-type interface-number*] [*module-name*]

View

Any view

Parameter

interface-type: Interface type supported by the switch, including Ethernet, GigabitEthernet, AUX, and Vlan-interface.

interface-number: Interface number.

module-name: Module name.

Description

Use the **display debugging** command to display debugging that has been enabled.

You can execute the **display debugging** to view the specific debugging that has been enabled. If the command is executed without any parameter specified, the system will display all debugging that has been enabled.

Related command: **debugging**.

Example

Display all debugging that has been enabled.

```
<SW8800> display debugging
Multicast packet forwarding debugging switch is on
```

display fiber-module

Syntax

display fiber-module [*interface-type interface-number*]

View

Any view

Parameter

interface-type: Interface type supported by switch, including Ethernet and GigabitEthernet.

interface-number: Interface number.

Description

Use the **display fiber-module** command to display the information of the optical modules connected with all the optical interfaces in position on the current shelf, including module information, optical module type, connector type, vendor name, manufacturer part number, single mode or multi-mode, wave length, and transmission distance.

Use the **display fiber-module** [*interface-type interface-number* | *interface-name*] command to display optical module information of the specified port.

Example

Display the optical module information of all optical interfaces in position on the current shelf.

```
<SW8800> display fiber-module
Pos3/1/1:
Card info: 10G-XFP
Fiber connect: LC
VendorName: Intel Corp
PartNumber: TXN181072013X07
Mode: SingleMode
WaveLength: 1310nm
Length for 9um: 10km

Pos4/1/1:
Card info: 100BASE-SFP
Fiber connect: LC
VendorName: AGILENT
PartNumber: HFBR-5760LP
Mode: MultiMode
WaveLength: Unknown
Length for 50/125um: 0m
Length for 62.5/125um: 2000m

Warning: This Port Use Wrong Optical Module !

Pos4/1/2:
Card info: 1000BASE-SFP
Fiber connect: LC
VendorName: Hitachi Cable
PartNumber: HTR6511R
Mode: SingleMode
WaveLength: 1310nm
Length for 9um: 10km

Warning: This Port Use Wrong Optical Module !
```

```
Pos4/1/3:
Card info: 2.5G-SFP
Fiber connect: LC
VendorName: FIBERXON INC
PartNumber: FTM-3125C-L2
Mode: SingleMode
WaveLength: 1310nm
Length for 9um: 2km

Pos4/1/4:
Card info: 1000BASE-SFP
Fiber connect: LC
VendorName: AGILENT
PartNumber: HFBR-5710L
Mode: MultiMode
WaveLength: 850nm
Length for 50/125um: 550m
Length for 62.5/125um: 270m

Warning: This Port Use Wrong Optical Module !

GigabitEthernet6/1/1:
Card info: 10G-XFP
Fiber connect: LC
VendorName: JDS Uniphase
PartNumber: 64P0215
Mode: SingleMode
WaveLength: 1310nm
Length for 9um: 10km

GigabitEthernet6/1/3:
Card info: 10G-XFP
Fiber connect: LC
VendorName: JDS Uniphase
PartNumber: 64P0215
Mode: SingleMode
WaveLength: 1310nm
Length for 9um: 10km
```

Please refer to the following table for the information above.

Table 151 Description on the fields of the display fiber-module command

Field	Description
Card info	Card information
Fiber connect	Fiber connector type
VendorName	Vendor name
PartNumber	Manufacturer part number
Mode	Single mode or multi-mode
WaveLength	Wave length
Length for X um: Y km/m	The transmission distance of X-um sized fiber is Y km/m
Length for A / B um: Y km/m	The transmission diatance of the fiber with an inner diameter of A um and outer diameter of B um is Y km/m.

display users

Syntax

display users [**all**]

View

Any view

Parameter

all: Displays all users connected to the switch.

Description

Use the **display users** command to view information about users connected to the switch.

Example

Display the information about all the active users on the console.

```
<SW8800> display users
        UI    Delay     Type   Ipaddress     Username
+ 0   CON 0   00:00:00
  130 VTY 0   00:00:05  TEL  192.168.1.253   tb
```

Display the information about all the users on the console.

```
<SW8800> display users all
        UI    Delay     Type   Ipaddress     Username
+ 0   CON 0   00:00:00
  129 AUX 0
+ 130 VTY 0   00:00:16  TEL  192.168.1.253   tb
  131 VTY 1
  132 VTY 2
  133 VTY 3
  134 VTY 4
```

Table 152 Description on the fields of the display users command

Field	Description
+	Information about an active user
UI	The first number is the absolute number of the UI (user interface), and the second number is the relative number of the UI.
Delay	The time elapsing after the last user input, in the format of hh:mm:ss
Type	User type, such as Telnet, SSH, PAD
Ipaddress	Initial connection location, that is, the IP address of the incoming host
Username	Name of the user who uses this UI, that is, the login username of this user. If the current terminal line is in anonymous login mode (AAA authentication is enabled on it), this field is null

display version

Syntax

display version

View

Any view

Parameter

None

Description

Use the **display version** command to view such information as software version, issue date and the basic hardware configurations.

Example

Display the information about the system version.

```
<SW8800> display version
Copyright Notice:
All rights reserved (Sep 15 2005).
Without the owner's prior written consent, no decompiling
nor reverse-engineering shall be allowed.
3Com-3Com Versatile Routing Platform Software
Copyright (c) 2004-2005 Hangzhou 3Com-3Com Technology Co.,Ltd. and
its licensors All rights reserved.
Copyright (c) 1998-2003 3Com Corporation Co.,Ltd. All rights reserved.
3Com Switch 8800 Family uptime is 0 week, 2 days, 1 hours, 17 minutes
SRPA 0:  uptime is 0 weeks,2 days,1 hour,17 minutes
3ComSwitch 8800 Family with 1 MPC755 Processor
512M    bytes SDRAM
16384K  bytes Flash Memory
512K    bytes NVRAM Memory
PCB Version      :   Ver.F
BootROM Version  :   111
CPLD Version     :   001
Software Version :   Switch 8800 Family-Comware 310-r1265

3CV17538:  uptime is 0 weeks,2 days,1 hour,15 minutes
3ComSwitch 8800 Family LPU with 1 MPC8245 Processor
128M    bytes SDRAM
0K      bytes NVRAM Memory
PCB Version      :   REV.0
BootROM Version  :   103
CPLD Version     :   002
Software Version :   Switch 8800 Family-Comware 310-r1265
CPUCard   1
  PCB Ver        :   .4
  CPLD Ver       :   001
  SubCard   1
  PCB Ver        :   Ver.B
  CPLD Ver       :   NONE
  SubCard   2
  PCB Ver        :   REV.0
  CPLD Ver       :   NONE
```

System Debug Commands

debugging

Syntax

debugging { **all** | **timeout** *interval* | *module-name* [*debugging-option*] }

undo debugging { **all** | *module-name* [*debugging-option*] }

View

User view

Parameter

all: Enables or disables all the debugging.

timeout *interval*: Specifies the interval (in minutes) during which the **debugging all** switch is on. The value ranges from 1 to 1440. With this configuration, all debugging takes the time at which it is enabled as the start time, and takes effect during the predefined time. And after that, all debugging is disabled.

module-name: Module name.

debugging-option: Debugging option.

Description

Use the **debugging** command to enable the system debugging.

Use the **undo debugging** command to disable the system debugging.

By default, all the debugging processes are disabled.

The switch provides various kinds of debugging functions for technical support personnel and experienced maintenance staff to troubleshoot the network.

Enabling the debugging will generate a large amount of debugging information and decrease the system efficiency. Specially, network system may collapse after all the debugging is enabled by the **debugging all** command. So it is not suggested to use the **debugging all** command. It is convenient for the user to disable all the debugging with **undo debugging all** command.

Related command: **display debugging**.

Example

Enable IP packet debugging.

```
<SW8800> debugging ip packet
IP packet debugging switch is on.
```

The above output shows that the IP packet debugging is enabled.

display diagnostic-information

Syntax

display diagnostic-information

View

Any view

Parameter

None

Description

Use the **display diagnostic-information** command to view the current configuration information about all running modules. You can use all the information to help diagnose and troubleshoot the switch.

When the switch does not run well, you can collect all sorts of information about the switch to locate the source of fault. However, each module has many corresponding display commands, which makes it difficult for you to collect all the information needed. In this case, you can use **display diagnostic-information** command.

Example

Display all system configuration information.

```
<SW8800> display diagnostic-information
This operation may take a few minutes, continue?[Y/N]y
------------------- display version --------------------
3Com-3Com Versatile Routing Platform Software
Comware(R) Software, Version COMWAREHZV300R001B08D018, Release 0001
Comware(tm) Lanswitch Platform Software Version COMWAREHZV300R001B08D018
Switch 8800 Family Software Version V100R002B02D018
Switch 8800 Family Product Version Switch 8800 Family-Comware 310-r1266
Copyright (c) 2004-2005 3Com-Corporation and its
licensors All rights reserved.
Copyright (c) 1998-2003 3Com Corporation Co.,Ltd. All rights reserved.
Compiled Sep 29 2005 03:43:00, RELEASE SOFTWARE
3Com Switch 8800 Family uptime is 0 week, 2 days, 5 hours, 31 minutes
This device is 3Com Switch 8807 (7-Slot Chassis)
.........
```

Network Connection Test Commands

ping

Syntax

ping [**ip**] [-**a** *ip-address* | **-c** *count* | **-d** | - **f** | -**h** *ttl* | -**i** *interface-type interface-number* | **-n** | **- p** *pattern* | **-q** | **-r** | **-s** *packetsize* | **-t** *timeout* | **-tos** *tos* | **-v** | **-vpn-instance** *vpn-instance-name*]* *host*

View

Any view

Parameter

-a *ip-address*: Specifies the source IP address to transmit ICMP ECHO-REQUEST.

-**c**: *count* Specifies how many times the ICMP ECHO-REQUEST packet will be transmitted. The *count* argument rangs from 1 to 4,294,967,295. The default value is five.

-**d**: Configures the socket to be in DEBUGGING mode. By default, the socket is other than DEBUGGING mode.

-f: Configures the packet to be dropped instead of being fragmented when the packet length is larger than interface MTU.

-**h** *ttl*: Configures the TTL value for echo requests to be sent. The TTL value ranges from 1 to 255. The default value is 255.

-i: **Specifies an interface to send packets**.

interface-type: Specifies the interface type.

interface-number: Specifies the interface number.

-**n**: Configures to take the host parameter as IP address without domain name resolution.

-**p**: *pattern* is the hexadecimal padding of ICMP echo-request, for example -p ff pads the packet completely with ff. By default, the starting padding is 0x01, crescent, and the ending padding is 0x09, and then repeat.

-q: Configures not to display any other detailed information except statistics.

-r: Record route. By default, the system does not record route.

-s *packetsize*: Specifies the length of ECHO-REQUEST (excluding IP and ICMP packet header) in bytes. The length of the echo-request packet defaults to 56 bytes.

-**t** *timeout*: Maximum waiting time after sending the echo-request (measured in ms). The time defaults to 2000 ms.

-tos *tos:* Specifies TOS value for echo requests to be sent, range from 0 to 255. The default value is 0.

-**v**: Displays other received ICMP packets (non echo-response). By default, no other non echo-response ICMP packets is displayed.

-**vpn-instance** *vpn-instance-nam*: VPN instance name.

host: Destination host domain name or IP address of the destination host.

ip: Chooses IP ICMP packet.

Description

Use the **ping** command to check the IP network connection and the reachability of the host.

The **ping** command sends ICMP ECHO-REQUEST message to the destination. If the network to the destination works well, then the destination host will send ICMP ECHO-REPLY to the source host after receiving ICMP ECHO-REQUEST.

Perform **ping** command to troubleshoot the network connection and line quality. The output information includes:

- Responses to each of the ECHO-REQUEST messages. If the response message is not received until timeout, output "Request time out". Or display response message bytes, packet sequence number, TTL and response time.

- The final statistics, including number of sent packets, number of response packets received, percentage of non-response packets and minimal/maximum/average value of response time.

If the network transmission rate is too low, you can increase the response message timeout.

*At present, the **ping -i** command only supports the direct route and is used to test the the connectivity of the direct route.*

Related command: **tracert**.

Example

Check whether the host 202.38.160.244 is reachable.

```
<SW8800> ping 202.38.160.244
ping 202.38.160.244 : 56 data bytes
Reply from 202.38.160.244 : bytes=56 sequence=1 ttl=255 time = 1ms
Reply from 202.38.160.244 : bytes=56 sequence=2 ttl=255 time = 2ms
Reply from 202.38.160.244 : bytes=56 sequence=3 ttl=255 time = 1ms
Reply from 202.38.160.244 : bytes=56 sequence=4 ttl=255 time = 3ms
Reply from 202.38.160.244 : bytes=56 sequence=5 ttl=255 time = 2ms
--202.38.160.244 ping statistics--
5 packets transmitted
5 packets received
0% packet loss
round-trip min/avg/max = 1/2/3 ms
```

tracert

Syntax

tracert [**-a** *source-IP* | **-f** *first-TTL* | **-m** *max-TTL* | **-p** *port* | **-q** *num-packet* | **-vpn-instance** *vpn-instance-name* | **-w** *timeout*] *string*

View

Any view

Parameter

-a *source-IP*: Configures the source IP address used by tracert command;

-**f**: Configures to verify the -f switch, *first-TTL* specifies an initial TTL, ranging from 0 to the maximum TTL.*first-TTL* defaults to 1;

-**m**: Configures to verify the -m switch, *max-TTL* specifies a maximum TTL larger than the initial TTL. *max-TTL* defaults to 30;

-p: Configures to verify the -p switch, *port* is an integer host port number. Generally, user need not modify this option. *port* defaults to 33434;

-q: Configures to verify the -q switch, *nqueries* is an integer specifying the number of query packets sent, larger than 0. *num-packet* defaults to 3;

-**vpn-instance** *vpn-instance-name*: VPN instance name;

-w: Configures to verify the -wf switch, *timeout* is an integer specifying IP packet timeout in seconds, larger than 0.*timeout* defaults to 5s;

string: IP address of the destination host or the hostname of the remote system.

Description

Use the command to Using **tracert** command, you can check the reachability of network connection and troubleshoot the network. User can test gateways passed by the packets transmitted from the host to the destination.

By default, when the parameters are not specified,

The **tracert** command sends a packet with TTL 1, and the first hop will send an ICMP error message back to indicate this packet cannot be transmitted (because of TTL timeout). Then this packet will be sent again with TTL 2, and the second hop will indicate a TTL timeout error. Perform this operation repeatedly till reaching the destination. These processes are operated to record the source address of each ICMP TTL timeout so as to provide a path to the destination for an IP packet.

After **ping** command finds some error on the network, perform **tracert** to locate the error.

The output of **tracert** command includes IP address of all the gateways to the destination. If a certain gateway times out, output "***".

CAUTION: *For the moment, you can not use the **tracert** command on the Switch 8800 Family routing switch to test whether the network connection is reachable or analyze where the fault happens in the network in the MPLS domain.*

Example

Test the gateways passed by the packets to the destination host at 18.26.0.115.

```
<SW8800> tracert 18.26.0.115
tracert to allspice.lcs.mit.edu (18.26.0.115), 30 hops max
1 helios.ee.lbl.gov (128.3.112.1) 0 ms 0 ms 0 ms
2 lilac-dmc.Berkeley.EDU (128.32.216.1) 19 ms 19 ms 19 ms
3 lilac-dmc.Berkeley.EDU (128.32.216.1) 39 ms 19 ms 19 ms
4 ccngw-ner-cc.Berkeley.EDU (128.32.136.23) 19 ms 39 ms 39 ms
5 ccn-nerif22.Berkeley.EDU (128.32.168.22) 20 ms 39 ms 39 ms
6 128.32.197.4 (128.32.197.4) 59 ms 119 ms 39 ms
7 131.119.2.5 (131.119.2.5) 59 ms 59 ms 39 ms
8 129.140.70.13 (129.140.70.13) 80 ms 79 ms 99 ms
9 129.140.71.6 (129.140.71.6) 139 ms 139 ms 159 ms
10 129.140.81.7 (129.140.81.7) 199 ms 180 ms 300 ms
11 129.140.72.17 (129.140.72.17) 300 ms 239 ms 239 ms
12 * * *
13 128.121.54.72 (128.121.54.72) 259 ms 499 ms 279 ms
14 * * *
15 * * *
16 * * *
17 * * *
18 ALLSPICE.LCS.MIT.EDU (18.26.0.115) 339 ms 279 ms 279 ms
```

62 PROTOCOL PORT SECURITY CONFIGURATION COMMANDS

Protocol Port security Configuration Commands

ip portsafe

Syntax

ip portsafe enable

undo ip portsafe enable

View

System view

Parameter

None

Description

Use the **ip portsafe enable** command to enable the protocol port security function to check all IP packets on the interface module. If the destination IP is the virtual interface IP of the switch, and the corresponding destination protocol port is not open, the packet will be dropped.

Use the **undo ip portsafe enable** command to disable the protocol port security function. Then all packets on the interface module are not checked.

By default, the fabric enables the protocol port security function. So do the standby module and the interface module.

At present, the following protocols are being checked:

Table 153 State of the protocol port

Protocol	Port	Default State
IGMP/IGSP	PROTOCOL:2	Close
OSPF	PROTOCOL:89	Close
PIM	PROTOCOL:123	Close
SSH	TCP:22	Close
TELNET	TCP:23	Close
HTTP	TCP:80	Open
BGP	TCP:179	Close
MPLS LDP	TCP:646	Close

Table 153 State of the protocol port

Protocol	Port	Default State
DHCP	UDP:67,68	Close
NTP	UDP:123	Close
SNMP-AGENT	UDP:161	Close
RIP	UDP:520	Close
MPLS LDP	UDP:646	Close
RADIUS CLIENT	UDP:1812	Close
RADIUS LOCAL SERVER	UDP:1645,1646	Open
PORTAL SERVER	UDP:2000	Close

The protocol port security function is short for TCP, UDP protocol port close checking function. If a protocol is not enabled, this function can drop the packet whose destination IP is the virtual interface IP of the switch, so that it reduces the unnecessary communications between the modules and the CPU operation of the fabric, and enhances the anti-interference ability of the switch to the packet.

Example

Enable the protocol port security function.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] ip portsafe enable
```

ip http shutdown

Syntax

ip http shutdown

undo ip http shutdown

View

System view

Parameter

None

Description

Use the **ip http shutdown** command to shutdown the port 80 of the HTTP protocol. After the execution of this command, all packets requiring the port 80 of this device will be dropped.

Use the **undo ip http shutdown** command to enable the port 80 of the HTTP protocol. After the execution of the command, all packets requiring the port 80 of thid device will be responsed.

By default, the port 80 of the HTTP protocol is enabled.

Example

Shutdown the port 80 of the HTTP protocol.

```
<SW8800> system-view
[SW8800] ip http shutdown
```

63
PORT PACKET STATISTICS COMMANDS

Port Packet Statistics Commands

set egress

Syntax

set egress { **counter0** | **counter1** } **slot** *slot-num* [**interface** *interface-type interface-number*] [**vlan** *vlan-id*] [**tc** *traffic-class*] [**dp** *drop-precedence*]

undo set egress { **counter0** | **counter1** } **slot** *slot-num*

View

System view

Parameter

counter0: Counter 0, used for packet statistics monitoring.

counter1: Counter 1, used for packet statistics monitoring.

slot-num: Card slot number.

interface-type interface-number: Port type and port number, which must match with the parameter *slot-num*. If you do not specify a specific port number, the command will apply to all the ports on the card. This command supports Ethernet ports.

vlan-id: VLAN ID defined in IEEE802.1Q. If you do not specify a specific VLAN, the command will apply to all VLANs.

traffic-class: Traffic class. If you do not specify a specific traffic class, the command will apply to all traffic classes.

drop-precedence: packet drop precedence. If you do not specify a drop precedence level, the command will apply to all drop precedence levels.

Description

Use the **set egress** command to set packet statistics counters.

Use the **undo set egress** command to cancel the configuration.

A card provides two sets of counters for monitoring egress packet statistics of the card. The monitored objects include ports, VLANs, ports+VLANs, and cards. In addition to these four types of objects, a traffic class (TC) or a drop precedence

(DP) can also be monitored. When monitoring a card, the counters can monitor all TCs and all DPs.

After you user the **set egress counter** command to set the monitoring mode of a card, the counters will be automatically reset.

By default, a card does not implement egress packet statistics.

Related command: **display egress**.

Note that:

- You cannot configure ports as the objects to be monitored by the egress packet statistics counters on GV48D, GT24D, GP24D, XP4B and XP4CA cards.
- After successful configuration, it is necessary to reset the counters to start counting again.

Example

Set the egress packet statistics mode of Counter 0 on slot 4 so that it monitors port GigabitEthernet4/1/1.

```
[SW8800] set egress counter0 slot 4 interface GigabitEthernet4/1/1
```

display egress counter

Syntax

display egress { **counter0** | **counter1** } **slot** *slot-num* [**clear**]

View

Any view

Parameter

counter0: Counter 0, used for packet statistics monitoring.

counter1: Counter 1, used for packet statistics monitoring.

slot-num: Card slot number.

clear: Clears the counting data after a counter is read.

Description

Use the **display egress** command to display egress packet statistics information and the monitoring objects of a counter. To clear the counter data, include the parameter **clear** in the command.

Related command: **set egress counter**.

Example

Query the egress packet statistics information of slot 4, and then clear the counter.

```
[SW8800] display egress counter0 slot 4 clear
Slot 4 egress counter0 mode:
  Interface: all
  VLAN: all
  Traffic Class: all
```

```
 Drop Precedence: all
The outgoing packets:
 Unicast: 0 packets
 Multicast: 0 packets
 Broadcast: 0 packets
 Bridege egress filtered packets: 0 packets
 TxQ filtered packets(Due to TxQ congestion ): 0 packets
```

64

PORT LOOPBACK DETECTION COMMANDS

Ethernet Port Detection Configuration Commands

loopback-detection enable

Syntax

loopback-detection enable

undo loopback-detection enable

View

System view

Parameter

None

Description

Use the **loopback-detection enable** command to enable the global port loopback detection function, so that the system can detecte whether there is an external loop on each port in a VLAN which is enabled with the loopback detection function.If a loop is found on a port, the switch will give out an alarm or give out an alarm and shutdown the port according to your configuration.

Use the **undo loopback-detection enable** command to disable the global port loopback function.

By default, the global port loopback detection function is disabled.

Related command: **display loopback-detection.**

Example

Enable the global port loopback detection function.

```
<SW8800> system-view
[SW8800] loopback-detection enable
```

loopback-detection enable vlan

Syntax

loopback-detection enable vlan { *vlanlist* | **all** }

undo loopback-detection enable vlan { *vlanlist* **| all** }

View

System view

Parameter

None

Description

Use the **loopback-detection enable vlan** command to enable the loopback detection function on a VLAN to perform the loopback detection on all ports in the VLAN.

Use the **undo loopback-detection enable vlan** command to disable the loopback detection on a VLAN.You can perform such configuration on up to 800 VLANs.

By default, the loopback detection is not performed on any VLAN.

Example

Configure the system to perform loopback detection on all ports belonging to VLAN 2.

```
<SW8800> system-view
[SW8800] loopback-detection enable vlan 2.
```

loopback-detection interval-time

Syntax

loopback-detection interval-time *time*

undo loopback-detection interval-time

View

System view

Parameter

time: Interval at which the external loopback detection is performed on ports, in the range of 60 to 7200, in seconds.The default value is 60 seconds.

Description

Use the **loopback-detection interval-time** command to set the interval at which the external loopback detection is performed on ports.

Use the **undo loopback-detection interval-time** command to restore this interval time to the default.

Related command: **display loopback-detection.**

Example

Set the interval for the external loopback detection on each port to 120 seconds.

```
<SW8800> system-view
[SW8800] loopback-detection interval-time 120#
```

loopback-detection control

Syntax

loopback-detection control

undo loopback-detection control

View

Ethernet port view

Parameter

None

Description

Use the **loopback-detection control** command to enable the control function of port loopback detection, that is, when finding a loop exist on a port of a VLAN, the system will report the trap information and shutdown the port as well.

Use the **undo loopback-detection control** command to disable the control function of port loopback detection, that is, when finding a loop exist on a port of a VLAN, the system only reports the trap information. The port will work normally.

By default, the loopback detection control function on ports is disabled.

Example

Enable the port loopback detection control function.

```
<SW8800> system-view
[SW8800] interface Ethernet 2/1/1
[3Com-GigabitEthernet2/1/1] loopback-detection control
```

loopback-detection disable

Syntax

loopback-detection disable

undo loopback-detection disable

View

Ethernet port view

Parameter

None

Description

Use the **loopback-detection disable** command to exclude the loopback detection on a port. The port executing this command will not receive the loopback detection packet sent by the CPU.

Use the **undo loopback-detection disable** command to restore the loopback detection function on a port.

By default, the port loopback detection function is enabled.

Example

Disable the port loopback detection.

```
<SW8800> system-view
[SW8800] interface Ethernet 2/1/1
[3Com-GigabitEthernet2/1/1] loopback-detection disable
```

display loopback-detection

Syntax

display loopback-detection

View

Ethernet port view

Parameter

None

Description

Use the **display loopback-detection** command to display whether the port loopback detection function is enabled or not. If the function is enabled, the command will display the interval for detections, the VLANs enabled with detection function, the existing loop, and the ports which are shutdown for loop.

Example

Display whether the port loopback detection function is enabled or not.

```
<SW8800> display loopback-detection
Loopback-detection is running on!
Detection interval time is 60 seconds!
Following vlans enable loopback-detection:
  1
Following ports are detected for loop:
  GigabitEthernet2/1/1

Following ports are shutdown for loop:
NULL
```

Table 154 Description on the fields of the display loopback-detection command

Filed	Description
Loopback-detection is running on!	Port loopback detection function is enabled.
Detection interval time is 60 seconds	Interval time for detection is 60 seconds.
Following ports are detected for loop:	Ports on which loop exists
Following ports are shutdown for loop:	Ports which are shutdown for loop

65 QinQ Configuration Commands

QinQ Configuration Commands

display port vlan-vpn

Syntax

display port vlan-vpn

View

Any view

Parameter

None

Description

Use the **display port vlan-vpn** command to display VLAN VPN-related information of the current system by port number, including current TPID, the information about VLAN-VPN ports, and the information about VLAN-VPN uplink ports.

Example

Display the VLAN VPN-related configuration of the current system.

```
[SW8800] display port vlan-vpn
VLAN-VPN TPID: 0x9100

GigabitEthernet1/1/1
 VLAN-VPN status: enabled
 VLAN-VPN VLAN: 1

GigabitEthernet1/1/2
VLAN-VPN uplink status: enabled
```

traffic-redirect

Syntax

Use the following command to deliver Layer 3 traffic classification rules.

traffic-redirect inbound ip-group { *acl-number* | *acl-name* } [**rule** *rule* [**system-index** *index*]] { **nested-vlan** *nested-vlanid* | **modified-vlan** *modified-vlanid* }

undo traffic-redirect inbound ip-group { *acl-number* | *acl-name* } [**rule** *rule*]

Use the following command to deliver Layer 2 and Layer 3 traffic classification rules simultaneously.

traffic-redirect inbound ip-group { *acl-number* | *acl-name* } [**rule** *rule*] **link-group** { *acl-number* | *acl-name* } [**rule** *rule*] { **nested-vlan** *nested-vlanid* | **modified-vlan** *modified-vlanid* }

undo traffic-redirect inbound ip-group { *acl-number* | *acl-name* } { **rule** *rule* **link-group** { *acl-number* | *acl-name* } [**rule** *rule*] | **link-group** { *acl-number* | *acl-name* } **rule** *rule* }

or

undo traffic-redirect inbound link-group { *acl-number* | *acl-name* } { **rule** *rule* **ip-group** { *acl-number* | *acl-name* } | **ip-group** { *acl-number* | *acl-name* } **rule** *rule* }

Use the following command to deliver Layer 2 traffic classification rules.

traffic-redirect inbound link-group { *acl-number* | *acl-name* } [**rule** *rule* [**system-index** *index*]] { **nested-vlan** *nested-vlanid* | **modified-vlan** *modified-vlanid* }

undo traffic-redirect inbound link-group { *acl-number* | *acl-name* } [**rule** *rule*]

View

Ethernet port view, port group view

Parameter

ip-group { *acl-number* | *acl-name* }: Specifies a basic or advanced ACL. The *acl-number* argument is the ACL number, in the range of 2,000 to 3,999. The *acl-name* argument is the ACL name, a string that is of 1 to 32 characters in length. The string must begin with an English letter (that is, a-z or A-Z]) and cannot contain spaces.

link-group { *acl-number* | *acl-name* }: Specifies a Layer 2 ACL. The *acl-number* argument is the ACL number, in the range of 4,000 to 4,999. The *acl-name* argument is the ACL name, a string that is of 1 to 32 characters in length. The string must begin with an English letter (that is, a-z or A-Z]) and cannot contain spaces.

rule *rule*: Specifies a rule of the ACL. The *rule* argument is in the range of 0 to 127. If you do not specify a rule, the system applies all rules of the ACL.

system-index *index*: Specifies the system index value of an ACL rule. The system assigns a system index to an ACL rule after delivering the ACL rule for indexing. Although not recommended, you can still specify a system index for an ACL rule manually when executing this command.

nested-vlan *nested-vlanid*: Specifies to insert VLAN tags in the packets that match the specified ACL rules as the outer VLAN tags. The *nested-vlanid* argument is the VLAN ID to be inserted.

modified-vlan *modified-vlanid*: Changes the outer VLAN tags of the packets that match the specified ACL rules. The *modified-vlanid* argument is the new VLAN ID to be inserted in the packets.

Description

Use the **traffic-redirect** { **nested-vlan** | **modified-vlan** } command to enable ACL-based traffic classification on the ports and set/modify the outer VLAN tags to be inserted in the packets that match the specified ACL rules. (Note that this command only applies to packets that match ACL rules with the **permit** keyword specified.)

Use the **undo traffic-redirect** command to remove the configuration.

- Make sure the VLAN identified by the *nested-vlanid* argument exists to prevent otherwise the packets from being discarded due to no outbound port found.
- The **traffic-redirect modified-vlan** command modifies the outer VLAN tag of a packet.
- At present, only 3C17514, 3C17516, and 3C17528 cards support the **traffic-redirect** { **nested-vlan** | **modified-vlan** } command.

Related commands: **traffic-redirect**, **acl**.

Example

Insert the VLAN tag of VLAN 4 in the packets that match ACL 4,100 as the outer VLAN tag. (With the assumption that ACL 4,100 and its rules already exist.)

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800]interface Ethernet2/1/1
[3Com-Ethernet2/1/1]traffic-redirect inbound link-group 4100 nested-vlan 4
```

vlan-vpn enable

Syntax

vlan-vpn enable

undo vlan-vpn

View

Ethernet port view/PVC view

Parameter

None

Description

Use the **vlan-vpn enable** command to enable VLAN VPN feature for the port or the PVC.

Use the **undo vlan-vpn** command to disable VLAN VPN feature for the port or the PVC.

With VLAN VPN enabled, a received packet is tagged with the default VLAN tag of the port no matter whether or not the packet carries a VLAN tag. So, if the packet already carries a VLAN tag, the default VLAN tag becomes a nested VLAN tag in the packet. Otherwise, the packet is transmitted with the default VLAN tag carried.

CAUTION:

- VLAN VPN cannot be enabled if the port has any of GVRP, STP, and 802.1x protocols enabled.
- VLAN VPN cannot be enabled on a port if the VLAN which the port belongs to has IGMP Snooping enabled or its VLAN interface has IGMP enabled. Similarly, if a port is VLAN VPN-enabled, you cannot enable IGMP Snooping in the VLAN to which the port belongs or enable IGMP on the VLAN interface of the VLAN.
- If you want to add VLAN VPN-enabled ports to a VLAN, make sure the VLAN is not IGMP Snooping-enabled, and the VLAN interface is not IGMP-enabled.
- If you have enabled VLAN VPN feature for the ports in the VLAN, the VLAN cannot be removed.

By default, the VLAN VPN feature is disabled on a port or PVC.

Example

Enable the VLAN VPN feature on the Ethernet2/1/1 port.

```
[3Com-Ethernet2/1/1] vlan-vpn enable
```

vlan-vpn tpid

Syntax

vlan-vpn tpid *value*

undo vlan-vpn tpid

View

System view

Parameter

value: TPID value to be set (in hexadecimal format). This argument ranges from 1 to 0xFFFF.

Description

Use the **vlan-vpn tpid** command to set the TPID value of the VLAN-VPN uplink ports.

Use the **undo vlan-vpn tpid** command to restore the default TPID value (0x8100) for VLAN-VPN uplink ports.

Do not set the TPID value to a value that may cause conflicts (such as the known protocol type value 0x0806, which is that of ARP packets). Otherwise, the packets may be discarded.

Table 155 Common protocol type values of an Ethernet frame

Protocol type	Value
ARP	0x0806
IP	0x0800
MPLS	0x8847/0x8848
IPX	0x8137
IS-IS	0x8000

Table 155 Common protocol type values of an Ethernet frame

Protocol type	Value
LACP	0x8809
802.1x	0x888E

Example

Set the TPID value to 0x9100.

```
[SW8800] vlan-vpn tpid 9100
```

Restore the default TPID value (0x8100).

```
[SW8800] undo vlan-vpn tpid
```

vlan-vpn tunnel

Syntax

vlan-vpn tunnel

undo vlan-vpn tunnel

View

System view

Parameter

None

Description

Use the **vlan-vpn tunnel** command to enable VLAN-VPN tunnel.

Use the **undo vlan-vpn tunnel** command to disable VLAN-VPN tunnel.

VLAN-VPN tunnel enables user networks in different regions to transmit BPDU packets transparently through VLAN VPN designated in the operator's network.

This function is disabled by default.

Example

Enable VLAN-VPN tunnel.note2

```
<SW8800>system-view
[SW8800] vlan-vpn tunnel
```

vlan-vpn uplink enable

Syntax

vlan-vpn uplink enable

undo vlan-vpn uplink

View

Ethernet port view

Parameter

None

Description

Use the **vlan-vpn uplink enable** command to set a port to be a VLAN-VPN uplink port.

Use the **undo vlan-vpn uplink** command to remove the configuration.

When sending a packet, a VLAN-VPN uplink port replaces the TPID value in the outer VLAN tag with the configured TPID value. You can use the **vlan-vpn tpid** command to set the TPID value used by the VLAN-VPN uplink port.

CAUTION:

- At present, 3C17512 and LSBM1TGX1 cards do not support this command.
- The **vlan-vpn uplink enable** command and the **vlan-vpn enable** command are mutually exclusive. That is, if you execute the **vlan-vpn enable** command on a port, you will fail to execute the **vlan-vpn uplink enable** command on the same port; if you execute the **vlan-vpn uplink enable** command on a port, you will fail to execute the **vlan-vpn enable** command on the same port either.

Example

Set Ethernet3/1/1 port to be a VLAN-VPN uplink port.

```
[3Com-Ethernet3/1/1] vlan-vpn uplink enable
```

Restore Ethernet3/1/1 port to a common port.

```
[3Com-Ethernet3/1/1] undo vlan-vpn uplink
VLAN-VPN uplink status: enabled
```

66 NQA CONFIGURATION COMMANDS

NQA Configuration Commands

This section describes the Network Quality Assurance(NQA) commands.

count

Syntax

count *times*

undo count

View

NQA test group view

Parameter

times: Number of probe packets to send.

Description

Use the **count** command to configure the number of probe packets to send.

Use the **undo count** command to restore the number of probe packets to send to the default value.

By default, one probe packet is sent.

If you specify a value bigger than 1 for the times argument, the system operates in either of the following two ways after sending the first probe packet.

- If the system receives a response packet, it sends a second probe packet.
- If the system does not receive a response packet, it sends a second probe packet after test operation timeout.

This process goes on until the last probe packet is sent

Example

Set the number of probe packets to send to 5.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] nqa administrator icmp
[3Com-administrator-icmp] count 5
```

datafill

Syntax

datafill *text*

undo datafill

View

NQA test group view

Parameter

text: Filler data of the test packet. It can be a string under 230 bytes in length.

Description

Use the **datafill** command to configure the filler data of the test packet.

Use the **undo datafill** command to restore the filler data of the test packet to the default value.

By default, no filler data of the test packet is configured, that is, the test packet is empty.

Related command: **datasize**.

When filling the ICMP packet, if the filler data of the packet is left blank, the system will in turn fill the bytes whose are 0, 1, 2... into the free filling space of the packet. Otherwise, the system uses text to fill in the space. If the content of text is too long, the system uses the part of the content in the front; if too short, the system fills the content in a cyclic way.

Example

Configure the filler data of the test packet as "Hello I'm here."

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] nqa administrator icmp
[3Com-administrator-icmp] datafill Hello I'm here.
```

datasize

Syntax

datasize *size*

undo datasize

View

NQA test group view

Parameter

size: Size, in bytes, of the test packet.

Description

Use the **datasize** command to configure the size of the filler data of the test packet.

Use the **undo datasize** command to restore the size to the default value.

By default, the size of filler data of the test packet is 56 bytes.

Related command: **datafill**.

The filler data refers to the area that can be freely filled in the packet, that is, the area outside the ICMP packet header. If the filler data is big in size, when sending the packet, the system fragments the packet to pieces on demand.

Example

Set the filler data size of the test packet to 50 bytes.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] nqa administrator icmp
[3Com-administrator-icmp] datasize 50
```

debugging nqa

Syntax

debugging nqa{ **all** | **error** | **event** }

undo debugging nqa { **all** | **error** | **event** }

View

User view

Parameter

all: Specifies all types of debugging for NQA..

error: Specifies debugging for NQA error information.

event: Specifies debugging for NQA event information.

Description

Use the **debugging nqa** command to enable debugging for NQA.

Use the **undo debugging nqa** command to disable debugging for NQA.

Example

Enable debugging for NQA error information.

```
<SW8800> debugging nqa error
```

description

Syntax

description *text*

undo description

View

NQA test group view

Parameter

text: Brief description of the operation, 1 to 230 characters long.

Description

Use the **description** command to configure the brief description of the operation.

Use the **undo description** command to delete the configured description information.

By default, there is no description information of the operation.

Example

Describes the test group as "Cary's icmp test".

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] nqa administrator icmp
[3Com-administrator-icmp] description Cary's icmp test
```

destination-ip

Syntax

destination-ip *ip-address*

undo destination-ip

View

NQA test group view

Parameter

ip-address: Destination IP address of the test.

Description

Use the **destination-ip** command to configure the destination IP address of the test.

Use the **undo destination-ip** command to delete the configured destination IP address.

By default, no destination IP address of the test is configured.

The test can be performed only after the destination IP address is configured.

Example

Set the destination IP address of the test to 192.168.80.80.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] nqa administrator icmp
[3Com-administrator-icmp] destination-ip 192.168.80.80
```

display nqa

Syntax

display nqa { **results** | **history** } [*administrator-name test-tag*]

View

Any view

Parameter

results: Displays the test results.

history: Displays the history test record information.

administrator-name: Name of the administrator who creates the operation.

test-tag: Tag of the test operation.

Description

Use the **display nqa** command to display the result of the test.

If you do not specify the *administrator-name* and the *test-operation-tag* arguments, results of all test groups are displayed. Otherwise, only the result of the specified test group is displayed.

Example

Display the test results.

```
<SW8800> display nqa results administrator icmp
      nqa entry(admin administrator, tag icmp) test result:
      Destinationip address:192.168.80.80
      Vpn-instance: NULL
      Send operation times: 5             Receive response times: 5
      Min/Max/Average Round Trip Time: 1/2/1
      Square-Sum of Round Trip Time: 13
      Last complete test time: 2005-11-02 16:28:55.0
      Extend result:
      Disconnect operation number:0        Operation timeout number:0
      System busy operation number:0       Connection fail number:0
      Operation sequence errors:0          Drop operation number:0
      Operation statistics errors:0
```

Table 156 Description on the fields of the display nqa result command

Field	Description
Destion ip address	Destination IP address
Vpn-instance	VPN identification, NULL means no identification is set.
Send operation times	Number of times the operation is sent
Receive response times	Number of times of the successful test operations
Min/Max/Average Round Trip Time	Minimum/maximum/average round trip time
Square-Sum of Round Trip Time	The square sum of the round trip time
Last complete test time	Time of the last successful test
Disconnect operation number	Number of times of disconnections by the opposite side
System busy operation number	Number of times the test fails because the system is busy
Operation sequence errors	Number of received sequence error packets
Operation timeout number	Number of timeouts
Connection fail number	Number of connection failures
Drop operation number	Number of system resource allocation errors
Operation statics errors	Number of other errors

```
<SW8800> display nqa history administrator icmp
    nqa entry(admin administrator, tag icmp) history record:
    Index     Response    Status      LastRC    Time
      1           1         1           0      2005-11-02 16:28:55.0
      2           1         1           0      2005-11-02 16:28:55.0
      3           1         1           0      2005-11-02 16:28:55.0
      4           1         1           0      2005-11-02 16:28:55.0
      5           1         1           0      2005-11-02 16:28:55.0
```

Table 157 Description on the fields of the display nqa history command

Field	Description
Response	Round trip test time in milliseconds, or the timeout time. 0 means the test fails.
Status	Test result value
LastRC	Receive the last response code based on the implementation ways. With ICMP echo enabled, if the system receives ICMP response which includes ICMP_ECHOREPLY(0), the probe has succeeds.
Time	Test time

Table 158 Description of the status value in the NQA history records

Status value	Description
1	Response received
2	Unknown error, (for example, the socket read error)
3	System internal error
4	Timeout waiting for response

frequency

Syntax

frequency *interval*

undo frequency

View

NQA test group view

Parameter

interval: Automatic test interval, in seconds.

Description

Use the **frequency** command to configure the automatic test interval.

Use the **undo frequency** command to cancel the automatic test.

By default, the automatic test interval is 0 seconds, that is, the system does not perform the automatic test.

If the *interval* is greater than 0, the system performs one automatic test at the configured interval.

In the process of test, parameters in the test group cannot be changed, except the brief description of the operations and the condition of sending Trap information to the network management system.

Example

Set the automatic test interval to 10 seconds.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] nqa-agent enable
```

```
[SW8800] nqa administrator icmp
[3Com-administrator-icmp] frequency 10
```

history-records

Syntax

history-records *number*

undo history-records

View

NQA test group view

Parameter

number: Number of test results which can be stored in the history record.

Description

Use the **history-records** command to configure the Number of test results that can be stored in the history record.

Use the **undo history-records** command to restore the Number of test results that can be stored in the history record to the default value.

By default, 50 test results can be stored in the history record.

When this command is executed, the switch checks the redundant history records and deletes them. Example: If the configuration allows 30 test results to be stored in the history record while there are 50 test results in the test group, the switch deletes the oldest 20 test results.

Example

Set the number of test results stored in the history records to 10.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] nqa-agent enable
[SW8800]nqa administrator icmp
[3Com-administrator-icmp] history-records 10
```

NQA

Syntax

nqa *administrator-name test-tag*

undo nqa *administrator-name test-tag*

View

System view

Parameter

administrator-name:Name of the test administrator, 1 to 32 characters long.

test-tag:

Tag of the test operation, 1 to 32 characters long, and including no "-" symbols.

Description

Use the **nqa** command to create a NQA test group (if there is no NQA test group before). You will enter the NQA test group view after this command is executed.

Use the **undo nqa** command to delete an NQA test group. At the same time, the test will be stopped, and the history record will be deleted.

Note that:

- You can perform the test operation only after creating a test group.
- You can create a maximum of 30 test groups.

Example

Create an NQA test group. Its name is administrator and its test tag is icmp.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] nqa administrator icmp
```

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 function.

Use the **undo nqa-agent enable** command to disable the NQA client function.

You can perform test operations only after you enable the NQA client function.

Example

Enable the NQA client.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] 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 test operations enabled simultaneously.

Description

Use the **nqa-agent max-requests** command to set the maximum number of test operations that can be enabled simultaneously.

Use the **undo nqa-agent max-requests** command to restore the number of test operations that can be enabled simultaneously to the default value.

By default, a maximum of 5 test operations can be enabled simultaneously.

If the configured value is smaller than the number of enabled test groups, the current test is not stopped.

Example

Configure that the system can enable a maximum of 4 test operations simultaneously.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] nqa-agent enable
[SW8800] nqa-agent max-requests 4
```

probe-failtimes

Syntax

probe-failtimes *times*

undo probe-failtimes

View

NQA test group view

Parameter

times: Number of times of constant probe failures.

Description

Use the **probe-failtimes** command to set the number of constant probe failures after which NQA will send the Trap information to the network management system.

Use the **undo probe-failtimes** command to restore the number of constant probe failures after which the Trap information will be sent to the default value.

By default, the system sends the Trap information to the network management system after one probe fails in an NQA test.

The current "probe failures times" will be reset to zero after a test is finished, that is, this "times" is only valid for a single test and can not cross two tests for constant statistics. If the probe succeeds, this statistic value is reset to zero too.

For the concept of test and probe, note the following content:

- When probing, the system sends one packet every time. While the test process is not always so.
- One test may include many probes. The test succeeds as long as there is one successful probe.
- The current "probe failure times" will be reset to zero after a test is finished, that is, the "times" is only valid for a single test and can not cross two tests for constant statistics. If the probe succeeds, this statistic value is reset to zero too.

Related command: **test-failtimes**.

Example

Set that the system sends Trap information after 3 times constant probe failures in an NQA test.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] nqa-agent enable
[SW8800] nqa administrator icmp
[3Com-administrator-icmp] probe-failtimes 3
```

sendpacket passroute

Syntax

sendpacket passroute

undo sendpacket passroute

View

NQA test group view

Parameter

None

Description

Use the **sendpacket passroute** command to assume the connection mode between the destination address and the equipment which enables the test as direct connection mode. So called direct connection mode is that the connection between the destination address and the equipment enabling the test is not through the Layer 3 data exchange equipment.

Use the **undo sendpacket passroute** command to cancel this assumption.

By default, no such assumption

- If you assume the connection mode to the destination address as direct connection mode, actually it equals to set the TTL to 1.
- If you assume the connection mode as direct mode, but set the TTL value at the same time, then the TTL value does not take effect. This value takes effect when you cancel the configuration on the connection mode.

Example

Set that the system assumes the connection mode as direct connection when sending the ICMP packet.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] nqa-agent enable
[SW8800] nqa administrator icmp
[3Com-administrator-icmp] sendpacket passroute
```

send-trap

Syntax

send-trap { **all** | { **probefailure** | **testcomplete** | **testfailure** } * }

undo send-trap { **all** | { **probefailure** | **testcomplete** | **testfailure** } * }

View

NQA test group view

Parameter

probefailure: Sends the Trap information to the network management system when the probe fails and the corresponding filter condition is satisfied.

testcomplete: Sends the Trap information to the network management system when the test is finished.

testfailure: Sends the Trap information to the network management system when the test fails and the corresponding filter condition is satisfied.

all: Sends the Trap information to the network management system when any of the above conditions happens.

Description

Use the **send-trap** command to configure the conditions of sending Trap information to the network management system.

Use the **undo send-trap** command to cancel the configured the conditions of sending Trap information.

By default, no Trap information is sent to the network management system.

The Trap information includes alert message or prompt message. The purpose of sending the trap information is to remind the administrator to manage the system.

Related command for filter conditions: **probe-failtimes** and **test-failtimes.**

Example

Configure the condition of sending Trap information as testcomplete.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] nqa-agent enable
[SW8800] nqa administrator icmp
[3Com-administrator-icmp] send-trap testcomplete
```

source-interface

Syntax

source-interface { *interface-type interface-number* }

undo source-interface

View

NQA test group view

Parameter

interface-type: Type of interface.

interface-number: Number of interface.

Description

Use the **source-interface** command to configure the source interface for sending test packet.

Use the **undo source-interface** command to disable the configured source interface.

By default, no source interface for sending test packet is configured.

*The source interface must be a Layer 3 interface. Otherwise, the system stops the test for not finding the corresponding IP address. If a source IP address is configured, no IP address of the source interface will be used. But the system still checks whether the interface is a Layer 3 interface or not as the ordinary **ping** operation does.*

Example

Configure the Vlan-interface 60 as the source interface for sending test packet.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] nqa-agent enable
[SW8800] nqa administrator icmp
[3Com-administrator-icmp] source-interface Vlan-interface 60
```

source-ip

Syntax

source-ip *ip-address*

undo source-ip

View

NQA test group view

Parameter

ip-address: Source IP address of the test.

Description

Use the **source-ip** command to configure the source IP address of the test.

Use the **undo source-ip** command to cancel the configured source IP address.

By default, no source IP address is configured. The system uses the IP address of the source interface as the source IP address.

Example

Set the source IP address of this test to 192.168.60.60.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] nqa-agent enable
[SW8800] nqa administrator icmp
[3Com-administrator-icmp] source-ip 192.168.60.60
```

test-enable

Syntax

test-enable

undo test-enable

View

NQA test group view

Parameter

None

Description

Use the **test-enable** command to execute the NQA test.

Use the **undo test-enable** command to compulsively stop the current NQA test.

- The test result can not be automatically displayed after the NQA test is executed. You need to use the **display nqa** command to display the test result.
- When the system is testing, parameters in the test group can not be changed except the brief description of the operation and the condition of sending Trap information to the network management system.

Example

Execute the NQA test.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] nqa-agent enable
[SW8800] nqa administrator icmp
[3Com-administrator-icmp] test-enable
```

test-failtimes

Syntax

test-failtimes *times*

undo test-failtimes

View

NQA test group view

Parameter

times: Number of constant test failures.

Description

Use the **test-failtimes** command to set the number of constant test failures after which the system will send the Trap information to the network management system.

Use the **undo test-failtimes** command to restore the number of constant test failures to the default value.

By default, the system sends the Trap information to the network management system after one NQA test fails.

For the concept of test and probe, note the following content:

- When probing, the system sends one packet every time. While the test process is not always so.
- One test may include many probes. The test succeeds as long as there is one successful probe.
- The current "probe failure times" will be reset to zero after a test is finished, that is, the "times" is only valid for a single test and can not cross two tests for constant statistics. If the probe succeeds, this statistic value is reset to zero too.

Related command: **probe-failtimes**.

Example

Set that the system sends Trap information after 3 constant probe failures in an NQA test.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] nqa-agent enable
[SW8800] nqa administrator icmp
[3Com-administrator-icmp] test-failtimes 3
```

test-type

Syntax

test-type *type*

View

NQA test group view

Parameter

type: Type of test, currently it is only the icmp type.

By default, the test type is icmp.

Description

Use the **test-type** command to configure the test type.

*The test type is required, so no **undo** command is provided.*

Example

Specify the test type as icmp.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] nqa-agent enable
[SW8800] nqa administrator icmp
[3Com-administrator-icmp] test-type icmp
```

timeout

Syntax

timeout *time*

undo timeout

View

NQA test group view

Parameter

time: Timeout time. Its unit is second.

Description

Use the **timeout** command to configure the timeout time of the test operation.

Use the **undo timeout** command to restore the timeout time to the default value.

By default, the timeout time of test operation is 3 seconds

Example

Set the timeout time to 10 seconds.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] nqa-agent enable
[SW8800] nqa administrator icmp
[3Com-administrator-icmp] timeout 10
```

tos

Syntax

tos *value*

undo tos

View

NQA test group view

Parameter

value: TOS (type of service) value in the NQA test packet header.

Description

Use the **tos** command to configure the TOS value in the NQA test packet header.

Use the **undo tos** command to restore the TOS value in the NQA test packet header to the default value.

By default, the TOS value in the NQA test packet header is 0, that is, no special service is specified

This parameter equals to the "-v" parameter in the **ping** command of the Windows operation system.

See the "RFC 1349" for detailed explanations of the service types.

Example

Configure the TOS value in the NQA test packet header to 4 (representing the highest reliability).

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] nqa-agent enable
[SW8800] nqa administrator icmp
[3Com-administrator-icmp] tos 4
```

ttl

Syntax

ttl *number*

undo ttl

View

NQA test group view

Parameter

number: Maximum number of hops that an NQA ICMP test packet can pass in the network, in the range of 1 to 255. This parameter equals to the "-i" parameter in the **ping** command of the Windows operation system.

Description

Use the **ttl** command to configure the maximum number of hops that an NQA ICMP test packet can pass in the network, that is, the "life time" of the NQA packet.

Use the **undo ttl** command to restore the maximum number of hops that a NQA ICMP test packet can pass in the network to the default value.

By default, the maximum number of hops that an NQA ICMP test packet can pass in the network is 20.

Example

Configure the maximum number of hops that an NQA test packet can pass in the network to 16.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] nqa-agent enable
[SW8800] nqa administrator icmp
[3Com-administrator-icmp] ttl 16
```

vpn-instance

Syntax

vpn-instance *name*

undo vpn-instance

View

NQA test group view

Parameter

name: Name of the specified VPN instance, a string of up to 19 characters.

Description

Use the **vpn-instance** command to set the name of the VPN instance for the test.

Use the **undo vpn-instance** command to cancel the name of the VPN instance for the test.

By default, no information of the VPN instance is set.

You must set the name for VPN instance. Otherwise, the test will fail for the system can not find the corresponding VPN index.

Example

Specify the name of the VPN instance for the test as vpn1.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] nqa-agent enable
[SW8800] nqa administrator icmp
[3Com-administrator-icmp] vpn-instance vpn1
```

67 PASSWORD CONTROL CONFIGURATION COMMANDS

Password Control Configuration Commands

display password-control

Syntax

display password-control

View

Any view

Parameter

None

Description

The **display password-control** command is used to view the password control information for all users, including the enabled/disabled state of password aging, the aging time, the enabled/disabled state of the minimum password length limitation and the configured minimum password length, the enabled/disabled state of history password recording, the maximum number of history records, the alert time before password expiration, the timeout time for password authentication, the maximum number of password input attempts, the processing mode after failed password input attempts, the time when the password history was last cleared, and so on

Example

Display the information about the current password control for all users.

```
<SW8800> display password-control
Global password settings for all users:

Password aging:                      Disabled
Password length:                     Disabled
Password history:                    Disabled
Password alert-before-expire :       7 days
Password authentication-timeout :     60 seconds
 Password attempt times :             3 times
Password attempt-failed action :     Lock for 120 minutes
```

display password-control blacklist

Syntax

display password-control blacklist [**username** *username* | **ipaddress** *ipaddress*]

View

Any view

Parameter

username:user name added into the blacklist.

ipaddress:user IP address added into the blacklist.

Description

Use the **display password-control blacklist** command to view the user information added into the backlist based on the user name or IP address after failed attempts of entering passwords.

Example

Display the information of all users added into the blacklist after failed attempts of entering passwords.

```
<SW8800> display password-control blacklist
USERNAME                          IP
Jack                              10.1.1.2
The number of users in blacklist is :1
```

display password-control super

Syntax

display password-control super

View

Any view

Parameter

None

Description

Use the **display password-control super** command to view the password control information for super passwords, including password aging time and the minimum password length.

Example

Display the **super** password control information.

```
<SW8800> display password-control super
 Super's password settings:
Password Aging :                 Enabled(10 days)
 Password Length:                 Enabled(10 Characters)
```

password

Syntax

password [**simple** | **cipher**] *password*

undo password

View

Local user view

Parameter

simple: Plain text, a string containing 1 to 63 characters.

cipher: Cipher text, a string containing 1 to 88 characters.

password: Login password.

Description

Use the **password** command to configure the password for a local user.

Use the **undo password** command to delete the user password.

By default, no password is set for local users.

To access the FTP server through FTP, you must perform this configuration.

For related configuration, refer to **password-control**.

Example

Set the system login password to 9876543210.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800]local-user test
[3Com-luser-test]password
Password:**********
confirm:**********
Updating the password file, please wait...
```

change the system login password to 0123456789.

```
[3Com-luser-test]password
Password:**********
Confirm :**********
Updating  password-file  ,please waiting ...
```

password-control

Syntax

password-control { **aging** *aging-time* | **length** *length* | **login-attempt** login-*times* [**exceed** { **lock** | **unlock** | **locktime**

[*time*] }]

| **history** *max-record-num* | **alert-before-expire** *alert-time* | **authentication-timeout** *authentication-timeout* }

undo password-control { **aging** | **length** | **login-attempt** | **history** | **alert-before-expire** | **authentication-timeout** | **exceed** { **lock** | **unlock** | **locktime** } }

View

System view

Parameter

aging-time: Configures the system password aging time. Value range 1 to 365 days, and the default value is 90 days.

Length: Configures the minimum password length. The value range is 4 to 32 characters, and the default value is 10.

login-times: Configures the maximum number of login attempts for each user. The value range is 2 to 10, and the default value is 3.

max-record-num: Configures the maximum number of history password records for each user. The value range is 2 to 10; default: 4.

alert-time: Configures the alert time before password expiration. The value range is 1 to 30 days, and the default value is 7 days.

authentication-timeout: Configures the timeout time for user authentication; The value range is 30 to 120 seconds, and the default value is 60 seconds.

Exceed: Configures the processing mode after failed login attempts.

Lock: Locks the login user so that the user will not be able to log in to the switch until the administrator removes the user from the blacklist manually.

locktime [*time*]: Specifies the time during which the user is locked. The value range is 3 to 360 seconds, and the default value is 120 seconds. A locked user can log in to the switch again after the configured lock time.

Unlock: The user can still log in after failed login attempts, without being locked.

The default processing mode is the **locktime** mode after password authentication fails. Namely, the system will lock the user, and allow the user to log in to the switch after the configured period of time.

Description

Use the **password-control aging** *aging-time* command to configure the aging time for system login passwords. This command can also be carried out in the local user view.

Use the **password-control length** *length* command to configure the minimum length for the system login passwords. This command can also be carried out in the local user view.

Use the **password-control login-attempt** *login-times* command to configure the number of password attempts allowed for each user.

Use the **password-control history** *max-record-num* command to configure the maximum number of history password records allowed for each user.

Use the **password-control alert-before-expire** *alert-time* command to configure the alert time before password expiration.

Use the **password-control authentication-timeout** *authentication-timeout* command to configure the timeout time for user password authentication.

Use the **password-control login-attempt** *attempt-time* **exceed** command to configure the processing mode used after password attempt fails.

Example

Configure the aging time of the system login passwords to 100 days.

```
<SW8800>system-view
System View: return to User View with Ctrl+Z.
[SW8800] password-control aging 100
```

Configure the minimum length of the system login passwords to 8 characters.

```
[SW8800] password-control length 8
```

Configure the number of password attempts allowed for each user to 5.

```
[SW8800] password-control login-attempt 5
```

Configure the maximum number of history password records allowed for each user to 10.

```
[SW8800] password-control history 10
```

Configure the alert time so that users are alerted 7 days before their passwords expire.

```
[SW8800] password-control alert-before-expire  7
```

Configure the timeout time of the user password authentication to 100 seconds.

```
[SW8800] password-control authentication-timeout 100
```

Configure the processing mode so that the system locks the user after failed password authentication attempts and allow the user to log in to the switch again 360 minutes later.

```
[SW8800] password-control login-attempt 3 exceed locktime 360
```

password-control enable

Syntax

password-control { **aging** | **length** | **history** } **enable**

undo password-control { **aging** | **length** | **history** } **enable**

View

System view

Parameter

None

Description

Use the **password-control enable** commands to enable the password control function of the system. The specific usage is as follows:

Use the **password-control aging enable** command to enable password aging. By default, the password aging time is 90 days.

Use the **password-control length enable** command to enable the limitation of the minimum password length. By default, the minimum password length is 10 characters.

Use the **password-control history enable** command to enable history password recording. When a login password expires, the system will require the user to input a new password and will save the old password automatically to a file in the flash memory. By recording the history passwords, the system can prevent the user from using a single password or repeated passwords when modifying a password, thus to enhance the security.

Use the **undo password-control** { **aging** | **length** | **history** } **enable** command to disable password control functions, such as password aging, the limitation of the minimum password length, and history password recording.

By default, all the above-mentioned password control functions are disabled.

Related command: **password-control**.

Example

Enable password aging.

```
[SW8800]password-control aging  enable
Password aging enabled for all users. Default: 90 days.
```

Enable the limitation of the minimum password length.

```
[SW8800]password-control length  enable
Password minimum length enabled for all users. Default: 10 characters.
```

Disable password aging.

```
[SW8800]undo password-control aging
```

Enable history password recording.

```
[SW8800]password-control history enable
Password history enabled for all users. Default: 10 history records
```

Disable history password recording.

```
[SW8800]undo password-control history
```

password-control super

Syntax

password-control super { **aging** *aging-time* | **length** *min-length* }

undo password-control super { **aging** | **length** }

View

System view

Parameter

aging-time: Specifies the aging time for super passwords. The value range is 1 to 365 days and the default value is 90 days.

min-length: Specifies the minimum length for super passwords. It ranges from 4 to 16 characters, and the default value is 10 characters.

Description

Use the **password-control super** command to configure some password control parameters for super commands, including the password aging time and the minimum password length. Use the **undo password-control super** command to restore the default settings.

Example

Set the password aging time for super commands to 10 days.

```
<SW8800> system-view
System View: return to User View with Ctrl+Z.
[SW8800] password-control super aging 10
```

reset password-control history-record

Syntax

reset password-control history-record [**username** *username*]

View

User view

Parameter

Username: Specifies a user whose history password record will be deleted.

Description

Use the **reset password-control history-record** command to delete the history password records of all users. Use the **reset password-control history-record username** *username* command to delete the history password record of a specified user.

After the history password record of a user is deleted, the configuration of a new password will not be restricted by the previously configured history password records.

Example

Delete the history password records of all users.

```
<SW8800> reset password-control history-record
Are you sure to delete all  the  history record?[Y/N]
```

If you type "Y", the system will delete the history password records of all users and gives the following prompt:

```
Updating the password file, please wait...
 All historical passwords have been cleared.
```

Delete the history password records of user named test.

```
<SW8800> reset password-control history-record user-name test
Are you sure to delete all the history record of user test ?[Y/N]
```

If you type "Y", the system will delete all the history password records of the specified user and gives the following prompt:

```
Updating the password file, please wait...
All historical passwords of this user have been cleared.
```

reset password-control history-record super

Syntax

reset password-control history-record super [**level** *level-value*]

View

User view

Parameter

level-value: Specifies to delete the history records of super passwords of users at a certain level. The value range is 1 to 3.

Description

Use the **reset password-control history-record super level** *level-value* command to delete the history records of the super passwords for the users at the specified level.

Use the **reset password-control history-record super** command to delete the history records of all super passwords.

After the history password record of a user is deleted, the configuration of a new password will not be restricted by the previously configured history password records.

Example

Delete the history records of super passwords for the users at level 2.

```
<SW8800>reset password-control history-record super level 2
Are you sure to clear  the  specified-level super password history records?[Y/N]
```

If you type "Y", the system will delete the history records of super passwords for users at level 2.

reset password-control blacklist

Syntax

reset password-control blacklist [**username** *username*]

View

User view

Parameter

username *username*: Specified a user name.

Description

Use the **reset password-control blacklist** command to remove all the users from the blacklist.

Use the **reset password-control blacklist username** *username* command to remove the specified user from the blacklist.

Example

Check the user information in the blacklist. Suppose the blacklist contains three users: test, tes, and test2.

```
<SW8800> display password-control blacklist
USERNAME                        IP
test                            192.168.30.25
tes                             192.168.30.24
test2                           192.168.30.23
```

Remove user "test" from the blacklist.

```
<SW8800> reset password-control blacklist user-name test
Are you sure to delete the  blacklist-users ?[Y/N]y
 All the blacklist users  have been cleared.
```

Check the current user information in the blacklist and verify that user "test" has been removed.

```
<SW8800> display password-control blacklist
USERNAME                        IP
tes                             192.168.30.24
test2                           192.168.30.23
```