3Com® Switch 7750 Family
Command Reference Guide

Switch 7750
Switch 7754
Switch 7757
Switch 7758

www.3Com.com
Part Number: 10015463 Rev. AD
Published: December 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.

CONTENTS

ABOUT THIS GUIDE

1 CLI CONFIGURATION COMMANDS

2 LOGIN COMMANDS

3 COMMANDS FOR USER CONTROL

4 CONFIGURATION FILE MANAGEMENT COMMANDS

5 VLAN CONFIGURATION COMMANDS

6 PORT-BASED VLAN CONFIGURATION COMMANDS

7 PROTOCOL-BASED VLAN CONFIGURATION COMMANDS

13 IPX CONFIGURATION COMMANDS

14 GARP CONFIGURATION COMMANDS

15 GVRP CONFIGURATION COMMANDS

16 QinQ Configuration Commands

17 Selective QinQ Configuration Commands

18 Shared VLAN Configuration Commands

19 Port Basic Configuration Commands

20 LINK AGGREGATION CONFIGURATION COMMANDS

21 PORT ISOLATION CONFIGURATION COMMANDS

22 PORT SECURITY COMMANDS

23 PORT BINDING COMMANDS

24 DLDP CONFIGURATION COMMANDS

29 STATIC ROUTE CONFIGURATION COMMANDS

30 RIP CONFIGURATION COMMANDS

31 OSPF CONFIGURATION COMMANDS

34 IP ROUTING POLICY CONFIGURATION COMMANDS

35 ROUTE CAPACITY CONFIGURATION COMMANDS

44 HABP Configuration Commands

45 AAA Configuration Commands

46 RADIUS Configuration Commands

47 HWTACACS CONFIGURATION COMMANDS

48 EAD CONFIGURATION COMMANDS

49 TRAFFIC ACCOUNTING CONFIGURATION COMMANDS

50 VRRP CONFIGURATION COMMANDS

51 HA CONFIGURATION COMMANDS

52 ARP CONFIGURATION COMMANDS

57 ACL COMMANDS

58 QOS COMMANDS

66 PoE Profile Configuration Commands

67 UDP-Helper Configuration Commands

68 SNMP Configuration Commands

69 RMON Configuration Commands

70 NTP Configuration Commands

71 SSH Server Configuration Commands

76 BIMS Configuration Commands

77 Information Center Commands

78 FTP SERVER CONFIGURATION COMMANDS

79 FTP CLIENT CONFIGURATION COMMANDS

80 TFTP CONFIGURATION COMMANDS

81 DNS CONFIGURATION COMMANDS

87 REMOTE-PING CLIENT COMMANDS

88 REMOTE-PING SERVER COMMANDS

89 RRPP Configuration Commands

90 NetStream Configuration Commands

91 Policy Routing Configuration Commands

92 Telnet Protection Configuration Commands

93 Smart Link Configuration Commands

ALPHABETICAL LISTING OF COMMANDS

A B C D E F G H I J K L M N O P Q R S T U V

A B C D E F G H I J K L M N O P Q R S T U V

A B C D E F G H I J K L M N O P Q R S T U V

A B C D E F G H I J K L M N O P Q R S T U V

A B C D E F G H I J K L M N O P Q R S T U V

A B C D E F G H I J K L M N O P Q R S T U V

ABOUT THIS GUIDE

This guide describes the 3Com® Switch 7750 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
ℹ	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.

Related Documentation

The following manuals offer additional information necessary for managing your Switch 7750:

- *Switch 7750 Getting Started Guide* — Provides detailed descriptions of the Switch 7750 hardware, instructions for installing the hardware and software and important information about how to get started using the Switch 7750.
- *Switch 7750 Configuration Guide*— Describes how to configure your Switch 7750 using the supported protocols and CLI commands.
- *Switch 7750 Quick Reference Guide*— Provides a brief description of each command available when using the Switch 7750 Family.

- *Switch 7750 Release Notes* — Contains the latest information about your product. If information in this guide differs from information in the release notes, use the information in the *Release Notes*.

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

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

1 CLI CONFIGURATION COMMANDS

command-privilege level

Syntax

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

undo command-privilege view *view command*

View

System view

Parameter

level: Command Level. This argument ranges from 0 to 3.

view: Command view. This argument can be any command view the switch supports.

command: Command to be specified.

Description

Use the **command-privilege level** command to set the level of the specified command in a specified view.

Use the **undo command-privilege view** command to restore the level of the specified command in the specified view to the default.

Commands fall into four command levels: visit, monitor, system, and manage, which are identified as 0, 1, 2, and 3 respectively. The administrator can change the level of a command to enable users of specific level to utilize the command.

By default, the **ping**, **tracert**, and **telnet** commands are at the visit level (level 0); the **display** and **debugging** commands are at the monitor level (level 1); all configuration commands are at the system level (level 2); and FTP/TFTP and file system related commands are at the manage level (level 3).

Example

Specify the **system-view** command in user view to be of level 0.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] command-privilege level 0 view shell system-view
```

display history-command

Syntax

display history-command

View

Any view

Parameter None

Description Use the **display history-command** command to display history commands. All the history commands are saved in the history command cache. When the history command cache is full, the old information in it will be overlaid.

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

Example # Display history commands.

```
<SW7750> display history-command
  system-view
  quit
  display history-command
```

super

Syntax **super** [*level*]

View User view

Parameter *level*: User level. This argument ranges from 0 to 3 and defaults to 3. If you execute this command with the *level* argument not provided, this command switches the current user level to level 3.

Description Use the **super** command to switch the current user level to the one identified by the *level* argument. If a password is previously set by using the **super password** [**level** *level*] { **simple** | **cipher** } *password* command, you need to provide the password as well to switch to the higher user level. You will remain in the original user level if you fail to provide the correct password.

Note that:

- *Users logging into a switch also fall into four levels, each of which corresponding to one of the command levels. Users at a specific level can only use the commands at the same level and the commands at the lower levels.*
- *You can specify an AUX user to provide a password when he switches from a lower user level to a higher user level and specify the password by using the* ***super password*** *[* ***level*** level *] {* ***simple*** *|* ***cipher*** *} password command. With a password configured, an AUX user remains in the original user level if the password provided is incorrect when the AUX user attempts to switch to a higher user level. If the password is not configured, an AUX user can switch to a higher user level directly.*
- *A password is necessary for a VTY user to switch to a higher user level. You can use the* ***super password*** *[* ***level*** level *] {* ***simple*** *|* ***cipher*** *} password command to set the password. With the password not configured, a VTY user is prompted the message reading "Password is not set" and remains in the previous level.*
- *An AUX user or a VTY user can switch to a lower user level directly regardless of the password.*

Related command: **super password**.

Example # Switch to user level 3.

```
<SW7750> super 3
Password:
Now user privilege is 3 level, and only those commands whose level is
equal to or less than this level can be used.
Privilege note: 0-VISIT, 1-MONITOR, 2-SYSTEM, 3-MANAGE
```

super password

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

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

View System view

Parameter *level*: User level. This argument ranges from 1 to 3 and defaults to 3. If you execute this command with the *level* argument not provided, this command sets the password to switch to level 3.

simple: Specifies to provide the password in plain text.

cipher: Specifies to provide the password in encrypted text.

password: Password to be set. If you specify the **simple** keyword, provide this argument in plain text. If you specify the **cipher** keyword, you can provide this argument in either encrypted text or plain text. In this case, a password containing no more than 16 characters (such as 123) is regarded to be in plain text and is converted to the corresponding 24-character encrypted form (such as 7-CZB#/YX]KQ=^Q'MAF4<1!!) automatically. You can also provide a 24-character encrypted password directly (such as 7-CZB#/YX]KQ=^Q'MAF4<1!!). In this case, you must know its corresponding plain-text password is 123.

Description Use the **super password** command to set the password for users to switch to a higher user level. To prevent unauthorized accesses, you can use this command to require users to provide the password when they switch to a higher user level. For security purpose, the password a user enters when switching to a higher user level is not displayed. A user will remain at the original user level if the user has tried three times to enter the correct password but fails to do this.

Use the **undo super password** command to cancel the configuration.

Note that no matter what form of the password (plain text or encrypted text) is in, the password entered for verification must be in plain text.

Example # Set the password to switch from the current user level to user level 3 to "1234567890".

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
```

```
[SW7750] super password level 3 simple 1234567890
Updating user(s) information, please wait..........
```

2 LOGIN COMMANDS

authentication-mode

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

View User interface view

Parameter **password**: Authenticates users using the local password.

scheme: Authenticates users locally or remotely using usernames and passwords.

command-authorization: Performs command authorization on TACACS authentication server.

none: Does not authenticate users.

Description Use the **authentication-mode** command to specify the authentication mode.

- If you specify the **password** keyword to authenticate users using the local password, remember to set the local password using the **set authentication password** { **cipher** | **simple** } *password* command.
- If you specify the **scheme** keyword to authenticate users locally or remotely using usernames and passwords, the actual authentication mode, that is, local or remote, depends on other related configuration.
- If this command is executed with the **command-authorization** keywords specified, authorization is performed on the TACACS server whenever you attempt to execute a command, and the command can be executed only when you pass the authorization. Normally, a TACACS server contains a list of the commands available to different users.

If you specify to perform local authentication when a user logs in through the Console port, a user can log into the switch with the password not configured. But for a VTY user interface, a password is needed for a user to log into the switch through it under the same circumstance.

By default, users logging in through the Console port are not authenticated, whereas modem users and Telnet users are authenticated.

CAUTION: *For a VTY user interface, to specify the* ***none*** *keyword or* ***password*** *keyword for login users, make sure that SSH is not enabled in the user interface. Otherwise, the configuration fails. Refer to "protocol inbound" on page 70 for related configuration.*

Example # Configure to authenticate users using the local password on the AUX interface.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] user-interface aux 0
[SW7750-ui-aux0] authentication-mode password
```

auto-execute command

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

undo auto-execute command

View User interface view

Parameter *text*: Command to be executed automatically.

Description Use the **auto-execute command** command to set the command that is executed automatically after a user logs in.

Use the **undo auto-execute command** command to disable the specified command from being automatically executed.

Normally, the **telnet** command is specified to be executed automatically to enable the user to Telnet to a specific network device automatically.

By default, no command is automatically executed.

CAUTION:

- *The **auto-execute command** command may cause you unable to perform common configuration in the user interface, so use it with caution.*
- *Before executing the **auto-execute command** command and save your configuration, make sure you can log into the switch in other modes and cancel the configuration.*

Example # Configure the **telnet** 10.110.100.1 command to be executed automatically after users log into VTY 0.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] user-interface vty 0
[SW7750-ui-vty0] auto-execute command telnet 10.110.100.1
% This action will lead to configuration failure through ui-vty0. Ar
e you sure?[Y/N]y
```

copyright-info enable

Syntax **copyright-info enable**

undo copyright-info enable

View System view

Parameter None

Description Use the **copyright-info enable** command to enable copyright information displaying.

Use the **undo copyright-info enable** command to disable copyright information displaying.

By default, copyright information displaying is disabled.

With copyright information displaying enabled on a switch, the copyright information is displayed after a user logs into the switch successfully.

These two commands apply to users logging in through the Console port and Telnet users.

Example # Disable copyright information displaying.

```
**************************************************************************
*  Copyright(c) 2004-2007 3Com Corporation                               *
*  Without the owner’s prior written consent,                            *
*  no decompiling or reverse-switch fabricering shall be allowed.        *
**************************************************************************
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] undo copyright-info enable
```

# After the above configuration, the copyright information is not displayed when a user logs into the switch successfully, as shown below.

```
<SW7750>
```

databits

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

undo databits

View User interface view

Parameter **7**: Sets the data bits to 7.

8: Sets the data bits to 8.

Description Use the **databits** command to set the databits for the user interface.

Use the **undo databits** command to revert to the default data bits.

Execute these two commands in AUX user interface view only.

The default data bits is 8.

Example # Set the data bits to 7.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] user-interface aux 0
[SW7750-ui-aux0] databits 7
```

display user-interface

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

View Any view

Parameter *type*: User interface type.

number: User interface number.

summary: Displays the summary information about a user interface.

Description Use the **display user-interface** command to display the information about a specified user interface or all user interfaces. If the **summary** keyword is not specified, this command displays user interface type, absolute/relative user interface number, transmission speed, available command level, authentication mode, and physical position. If the **summary** keyword is specified, this command displays the number and type of the user interfaces, including those that are in use and those that are not in use.

Example # Display the information about user interface 0.

```
<SW7750> display user-interface 0
  Idx  Type     Tx/Rx      Modem Privi Auth  Int
F 0    AUX 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 1 Descriptions on the fields of the **display user-interface** command

Filed	Description
+	The user interface is in use.
F	The user interface operates in asynchronous mode.
Idx	The absolute index of the user interface
Type	User interface type and the relative index
Tx/Rx	Transmission speed of the user interface
Modem	Indicates whether or not a modem is used.
Privi	Available command level

Table 1 Descriptions on the fields of the **display user-interface** command

Filed	Description
Auth	Authentication mode
Int	Physical position of the user interface
A	The current user is authenticated by AAA.
N	Users are not authenticated.
P	Users need to provide passwords to pass the authentication.

# Display the summary information about the user interface.

```
<SW7750>display user-interface summary
  User interface type : [AUX]
            0:UXXX XXXX
  User interface type : [VTY]
            8:UUUU X
    5 character mode users.      (U)
    8 UI never used.             (X)
    5 total UI in use
```

display users

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

View Any view

Parameter **all**: Displays the information about all user interfaces.

Description Use the **display users** command to display the information about user interfaces. If you do not specify the **all** keyword, only the information about the current user interface is displayed.

Example # Display the information about the current user interface.

```
<SW7750> display users
        UI    Delay     Type   Ipaddress       Username        Userlevel
F 0   AUX 0   00:00:00                                             3
1   VTY 0   00:06:08  TEL    192.168.0.3
 +   : Current operation user.
 F   : Current operation user work in async mode.F 0   AUX 0   00:00:00
```

Table 2 Descriptions on the fields of the **display users** command

Field	Description
F	The information is about the current user interface, and the current user interface operates in asynchronous mode.
UI	The numbers in the left sub-column are the absolute user interface indexes, and those in the right sub-column are the relative user interface indexes.
Delay	The period (in seconds) the user interface idles for.
Type	User type
IPaddress	The IP address form which the user logs in.
Username	The login name of the user that logs into the user interface.

Table 2 Descriptions on the fields of the **display users** command

Field	Description
Userlevel	The level of the commands available to the users logging into the user interface
+	The user interface is in use.

flow-control

Syntax

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

undo flow-control

View

User interface view

Parameter

hardware: Performs hardware flow control.

none: Performs no flow control.

software: Performs software flow control.

Description

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

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

By default, flow control is not performed.

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

Example

Set flow control mode to software flow control.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] user-interface aux 0
[SW7750-ui-aux0] flow-control software
```

free user-interface

Syntax

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

View

User view

Parameter

type: User interface type.

number: Index of the user interface. This argument can be an absolute user interface index (if you do not provide the *type* argument) or a relative user interface index (if you provide the *type* argument).

Description

Use the **free user-interface** command to release a specified user interface. If you execute this command, the corresponding user interface will be disconnected.

Note that the current user interface cannot be released.

Example

Release user interface VTY 0.

```
<SW7750> free user-interface vty 0
Are you sure you want to free user-interface vty0 [Y/N]? y
 [OK]
```

After you execute this command, user interface VTY 0 will be disconnected. The user in it must log in again to connect to the switch.

header

Syntax

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

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

View

System view

Parameter

Incoming: Sets the login banner for users that log in through modems. If you specify to authenticate login users, the banner appears after a user passes the authentication. (The session does not appear in this case.)

login: Sets the login banner. The banner set by this keyword is valid only when users are authenticated before they log into the switch and appears while the switch prompts for user name and password.

shell: Sets the session banner, which appears after a session is established. If you specify to authenticate login users, the banner appears after a user passes the authentication.

text: Banner to be displayed. If no keyword is specified, this argument is the login banner. You can provide this argument in two ways. One is to enter the banner in the same line as the command (A command line can accept up to 255 characters.) The other is to enter the banner in multiple lines (you can start a new line by pressing <Enter>,) where you can enter a banner that can contain up to 2000 characters (including the invisible characters). Note that the first character is the beginning character and the end character of the banner. After entering the end character, you can press <Enter> to exit the interaction.

Description

Use the **header** command to set the banners that are displayed when a user logs into a switch. The login banner is displayed on the terminal when the connection is established. And the session banner is displayed on the terminal if a user successfully logs in.

Use the **undo header** command to disable displaying a specific banner or all banners.

Note that if you specify any one of the three keywords without providing the *text* argument, the specified keyword will be regarded as the login information.

You can specify the banner in the following three ways, each of which requires that the first character and the last character of the banner be the same.

- Enter the banner in multiple lines. If you only type one character in the first line of a banner, the character and the last character do not act as part of the banner. The following gives an example of this way.

```
[SW7750] header shell 0
Input banner text, and quit with the character ’0’.
Welcome!0
```

When you log in the next time, "Welcome!" is displayed as the banner. The beginning character and the end character (character 0) do not appear.

- Enter the banner in multiple lines. If you type multiple characters in the first line of a banner and the beginning and the end characters of the banner in this line are not the same, the beginning character is part of the banner. The following is an example.

```
[SW7750] header shell hello
Input banner text, and quit with the character ’h’.
my friend !
h
```

When you log in the next time, "hello" and "my friend !" is displayed respectively in two lines as the banner. The beginning character "h" appears in the banner.

- Enter the banner in a single line. You can also specify the banner in a single line. In this case, the banner does contain the beginning and the end character. The following is an example.

```
[SW7750] header shell 0welcome,my friend!0
```

When you log in the next time, "welcome, my friend!" is displayed as the banner.

Example # Set the session banner.

Option 1: Enter the banner in the same line as the command.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] header shell %SHELL: Hello! Welcome%
```

(Make sure the beginning and end characters of the banner are the same.)

When you log in the next time, the session banner appears on the terminal as the following:

```
[SW7750] quit
<SW7750> quit
Please press ENTER
SHELL: Hello! Welcome
```

(The beginning and end characters of the banner are not displayed.)

```
<SW7750>
```

Option 2: Enter the banner in multiple lines.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] header shell %SHELL:
```

(Following appears after you press <Enter>:)

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

Continue entering the banner and end the banner with the character identical with the beginning character of the banner.

```
Hello! Welcome %
```

(Press <Enter>.)

```
[SW7750]
```

When you log in the next time, the session banner appears on the terminal as the following:

```
[SW7750] quit
<SW7750> quit
Please press ENTER
%SHELL:
```

(Note that the beginning character of the banner appears.)

```
Hello! Welcome
<SW7750>
```

history-command max-size

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

undo history-command max-size

View User interface view

Parameter *value*: Size of the history command buffer. This argument ranges from 0 to 256 and defaults to 10. That is, the history command buffer can store 10 commands by default.

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

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

Example # Set the size of the history command buffer of AUX 0 to 20 to enable it to store up to 20 commands.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] user-interface aux 0
[SW7750-ui-aux0] history-command max-size 20
```

idle-timeout

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

undo idle-timeout

View User interface view

Parameter *minutes*: Number of minutes. This argument ranges from 0 to 35,791.

seconds: Number of seconds. This argument ranges from 0 to 59.

Description Use the **idle-timeout** command to set the timeout time. The connection to a user interface is terminated if no operation is performed in the user interface within the timeout time.

Use the **undo idle-timeout** command to revert to the default timeout time.

You can use the **idle-timeout** 0 command to disable the timeout function.

The default timeout time is 10 minutes.

Example # Set the timeout time of AUX 0 to 1 minute.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] user-interface aux 0
[SW7750-ui-aux0] idle-timeout 1 0
```

ip http shutdown

Syntax **ip http shutdown**

undo ip http shutdown

View System view

Parameter None

Description Use the **ip http shutdown** command to shut down the WEB Server.

Use the **undo ip http shutdown** command to launch the WEB Server.

By default, the WEB Server is launched.

To improve security and prevent attacks to the unused Sockets, TCP 80 port for HTTP service will be enabled or disabled after corresponding configurations.

- *TCP 80 port is enabled only after you use the* ***undo ip http shutdown*** *command to enable the Web server.*
- *If you use the* ***ip http shutdown*** *command to disabled the Web server, TCP 80 port is disabled.*

Example

Shut down the WEB Server.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ip http shutdown
```

# Launch the WEB Server.

```
[SW7750] undo ip http shutdown
```

lock

Syntax

lock

View

User view

Parameter

None

Description

Use the **lock** command to lock the current user interface to prevent unauthorized operations in the user interface.

With the execution of this command, the system prompts to enter and confirm the password, and then locks the user interface. You can set the password in the range of 1 to 16 characters.

Enter the correct password to cancel the lock. If your password contains more than 16 characters, the system will cancel the lock as long as the first 16 characters are matched.

Example

Lock the current user interface.

```
<SW7750> lock
Password:
Again:
                  locked !
```

# In this case, the user interface is locked. To operate the user interface again, you need to press Enter and provide the password as prompted

```
Password:
<SW7750>
```

modem

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

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

View User interface view

Parameter **call-in**: Permits call in.

both: Permits both call in and call out.

Description Use the **modem** command to configure the **both** attribute of the Modem.

Use the **undo modem** command to disable the **both** configuration.

Both call in and call out are allowed when the **modem** command is executed without any keyword.

Both call in and call out are disabled when the **undo modem** command is executed without any keyword.

note3The command can only be executed in AUX user interface view.

Example # Enable Modem call in and call out.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] user-interface aux 0
[SW7750-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 set the answer mode to auto answer.

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

By default, manual answer mode is adopted.

note3The command can only be executed in AUX user interface view.

Example # Set the answer mode of Modem to auto answer.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] user-interface aux 0
[SW7750>-ui-aux0] modem auto-answer
```

modem timer answer

Syntax **modem timer answer** *seconds*

undo modem timer answer

View User interface view

Parameter *seconds*: Waiting timeout time, in seconds, ranging from 1 to 60.The default value is 30 seconds.

Description Use **the modem timer answer** to configure the carrier detection timeout time after off-hook during call-in connection setup.

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

note3The command can only be executed in AUX user interface view.

Example # Set the timeout time to 45 seconds.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] user-interface aux 0
[SW7750-ui-aux0] modem timer answer 45
```

parity

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

undo parity

View User interface view

Parameter **mark**: Performs mark checks.

even: Performs even checks.

none: Does not check.

odd: Performs odd checks.

space: Performs space checks.

Description

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

Use the **undo parity** command to revert to the default check mode.

note3Use these two commands in AUX user interface view only.

No check is performed by default.

Example

Set to perform even checks.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] user-interface aux 0
[SW7750-ui-aux0] parity even
```

protocol inbound

Syntax

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

View

User interface view

Parameter

all: Supports both Telnet protocol and SSH protocol.

ssh: Supports SSH protocol.

telnet: Supports Telnet protocol.

Description

Use the **protocol inbound** command to specify the protocols supported by the user interface.

Both Telnet protocol and SSH protocol are supported by default.

Related command:

user-interface.

CAUTION: To configure a user interface to support SSH, you need to set the authentication mode to scheme for users to log in successfully. If the authentication mode is set to password or none for login users, the ***protocol inbound*** *ssh command will fail. Refer to "authentication-mode" on page 57 for the related configuration.*

Example

Configure that only SSH protocol is supported in VTY 0.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] user-interface vty 0
[SW7750-ui-vty0] protocol inbound ssh
```

screen-length

Syntax

screen-length *screen-length*

undo screen-length

View User interface view

Parameter *screen-length*: Number of lines the screen can contain. This argument ranges from 0 to 512 and defaults to 24.

Description Use the **screen-length** command to set the number of lines the terminal screen can contain.

Use the **undo screen-length** command to revert to the default number of lines.

By default, the terminal screen can contain up to 24 lines.

You can use the **screen-length** 0 command to disable the function to display information in pages.

Example # Set the number of lines the terminal screen can contain to 20.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] user-interface aux0
[SW7750-ui-aux0] screen-length 20
```

send

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

View User view

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

type: User interface type.

number: Absolute or relative index of the user interface.

Description Use the **send** command to send messages to a specified user interface or all user interfaces.

Example # Send "hello" to all user interfaces.

```
<SW7750> send all
Enter message, end with CTRL+Z or Enter; abort with CTRL+C:
hello^Z
Send message? [Y/N]y
<SW7750>
***
***
***Message from aux0 to all terminals:
***
hello
```

service-type

Syntax **service-type** { **ftp** [**ftp-directory** *directory*] | **lan-access** | { **ssh** | **telnet** | **terminal** }* [**level** *level*] }

undo service-type { **ftp** [**ftp-directory**] | **lan-access** | { **ssh** | **telnet** | **terminal** }* }

View Local user view

Parameter **ftp**: Specifies the users to be of FTP type.

ftp-directory *directory*: Specifies the path for FTP users. The *directory* argument is a string up to 64 characters.

lan-access: Specifies the users to be of LAN-access type, which normally means Ethernet users, such as 802.1x users.

ssh: Specifies the users to be of SSH type.

telnet: Specifies the users to be of Telnet type.

terminal: Makes Terminal services available to users logging in through the Console port.

level *level*: Specifies the user level for Telnet users, Terminal users, or SSH users. The *level* argument ranges from 0 to 3 and defaults to 0.

Description Use the **service-type** command to specify the login type and the corresponding available command level.

Use the **undo service-type** command to cancel login type configuration.

Commands fall into four command levels: access, monitor, system, and administration, which are described as follows:

- Access level: Commands of this level are used to diagnose network and change the language mode of user interface, such as the **ping**, **tracert**, and **language-mode** command. The **Telnet** command is also of this level. Commands of this level cannot be saved in configuration files.
- Monitor level: Commands of this level are used to maintain the system, to debug service problems, and so on. The **display** and **debugging** command are of monitor level. Commands of this level cannot be saved in configuration files.
- System level: Commands of this level are used to configure services. Commands concerning routing and network layers are of system level. You can utilize network services by using these commands.
- Administration level: Commands of this level are for the operation of the entire system and the system supporting modules. Services are supported by these commands. Commands concerning file system, file transfer protocol (FTP),

trivial file transfer protocol (TFTP), downloading using XModem, user management, and level setting are of administration level.

Example # Configure commands of level 0 are available to the users logging in using the user name of "zbr".

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] local-user zbr
[SW7750-luser-zbr] service-type telnet level 0
```

# To verify the above configuration, you can quit the system, log in again using the user name of "zbr", and then list the available commands, as listed in the following.

```
[SW7750] quit
<SW7750> ?
User view commands:
  cluster            Run cluster command
  debugging          Enable system debugging functions
  language-mode      Specify the language environment
  ping               Send echo messages
  quit               Exit from current command view
  super              Privilege the current user a specified priority
level
  telnet             Establish one TELNET connection
  tracert            Trace route function
  undo               Cancel current setting
```

set authentication password

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

undo set authentication password

View User interface view

Parameter **cipher**: Specifies to display the local password in encrypted text when you display the current configuration.

simple: Specifies to display the local password in plain text when you display the current configuration.

password: Password. The password must be in plain text if you specify the **simple** keyword in the **set authentication password** command. If you specify the **cipher** keyword, the password can be in either encrypted text or plain text. When you enter the password in plain text containing up to 16 characters (such as 123), the system converts the password to the corresponding 24-character encrypted password (such as 7-CZB#/YX]KQ=^Q'MAF4<1!!). Make sure you are aware of the corresponding plain password if you enter the password in ciphered text (such as 7-CZB#/YX]KQ=^Q 'MAF4<1!!).

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

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

Note that only plain text passwords are expected when users are authenticated.

By default, modem users and Telnet users need to provide their passwords to log in. If no password is set, the "Login password has not been set !" message appears on the terminal when users log in.

Example # Set the local password of VTY 0 to "123".

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] user-interface vty 0
[SW7750-ui-vty0] set authentication password simple 123
```

shell

Syntax **shell**

undo shell

View User interface view

Parameter None

Description Use the **shell** command to make terminal services available for the user interface.

Use the **undo shell** command to make terminal services unavailable to the user interface.

By default, terminal services are available in all user interfaces.

Note the following when using the **undo shell** command:

- This command is available in all user interfaces except the AUX (Console) user interface.
- This command is unavailable in the current user interface.
- This command prompts for confirmation when being executed in any valid user interface.

Example # Log into user interface 0 and make terminal services unavailable in VTY 0 through VTY 4.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] user-interface vty 0 4
[SW7750-ui-vty0-4] undo shell
% Disable ui-vty0-4 , are you sure ? [Y/N] y
```

speed

Syntax

speed *speed-value*

undo speed

View

User interface view

Parameter

speed-value: Transmission speed (in bps). This argument can be 300, 600, 1200, 2400, 4800, 9600, 19,200, 38,400, 57,600, and 115,200 and defaults to 9,600.

Description

Use the **speed** command to set the transmission speed of the user interface.

Use the **undo speed** command to revert to the default transmission speed.

note3Use these two commands in the AUX user interface view only.

Example

Set the transmission speed of the AUX user interface to 115,200 bps.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] user-interface aux 0
[SW7750-ui-aux0] speed 115200
```

stopbits

Syntax

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

undo stopbits

View

User interface view

Parameter

1: Sets the stop bits to 1.

1.5: Sets the stop bits to 1.5.

2: Sets the stop bits to 2.

Description

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

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

note3Use these two commands in the AUX user interface only.

By default, the stop bits is 1.

- *The stopbits cannot be 1.5 on an Switch 7750 Ethernet switch.*
- *Changing the stop bits value of the switch to a value different from that of the terminal emulation utility does not affect the communication between them.*

Example

Set the stop bits to 2.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] user-interface aux 0
[SW7750-ui-aux0] stopbits 2
```

telnet

Syntax

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

View

User view

Parameter

hostname: Host name of the remote switch. You can use the **ip host** command to assign a host name to a switch.

ip-address: IP address of the remote switch.

service-port: TCP port number of the port that provides Telnet service on the switch. This argument ranges from 0 to 65,535.

Description

Use the **telnet** command to Telnet to another switch from the current switch to manage the former remotely. You can terminate a Telnet connection by pressing <Ctrl + K> or by executing the **quit** command.

The default TCP port number is 23.

Related command:

display tcp status, and **ip host**.

Example

Telnet to the switch with the host name of 3Com2 and IP address of 129.102.0.1 from the current switch (with the host name of 3Com1).

```
<SW77501> telnet 129.102.0.1
Trying 129.102.0.1 ...
Press CTRL+K to abort
Connected to 129.102.0.1 ...
*******************************************************************
* Copyright(c) 2004-2007 3Com Corporation                         *
* Without the owner’s prior written consent,                      *
* no decompiling or reverse-switch fabricering shall be allowed.  *
*******************************************************************
<SW77502>
```

user-interface

Syntax

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

View

System view

Parameter

type: User interface type.

first-number: User interface index, which identifies the first user interface to be configured.

last-number: User interface index, which identifies the last user interface to be configured.

Description Use the **user-interface** command to enter one or more user interface views to perform configuration.

Example # Enter VTY 0 user interface view.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] user-interface vty 0
[SW7750-ui-vty0]
```

user privilege level

Syntax **user privilege level** *level*

undo user privilege level

View User interface view

Parameter *level*: Command level ranging from 0 to 3.

Description Use the **user privilege level** command to configure the command level available to the users logging into the user interface.

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

By default, the commands of level 3 are available to the users logging into the AUX user interface. The commands of level 0 are available to the users logging into VTY user interfaces.

Example # Configure that commands of level 0 are available to the users logging into VTY 0.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] user-interface vty 0
[SW7750-ui-vty0] user privilege level 0
```

# You can verify the above configuration by Telneting to VTY 0 and displaying the available commands, as listed in the following.

```
<SW7750> ?
User view commands:
  cluster           Run cluster command
  debugging         Enable system debugging functions
  language-mode     Specify the language environment
  ping              Send echo message
```

```
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 COMMANDS FOR USER CONTROL

acl

Syntax **acl** *acl-number* { **inbound** | **outbound** }

undo acl { **inbound** | **outbound** }

View User interface view

Parameter *acl-number*: ACL number ranging from 2,000 to 3,999.

inbound: Filters the users Telneting to the current switch.

outbound: Filters the users Telneting to other switches from the current switch.

Description Use the **acl** command to apply an ACL to filter Telnet users.

Use the **undo acl** command to disable the switch from filtering Telnet users using the ACL.

By default, Telnet users are not filtered by ACLs.

Example # Apply ACL 2000 to filter users Telneting to the current switch (assuming that ACL 2,000 already exists.)

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] user-interface vty 0 4
[SW7750-ui-vty0-4] acl 2000 inbound
```

free web-users

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

View User view

Parameter **all**: Specifies all Web users.

user-id: Web user ID, an eight-digit hexadecimal number.

user-name: User name of the Web user. This argument can contain 1 to 80 characters.

Description Use the **free web-users** command to disconnect a specified Web user or all Web users by force.

Example # Disconnect all Web users by force.

```
<SW7750> free web-users all
```

ip http acl

Syntax **ip http acl** *acl-number*

undo ip http acl

View System view

Parameter *acl-number*: ACL number ranging from 2000 to 2999.

Description Use the **ip http acl** command to apply an ACL to filter Web users.

Use the **undo ip http acl** command to disable the switch from filtering Web users using the ACL.

By default, the switch does not use the ACL to filter Web users.

Example # Apply ACL 2000 to filter Web users (assuming that ACL 2000 already exists.)

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ip http acl 2000
```

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**: Specifies that the community has read-only permission in the specified view.

Write: Specifies that the community has read/write permission in the specified view.

community-name: Community name. A string ranges from 1 to 32 characters.

mib-view: Sets the name of the MIB view accessible to the community.

view-name: MIB view name, 1 to 32 characters long.

acl *acl-number*: Specifies the ACL number. The *acl-number* argument ranges from 2,000 to 2,999.

Description Use the **snmp-agent community** command to set a community name and to enable users to access the switch through SNMP. You can also optionally use this command to apply an ACL to filter network management users.

Use the **undo snmp-agent community** command to cancel community-related configuration for the specified community.

By default, SNMPv1 and SNMPv2c access a switch by community names.

Example # Set the community name to "h123", enable users to access the switch in the name of the community (with read-only permission), and apply ACL 2,000 to filter network management users (assuming that ACL 2000 already exists.)

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] snmp-agent community read h123 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**: Specifies to adopt v1 security scheme.

v2c: Specifies to adopt v2c security scheme.

v3: Specifies to adopt v3 security scheme.

group-name: Group name. This argument can be of 1 to 32 characters.

authentication: Specifies to authenticate SNMP data without encrypting the data.

privacy: Authenticates and encrypts packets.

read-view: Sets a read-only view.

read-view: Name of the view to be set to read-only. This argument can be of 1 to 32 characters.

write-view: Sets a readable & writable view.

write-view: Name of the view to be set to readable & writable. This argument can be of 1 to 32 characters.

notify-view: Sets a notifying view.

notify-view: Name of the view to be set to a notifying view. This argument can be of 1 to 32 characters.

acl *acl-number*: Specifies an ACL. The *acl-number* argument ranges from 2,000 to 2,999.

Description Use the **snmp-agent group** command to create a SNMP group. You can also optionally use this command to apply an ACL to filter network management users.

Use the **undo snmp-agent group** command to remove a specified SNMP group.

By default, the **snmp-agent group v3** *group-name* command is provided without the **authentication** and **privacy** keyword. That is, the switch does not authenticate or encrypt the specified group.

Example # Create a SNMP group named "h123" and apply ACL 2001 to filter network management users (assuming that ACL 2001 already exists).

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] snmp-agent group v1 h123 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** | **switch fabricid** *switch fabricid-string* }

View System view

Parameter **v1**: Specifies to adopt V1 security scheme.

v2c: Specifies to adopt V2 security scheme.

v3: Specifies to adopt V3 security scheme.

user-name: User name. This argument can be of 1 to 32 characters.

group-name: Group name the user corresponds to. This argument can be of 1 to 32 characters.

authentication-mode: Specifies to authenticate users.

md5: Specifies the authentication protocol to be HMAC-MD5-96.

sha: Specifies the authentication protocol to be HMAC-SHA-96.

auth-password: Authentication password. This argument can be of 1 to 64 characters.

privacy: Specifies to encrypt data.

des56: Specifies the encrypting protocol to be DES.

priv-password: Encrypting password string. This argument can be of 1 to 64 characters.

acl *acl-number*: Specifies the ACL number. The *acl-number* argument ranges from 2,000 to 2,999.

local: Specifies the user to be a local user entity.

switch fabricid: Specifies the ID of the switch fabric associated with the user.

switch fabricid-string: Engine ID, a string comprising 10 to 64 characters.

Description

Use the **snmp-agent usm-user** command to add a user to a specified SNMP group. You can also optionally use this command to apply an ACL to filter network management users.

Use the **undo snmp-agent usm-user** command to remove a user from the corresponding SNMP group. The operation also frees the user from the corresponding ACL-related configuration.

Example

Add the user named "3com" to the SNMP group named "3comgroup", specifying to authenticate the user, specifying the authentication protocol to be HMAC-MD5-96, the authentication password to be "3Com", and applying ACL 2002 to filter network management users (assuming that ACL 2002 already exists).

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] snmp-agent usm-user v3 3com 3comgroup authentication-mode m
d5 3Com acl 2002
```

4 CONFIGURATION FILE MANAGEMENT COMMANDS

display current-configuration

Syntax **display current-configuration** [[**interface** [*interface-type* [*interface-number*]] | **configuration** [*configuration*]] [**|** { **begin** | **exclude** | **include** } *text*]] | [**vlan** [*vlan-id*]]

View Any view

Parameter **interface**: View the configuration information of interfaces.

interface-type: Type of the interface, which may be Aux, GigabitEthernet, NULL, Vlan-interface, or M-Ethernet.

interface-number: Number of the interface.

configuration *configuration*: View the configuration information excluding the port information. The value of the *configuration* argument is the keyword of the configuration on the switch, such as:

- **acl-adv**: Views the configuration information of advanced ACLs.
- **ospf**: Views the configuration information of the OSPF protocol.
- **system**: Views the name of the host.
- **timerange**: Views the configuration information of the time range.

The optional configuration keywords are available only after the related functions are enabled on the switch.

vlan [*vlan-id*]: Displays the VLAN configuration in the system. If the *vlan-id* argument is not specified, the configuration information of all VLANs in the system is displayed; if the *vlan-id* argument is specified, the configuration information of the specified VLAN is displayed.

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

begin: Displays the configuration beginning with the specified characters.

exclude: Displays the configuration excluding the specified characters.

include: Displays the configuration including the specified characters.

text: Text included in a configuration item, expressed in a regular expression. .

Table 3 Description on the special characters in the regular expression

Character	Meaning	Description
_	Underline, which can represent the following characters: (^|$|[,{}]), space, starting character, and ending character.	If the first character of a regular expression is not "_", the number of the underline characters in a regular expression is only limited by the length of a command line. If the first character of a regular expression is "_", there can be up to four other successive underline characters following it. If the underline characters are not successive, only the first underline character group is matched. The subsequent underline groups are ignored.
^	Matches the character string starting with the subsequent sub-expression	^user matches the configuration starting with "user"
$	Matches the character string starting with the sub-expression before $	user$ matches the configuration information ending with "user"
(	Left parenthesis, push-in-stack signal	You are not recommended to use this character in a regular expression.
.	Period, a wildcard	It can match any single character excluding a line feed
*	Asterisk. It means that the preceding sub-expression can be matched for zero or multiple times.	zo* matches "z" and "zoo".
+	Plus sign. It means that the preceding sub-expression can be matched for one or multiple times.	zo+ matches "zo" and "zoo", but not "z".

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.

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

Example # View the running configuration parameters of the switch.

```
<SW7750> display current-configuration
#
 sysname 3Com
#
```

```
 ftp server enable
#
 local-server nas-ip 127.0.0.1
#
 domain default enable system
#
 nat address-group 0 1.1.1.1 1.1.1.2
 nat address-group 1 2.2.2.2 2.2.2.3
 nat blacklist start slot 2
 nat blacklist mode all
 nat blacklist limit amount 202
#
 temperature-limit 0 10 70
 temperature-limit 1 10 70
 temperature-limit 2 10 80
 temperature-limit 3 10 70
#
 poe power max-value 2400
#
 attack-protection disable-defaultroute
#
 password-control login-attempt 3 exceed lock-time 120
#
traffic-accounting traffic-group somegroup
 network 1.1.0.0 255.255.0.0
#
radius scheme system
 primary authentication 127.0.0.1 1645
 primary accounting 127.0.0.1 1646
 user-name-format without-domain
#
domain new
 vlan-assignment-mode integer
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
 messenger time disable
 accounting-mode traffic
 traffic-group somegroup rate 2
domain system
 vlan-assignment-mode integer
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
 messenger time disable
#
 stp instance 0 PortLog
 stp TC-protection enable
#
acl number 2001
 rule 0 deny
#
vlan 1
 description TestVlan1
 igmp-snooping enable
#
```

```
vlan 2
#
vlan 5
#
vlan 6
#
vlan 7
#
interface Vlan-interface1
 ip address 192.168.0.68 255.255.255.0
 nat outbound 2001 address-group 0 slot 2
#
interface Aux0/0/0
#
interface M-Ethernet0/0/0
#
interface GigabitEthernet0/0/1
#
interface GigabitEthernet0/0/2
#
interface GigabitEthernet0/0/3
#
interface GigabitEthernet0/0/4
#
interface GigabitEthernet3/0/1
#
interface GigabitEthernet3/0/2
#
interface GigabitEthernet3/0/3
#
interface GigabitEthernet3/0/4
#
interface GigabitEthernet3/0/5
#
interface GigabitEthernet3/0/6
#
interface GigabitEthernet3/0/7
#
interface GigabitEthernet3/0/8
#
interface GigabitEthernet3/0/9
#
interface GigabitEthernet3/0/10
#
interface GigabitEthernet3/0/11
#
interface GigabitEthernet3/0/12
#
interface GigabitEthernet3/0/13
#
interface GigabitEthernet3/0/14
#
interface GigabitEthernet3/0/15
#
interface GigabitEthernet3/0/16
#
interface GigabitEthernet3/0/17
#
```

```
interface GigabitEthernet3/0/18
#
interface GigabitEthernet3/0/19
#
interface GigabitEthernet3/0/20
#
interface GigabitEthernet3/0/21
#
interface GigabitEthernet3/0/22
#
interface GigabitEthernet3/0/23
#
interface GigabitEthernet3/0/24
#
interface GigabitEthernet3/0/25
#
interface GigabitEthernet3/0/26
#
interface GigabitEthernet3/0/27
#
interface GigabitEthernet3/0/28
#
interface GigabitEthernet3/0/29
#
interface GigabitEthernet3/0/30
#
interface GigabitEthernet3/0/31
#
interface GigabitEthernet3/0/32
#
interface GigabitEthernet3/0/33
#
interface GigabitEthernet3/0/34
#
interface GigabitEthernet3/0/35
#
interface GigabitEthernet3/0/36
#
interface GigabitEthernet3/0/37
#
interface GigabitEthernet3/0/38
#
interface GigabitEthernet3/0/39
#
interface GigabitEthernet3/0/40
#
interface GigabitEthernet3/0/41
#
interface GigabitEthernet3/0/42
#
interface GigabitEthernet3/0/43
#
interface GigabitEthernet3/0/44
#
interface GigabitEthernet3/0/45
#
interface GigabitEthernet3/0/46
#
```

```
interface GigabitEthernet3/0/47
#
interface GigabitEthernet3/0/48
 port access vlan 300
#
interface RprGE1/0/1
#
interface RprGE1/0/1.1
#
interface RprGE1/0/1.2
#
interface NULL0
#
interface LoopBack103
 ip address 103.1.1.1 255.255.255.0
#
rip
 default cost 5
 network 103.0.0.0
 network 101.0.0.0
 network 100.0.0.0
 network 192.168.0.0
#
traffic-accounting accounting-slot 2
 traffic-slot 1
 accounting enable
#
user-interface aux 0
user-interface vty 0 4
 authentication-mode none
 user privilege level 3
#
return
```

# Display the configuration information that takes effect on VLAN1.

```
<SW7750> display current-configuration vlan 1
#
vlan 1
 description TestVlan1
 igmp-snooping enable
#
return
```

# Display configuration information lines containing 10*. * indicates that the number zero before * can be displayed multiple times consecutively or is not displayed.

```
<SW7750> display current-configuration | include 10*
local-server nas-ip 127.0.0.1
 nat address-group 0 1.1.1.1 1.1.1.2
 nat address-group 1 2.2.2.2 2.2.2.3
 temperature-limit 0 10 70
 temperature-limit 1 10 70
 temperature-limit 2 10 80
 temperature-limit 3 10 70
 password-control login-attempt 3 exceed lock-time 120
 network 1.1.0.0 255.255.0.0
 primary authentication 127.0.0.1 1645
 primary accounting 127.0.0.1 1646
acl number 2001
vlan 1
 description TestVlan1
interface Vlan-interface1
 ip address 192.168.0.68 255.255.255.0
 nat outbound 2001 address-group 0 slot 2
interface GigabitEthernet0/0/1
interface GigabitEthernet3/0/1
interface GigabitEthernet3/0/10
interface GigabitEthernet3/0/11
interface GigabitEthernet3/0/12
interface GigabitEthernet3/0/13
interface GigabitEthernet3/0/14
interface GigabitEthernet3/0/15
interface GigabitEthernet3/0/16
interface GigabitEthernet3/0/17
interface GigabitEthernet3/0/18
interface GigabitEthernet3/0/19
interface GigabitEthernet3/0/21
interface GigabitEthernet3/0/31
interface GigabitEthernet3/0/41
interface RprGE1/0/1
interface RprGE1/0/1.1
interface RprGE1/0/1.2
interface LoopBack103
 ip address 103.1.1.1 255.255.255.0
 network 103.0.0.0
 network 101.0.0.0
 network 100.0.0.0
 network 192.168.0.0
 traffic-slot 1
```

# Display the configuration information starting with "user".

```
<SW7750> display current-configuration | include ^user
user-interface aux 0
user-interface vty 0 4
```

# Display the configuration information excluding port configuration.

```
<SW7750> display current-configuration configuration
#
 sysname 3Com
#
 ftp server enable
#
 local-server nas-ip 127.0.0.1
#
 domain default enable system
#
 nat address-group 0 1.1.1.1 1.1.1.2
 nat address-group 1 2.2.2.2 2.2.2.3
 nat blacklist start slot 2
 nat blacklist mode all
 nat blacklist limit amount 202
```

```
#
 temperature-limit 0 10 70
 temperature-limit 1 10 70
 temperature-limit 2 10 80
 temperature-limit 3 10 70
#
 poe power max-value 2400
#
 attack-protection disable-defaultroute
#
 password-control login-attempt 3 exceed lock-time 120
#
traffic-accounting traffic-group somegroup
 network 1.1.0.0 255.255.0.0
#
radius scheme system
 primary authentication 127.0.0.1 1645
 primary accounting 127.0.0.1 1646
 user-name-format without-domain
#
domain new
 vlan-assignment-mode integer
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
 messenger time disable
 accounting-mode traffic
 traffic-group somegroup rate 2
domain system
 vlan-assignment-mode integer
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
 messenger time disable
#
 stp instance 0 PortLog
 stp TC-protection enable
#
acl number 2001
 rule 0 deny
#
rip
 default cost 5
 network 103.0.0.0
 network 101.0.0.0
 network 100.0.0.0
 network 192.168.0.0
#
traffic-accounting accounting-slot 2
 traffic-slot 1
 accounting enable
#
user-interface aux 0
user-interface vty 0 4
 authentication-mode none
 user privilege level 3
```

```
#
return
```

# Display the configuration information of all the VLANs.

```
<SW7750> display current-configuration vlan
#
vlan 1
 description TestVlan1
 igmp-snooping enable
#
vlan 2
#
vlan 5
#
vlan 6
#
vlan 7
#
return
```

display saved-configuration

Syntax **display saved-configuration**

View Any view

Parameter None

Description Use the **display saved-configuration** command to display the configuration files saved in the switch flash memory.

If the Ethernet switch cannot work normally after being booted, you can use this command to view the booting configuration of this Ethernet switch.

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

Example # Display the configuration files saved in the flash memory.

```
<SW7750> display saved-configuration
#
 sysname 3Com
#
 local-server nas-ip 127.0.0.1
#
 domain default enable system
#
 temperature-limit 0 10 70
 temperature-limit 1 10 70
 temperature-limit 2 10 80
 temperature-limit 3 10 70
#
 poe power max-value 2400
```

```
#
radius scheme system
 primary authentication 127.0.0.1 1645
 primary accounting 127.0.0.1 1646
 user-name-format without-domain
#
domain system
 vlan-assignment-mode integer
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
 messenger time disable
#
 stp TC-protection enable
#
vlan 1
#
interface Vlan-interface1
 ip address 192.168.0.68 255.255.255.0
#
interface Aux0/0/0
#
interface M-Ethernet0/0/0
#
interface GigabitEthernet0/0/1
#
interface GigabitEthernet0/0/2
#
interface GigabitEthernet0/0/3
#
interface GigabitEthernet0/0/4
#
interface GigabitEthernet3/0/1
#
interface GigabitEthernet3/0/2
#
interface GigabitEthernet3/0/3
#
interface GigabitEthernet3/0/4
#
interface GigabitEthernet3/0/5
#
interface GigabitEthernet3/0/6
#
interface GigabitEthernet3/0/7
#
interface GigabitEthernet3/0/8
#
interface GigabitEthernet3/0/9
#
interface GigabitEthernet3/0/10
#
interface GigabitEthernet3/0/11
#
interface GigabitEthernet3/0/12
#
interface GigabitEthernet3/0/13
```

```
#
interface GigabitEthernet3/0/14
#
interface GigabitEthernet3/0/15
#
interface GigabitEthernet3/0/16
#
interface GigabitEthernet3/0/17
#
interface GigabitEthernet3/0/18
#
interface GigabitEthernet3/0/19
#
interface GigabitEthernet3/0/20
#
interface GigabitEthernet3/0/21
#
interface GigabitEthernet3/0/22
#
interface GigabitEthernet3/0/23
#
interface GigabitEthernet3/0/24
#
interface GigabitEthernet3/0/25
#
interface GigabitEthernet3/0/26
#
interface GigabitEthernet3/0/27
#
interface GigabitEthernet3/0/28
#
interface GigabitEthernet3/0/29
#
interface GigabitEthernet3/0/30
#
interface GigabitEthernet3/0/31
#
interface GigabitEthernet3/0/32
#
interface GigabitEthernet3/0/33
#
interface GigabitEthernet3/0/34
#
interface GigabitEthernet3/0/35
#
interface GigabitEthernet3/0/36
#
interface GigabitEthernet3/0/37
#
interface GigabitEthernet3/0/38
#
interface GigabitEthernet3/0/39
#
interface GigabitEthernet3/0/40
#
interface GigabitEthernet3/0/41
#
interface GigabitEthernet3/0/42
```

```
#
interface GigabitEthernet3/0/43
#
interface GigabitEthernet3/0/44
#
interface GigabitEthernet3/0/45
#
interface GigabitEthernet3/0/46
#
interface GigabitEthernet3/0/47
#
interface GigabitEthernet3/0/48
#
interface RprGE1/0/1
#
interface RprGE1/0/1.1
#
interface RprGE1/0/1.2
#
interface NULL0
#
user-interface aux 0
user-interface vty 0 4
 authentication-mode none
 user privilege level 3
#
return
```

The mentioned-above information describes global configuration, port configuration, and user interface configuration respectively.

display this

Syntax **display this**

View Any view

Parameter None

Description Use the **display this** command to display the configuration of the current view. After finishing configuration in the current view, you can use this command to display parameters that take effect.

If the configuration parameters are the same as default parameters, the system does not display such parameters. The system does not display the configuration parameters that do not take effect, either.

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**, and **display current-configuration**

Example # Display the configuration parameters that take effect in system view.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] display this
#
 sysname 3Com
#
 ftp server enable
#
 local-server nas-ip 127.0.0.1
#
 domain default enable system
#
 nat address-group 0 1.1.1.1 1.1.1.2
 nat address-group 1 2.2.2.2 2.2.2.3
 nat blacklist start slot 2
 nat blacklist mode all
 nat blacklist limit amount 202
#
 temperature-limit 0 10 70
 temperature-limit 1 10 70
 temperature-limit 2 10 80
 temperature-limit 3 10 70
#
 poe power max-value 2400
#
 attack-protection disable-defaultroute
#
 password-control login-attempt 3 exceed lock-time 120
#
return
```

display startup

Syntax **display startup**

View Any view

Parameter None

Description Use the **display startup** command to display the configuration file names used for the current and the next start-ups.

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

Example # Display the configuration filenames used for the current and the next start-ups.

```
<SW7750> display startup
MainBoard:
```

```
Startup saved-configuration file:         flash:/config.cfg
Next startup saved-configuration file:    flash:/config.cfg
```

reset saved-configuration

Syntax **reset saved-configuration**

View User view

Parameter None

Description Use the **reset saved-configuration** command to erase configuration files from the flash memory of the Ethernet 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 **reset saved-configuration** command to erase the old configuration files.
- If a used Ethernet Switch is applied to the new circumstance and the original configuration files cannot meet the new requirements, the Ethernet Switch should be configured again. Erase the original configuration files for reconfiguration.

If the configuration files do not exist in the flash memory when Ethernet 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 Ethernet Switch.

```
<SW7750> reset saved-configuration
The saved configuration will be erased.
Are you sure?[Y/N]y
Configuration in flash memory is being cleared.
Please wait ...
....
Configuration in flash memory is cleared.
```

save

Syntax **save** [*file-name* | **safely**]

View User view

Parameter *file-name*: File name with the extension name ".cfg", a character string of 5 to 56 characters.

safely: Saves the configuration files to the flash memory in the **safely** mode.

Description Use the **save** command to save the current configuration files to the 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.

The configured files can be saved in one of the following two ways:

- Fast saving: in this mode, the configuration files are saved fast. However, if restart or power-off occurs in the saving procedure, the configuration files will be lost.
- Safely saving: in this mode, the configuration files are saved slowly. However, even if restart or power-off occurs in the saving procedure, the configuration files still exist.

If the **save** command is executed without the **safely** keyword, the configuration files are saved in the fast saving mode. If the **save** command is executed with the **safely** keyword, the configuration files are saved in the safely saving mode.

You are recommended to adopt the fast saving mode in the conditions of stable power and adopt the safely saving mode in the conditions of unstable power or remote maintenance.

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

Example # Get the current configuration files stored in the flash memory.

```
<SW7750> save
The configuration will be written to the device.
Are you sure?[Y/N]y
 Please input the file name(*.cfg)[flash:/config.cfg]:123.cfg
.......
Now saving current configuration to the device.
Saving configuration flash:/123.cfg. Please wait...
...
Configuration is saved to flash memory successfully.
```

startup saved-configuration

Syntax **startup saved-configuration** { *cfgfile* | *device-name* }

View User view

Parameter

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

device-name: Name of the current storage device.

Description

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

Note that the configuration file must use ".cfg" as its extension name and is saved under the root directory of the Flash.

Related command: **display startup**.

Example

Configure the configuration file for the next start-up as config.cfg.

```
<SW7750> startup saved-configuration config.cfg ......
```

5 VLAN CONFIGURATION COMMANDS

broadcast-suppression

Syntax **broadcast-suppression** { *ratio* | **pps** *pps* }

undo broadcast-suppression

View VLAN view

Parameter *ratio*: Specifies the bandwidth ratio for the maximum broadcast traffic in specific VLAN. Its value ranges from 1 to 100 and defaults to 100. The smaller the ratio is, the less the allowed broadcast traffic can pass.

pps *pps*: Specifies the maximum number of broadcast packets that can pass through a specific VLAN per second. Its value ranges from 1 to 148800.

Description Use the **broadcast-suppression** command to suppress broadcast traffic through a VLAN.

Use the **undo broadcast-suppression** command to reset the allowed broadcast traffic through a VLAN to the default value.

By default, the switch does not suppress broadcast traffic.

When the actual broadcast traffic exceeds the specified value, the system will discard the extra packets so that the bandwidth occupied by broadcast traffic can be kept within a specific ratio to ensure normal network operation.

The modules of Switch 7750s support different broadcast storm suppression modes, as listed in Table 4.

Table 4 Broadcast storm suppression modes and module types

Broadcast storm suppression mode	Type A card	Non-Type-A card
VLAN pps suppression	Supported	Not supported
VLAN bandwidth ratio suppression	Supported	Not supported

Type A modules include 3C16860, 3C16861, LS81FS24A, 3C16858, 3C16859, and 32Gbps and 64Gbps Switch Fabrics.

A VLAN only supports one broadcast storm suppression mode at one time. If you configure broadcast storm suppression modes multiple times for a VLAN, the latest configuration will overwrite the previous configuration.

Example # Allow broadcast traffic to occupy 20% bandwidth in VLAN2.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] vlan 2
[SW7750-vlan2] broadcast-suppression 20
```

description

Syntax **description** { *string* | *text* }

undo description

View VLAN view, VLAN interface view

Parameter *string*: Contiguous string describing the VLAN. It contains 1 to 32 characters without space.

text: Text describing the VLAN interface. It contains 1 to 80 characters and space is allowed.

Description Use the **description** command to set the description string or text for the current VLAN or VLAN interface.

Use the **undo description** command to restore the default description string or text.

By default, the description string of a VLAN is its VLAN ID, for example, "VLAN 0001"; the descriptive text of a VLAN interface is its name, for example, "Vlan-interface 1 Interface".

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

Example # Specify the description string of VLAN 1 as "research".

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] vlan 1
[SW7750-vlan1] description research
```

display interface Vlan-interface

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

View Any view

Parameter

vlan-id: ID of the specific VLAN interface.

Description

Use the **display interface Vlan-interface** command to display the related information of a VLAN interface, including, physical state and link state of the VLAN interface, format of the sent frames, MAC address, IP address and subnet mask of the VLAN interface, and descriptive string and MTU of the VLAN interface

If the *vlan-id* argument is specified, the information about the specified VLAN interface is displayed; if the *vlan-id* argument is not specified, the information about all the created VLAN interfaces is displayed.

Related command:

interface Vlan-interface.

Example

Display the information about Vlan-interface 2.

```
<SW7750> display interface Vlan-interface 2
Vlan-interface2 current state :DOWN
Line protocol current state :DOWN
IP Sending Frames’ Format is PKTFMT_ETHNT_2, Hardware address is 0012-a990-2241
Internet Address is 10.1.1.1/24 Primary
Description : Vlan-interface2 Interface
The Maximum Transmit Unit is 1500
```

Table 5 Description of the fields of the **display interface Vlan-interface** command

Field	Description
Vlan-interface2 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 frames that IP sends
Hardware address	MAC address corresponding to the VLAN interface
Internet Address	IP address corresponding to the VLAN interface
Description	Description on the VLAN interface
The Maximum Transmit Unit	Maximum transmission unit

display vlan

Syntax

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

View

Any view

Parameter

vlan-id: Specifies the VLAN ID, ranging from 1 to 4094.

to: Specifies multiple contiguous VLAN IDs.

all: Specifies to display the information about all the VLANs.

static: Specifies to display the VLANs created statically.

dynamic: Specifies to display the VLANs created dynamically.

Description

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

If the *vlan-id* argument or the **all** keyword is specified, the information about the specified VLANs or the all VLANs is displayed, including VLAN ID, VLAN type (dynamic or static), routing function status (If enabled, the primary IP address and mask are displayed), VLAN description and VLAN name, VLAN broadcast storm suppression ratio, and VLAN member ports.

If no argument or keyword is specified, this command displays the list of all the existing VLANs. If the **dynamic** or **static** keyword is specified, this command displays the list of the VLANs that are created dynamically or statically.

Related command: **vlan**.

Example # Display the information about VLAN 2.

```
<SW7750> display vlan 2
 VLAN ID: 2
 VLAN Type: static
 Route Interface: not configured
Description: VLAN 0002
 Name: VLAN 0002
Broadcast MAX-ratio: 100
 Tagged   Ports: none
 Untagged Ports:
  Ethernet3/0/30
```

Table 6 Description of the fields of the **display vlan** command

Field	Description
VLAN ID	VLAN ID
VLAN Type	VLAN type (dynamic or static)
Route Interface	Whether the routing interface function is enable for this VLAN
Description	Description on the VLAN
Name	VLAN name
Broadcast MAX-ratio	VLAN broadcast storm suppression ratio
Tagged Ports	The ports that keep packets' tags when sending packets
Untagged Ports	The ports that strip off packet tags when sending packets

interface Vlan-interface

Syntax **interface Vlan-interface** *vlan-id*

undo interface Vlan-interface *vlan-id*

View System view

Parameter *vlan-id*: ID of the VLAN interface, in the range of 1 to 4,094.

Description Use the **interface Vlan-interface** command to create a VLAN interface or enter VLAN interface view.

Use the **undo interface Vlan-interface** command to delete the VLAN interface.

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

Example # Enter Vlan-interface 1 view

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 1
[SW7750-Vlan-interface1]
```

name

Syntax **name** *string*

undo name

View VLAN view

Parameter *string*: String that refers to the VLAN name. It contains 1 to 32 characters.

Parameter Use the **name** command to assign a name to the current VLAN.

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

By default, the name of a VLAN is its VLAN ID, for example, "VLAN 0001".

Example # Specify the name of VLAN 2 to "hello".

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] vlan 2
[SW7750-vlan2] name hello
```

shutdown

Syntax **shutdown**

undo shutdown

View VLAN interface view

Parameter None

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

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

By default, a VLAN interface is enabled. In this scenario, the VLAN interface's status is determined by the status of its ports, that is, if all the ports of the VLAN interface are down, the VLAN interface is down (disabled); if one or more ports of the VLAN interface are up, the VLAN interface is up (enabled).

If a VLAN interface is disabled, its status is not determined by the status of its ports.

You can use the **undo shutdown** command to enable a VLAN interface when its related parameters and protocols are configured. When a VLAN interface fails, you can use the **shutdown** command to disable the interface, and then use the **undo shutdown** command to enable this interface again, which may restore the interface.

The operation of enabling/disabling a VLAN interface does not influence all the Ethernet ports belonging to this VLAN.

Example # Disable Vlan-interface2 and then enable it.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 2
[SW7750-Vlan-interface2] shutdown
[SW7750-Vlan-interface2] undo shutdown
```

vlan

Syntax **vlan** *vlan-id*

undo vlan *vlan-id*

View System view

Parameter *vlan-id*: ID of the VLAN that you want to enter. Its value ranges from 1 to 4094.

Description Use the **vlan** command to enter a VLAN view. If the VLAN identified by the *vlan-id* argument does not exist, this command creates the VLAN and then enters the VLAN view.

Use the **undo vlan** command to remove a VLAN.

⚠ ***CAUTION:*** *You cannot use the* ***undo vlan*** *command to remove the following kinds of VLANs directly.*

- *RRPP-controlled VLAN*
- *Guest VLAN*
- *VLAN that belongs to a VRRP group*
- *Portal-running VLAN*
- *Isolate-user-VLAN and all its mapping secondary VLANs.*
- *Voice VLAN*

- *Protocol-based VLAN*
- *Shared-VLAN*

*When you use the **undo vlan** command to remove a VLAN which is the default VLAN of an access port, a trunk port or a hybrid port on the device, the port will use VLAN 1 as the default VLAN after the **undo vlan** command is executed.*

Related command: **display vlan**

Example # Enter VLAN 1 view.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] vlan 1
[SW7750-vlan1]
```

vlan to

Syntax **vlan** *vlan-id1* **to** *vlan-id2*

undo vlan *vlan-id1* **to** *vlan-id2*

View System view

Parameter *vlan-id1*: ID of the first VLAN to be created, in the range of 1 to 4094.

to: Specifies a VLAN range. The VLAN ID after **to** must be greater than or equal to that before **to**.

vlan-id2: ID of the last VLAN to be created, in the range of 1 to 4094, and cannot be less than *vlan-id2*.

Description Use the **vlan to** command to create a range of VLANs.

Use the **undo vlan to** command to remove a range of VLANs.

***CAUTION:** You cannot use the **undo vlan to** command to remove the following kinds of VLANs directly.*

- *RRPP-controlled VLAN*
- *Guest VLAN*
- *VLAN that belongs to a VRRP group*
- *Portal-running VLAN*
- *Isolate-user-VLAN and all its mapping secondary VLANs.*
- *Voice VLAN*
- *Protocol-based VLAN*
- *Shared-VLAN*

As the default VLAN, VLAN 1 needs not to be created and cannot be removed.

Example

Create VLAN 4 through VLAN 100 at a time.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] vlan 4 to 100
This operation may take a few minutes.
 Please wait...
Done.
[SW7750]
```

# Display existing VLANs on the device after you create VLANs in a bulk.

```
[SW7750] display vlan
 Now, the following VLAN exist(s
  1(default), 4-100
 ---  98 VLAN(s) found  ---
```

vlan all

Syntax

vlan all

undo vlan all

View

System view

Parameter

None

Description

Use the **vlan all** command to create all VLANs, that is, to create VLANs from VLAN 2 through VLAN 4094.

Use the **undo vlan all** command to remove all VLANs.

CAUTION: *You cannot use the **undo vlan all** command to remove the following kinds of VLANs directly.*

- *RRPP-controlled VLAN*
- *Guest VLAN*
- *VLAN that belongs to a VRRP group*
- *Portal-running VLAN*
- *Isolate-user-VLAN and all its mapping secondary VLANs.*
- *Voice VLAN*
- *Protocol-based VLAN*
- *Shared-VLAN*

- *As the default VLAN, VLAN 1 needs not to be created and cannot be removed.*
- *Operations of creating and removing all VLANs take much of the system resource, which may cause the system not to respond to the current user*

interface. And during the operations, you cannot perform VLAN configurations in other user interfaces, either.

Example # Create all VLANs

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] vlan all
This operation may take a few minutes.
 Please wait...
Done.
```

# Remove all VLANs, in which VLAN 2, VLAN 5, and VLAN 20 has been configured as the shared-VLAN, voice VLAN, and remote probe VLAN respectively.

```
[SW7750] undo vlan all
This may delete all static VLAN except the VLAN kept by protocol and
 the default
 VLAN.
Continue?[Y/N]:y
 This operation may take a few minutes.
 Please wait...
 Can’t delete vlan when shared-vlan enabled!
 Can’t delete vlan when voice vlan enabled
 Cannot delete remote probe VLAN
 Fail to delete VLAN: 2, 5, 20
Done.
```

6 PORT-BASED VLAN CONFIGURATION COMMANDS

display port

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

View Any view

Parameters **hybrid**: Displays hybrid ports.

trunk: Displays trunk ports.

Description Use the **display port** command to check whether there are hybrid or trunk ports in the current system and display such ports (if available).

Examples # Display the hybrid ports in the current system.

```
<SW7750> display port hybrid
The following hybrid ports exist:
  Ethernet2/0/1          Ethernet2/0/2
```

The above information shows the current system has two hybrid ports: Ethernet 2/0/1 and Ethernet 2/0/2.

port

Syntax **port** *interface-list*

undo port *interface-list*

View VLAN view

Parameter *interface-list*: List of Ethernet ports to be added to or removed from a VLAN. You need to provide this argument in the form of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-10>, where:

- *interface-type* is port type and *interface-number* is port number.
- The port number to the right of the **to** keyword must be larger than or equal to the one to the left of the keyword.
- &<1-10> means that you can provide up to 10 ports or ports lists.

Parameter Use the **port** command to add a port or multiple ports to a VLAN.

Use the **undo port** command to remove a port or multiple ports from a VLAN.

Related command: **display vlan**.

Example # Add Ethernet2/0/2 through Ethernet2/0/4 to VLAN 2.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] vlan 2
[SW7750-vlan2] port Ethernet 2/0/2 to Ethernet 2/0/4
```

port access vlan

Syntax **port access vlan** *vlan-id*

undo port access vlan

View Ethernet port view

Parameters *vlan-id*: VLAN ID defined in IEEE802.1Q, in the range of 1 to 4094.

CAUTION: *All access ports belong to VLAN 1, which is the default VLAN of the system, so you are not allowed to add an access port to VLAN 1 or remove an access port from VLAN 1. Otherwise, the system will prompt: "Can't delete ports from or add ports to the default VLAN!".*

Description Use the **port access vlan** command to add the access port into the specified VLAN.

Use the **undo port access vlan** command to remove the access port from the specified VLAN.

You must specify the ID of an existing VLAN in the command.

Examples # Add Ethernet 2/0/1 into VLAN 3.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] vlan 3
[SW7750-vlan3] quit
[SW7750] interface ethernet 2/0/1
[SW7750-Ethernet2/0/1] port access vlan 3
```

port hybrid pvid vlan

Syntax **port hybrid pvid vlan** *vlan-id*

undo port hybrid pvid

View Ethernet port view

Parameters *vlan-id*: VLAN ID defined in IEEE802.1Q, in the range of 1 to 4094. It is 1 by default.

Description Use the **port hybrid pvid vlan** command to set the default VLAN ID for the hybrid port.

Use the **undo port hybrid pvid** command to restore the default VLAN ID of the port.

Related commands: **port link-type**.

*CAUTION: You are recommended to set the default VLAN ID of the local hybrid or trunk **port**s to the same value as that of the hybrid or trunk **port**s on the peer switch. Otherwise, packet forwarding may fail on the **port**s.*

Examples # After configuring Ethernet 2/0/1 as a hybrid port, set the default VLAN ID to 100.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface ethernet2/0/1
[SW7750-Ethernet2/0/1] port link-type hybrid
[SW7750-Ethernet2/0/1] 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

Parameters *vlan-id-list*: VLAN range to which the hybrid port will be added. *vlan-id-list* = [*vlan-id1* [**to** *vlan-id2*]]&<1-10>, where, *vlan-id* is in the range of 1 to 4094 and can be discrete, and &<1-10> means you can input up to ten VLAN IDs/ID ranges.

tagged: Keeps VLAN tags when the packets of the specified VLANs are forwarded on this port.

untagged: Keeps no VLAN tags when the packets of the specified VLANs are forwarded on this port.

Description Use the **port hybrid vlan** command to add the hybrid port into specified VLANs.

Use the **undo port hybrid vlan** command to remove the hybrid port from specified VLANs.

A hybrid port can belong to multiple VLANs. When you use the command several times, all VLAN specified in the commands will be allowed to pass the port.

The VLAN specified by the *vlan-id* argument must exist. Otherwise, this command is invalid.

Related commands: **port link-type**.

Examples # Add the hybrid port Ethernet 2/0/1 to VLAN 2, VLAN 4 and VLAN 50 through VLAN 100, with tags assigned to their packets.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] vlan 2
[SW7750-vlan2] quit
[SW7750] interface ethernet 2/0/1
[SW7750-Ethernet2/0/1] port link-type hybrid
[SW7750-Ethernet2/0/1] port hybrid vlan 2 4 50 to 100 tagged
 Operation complete, except these VLAN(s):
 Non-existent VLAN(s)
```

port link-type

Syntax **port link-type** { **access** | **hybrid** | **trunk** }

undo port link-type

View Ethernet port view

Parameters **access**: Sets the port as an access port.

hybrid: Sets the port as a hybrid port.

trunk: Sets the port as a trunk port.

Description Use the **port link-type** command to set the link type of the current Ethernet port.

Use the **undo port link-type** command to restore the default link type.

By default, the link type of any port is access.

Pay attention to the following:

The three types of ports can co-exist on the same Ethernet switch. However, a trunk port cannot be directly switched to a hybrid port, and vice versa. To set a trunk/hybrid port to another type (different from access), you must first set the port to an access port and then set the access port to the required type. For example, a trunk port cannot be directly set to a hybrid port. You must set the trunk port to an access port and then set it to a hybrid port.

Examples # Set Ethernet 2/0/1 as a trunk port.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
```

```
[SW7750] interface ethernet 2/0/1
[SW7750-Ethernet2/0/1] port link-type trunk
```

port trunk permit vlan

Syntax **port trunk permit vlan** { *vlan-id-list* | **all** }

undo port trunk permit vlan { *vlan-id-list* | **all** }

View Ethernet port view

Parameters *vlan-id-list*: VLAN range to which the trunk port will be added. *vlan-id-list* = [*vlan-id1* [**to** *vlan-id2*]]&<1-10>, where, *vlan-id* is in the range of 1 to 4094 and can be discrete, and &<1-10> means you can input up to ten VLAN IDs/ID ranges.

all: Adds the trunk port into all VLANs.

Description Use the **port trunk permit vlan** command to add the trunk port into the specified VLAN.

Use the **undo port trunk permit vlan** command to remove the hybrid port from the specified VLAN.

A trunk port can belong to multiple VLANs. When you use the command several times, all VLAN specified in the commands will be allowed to pass the port.

Related commands: **port link-type**.

Examples # Add the trunk port Ethernet 2/0/1 to VLAN 2, VLAN 4 and VLAN 50 through VLAN 100.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface ethernet 2/0/1
[SW7750-Ethernet2/0/1] port link-type trunk
[SW7750-Ethernet2/0/1] port trunk permit vlan 2 4 50 to 100
 Please wait... Done.
```

port trunk pvid vlan

Syntax **port trunk pvid vlan** *vlan-id*

undo port trunk pvid

View Ethernet port view

Parameters *vlan-id*: VLAN ID defined in IEEE802.1Q, in the range of 1 to 4094. It is 1 by default.

Description

Use the **port trunk pvid vlan** command to set the default VLAN ID for the trunk port.

Use the **undo port trunk pvid** command to restore the default setting.

To guarantee the proper packet transmission, the default VLAN ID of the local trunk port must be identical with that of the trunk port on the peer switch connected with the local trunk port.

Related commands: **port link-type**.

Examples

Set the default VLAN ID of the trunk port Ethernet 2/0/1 to 100.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface ethernet 2/0/1
[SW7750-Ethernet2/0/1] port link-type trunk
[SW7750-Ethernet2/0/1] port trunk pvid vlan 100
```

7 PROTOCOL-BASED VLAN CONFIGURATION COMMANDS

display protocol-vlan interface

Syntax **display protocol-vlan interface** { { *interface-type interface-number* [**to** *interface-type interface-number*] } | **all** }

View Any view

Parameter { *interface-type interface-number* [**to** *interface-type interface-number*] }: Specifies the port number of the protocol to be displayed. If you do not use the **to** keyword, only one port is specified. If you use the **to** keyword, multiple contiguous ports are specified. The *interface-type* argument refers to the port type and the *interface-number* argument refers to the port number.

all: Displays the protocol-related information about all ports.

Description Use the **display protocol-vlan interface** command to display the protocol-based VLAN information, including VLAN ID, protocol index and protocol type.

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

Example # Display protocol information and protocol index configured for Ethernet2/0/1 and Ethernet2/0/2 ports.

```
<SW7750> display protocol-vlan interface Ethernet 2/0/1 to Ethernet
2/0/2
Interface: Ethernet2/0/1
VLAN ID  Protocol-Index     Protocol-type
    50        1               ip 192.168.10.1 255.255.255.0
    80        2               ip 101.120.34.0 255.255.0.0
    100       1               ip 104.232.43.0 255.255.255.0
    100       2               ipx ethernetii
Interface: Ethernet2/0/2
VLAN ID  Protocol-Index     Protocol-type
    50        5               ipx raw
    80        1               at
    100       3               snap etype 0x0abc
    100       5               llc dsap 0xac ssap 0xbd
```

display protocol-vlan slot

Syntax **display protocol-vlan slot** { *slot-number* [**to** *slot-number*] | **all** }

View Any view

Parameter *slot-number* [**to** *slot-number*]: Specifies to display information about the protocol-based VLANs on the card(s) specified by slot number. The **to** keyword is used to specify multiple modules.

all: Specifies to display information about the protocol-based VLANs on all modules.

Description Use the **display protocol-vlan slot** command to display the protocol-based VLAN information in specific module, including VLAN ID, protocol index and protocol type.

Example # Display the protocol-based VLAN information of all modules.

```
<SW7750> display protocol-vlan slot all
 Slot: 0
     VLAN ID        Protocol-Index     Protocol-Type
         4              0                 ip 10.1.1.1 255.255.255.0
         4              1                 ip 192.168.1.1 255.0.0.0
         4              2                 ip 10.1.0.4 255.0.0.0
         4              3                 ip 172.168.0.1 255.255.0.0
         4              4                 ip 172.168.1.1 255.255.255.0
```

display protocol-vlan vlan

Syntax **display protocol-vlan vlan** { *vlan-id* [**to** *vlan-id*] | **all** }

View Any view

Parameter *vlan-id*: VLAN ID, ranging from 1 to 4094.

to: Specifies the range of VLAN IDs.

all: Specifies all VLANs.

Description Use the **display protocol-vlan vlan** command to display the protocol information and protocol index configured for specified VLANs.

Related command: **display vlan**.

Example # Display the protocol information and protocol indices configured for VLAN 2 through VLAN 20..

```
<SW7750> display protocol-vlan vlan 2 to 20
VLAN ID: 2
VLAN Type: Protocol-based VLAN
```

```
 Protocol Index        Protocol Type
           0                   ip 1.1.1.0 255.255.255.0

VLAN ID: 20
VLAN Type: Protocol-based VLAN
     Protocol Index        Protocol Type
           0                   ip 192.168.0.0 255.255.255.0
           1                   ipx ethernetii
           2                   snap etype 0x0abc
           3                   llc dsap 0xac ssap 0xbd
```

port hybrid protocol-vlan vlan

Syntax **port hybrid protocol-vlan vlan** *vlan-id* { *protocol-index* [**to** *protocol-end*] | **all** }

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

View Ethernet port view

Parameter *vlan-id*: VLAN ID, ranging from 1 to 4094.

to: Specifies the range for VLAN IDs.

protocol-index: Beginning protocol index, ranging from 0 to 6. Its value must be smaller than or equal to the value of the *protocol-end* argument.

protocol-end: End protocol index, ranging from 0 to 6. Note that its value must be larger than or equal to the value of the *protocol-index* argument.

all: Specifies all protocol indices.

Description Use the **port hybrid protocol-vlan vlan** command to associate a port with the protocol-based VLAN.

Use the **undo port hybrid protocol-vlan vlan** command to remove the association between the specified protocol-based VLAN and a port.

Related command: **protocol-vlan vlan slot** and **display protocol-vlan interface**.

Example # Associate port Ethernet2/0/1 with the protocol-based VLAN 3, whose protocol index is from 0 to 6.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet2/0/1
[SW7750-Ethernet2/0/1] port hybrid protocol-vlan vlan 3 0 to 6
```

protocol-vlan vlan slot

Syntax

protocol-vlan vlan *vlan-id* { *protocol-index* [**to** *protocol-end*] | **all** } { **slot** *slot-number* | **mainboard** }

undo protocol-vlan vlan *vlan-id* { *protocol-index* [**to** *protocol-end*] | **all** } { **slot** *slot-number* | **mainboard** }

View

System view

Parameter

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

protocol-index: Beginning protocol index, ranging from 0 to 6. Its value must be smaller than or equal to the value of the *protocol-end* argument.

protocol-end: End protocol index, ranging from 0 to 6. Note that its value must be larger than or equal to the value of the *protocol-index* argument.

all: Specifies all protocol indices.

slot *slot-number*: Specifies to associate a module with protocol-based VLAN. The *slot-number* argument specifies module slot number.

mainboard: Specifies to associate the Fabric with the protocol-based VLAN.

Description

Use the **protocol-vlan vlan slot** command to associate a module with protocol-based VLAN.

Use the **undo protocol-vlan vlan slot** command to cancel the association.

Note that it is necessary to add those ports that require protocol in the module to the protocol-based VLAN. Currently, only non-Type-A modules, including I/O Modules and Fabrics, support this command.

Table 7 shows the supported protocol-based VLAN creation commands on different modules.

Table 7 Protocol-based VLAN creation commands on different cards

Command description	Type A card	Non-Type-A card
Create protocol-based VLAN on specific module in system view.	Not supported	Supported (for all IP protocols and subnet IP protocols.)
Create protocol-based VLAN on specific port in Ethernet port view.	Supported	Supported (exclude all IP protocols and subnet IP protocols, AppleTalk protocol, and the user-defined LLC template which defines only one of *dsap-id* and *ssap-id*.)

Type A modules include 3C16860, 3C16861, LS81FS24A, 3C16858, 3C16859, and 32Gbps and 64Gbps Switch Fabrics.

Related command: **port hybrid protocol-vlan vlan** and **display protocol-vlan interface**.

Example # Associate protocols 0 to 6 in VLAN3 with module 5.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] protocol-vlan vlan 3 0 to 6 slot 5
```

protocol-vlan

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

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

View VLAN view

Parameter **at**: Specifies an AppleTalk-based VLAN.

ip [*ip-address* [*net-mask*]]: Specifies an IP-based VLAN. The *ip-address* argument specifies IP address and the *net-mask* argument specifies subnet mask. The default subnet mask is the mask of the network where *ip-address* belongs.

ipx { **ethernetii** | **llc** | **raw** I **snap** }: Specifies IPX protocol-based VLAN. The **ethernetii**, **llc**, **raw** and **snap** keywords indicate four encapsulation types.

mode: Specifies VLAN based on other protocol type and encapsulation format.

ethernetii [**etype** *etype-id*]: Specifies EthernetII encapsulation-based VLAN. The *etype-id* argument indicates the Ethernet type of the incoming packets, and its value ranges from 600 to FFFF.

llc [**dsap** *dsap-id* [**ssap** *ssap-id*] | **ssap** *ssap-id*]: Specifies VLAN based on logical link control encapsulation format. The *dsap-id* argument indicates the destination service access point and its value ranges from 0 to FF. The *ssap-id* argument indicates the source service access point and its value ranges from 0 to FF.

snap [**etype** *etype-id*]: Specifies VLAN based on sub-network access protocol (SNAP) encapsulation format. The *etype-id* argument indicates the Ethernet type of incoming packets and its value ranges from 600 to FFFF.

protocol-index: Beginning protocol index, ranging from 0 to 6. Its value must be smaller than or equal to the value of the *protocol-end* argument. If this argument is not specified, the system will assign an index automatically.

protocol-end: End protocol index, ranging from 0 to 6. Note that its value must be larger than or equal to the value of the *protocol-index* argument.

all: Specifies all protocol indices.

Description Use the **protocol-vlan** command to configure the protocol template used for classifying protocol-based VLANs.

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

***CAUTION:** In a VLAN, it is not allowed to configure two templates with the same protocol type and encapsulation format. If any parameter in a user-defined template has the same value as the corresponding parameter in the standard template, the user-defined template and the standard template cannot be configured in the same VLAN.*

Pay attention to the following notices about the template configuration

- *It is not allowed to configure both **ipx llc** standard template and LLC user-defined template in the same VLAN.*
- *It is not allowed to configure both ipx raw standard template and LLC user-defined template whose **dsap** and **ssap** are both ff in the same VLAN.*
- *It is not allowed to configure both **ipx ethernetii** standard template and EthernetII user-defined template whose **etype** is 8137 in the same VLAN.*
- *It is not allowed to configure both **ipx snap** standard template and SNAP user-defined template whose **etype** is 8137 in the same VLAN.*
- *When the values of the dsap-id and ssap-id arguments are AA, the packet encapsulation type is not **llc** but **snap**. To avoid template conflict, the system disable the value AA for the dsap-id and ssap-id arguments when you configure LLC user-defined template.*

In addition, pay attention to the following notices about IP template

- *If a packet can match both Ipv4-based VLAN and the VLAN based on other protocol, Ipv4-based VLAN takes higher priority.*
- ***ip** [ip-address [net-mask]] defines IPv4-based VLAN. If you want to define the VLANs based on IP or other encapsulation formats, use **mode** { **ethernetii** [**etype** etype-id] } and **snap** [**etype** etype-id], in which, etype-id is 0x0800.*

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

Example # Configure VLAN 3 as a VLAN based on all IP packets.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] vlan 3
[SW7750-vlan3] protocol-vlan ip
```

# Configure VLAN 5 as a VLAN based on network segment 123.34.56.0.

```
[SW7750-vlan3] vlan 5
[SW7750-vlan5] protocol-vlan ip 123.34.56.0
```

# Cancel protocols 0 to 5 in VLAN 5.

```
[SW7750-vlan5] undo protocol-vlan 0 to 5
```

8 VOICE VLAN CONFIGURATION COMMANDS

display voice vlan oui

Syntax **display voice vlan oui**

View Any view

Parameter None

Description Use the **display voice vlan oui** command to display the currently supported OUI addresses and the related information.

Related command: **voice vlan**, **voice vlan enable**.

Example # Display the OUI addresses of the voice VLAN.

```
<SW7750> display voice vlan oui
Oui Address     Mask                 Description
0003-6b00-0000  ffff-ff00-0000  Cisco phone
000f-e200-0000  ffff-ff00-0000  3Com Aolynk phone
00d0-1e00-0000  ffff-ff00-0000  Pingtel phone
00e0-7500-0000  ffff-ff00-0000  Polycom phone
00e0-bb00-0000  ffff-ff00-0000  3com phone
```

display voice vlan status

Syntax **display voice vlan status**

View Any view

Parameter None

Description Use the **display voice vlan status** command to display voice VLAN-related information, including voice VLAN status (disabled/enabled), security mode, aging time, port mode (manual mode or automatic mode), and so on.

Related command: **voice vlan**, **voice vlan enable**.

Example # Display the information about the voice VLAN.

```
<SW7750> display voice vlan status
Voice Vlan security mode: Security
Voice Vlan aging time: 1440 minutes
Current voice vlan enabled port mode:
PORT                      MODE     STATUS             Voice Vlan ID
--------------------------------------------------------------------
Ethernet2/0/5           MANUAL  ENABLE                3
```

Table 8 Field descriptions of the **display voice vlan status** command

Field	Description
Voice Vlan security mode	The status of voice VLAN security mode: enabled/disabled.
Voice Vlan aging time	The voice VLAN aging time
Current voice vlan enabled port mode	The operation mode of ports with the voice VLAN function enabled
PORT	Port type and port number
MODE	Operation mode of the voice VLAN bound to the port
STATUS	Voice VLAN status on the port (**ENABLE** or **DISABLE**)
Voice VLAN ID	ID of the voice VLAN bound to the port

CAUTION: *The "Current voice vlan enable port mode" field lists the ports with the voice VLAN function enabled. Note that a port listed in this field may not currently operate in a voice VLAN. To check the ports operating in the current voice VLAN, use the* ***display vlan*** *command, which is described in section "display vlan" on page 124.*

display vlan

Syntax **display vlan** *vlan-id*

View Any view

Parameter *vlan-id*: Voice VLAN ID in the range of 1 to 4094.

Description Use the **display vlan** command to display the automatic/manual ports in the current voice VLAN.

Related command: **voice vlan**.

Example # Display the ports included in the current voice VLAN, assuming that the current voice VLAN is VLAN 6.

```
<SW7750> display vlan 6
 VLAN ID: 6
 VLAN Type: static
 Route Interface: not configured
 Description: VLAN 0006
 Name: VLAN 0006
 Tagged   Ports:
  GigabitEthernet2/0/5
 Untagged Ports:
  GigabitEthernet2/0/6
```

The output indicates that GigabitEthernet2/0/5 and GigabitEthernet2/0/6 ports are in the current voice VLAN.

voice vlan

Syntax **voice vlan** *vlan-id*

undo voice vlan *vlan-id*

View Ethernet port view

Parameter *vlan-id*: ID of the VLAN to be bound to the port as a voice VLAN, in the range of 2 to 4094.

Description Use the **voice vlan** command to bind a VLAN to the port as a voice VLAN.

Use the **undo voice vlan** command cancel a voice VLAN-to-port binding.

⚠ ***CAUTION:***

- *Before binding a VLAN to a port as a voice VLAN, make sure the VLAN already exists.*
- *To remove a VLAN bound to a port as a voice VLAN, you need to cancel the voice VLAN-to-port binding first.*

Related command: **display voice vlan status**.

Example # Bind VLAN 2 to Ethernet 2/0/2 as a voice VLAN.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet 2/0/2
[SW7750-Ethernet2/0/2] voice vlan 2
```

voice vlan aging

Syntax **voice vlan aging** *minutes*

undo voice vlan aging

View System view

Parameter *minutes*: Aging time (in minutes) to be set for a voice VLAN. This argument ranges from 5 to 43,200.

Description Use the **voice vlan aging** command to set the aging time for a voice VLAN.

Use the **undo voice vlan aging** command to restore the default aging time for a voice VLAN.

By default, the aging time of a voice VLAN is 1,440 minutes.

Related command: **display voice vlan status**.

Example # Set the aging time of the voice VLAN to 100 minutes.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] voice vlan aging 100
```

voice vlan enable

Syntax **voice vlan enable**

undo voice vlan enable

View Ethernet port view

Parameter None

Description Use the **voice vlan enable** command to enable the voice VLAN function for a port.

Use the **undo voice vlan enable** command to disable the voice VLAN function for a port.

By default, the voice VLAN function is disabled on all ports.

- The voice VLAN function takes effect on a port only when it is enabled in both system view and port view.
- The access port working in automatic mode does not support the voice VLAN function.

- *After the voice VLAN function is enabled on a port, you cannot enable the QinQ feature on the port.*
- *After the QinQ feature is enabled on a port, you cannot enable the voice VLAN function on the port.*

Related command: **display voice vlan status**.

Example # Enable the voice VLAN function for Ethernet2/0/2 port.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet 2/0/2
[SW7750-Ethernet2/0/2] voice vlan enable
```

voice vlan legacy

Syntax **voice vlan legacy**

undo voice vlan legacy

View Ethernet port view

Parameter None

Description Use the **voice vlan legacy** command to enable the voice VLAN legacy function. This function realizes the communication between 3Com's devices and other vendors' voice devices by automatically adding the voice VLAN tags to the voice data coming from other vendors' voice devices.

Use the **undo voice vlan legacy** command to disable the voice VLAN legacy function.

By default, the voice VLAN legacy function is disabled.

Example # Enable the voice VLAN legacy function on Ethernet2/0/1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet 2/0/1
[SW7750-Ethernet2/0/1] voice vlan legacy
```

voice vlan mac-address

Syntax **voice vlan mac-address** *oui* **mask** *oui-mask* [**description** *text*]

undo voice vlan mac-address *oui*

View System view

Parameter *oui*: OUI address to be set. You need to provide this argument in the format of H-H-H.

Organizationally unique identifier (OUI) is the first 24 bits of a MAC address. It is the global unique identifier assigned by IEEE for different device supplier.

oui-mask: Valid bits of OUI address, indicated by mask in the format of H-H-H.

text: Description string of the OUI address. This argument can contain 1 to 30 characters.

Description Use the **voice vlan mac-address** command to set an OUI address used for a voice VLAN to identify voice devices.

Use the **undo voice vlan mac-address** command to disable an OUI address from being used to identify voice devices.

A switch can use up to 16 OUI addresses to identify voice devices, including the five default OUI addresses (as listed in Table 9). When the number of OUI addresses reaches 16, you will fail to add new OUI addresses.

Table 9 Default OUI addresses of a switch

Number	OUI addresses	Vendor
1	0003-6b00-0000	Cisco phone
2	000f-e200-0000	3Com Aolynk phone
3	00d0-1e00-0000	Pingtel phone
4	00e0-7500-0000	Polycom phone
5	00e0-bb00-0000	3com phone

Related command: **display voice vlan oui**.

Example # Specify 00aa-bb00-0000 as an OUI address, with the description string being "ABC".

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] voice vlan mac-address 00aa-bb00-0000 mask ffff-ff00-0000 d
escription ABC
```

voice vlan mode

Syntax **voice vlan mode auto**

undo voice vlan mode auto

View Ethernet port view

Parameter None

Description Use the **voice vlan mode auto** command to configure an Ethernet port to operate in the automatic voice VLAN mode.

Use the **undo voice vlan mode auto** command to configure an Ethernet port to operate in the manual voice VLAN mode.

By default, an Ethernet port operates in the automatic voice VLAN mode.

Related command: **display voice vlan status**.

Example # Configure GigabitEthernet3/0/2 port to operate in the manual voice VLAN mode.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface GigabitEthernet 3/0/2
[SW7750-GigabitEthernet3/0/2] undo voice vlan mode auto
```

voice vlan security enable

Syntax **voice vlan security enable**

undo voice vlan security enable

View System view

Parameter None

Description Use the **voice vlan security enable** command to enable the voice VLAN security mode.

Use the **undo voice vlan security enable** command to disable the voice VLAN security mode.

In the voice VLAN security mode, the ports in a voice VLAN and with voice devices attached to can only forward voice data. Data packets with their MAC addresses not among the OUI addresses that can be identified by the system will be dropped. This mode has no effects on other VLANs.

By default, the voice VLAN security mode is enabled.

Related command: **display voice vlan status**.

Example # Disable the voice VLAN security mode.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] undo voice vlan security enable
```

9 ISOLATE-USER-VLAN CONFIGURATION COMMANDS

You need to configure the hybrid attribute for a port in the process of configuring an isolate-user-VLAN. For hybrid port-related commands, refer to “Port-Based VLAN Configuration Commands” on page 111.

display isolate-user-vlan

Syntax **display isolate-user-vlan** [*vlan-id*]

View Any view

Parameter *vlan-id*: VLAN ID of the configured isolate-user-VLANs, ranging from 1 to 4,094.

Description Use the **display isolate-user-vlan** command to display the mapping between the isolate-user-VLAN and the secondary VLAN, and the current status and port information of the isolate-user-VLAN and the secondary VLAN.

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

Example # Display the mapping between the isolate-user-VLAN and the secondary VLAN.

```
<SW7750> display isolate-user-vlan
 Isolate-user-VLAN   Vlan ID : 3
 Secondary Vlan ID : 4-5
 Vlan ID: 3
 Vlan Type: static
 Isolate-user-VLAN type : isolate-user-VLAN
 Route Interface: not configured
 Description: VLAN 0003
 Tagged   Ports: none
 Untagged Ports:
             Ethernet2/0/4          Ethernet2/0/8          Ethernet2/0/18
 Vlan ID: 4
 Vlan Type: static
 Private-vlan Type : Secondary
 Route Interface: not configured
 Description: VLAN 0004
 Tagged   Ports: none
 Untagged Ports:
             Ethernet2/0/4          Ethernet2/0/8
 Vlan ID: 5
 Vlan Type: static
 Private-vlan Type : Secondary
 Route Interface: not configured
 Description: VLAN 0004
 Tagged   Ports: none
 Untagged Ports:
             Ethernet2/0/4          Ethernet2/0/18
```

isolate-user-vlan

Syntax **isolate-user-vlan** *vlan-id* **secondary** *vlan-list*

undo isolate-user-vlan *vlan-id* [**secondary** *vlan-list*]

View System view

Parameter *vlan-id*: VLAN ID of an isolate-user-VLAN, ranging from 1 to 4,094.

vlan-list: List of the secondary VLAN that needs to establish the mapping with the isolate-user-VLAN, provided in the form of *vlan-list* = { *vlan-id* [**to** *vlan-id*] }&<1-4093>, where the *vlan-id* is the VLAN ID of the secondary VLAN. VLAN ID after **to** must not be less than that before **to**. You can input this argument repeatedly to establish the mapping between the isolate-user-VLAN and all other VLANs.

Description Use the **isolate-user-vlan** command to establish the mapping between the isolate-user-VLAN and the secondary VLAN.

Use the **undo isolate-user-vlan** command to cancel the mapping between the isolate-user-VLAN and the secondary VLAN.

Without the parameter **secondary** *vlan-list*, the **undo isolate-user-vlan** command can cancel the mapping between all the secondary VLANs and the specified isolate-user-VLAN. With this parameter, the command can cancel the mapping between the specified secondary VLAN and the specified isolate-user-VLAN.

Note that, establishing or canceling the mapping between the isolate-user-VLAN and the secondary VLAN does not affect the port status in each VLAN.

By default, the user-created isolate-user-VLAN does not map the secondary VLAN.

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

Example # Map the isolate-user-VLAN 10 with the secondary VLAN 2, 3, 4, 5, and 9.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] 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 specify a VLAN as an isolate-user-VLAN.

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

By default, no VLAN is enabled with the isolate-user-VLAN function.

- *Multiple isolate-user-VLANs can be configured for a switch.*
- *With GVRP function enabled, a switch cannot be enabled with isolate-user-VLAN function.*
- *The isolate-user-VLAN function and super VLAN function cannot be enabled simultaneously for a VLAN. If a VLAN is specified as an isolate-user-VLAN or a secondary VLAN, you cannot configure it as a super VLAN or a sub VLAN additionally.*

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

Example # Configure VLAN 5 as an isolate-user-VLAN.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] vlan 5
[SW7750-vlan5] isolate-user-vlan enable
```

10 SUPER VLAN CONFIGURATION COMMANDS

Only the 96Gbps series switch fabric supports this feature.

dhcp-server

Syntax **dhcp-server** *groupNo*

undo dhcp-server

View VLAN interface view

Parameter *groupNo*: Number of DHCP server, ranging from 0 to 19.

Description Use the **dhcp-server** command to specify which DHCP server group a VLAN interface belongs to.

Use the **undo dhcp-server** command to cancel this mapping.

For configurations of a DHCP server group, refer to "DHCP Server Configuration Commands" on page 705.

Example # Configure VLAN-interface1 to belong to DHCP server group 1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 1
[SW7750-Vlan-interface1] dhcp-server 1
```

display supervlan

Syntax **display supervlan** [*supervlan-id*]

View Any view

Parameter *supervlan-id*: ID of Super VLAN, range from 1 to 4,094.

Description Use the **display supervlan** command to view the mapping relationship between Super VLAN and Sub VLAN, and the ports identifying mapping relationship between super VLAN and sub VLAN.

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

Example # Display the mapping relationship between Super VLAN 100 and the sub VLANs.

```
<SW7750> display supervlan 100
 Supervlan ID :  100
 Subvlan ID :  101-102
 VLAN ID: 100
 VLAN Type: static
 It is a Super VLAN.
 Route Interface: not configured
 Description: VLAN 0100
 Name: VLAN 0100
 Broadcast MAX-ratio: 100
 Tagged   Ports: none
 Untagged Ports: none
 VLAN ID: 101
 VLAN Type: static
 It is a Sub VLAN. And the Super VLAN is VLAN 100
 ARP proxy disabled.
 Route Interface: not configured
 Description: VLAN 0101
 Name: VLAN 0101
 Broadcast MAX-ratio: 100
 Tagged   Ports: none
 Untagged Ports:
Ethernet3/0/3
 VLAN ID: 102
 VLAN Type: static
 It is a Sub VLAN. And the Super VLAN is VLAN 100
 ARP proxy disabled.
 Route Interface: not configured
 Description: VLAN 0102
 Name: VLAN 0102
 Broadcast MAX-ratio: 100
 Tagged   Ports: none
 Untagged Ports:
Ethernet3/0/4
```

subvlan

Syntax **subvlan** *vlan-list*

undo subvlan [*vlan-list*]

View VLAN view of the super VLAN

Parameter *vlan-list*: List of sub VLANs, provided in the format of *vlan-list* = { *vlan-id* [**to** *vlan-id*] }*&<1-10>,* where the *vlan-id* is the VLAN ID of a sub VLAN, and the *&<1-10>* means you can specify ten sub VLANs or sub VLAN lists.

Description Use the **subvlan** commmand to establish the mapping relationship between sub VLAN and super VLAN.

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

Without the argument *vlan-list*, the **undo subvlan** command can cancel the mapping between all the sub VLANs and the isolate-user-VLAN. With this argument, the command can cancel the mapping between the specified sub VLAN and the isolate-user-VLAN.

CAUTION:

- *The sub VLAN must exist before you create mapping between the sub VLAN and the super VLAN.*
- *After establishing the mapping between the sub VLAN and the super VLAN, you can still add (or delete) ports to (from) the sub VLAN.*
- *A super VLAN can establish mappings with 128 sub VLANs.*
- *The system can create up to 1024 sub VLANs.*

Related command: **display supervlan**.

Example # Establish the mapping relationship between sub VLAN 3, 4, 5, 9 and super VLAN 10.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] vlan 10
[SW7750-vlan10] supervlan
[SW7750-vlan10] subvlan 3 to 5 9
```

supervlan

Syntax **supervlan**

undo supervlan

View VLAN view

Parameter None

Description Use the **supervlan** commmand to set current VLAN to super VLAN.

Use the **undo supervlan** commmand to restore the current VLAN type to ordinary VLAN.

Note that:

You can not configure a VLAN which includes Ethernet ports as a super VLAN; and after you configure a super VLAN, you cannot add any Ethernet port to it.

Related command: **display supervlan**.

Example

Set the VLAN 2 to super VLAN.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] vlan 2
[SW7750-vlan2] supervlan
```

11 IP ADDRESS CONFIGURATION COMMANDS

display ip interface

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

View Any view

Parameter *interface-type interface-number*: *interface-type* indicates a port type and *interface-number* indicates a port number. For details, see **interface** on page 205.

brief: Displays the basic interface configuration information.

Description Use the **display ip interface** command to display information about one specific or all interfaces.

Example # Display information about VLAN interface 1.

<SW7750> display ip interface Vlan-interface 1

```
Vlan-interface1 current state :UP
Line protocol current state :UP
Internet Address is 192.168.0.39/24 Primary
Broadcast address : 192.168.0.255
The Maximum Transmit Unit : 1500 bytes
IP packets input number: 9678, bytes: 475001, multicasts: 7
IP packets output number: 8622, bytes: 391084, 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
```

Table 10 Field descriptions of the **display ip interface** command

Field	Description
Vlan-interface1 current state	Current state of 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	Max transmit unit
IP packets input number: 9678, bytes: 475001, multicasts: 7	Number of input/output unicast packets, bytes, and multicast packets
IP packets output number: 8622, bytes: 391084, multicasts: 0	
TTL invalid packet number	Number of received invalid TTL packets
ICMP packet input number: 0	Total number of received ICMP packets, including:
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	Echo reply packet, unreachable packet, source quench packet, routing redirect packet, Echo request packet, router advert packet, router solicit packet, time exceed packet, IP header bad packet, timestamp request packet, timestamp reply packet, information request packet, information reply packet, netmask request packet, netmask reply packet, and unknown types of packets.

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/M-Ethernet interface view

Parameter *ip-address*: IP address, in dotted decimal notation.

mask: Subnet mask, in dotted decimal notation.

mask-length: Length of a subnet mask.

sub: Secondary IP address of a VLAN or loopback interface.

Description Use the **ip address** command to specify an IP address and mask for a VLAN or loopback interface.

Use the **undo ip address** command to remove an IP address and mask of a VLAN or loopback interface.

By default, a VLAN or loopback interface has no IP address.

Generally, it is enough to configure one IP address for an interface. However, you can configure up to eight IP addresses for an interface so that it can be connected to several subnets. Among these IP addresses, one is the primary IP address and all the others are secondary ones. The relationship between the primary address and the secondary addresses is as follows:

- When you configure a primary IP address for an interface which already has a primary IP address, the new address will replace the old one.
- If you execute the **undo ip address** command without any parameter, the switch deletes both primary and secondary IP addresses of the interface. The **undo ip address** *ip-address* { *mask* | *mask-length* } command is used to delete the primary IP address. The **undo ip address** *ip-address* { *mask* | *mask-length* } **sub** command is used to delete secondary IP addresses.

Related command: **display ip interface**.

Example # Specify the IP address and subnet mask of VLAN interface 1 to 129.12.0.1 and 255.255.255.0 respectively.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 1
[SW7750-Vlan-interface1] ip address 129.12.0.1 255.255.255.0
```

12 IP PERFORMANCE CONFIGURATION COMMANDS

display fib

Syntax **display fib** *fib-rule*

View Any view

Parameter *fib-rule*: Specifies FIB entries that conform to specific rules. It can be a combination of multiple rules. The following table describes the combinations.

Table 11 Display combination of specified FIB entries

Description	Form of fib-rule
Display FIB entries of the specified slot	*slot-number*
Display FIB entries matching the specified destination IP address/mask pair and all the FIB entries matching the specified IP address/mask (in the natural mask range) pair	*ip-address1* [{ *mask1* | *mask-length1* } [*ip-address2* { *mask2* | *mask-length2* } | **longer**] | **longer**]
Display FIB statistics	**statistics**
Display the FIB entries which are output from the buffer according to the regular expression and are related to the specific character string	**|** { **begin** | **exclude** | **include** } *text*
Display the FIB entries matching a specific ACL	**acl** { *number* | *name* }
Display the FIB entries matching the specific prefix list	**ip-prefix** *listname*

Description Use the **display fib** command to view the summary of the forwarding information base (FIB). Each line indicates an FIB entry. The information includes: destination address/mask length, next hop, current flag, timestamp, and output interface. For the ACL configuration, refer to “ACL Commands” on page 755.

Example # Display all the FIB summary.

```
<SW7750> display fib
Destination/Mask        Nexthop     Flag TimeStamp      Interface
211.71.75.0/24      1.1.1.2     GSU  t[250763]      Vlan-interface2
1.1.2.1/32          127.0.0.1   GHU  t[37]          InLoopBack0
127.0.0.1/32            127.0.0.1   GHU  t[37]          InLoopBack0
127.0.0.0/8         127.0.0.1   U    t[37]          InLoopBack0
1.1.1.1/32          127.0.0.1   GHU  t[37]          InLoopBack0
1.1.1.0/24          1.1.1.1     U    t[37]          Vlan-interface2
```

Table 12 Field descriptions of the **display fib** command

Field	Description
Destination/Mask	Destination address/mask length
Nexthop	Next hop address
Flag	Flags: U: A route is up and available. G: Gateway route H: Local host route B: Blackhole route D: Dynamic route S: Static route R: Rejected route E: Multi-path equal-cost route L: Route generated by ARP or ESIS
TimeStamp	Timestamp
Interface	Forwarding interface

# Display ACL 2001.

```
<SW7750> display acl config 2001
Basic ACL  2001, 1 rule
rule 0 permit source 211.71.75.0 0.0.0.255 (0 times matched)
```

# Display the FIB entries filtered by ACL 2001.

```
<SW7750> display fib acl 2001
Route Entry matched by access-list 2001
  Summary Counts :1
Destination/Mask   Nexthop         Flag TimeStamp     Interface
211.71.75.0/24     1.1.1.2         GSU  t[250763]     Vlan-interface2
```

# Display all the lines from the line containing the string 1.1.1.1.

```
<SW7750> display fib | begin 1.1.1.1
1.1.1.1/32         127.0.0.1       GHU  t[37]         InLoopBack0
1.1.1.0/24         1.1.1.1         U    t[37]         Vlan-interface2
```

# Display the total number of FIB entries.

```
<SW7750> 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 about ICMP packets.

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

Example # Display the statistics about ICMP packets.

```
<SW7750> 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 Field descriptions of the display icmp statistics command

Field	Description
bad formats	Number of input packets in bad formats
bad checksum	Number of input packets with bad 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 problem
timestamp	Number of input/output timestamp packets
information request	Number of input information request packets
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 time exceeded packets

display ip socket

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

View Any view

Parameter *sock-type*: Type of a socket, ranging from 1 to 3. These values correspond to SOCK_STREAM (TCP socket), SOCK_DGRAM (UDP socket or socket based on the link layer), and SOCK_RAW (RAW IP socket).

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

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

Description Use the **display ip socket** command to display the information of the current socket.

Example # Display the information about the socket of the TCP type.

```
<SW7750> 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_SETKEEPAL
IVE,
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_SETKEEPALI
VE,
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_SETKEEPALI
VE,
socket state = SS_ISCONNECTED SS_PRIV SS_ASYNC
```

Table 14 Field descriptions of the display ip socket command

Field	Description
SOCK_STREAM	Type of a socket. Three types are available: SOCK_STREAM (TCP socket), SOCK_DGRAM (UDP socket or socket supporting link layer access), and SOCK_RAW (RAW IP socket).
Task	Task ID
socketid	Socket ID
Proto	Protocol number used by the socket
sndbuf	Sending buffer size of the socket
rcvbuf	Receiving buffer size of the socket
sb_cc	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	Current data size in the receiving buffer
socket option	Option of a socket
socket state	State of a socket

display ip statistics

Syntax **display ip statistics**

View Any view

Parameter None

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

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

Example # Display the statistics about IP packets.

```
<SW7750> 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 Field descriptions of the display ip statistics command

Field		Description
Input:	sum	Sum of input packets
	Local	Number of received packets whose destination address 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 bad checksum
	bad options	Number of packets with wrong options
Output:	forwarding	Number of forwarded packets
	local	Number of packets 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 reassembled packets
	timeouts	Number of timeout fragment packets

display tcp statistics

Syntax **display tcp statistics**

View Any view

Parameter None

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

Related command: **display tcp status** and **reset tcp statistics**.

Example # Display the statistics about TCP packets.

```
<SW7750> 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 out of 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 disco
nnected : 0
Initiated connections: 0, accepted connections: 0, established connections: 0
Closed connections: 0 (dropped: 0, initiated dropped: 0)
Packets dropped with MD5 authentication: 0
Packets permitted with MD5 authentication: 0
```

Table 16 Field descriptions of the display tcp statistics command

Field		Description
Received packets	Total	Total number of received packets
	packets in sequence	Number of packets in sequence
	window probe packets/ window update packets	Number of window probe packets/number of window update packets
	checksum error/ offset error/ short error	Number of checksum errors/number of offset errors/number of short errors
	duplicate packets/ partially duplicate packets	Number of duplicate packets/number of partially duplicate packets
	out-of-order packets	Number of out-of-order packets
	packets of data out of window	Number of packets out of window
	packets received after close	Number of received packets after close
	ACK packets	Number of ACK packets
	duplicate ACK packets/ too much ACK packets	Number of duplicate ACK packets/number of ACK packets for data not sent.
Sent packets	Total	Total number of sent packets
	urgent packets	Number of urgent packets
	control packets (including 1 RST)	Number of control packets, including one retransmitted packet
	window probe packets/ window update packets	Number of window probe packets/number of window update packets
	data packets/ data packets retransmitted	Number of data packets/number of retransmitted packets
	ACK-only packets	Number of ACK packets (28 delay ACK packets)
Retransmitted timeout/ connections dropped in retransmitted timeout		Times of retransmission timer timeout/number of dropped connections because retransmission times exceed the limit
Keepalive timeout/ keepalive probe/ Keepalive timeout, so connections disconnected		Times of keepalive timer timeout/number of transmitted keepalive probe packets/number of dropped connections due to keepalive probe failure
Initiated connections/ accepted connections/ established connections		Number of initiated connections/number of accepted connections/number of established connections
Closed connections (dropped: initiated dropped:)		Number of closed connections (number of dropped connections umber of failed connection attempts)
Packets dropped with MD5 authentication		Number of dropped packets with MD5 authentication
Packets permitted with MD5 authentication		Number of permitted packets with MD5 authentication

display tcp status

Syntax **display tcp status**

View Any view

Parameter None

Description Use the **display tcp status** command to view the state of all the TCP connections so that you can monitor TCP connections in real time.

Example # Display the state of all the TCP connections.

```
<SW7750> 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
```

Table 17 Field descriptions of the display tcp status command

Field	Description
TCPCB	Address of the TCP control block
Local Add:port	Local IP address; port number
Foreign Add:port	Remote IP address; port number
State	TCP connection state

display udp statistics

Syntax **display udp statistics**

View Any view

Parameter None

Description Use the **display udp statistics** command to view the statistics about UDP packets.

Related command: **reset udp statistics**.

Example # Display the statistics about UDP packets.

```
<SW7750> display udp statistics
Received packets:
     Total: 26320
     checksum error: 0
     shorter than header: 0, data length larger than packet: 0
     no socket on port: 0
     total broadcast or multicast packets : 25006
     no socket broadcast or multicast packets: 24989
     not delivered, input socket full: 0
     input packets missing pcb cache: 1314
Sent packets:
     Total: 7187
```

Table 18 Field descriptions of the display udp statistics command

Field		Description
Received packets:	Total	Total number of received UDP packets
	checksum error	Number of packets with checksum errors
	shorter than header,	Number of packets whose lengths are shorter than their headers
	data length larger than packet	Number of packets whose lengths are larger than the packets
	no socket on port	Number of packets dropped because the socket corresponding to the port number is not found
	total broadcast or multicast packets	Total number of transmitted broadcast or multicast packets
	no socket broadcast or multicast packets	Total number of transmitted broadcast or multicast packets whose sockets are not found
	not delivered, input socket full	Number of not delivered packets because the socket cache is full
	input packets missing pcb cache	Number of packets missing pcb cache
Sent packets:	Total	Total number of transmitted UDP packets

icmp redirect send

Syntax **icmp redirect send**

undo icmp redirect send

View System view

Parameter None

Description Use the **icmp redirect send** command to enable ICMP redirect message sending.

Use the **undo icmp redirect send** command to disable ICMP redirect message sending.

By default, ICMP redirect message sending is enabled.

Example # Disable ICMP redirect message sending.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] undo icmp redirect send
```

ip

Syntax

ip { **ttl-expires** | **unreachables** }

undo ip { **ttl-expires** | **unreachables** }

View

System view

Parameter

ttl-expires: Configure whether to send TTL timeout packets to CPU.

unreachables: Configure whether to send unreachable packets to CPU.

Description

Use the **ip** { **ttl-expires** | **unreachables** } command to configure to send TTL timeout packets and unreachable packets to CPU.

Use the **undo ip** { **ttl-expires** | **unreachables** } command to cancel the configuration.

By default, unreachable packets are not sent to the CPU, while TTL timeout packets are sent to the CPU.

Example

Configure to send unreachable packets to CPU.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ip unreachables
```

ip forward-broadcast

Syntax

ip forward-broadcast [*acl-number*]

undo ip forward-broadcast

View

VLAN interface view

Parameter

acl-number: Number of the ACL used for filtering directed broadcast packets, in the range of 2000 to 3997.

Description

Use the **ip forward-broadcast** command to enable forwarding of directed broadcast packets to a directly connected network.

Use the **undo ip forward-broadcast** command to restore the default.

By default, the switch does not forward directed broadcast packets to a directly connected network.

Note that:

- *If you reference an ACL, only the directed broadcasts that pass the ACL filtering can be forwarded to the directly connected networks.*

- *If you reference a non-existent ACL, all the directed broadcasts to directly connected networks cannot be forwarded.*
- *If no ACL is referenced, all the directed broadcasts to directly connected networks can be forwarded.*

Example # Reference ACL 2000 to filter directed broadcasts to directly connected networks.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 1
[SW7750-Vlan-interface1] ip forward-broadcast 2000
```

reset ip statistics

Syntax **reset ip statistics**

View User view

Parameter None

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

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

Example # Clear the statistics information about IP packets.

```
<SW7750> 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 statistics information about TCP packets.

Related command: **display tcp statistics**.

Example # Clear the statistics information about TCP packets.

```
<SW7750> reset tcp statistics
```

reset udp statistics

Syntax **reset udp statistics**

View User view

Parameter None

Description Use the **reset udp statistics** command to clear the statistics information about UDP packets.

Example # Clear the statistics information about UDP packets.

```
<SW7750> 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 seconds, with the value ranging from 76 to 3600.

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.

The default value is 675 seconds.

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 finwait timer time outs, the TCP connection will be terminated.

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

Example # Configure the default value of the TCP finwait timer to 800 seconds.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] 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, in seconds, with the value ranging from 2 to 600.

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 TCP synwait timer.

The default value is 75 seconds.

When sending the SYN packet, TCP starts the synwait timer. If the response packet is not received before synwait times out, the TCP connection will be terminated.

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

Example # Configure the default value of the TCP synwait timer to 80 seconds.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] 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 transmission and receiving buffers measured in kilobytes (KB), whose value ranges from 1 to 32.

Description Use the **tcp window** command to configure the size of the transmission and receiving buffers of the connection-oriented socket.

Use the **undo tcp window** command to restore the default size of the transmission and receiving buffers of the connection-oriented socket.

By default, the size of the transmission and receiving buffers of the connection-oriented socket is 8 KB.

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

Example # Configure the size of the transmission and receiving buffers to 3KB.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] tcp window 3
```

13 IPX Configuration Commands

display ipx interface

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

View Any view

Parameter *vlan-id*: Specifies a VLAN interface by specifying its VLAN ID.

Description Use the **display ipx interface** command to view the IPX information of the specified VLAN interface.

If no *vlan-id* is specified, the IPX information of all the IPX-enabled VLAN interfaces will be displayed.

Example # Display the IPX information of VLAN interface 1.

```
<SW7750> display ipx interface Vlan-interface 1
Vlan-interface1 is down
   IPX address is 1.0020-9c68-448e [down]
   SAP is enabled
   Split horizon is enabled
   Update change only is disabled
   Forwarding of IPX type 20 propagation packet is disabled
   Delay of this IPX interface, in ticks is 1
   SAP GNS response is enabled
   RIP packet maximum size is 432 bytes
   SAP packet maximum size is 480 bytes
   IPX encapsulation is Netware 802.3
   0 received, 0 sent
   0 bytes received, 0 bytes sent
   0 RIP received, 0 RIP sent, 0 RIP discarded
   0 RIP specific requests received, 0 RIP specific responses sent
   0 RIP general requests received, 0 RIP general responses sent
   0 SAP received, 0 SAP sent, 0 SAP discarded
   0 SAP requests received, 0 SAP responses sent
```

Table 19 Field descriptions of the display ipx interface command

Field	Description
Vlan-interface1 is down	State of the current VLAN interface
IPX address	IPX network number and node address of the current VLAN interface
[down]	State of the IPX protocol

Table 19 Field descriptions of the display ipx interface command

Field	Description
SAP	Indicates whether SAP is enabled on the current VLAN interface
Split horizon	Indicates whether split horizon is enabled on the current VLAN interface
Update change only	Indicates whether triggered update is enabled on the current VLAN interface
Forwarding of IPX type 20 propagation packet	Indicates whether the IPX packets whose broadcast type is 20 are forwarded through the current VLAN interface
Delay of this IPX interface	Delay of the current VLAN interface
SAP GNS response	Indicates whether SAP GNS reply is enabled on the current VLAN interface
RIP packet maximum size	Maximum length of the RIP update packets that the current VLAN interface can send
SAP packet maximum size	Maximum length of the SAP update packets that the current VLAN interface can send
IPX encapsulation	IPX encapsulation format of the current VLAN interface
0 received, 0 sent 0 bytes received, 0 bytes sent 0 RIP received, 0 RIP sent, 0 RIP discarded 0 RIP specific requests received, 0 RIP specific responses sent 0 RIP general requests received, 0 RIP general responses sent 0 SAP received, 0 SAP sent, 0 SAP discarded 0 SAP requests received, 0 SAP responses sent	The number of IPX packets and bytes sent and received by the current VLAN interface; the number of received, sent, and dropped IPX RIP packets; the number of received special request packets and response packets; the number of received general request packets and response packets; the number of received, transmitted, and dropped IPX SAP packets; the number of received IPX SAP packets and response packets

display ipx routing-table

Syntax **display ipx routing-table** [*network* [**verbose**] | **protocol** { **default** | **direct** | **rip** | **static** } [**inactive** | **verbose**] | **statistics** | **verbose**]

View Any view

Parameter *network*: Displays IPX routing information by specifying a destination network number, which comprises eight hexadecimal numbers and is in the range of 1 to 0xFFFFFFFE.

protocol: Displays the IPX routing information of the specified route type.

default: Displays the information of all the default routes.

direct: Displays information of all the direct routes.

rip: Displays all the IPX RIP routing information.

static: Displays all the IPX static routing information.

inactive: Displays the information of the inactive routes.

verbose: Displays the detailed IPX routing information, including the active and inactive routes.

statistics: Displays the IPX routing statistics.

Description

Use the **display ipx routing-table** command to view the IPX routing information.

If no parameters are specified, the information of all the active IPX routes will be displayed.

Example

Display the information of the active IPX routes.

```
<SW7750> display ipx routing-table
Routing tables:
Summary count: 2

Dest_Ntwk_ID    Proto  Pre Ticks Hops Nexthop           Interface
0x1         Direct 0   1      0    0.0000-0000-0000  Vlan-interface1
0x2         Static 60  1      1    1.000e-0001-0000  Vlan-interface1
```

Table 20 Field descriptions of the display ipx routing-table command

Field	Description
Dest_Ntwk_ID	Destination network number of the route
Proto	Protocol type of the route
Pre	Route preference
Ticks	Tick count of the route
Hops	Hop count of the route
Nexthop	Next hop of the route
Interface	Outgoing interface of the route

# Display the detailed IPX routing information, including the active and inactive routes.

```
<SW7750> display ipx routing-table verbose
Routing tables:
  Destinations: 2        Routes: 3
Destination Network ID: 0x1
          Protocol: Direct                    Preference: 0
          Ticks: 1                            Hops: 0
          Nexthop: 0.0000-0000-0000           Time: 0
          Interface: 1.0020-9c68-448e(Vlan-interface1)
          State: <Active>
          Protocol: Static                    Preference: -60
          Ticks: 1                            Hops: 1
          Nexthop: 2.000e-0001-0000           Time: 0
          Interface: 2.0020-9c68-448f(Vlan-interface2)
          State: <Inactive>
```

```
Destination Network ID: 0x2
          Protocol: Static                    Preference: 60
          Ticks: 1                            Hops: 1
          Nexthop: 1.000e-0001-0000           Time: 0
          Interface: 1.0020-9c68-448e(Vlan-interface1)
          State: <Active>
```

Table 21 Field descriptions of the display ipx routing-table verbose command

Field	Description
Time	Route aging time; it is 0 for the direct and static routes, meaning they never time out.
State	The state of the route. It can be active, inactive, or delete. Active indicates that this route is an active route. Inactive indicates that this route is an inactive route. Delete indicate that this route has been deleted, but it is not released.

# Display the IPX routing statistics.

```
<SW7750> display ipx routing-table statistics
Routing tables:
Proto/State     route      active     added      deleted    freed
Direct           1           1          2          1          1
Static           2           1          2          0          0
RIP               0           0          0          0          0
Default          0           0          0          0          0

Total            3           2          4          1          1
```

Table 22 Field descriptions of the display ipx routing-table statistics command

Field	Description
Proto/State	Routing protocol
Route	Number of routes, including active and inactive routes
Active	Number of active routes
Added	Number of added routes
Deleted	Number of deleted, but not released routes
Freed	Number of released routes

display ipx service-table

Syntax **display ipx service-table** [**inactive** | **name** *name* | **network** *network* | **order** { **network** | **type** } | **type** *service-type*] [**verbose**]

View Any view

Parameter **inactive**: Displays the information of the inactive services.

name *name*: Displays the name information of the specified server. It is a string of 1 to 47 characters.

network *network*: Displays the network number information of the specified server. The network number comprises eight hexadecimal numbers and is in the range of 0x1 to 0xFFFFFFFF. The leading 0s can be omitted when you input a network number.

order { **network** | **type** }: Displays the service information by network number or by service type.

type *service-type*: Displays the service information with a specified service type. It comprises four hexadecimal numbers, ranging from 0 to FFFF. 0 indicates all the service types.

verbose: Displays the detailed service information.

Description Use the **display ipx service-table** command to view the contents of the IPX service information table.

Example # Display the contents of the IPX service information table.

```
[SW7750] display ipx service-table
Abbreviation: S - Static, Pref - Preference(Decimal), NetId - Network number,
NodeId - Node address, hop - Hops(Decimal), Recv-If - Interface from which the service is received

  Number of Static Entries:  2
  Number of Dynamic Entries: 0
 Name                                                 Type      NetId
S Prn1                                                 0005      000d
S Prn2                                                 0005      0008
```

# Display the details about the IPX service information table.

```
[SW7750] display ipx service-table verbose
Abbreviation: S - Static, Pref - Preference(Decimal), NetId - Network number,
NodeId - Node address, hop - Hops(Decimal), Recv-If - Interface from which the service is received

  Number of Static Entries:  2
  Number of Dynamic Entries: 0
  Name  Type      NetId NodeId          Sock     Pref Hops  Recv-If
S Prn1  0005      000d  000a-000a-000a  0452     500   02      Vlan-interface1
S Prn2  0005      0008  000a-000a-000a  0452     500   03      Vlan-interface1
```

Table 23 Field descriptions of the display ipx service-table command

Field	Description
Name	Server name
Type	Service type
NetId	Network number
NodeId	Node number
Sock	Socket
Pref	Preference
Hops	Hop count
Recv-If	Name of the interface receiving services

display ipx statistics

Syntax **display ipx statistics**

View Any view

Parameter None

Description Use the **display ipx statistics** command to view the IPX statistics.

Example # Display the IPX packet statistics.

```
<SW7750> display ipx statistics
Received:   0 total, 0 packets pitched
            0 packets size errors, 0 format errors
            0 bad hops(>16), 0 discarded(hops=16)
            0 other errors, 0 local destination
            0 can not be dealt with
 Sent:  0 forwarded, 0 generated
            0 no route, 0 discarded
 RIP:       0 sent, 0 received
            0 responses sent, 0 responses received
            0 requests received, 0 requests dealt
            0 requests sent, 0 periodic updates
 SAP:       0 general requests received
            0 specific requests received
            0 GNS requests received
            0 general responses sent
            0 specific responses sent
            0 GNS responses sent
            0 periodic updates, 0 errors
 PING:  0 requests sent, 0 requests received
            0 responses sent, 0 responses received
            0 responses in time, 0 responses time out
```

Table 24 Field descriptions of the display ipx statistics command

Field	Description
Received: 0 total, 0 packets pitched 0 packets size errors, 0 format errors 0 bad hops(>16), 0 discarded(hops=16) 0 other errors, 0 local destination 0 can not be dealt with	Statistics of received packets: the total number of received packets, the number of filled packets, the number of packets with incorrect length, the number of incorrectly encapsulated packets, the number of packets whose hop count exceeds 16, the number of packets whose hop count is equal to 16, the number of other incorrect packets, the number of packets whose destination is the local switch, and the number of packets that cannot be handled
Sent: 0 forwarded, 0 generated 0 no route, 0 discarded	Statistics of transmitted packets: the number of forwarded packets, the number of packets transmitted from the local switch, the number of packets that fail to find routes, and the number of dropped packets
RIP: 0 sent, 0 received 0 responses sent, 0 responses received 0 requests received, 0 requests dealt 0 requests sent, 0 periodic updates	Statistics of IPX RIP packets: the total number of received, transmitted IPX RIP packets, the number of transmitted/received response packets, the number of received/transmitted/handled packets, and the number of the periodic update packets

Table 24 Field descriptions of the display ipx statistics command

Field	Description
SAP: 0 general requests received 0 specific requests received 0 GNS requests received 0 general responses sent 0 specific responses sent 0 GNS responses sent 0 periodic updates, 0 errors	Statistics of SAP packets: the number of received general request packets, the number of special request packets, the number of latest request packets, the number of transmitted periodic update packets, and the number of received error packets
PING: 0 requests sent, 0 requests received 0 responses sent, 0 responses received 0 responses in time, 0 responses time out	Statistics of Ping packets: the number of transmitted/received request packets, the number of transmitted/received response packets, the number of prompt response packets, and the number of timeout response packets

ipx enable

Syntax

ipx enable

undo ipx enable

View

System view

Parameter

None

Description

Use the **ipx enable** command to enable IPX.

Use the **undo ipx enable** command to disabled IPX and delete all the IPX configurations.

Note that after the **undo ipx enable** command is executed, the IPX configurations cannot be recovered with the **ipx enable** command.

Example

Enable IPX.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750]ipx enable
```

ipx encapsulation

Syntax

ipx encapsulation [**dot2** | **dot3** | **ethernet-2** | **snap**]

undo ipx encapsulation

View

VLAN interface view

Parameter

dot2: Sets the encapsulation format to Ethernet_802.2.

dot3: Sets the encapsulation format to Ethernet_802.3.

ethernet-2: Sets the encapsulation format to Ethernet_II.

snap: Sets the encapsulation format to Ethernet_SNAP.

Description

Use the **ipx encapsulation** command to configure an IPX frame encapsulation format on the current VLAN interface.

Use the **undo ipx encapsulation** command to restore the encapsulation format to the default format.

By default, the IPX frame encapsulation format is Ethernet_802.3 (**dot3**).

Example

Set the IPX frame encapsulation format to Ethernet_II on VLAN interface 2.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 2
[SW7750-Vlan-interface2] ipx encapsulation ethernet-2
```

ipx netbios-propagation

Syntax

ipx netbios-propagation

undo ipx netbios-propagation

View

VLAN interface view

Parameter

None

Description

Use the **ipx netbios-propagation** command to enable the current VLAN interface to forward type 20 broadcast packets.

Use the **undo ipx netbios-propagation** command to disable the current VLAN interface from forwarding type 20 broadcast packets.

By default, type 20 broadcast packets are not forwarded.

Example

Allow the current interface to forward type 20 broadcast packets.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 2
[SW7750-Vlan-interface2] ipx netbios-propagation
```

ipx network

Syntax

ipx network *network*

undo ipx network

View

VLAN interface view

Parameter

network: Hexadecimal IPX network number in the range 0x1 to 0xFFFFFFFD. The leading 0s can be omitted when you input a network number.

Description

Use the **ipx network** command to assign an IPX network number to the VLAN interface.

Use the **undo ipx network** command to delete the IPX network number of the VLAN interface.

By default, no network number is assigned to VLAN interfaces; therefore, IPX is disabled on all the VLAN interfaces even after it is enabled globally.

Example

Assign the network number 675 to VLAN interface 2.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 2
[SW7750-Vlan-interface2] ipx network 675
```

ipx rip import-route static

Syntax

ipx rip import-route static

undo ipx rip import-route static

View

System view

Parameter

None

Description

Use the **ipx rip import-route static** command to enable RIP to import static routes. The imported routes are included in the update packets of RIP.

Use the **undo ipx rip import-route static** command to disable RIP from importing static routes.

By default, IPX RIP does not import static routes.

Note that IPX RIP imports only active static routes; inactive static routes are neither imported nor forwarded.

Example

Import static routes into IPX RIP.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ipx rip import-route static
```

ipx rip mtu

Syntax **ipx rip mtu** *bytes*

undo ipx rip mtu

View VLAN interface view

Parameter *bytes*: The maximum size of IPX RIP update packets, in bytes. It is in the range of 432 to 1500.

Description Use the **ipx rip mtu** command to configure the IPX RIP update packet size.

Use the **undo ipx rip mtu** command to restore the default size.

By default, the default size of IPX RIP update packets is 432 bytes.

Example # Set the maximum RIP update packet size to 500 bytes on VLAN interface 2.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 2
[SW7750-Vlan-interface2] ipx rip mtu 500
```

ipx rip multiplier

Syntax **ipx rip multiplier** *multiplier*

undo ipx rip multiplier

View System view

Parameter *multiplier:* A multiplier of the update interval, decides the aging period of the RIP routing entries together with the update interval. It is in the range 1 to 1000. Multiplying the update interval by the *multiplier*, you can get the actual aging period.

Description Use the **ipx rip multiplier** command to configure the aging period of the IPX RIP routing entries.

Use the **undo ipx rip multiplier** command to restore the default value. The aging period of IPX RIP is a multiple of the IPX RIP update interval. You can set multiple update intervals as an aging period.

By default, the aging period of the IPX RIP routing entries is three times the RIP updating interval.

Related command: **ipx rip timer update**

Example # Set the RIP aging period of the routing entries to five times the update interval.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ipx rip multiplier 5
```

ipx rip timer update

Syntax **ipx rip timer update** *seconds*

undo ipx rip timer update

View System view

Parameter *seconds*: RIP update interval, in seconds. It is in the range of 10 to 60,000.

Description Use the **ipx rip timer update** command to configure a RIP update interval.

Use the **undo ipx rip timer update** command to restore the default value.

By default, the update interval of IPX RIP is 60 seconds.

Related command: **ipx rip multiplier**

Example # Set the RIP update interval to 30 seconds.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ipx rip timer update 30
```

ipx route load-balance-path

Syntax **ipx route load-balance-path** *paths*

undo ipx route load-balance-path

View System view

Parameter *paths*: The maximum number of equivalent routes to the same destination. It is in the range of 1 to 64.

Description Use the **ipx route load-balance-path** command to configure the maximum number of equivalent routes to the same destination.

Use the **undo ipx route load-balance-path** command to restore the default value.

By default, the maximum number of equivalent routes to the same destination is 1.

The maximum number of equivalent routes is the maximum number of active equivalent routes to the same destination in the current system. If the new number is less than the number of the current active routes, the system deactivates those excessive routes.

Example # Set the maximum number of equivalent routes to the same destination to 30.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ipx route load-balance-path 30
```

ipx route max-reserve-path

Syntax **ipx route max-reserve-path** *paths*

undo ipx route max-reserve-path

View System view

Parameter *paths*: The maximum number of dynamic routes saved in the device to the same destination. It is in the range of 1 to 255.

Description Use the **ipx route max-reserve-path** command to configure the maximum number of dynamic routes saved in the device to the same destination.

Use the **undo ipx route max-reserve-path** command to restore the default value.

By default, the maximum number of dynamic routes to the same destination is 4.

When the number of dynamic routes saved in the device to the same destination exceeds the specified maximum value, the new dynamic routes are dropped directly without being added into the routing table. When the configured new value is less than the old one, the switch, however, does not delete the excessive route entries. These route entries either time out or are manually deleted.

Example # Set the maximum number of dynamic routes saved in the device to the same destination to 200.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ipx route max-reserve-path 200
```

ipx route-static

Syntax **ipx route-static** *network network.node* [**preference** *value*] [**tick** *ticks* **hop** *hops*]

undo ipx route-static { *network* [*network.node*] | **all** }

View

System view

Parameter

network: Destination network number of an IPX static route. It comprises eight hexadecimal numbers and is in the range of 1 to 0xFFFFFFFE. IPX static routes whose destination network number is 0xFFFFFFFE are default routes.

network.node: Next hop address of the IPX static route. *network* defines the network number; *node* defines the node address using 12 hexadecimal numbers that are separated into three parts using "-", each part in the range of 1 to 0xFFFF.

preference *value*: Static route preference in the range of 1 to 255. A smaller value indicates a higher preference. By default, the preference values of the static routes, direct routes, and dynamic RIP IPX routes are 60 (user-configurable), 0, and 100.

ticks *ticks*: Time that a packet must take to reach the destination network, with 1 tick = 1/18 seconds. The value ranges from 1 to 65534. The default value is 1.When the tick value of a VLAN interface is modified, the tick value of the static route also changes. You must configure both the tick value and the hop count.

hop *hops*: Number of the switches on the way to the destination network. It is in the range 1 to 15 and defaults to 1. You must configure both the hop count and tick value.

all: All the IPX static routes.

Description

Use the **ipx route-static** command to configure a static IPX route.

Use the **undo ipx route-static** command to delete the static IPX route.

The IPX static routes whose destination network number is 0xFFFFFFFE are default routes.

Example

Configure an IPX static route, with the destination network number being 0x5a, next hop being 675.0-0c91-f61f, tick value being 10 and hop count being 2.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ipx route-static 5a 675.0-0c91-f61f tick 10 hop 2
```

ipx sap disable

Syntax

ipx sap disable

undo ipx sap disable

View

VLAN interface view

Parameter

None

Description

Use the **ipx sap disable** command to disable SAP on the current VLAN interface.

Use the **undo ipx sap disable** command to enable SAP on the current VLAN interface.

By default, SAP is enabled as soon as IPX is enabled on the VLAN interface.

Example # Disable SAP on VLAN interface 1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 2
[SW7750-Vlan-interface2] ipx sap disable
```

ipx sap gns-disable-reply

Syntax **ipx sap gns-disable-reply**

undo ipx sap gns-disable-reply

View VLAN interface view

Parameter None

Description Use the **ipx sap gns-disable-reply** command to disable IPX GNS reply on the current VLAN interface.

Use the **undo ipx sap gns-disable-reply** command to enable IPX GNS reply on the current VLAN interface.

By default, GNS reply is enabled on the current VLAN interface.

Example # Disable GNS reply on VLAN interface 2.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 2
[SW7750-Vlan-interface2] ipx sap gns-disable-reply
```

ipx sap gns-load-balance

Syntax **ipx sap gns-load-balance**

undo ipx sap gns-load-balance

View System view

Parameter None

Description Use the **ipx sap gns-load-balance** command to configure the switch to respond to GNS requests through Round-Robin polling.

Use the **undo ipx sap gns-load-balance** command to configure the switch to respond to GNS requests with information of the nearest server.

By default, the switch responds to SAP GNS requests with the information of a server that is picked out in turn from all the known servers. This prevents a server from getting overloaded.

Related command: **ipx sap gns-disable-reply**

Example # Respond to GNS requests with the information of the nearest server.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] undo ipx sap gns-load-balance
```

ipx sap max-reserve-servers

Syntax **ipx sap max-reserve-servers** *length*

undo ipx sap max-reserve-servers

View System view

Parameter *length*: The maximum length of the service information reserve queue for one service type. It is in the range of 1 to 2048.

Description Use the **ipx sap max-reserve-servers** command to configure the maximum length of the service information reserve queue for one service type.

Use the **undo ipx sap max-reserve-servers** command to restore the default value.

By default, the maximum length of the service information reserve queue for one service type is 2,048.

Example # Set the maximum length of the service information reserve queue for one service type to 1024.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ipx sap max-reserve-servers 1024
```

ipx sap mtu

Syntax **ipx sap mtu** *bytes*

undo ipx sap mtu

View VLAN interface view

Parameter *bytes*: The maximum SAP packet size, in bytes. It is in the range of 480 to 1500.

Description Use the **ipx sap mtu** command to configure the maximum size of SAP update packets.

Use the **undo ipx sap mtu** command to restore the default value.

By default, the default size of SAP update packets is 480 bytes.

Example # Set the maximum size of SAP update packets to 674 bytes, allowing 10 service entries on VLAN interface 2.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 2
[SW7750-Vlan-interface2] ipx sap mtu 674
```

ipx sap multiplier

Syntax **ipx sap multiplier** *multiplier*

undo ipx sap multiplier

View System view

Parameter *multiplier:* A multiplier of the update interval, decides the aging period of the SAP routing entries together with the update interval. It is in the range of 1 to 1000. Multiplying the update interval by the *multiplier*, you can get the actual aging period.

Description Use the **ipx sap multiplier** command to configure the aging period of the SAP routing entries.

Use the **undo ipx sap multiplier** command to restore the default value.

By default, the aging period of the SAP service information entries is 3.

Related command: **ipx sap timer update**

Example # Set the aging period of the SAP service entries to five times the update interval.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ipx sap multiplier 5
```

ipx sap timer update

Syntax **ipx sap timer update** *seconds*

undo ipx sap timer update

View System view

Parameter *seconds*: SAP update interval. It is in the range of 10 to 60,000.

Description Use the **ipx sap timer update** command to configure a SAP update interval.

Use the **undo ipx sap timer update** command to restore the default value.

By default, the SAP update interval is 60 seconds.

Note that this command is invalid if the triggered updates feature is applied on the VLAN interface.

Related command: **ipx sap multiplier** and **ipx update-change-only**.

Example # Set the SAP update interval to 300 seconds.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ipx sap timer update 300
```

ipx service

Syntax **ipx service** *service-type name network.node socket* **hop** *hops* [**preference** *preference*]

undo ipx service { *service-type* [*name* [*network.node*]] [**preference** *preference*] | **all** }

View System view

Parameter *service-type*: A 4-byte hexadecimal number ranging from 0 to FFFF. 0 indicates all the service types.

name: Specifies the server providing the specified service, a string of 1 to 47 characters.

network.node: Network number and node value of the server. The network number comprises eight hexadecimal numbers and is in the range of 0x1 to 0xFFFFFFFD. A node address identifies a node in the network; it is 48 bits long and comprises 12 hexadecimal numbers that are separated into three parts by "-". The leading 0s can be omitted when you input a network number.

socket: Comprises four hexadecimal numbers and is in the range 0x1 to 0xFFFF.

hop *hops*: Number of hops to the server, written in decimal and in the range of 1 to 15. The hop count equal to or exceeding 16 indicates that the service is unreachable.

preference: Service preference value. The value ranges from 1 to 255. A smaller number indicates a higher preference. By default, the preference value of the static service entries is 60 (configurable); the preference value of the dynamic service entries is fixed to 500.

all: Deletes all the static service entries.

Description Use the **ipx service** command to add a static service entry to the service information table.

Use the **undo ipx service** command to delete a static service entry from the service information table.

By default, no static service entry is found in the service information table.

Example # Add a static service entry, setting service type to 4, server name to FileServer, server network number to 130, node number to 0000-0a0b-abcd, hop count to 1 and server preference to 60.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ipx service 4 FileServer 130.0000-0a0b-abcd 451 hop 1 prefe
rence 60
```

ipx split-horizon

Syntax **ipx split-horizon**

undo ipx split-horizon

View VLAN interface view

Parameter None

Description Use the **ipx split-horizon** command to enable split horizon on the current VLAN interface.

Use the **undo ipx split-horizon** command to disable split horizon on the current VLAN interface.

By default, split horizon is enabled.

Example # Enable split horizon on VLAN interface 2.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 2
[SW7750-Vlan-interface2] ipx split-horizon
```

ipx tick

Syntax **ipx tick** *ticks*

undo ipx tick

View VLAN interface view

Parameter *ticks*: Delay, in ticks; ranging from 0 to 30000. One tick is equal to 1/18 seconds.

Description Use the **ipx tick** command to configure an IPX packet forwarding delay on a VLAN interface.

Use the **undo ipx tick** command to restore the default value.

By default, the forwarding delay on the VLAN interface is one tick.

Example # Configure VLAN interface 2 to experience a delay of five ticks before forwarding IPX packets.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 2
[SW7750-Vlan-interface2] ipx tick 5
```

ipx update-change-only

Syntax **ipx update-change-only**

undo ipx update-change-only

View VLAN interface view

Parameter None

Description Use the **ipx update-change-only** command to enable triggered update on the current VLAN interface.

Use the **undo ipx update-change-only** command to disable triggered update on the current VLAN interface.

By default, triggered update of IPX is disabled.

Example # Enable triggered update of IPX on VLAN interface 2.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 2
[SW7750-Vlan-interface2] ipx update-change-only
```

reset ipx routing-table statistics protocol

Syntax **reset ipx routing-table statistics protocol** { **all** | **default** | **direct** | **rip** | **static** }

View User view

Parameter **all**: Clears the statistics of all the IPX routes.

default: Clears the statistics of the default IPX routes.

direct: Clears the statistics of the direct IPX routes.

rip: Clears the statistics of the IPX RIP routes.

static: Clears the statistics of the static IPX routes.

Description Use the **reset ipx routing-table statistics protocol** command to clear the statistics on the IPX routes of a specific route type.

Related command: **display ipx routing-table** statistics.

Example # Clear the statistics of the IPX static routes.

```
<SW7750> reset ipx routing-table statistics protocol static
```

reset ipx statistics

Syntax **reset ipx statistics**

View User view

Parameter None

Description Use the **reset ipx statistics** command to clear the IPX statistics.

Example # Clear the IPX statistics.

```
<SW7750> reset ipx statistics
```

14 GARP CONFIGURATION COMMANDS

display garp statistics

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

View Any view

Parameter *interface-list*: List of Ethernet ports. You can specify multiple Ethernet ports by providing this argument in the form of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-10>, where &<1-10> means that you can provide up to 10 port indexes/port index lists for this argument.

Description Use the **display garp statistics** command to display the GARP statistics of specified ports or all ports.

This command displays the following information:

- Number of the GMRP packets received
- Number of the GVRP packets received
- Number of the GMRP packets transmitted
- Number of the GVRP packets transmitted
- Number of the packets discarded

Example # Display the GARP statistics of port Ethernet2/0/1.

```
<SW7750> display garp statistics interface Ethernet2/0/1
        GARP statistics on port Ethernet2/0/1
        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
```

display garp timer

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

View Any view

Parameter *interface-list*: List of Ethernet ports. You can specify multiple Ethernet ports by providing this argument in the form of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-10>, where &<1-10> means that you can provide up to 10 port indexes/port index lists for this argument.

Description Use the **display garp timer** command to display the settings of the GARP timers on specified ports or all ports.

This command displays the settings of the following timers:

- Join timer
- Leave timer
- LeaveAll timer
- Hold timer

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

Example # Display the settings of the GARP timers on port Ethernet2/0/1.

```
<SW7750> display garp timer interface Ethernet2/0/1
        GARP timers on port Ethernet2/0/1

                Garp Join Time          : 20 centiseconds
                Garp Leave Time         : 60 centiseconds
                Garp LeaveAll Time      : 1000 centiseconds
                Garp Hold Time          : 10 centiseconds
```

garp timer

Syntax **garp timer** { **hold** | **join** | **leave** } *timer-value*

undo garp timer { **hold** | **join** | **leave** }

View Ethernet port view

Parameter **hold**: Sets the GARP Hold timer. When a GARP entity receives a piece of registration information, it does not send out a Join message immediately. Instead, to save the bandwidth resources, it starts the Hold timer, puts all registration information it receives before the timer times out into one Join message and sends out the message after the timer times out.

join: Sets the GARP Join timer. To transmit the Join messages reliably to other entities, a GARP entity sends each Join message two times. The Join timer is used to define the interval between the two sending operations of each Join message.

leave: Sets the GARP Leave timer. When a GARP entity expects to deregister a piece of attribute information, it sends out a Leave message. Any GARP entity receiving this message starts its Leave timer, and deregisters the attribute information if it does not receives a Join message again before the timer times out.

timer-value: Timeout time (in centiseconds) of the GARP timer (Hold, Join or Leave) to be set. This argument needs to be a multiple of 5. By default, it is 10, 20, and 60 for Hold, Join and Leave timers respectively.

Description Use the **garp timer** command to set a GARP timer (that is, the Hold timer, the Join timer, or the Leaver timer) for an Ethernet port.

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

The timeout ranges of the timers vary depending on the timeout values you set for other timers. If you want to set the timeout time of a timer to a value out of the current range, you can set the timeout time of the associated timer to another value to change the timeout range of this timer.

The following table describes the relations between the timers:

Table 25 Relations between the timers

Timer	Lower threshold	Upper threshold
Hold	10 centiseconds	This upper threshold is less than or equal to one-half of the timeout time of the Join timer. You can change the threshold by changing the timeout time of the Join timer.
Join	This lower threshold is greater than or equal to twice the timeout time of the Hold timer. You can change the threshold by changing the timeout time of the Hold timer.	This upper threshold is less than one-half of the timeout time of the Leave timer. You can change the threshold by changing the timeout time of the Leave timer.
Leave	This lower threshold is greater than twice the timeout time of the Join timer. You can change the threshold by changing the timeout time of the Join timer.	This upper threshold is less than the timeout time of the LeaveAll timer. You can change the threshold by changing the timeout time of the LeaveAll timer.
LeaveAll	This lower threshold is greater than the timeout time of the Leave timer. You can change threshold by changing the timeout time of the Leave timer.	32,765 centiseconds

Related command: **display garp timer**.

Example # Set the GARP Join timer to 25 centiseconds for port Ethernet2/0/1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet2/0/1
[SW7750-Ethernet2/0/1] garp timer join 25
```

garp timer leaveall

Syntax **garp timer leaveall** *timer-value*

undo garp timer leaveall

View System view

Parameter *timer-value*: Setting (in centiseconds) of the GARP LeaveAll timer. You need to set this argument with the Leave timer settings of other Ethernet ports as references. That is, this argument needs to be larger than the Leave timer settings of any Ethernet ports. Also note that this argument needs to be a multiple of 5 and cannot be larger than 32,765.

By default, the LeaveAll timer is set to 1,000 centiseconds (that is, 10 seconds).

Description Use the **garp timer leaveall** command to set the GARP LeaveAll timer.

Use the **undo garp timer leaveall** command to restore the default setting of the GARP LeaveAll timer.

Once a GARP entity starts up, it starts the LeaveAll timer, and sends out a LeaveALL message after the timer times out, so that other GARP entities can re-register all the attribute information on this entity. After that, the entity restarts the LeaveAll timer to begin a new cycle.

Related command: **display garp timer**.

Example # Set the GARP LeaveAll timer to 100 centiseconds.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] garp timer leaveall 100
```

reset garp statistics

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

View User view

Parameter *interface-list*: List of Ethernet ports. You can specify multiple Ethernet ports by providing this argument in the form of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-10>, where &<1-10> means that you can provide up to 10 port indexes/port index lists for this argument.

Description Use the **reset garp statistics** command to clear the GARP statistics (such as the information about the packets received/sent/discarded by GVRP/GMRP) on specified or all ports.

Executing the **reset garp statistics** command without any parameter clears the GARP statistics of all ports.

Related command: **display garp statistics**.

Example

Clear GARP statistics of all ports.

```
<SW7750> reset garp statistics
```

15 GVRP CONFIGURATION COMMANDS

display gvrp statistics

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

View Any view

Parameter *interface-list*: List of Ethernet ports. You can specify multiple Ethernet ports by providing this argument in the form of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-10>, where &<1-10> means that you can provide up to 10 port indexes/port index lists for this argument.

Description Use the **display gvrp statistics** command to display the GVRP statistics of specified or all trunk ports.

This command displays the following information:

- GVRP status
- Whether GVRP is running
- Number of the GVRP entries that fail to be registered
- Source MAC address of the previous GVRP PDU
- GVRP registration type of a port

Example # Display the GVRP statistics of port Ethernet2/0/1, assuming that the port is a trunk port.

```
<SW7750> display gvrp statistics interface Ethernet2/0/1
        GVRP statistics on port Ethernet2/0/1

                GVRP Status                     : Enabled
                GVRP Running                    : Yes
                GVRP Failed Registrations       : 0
                GVRP Last Pdu Origin            : 0000-0000-0000
                GVRP Registration Type          : Normal
```

display gvrp status

Syntax **display gvrp status**

View

Any view

Parameter

None

Description

Use the **display gvrp status** command to display the global GVRP status (enabled or disabled).

Example

Display the global GVRP status.

```
<SW7750> display gvrp status
GVRP is enabled
```

The above information indicates that GVRP is enabled globally.

gvrp

Syntax

gvrp

undo gvrp

View

System view, Ethernet port view

Parameter

None

Description

Use the **gvrp** command to enable GVRP globally (in system view) or for a port (in Ethernet port view).

Use the **undo gvrp** command to disable GVRP globally (in system view) or on a port (in Ethernet port view).

By default, GVRP is disabled both globally and on ports.

Note that:

- *To enable GVRP for a port, you need to enable GVRP globally first.*
- *GVRP is disabled on any ports if GVRP is disabled globally. In this case, you cannot enable GVRP for a port.*
- *You can enable/disable GVRP only on trunk ports.*
- *After you enable GVRP on a trunk port, you cannot change the port to other types.*

Related command:

display gvrp status.

Example

Enable GVRP globally.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] gvrp
GVRP is enabled globally.
```

gvrp registration

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

undo gvrp registration

View Ethernet port view

Parameter **fixed**: Allows to add or register the current port to the manually created VLAN, and prohibits to register or deregister the current port to the dynamic VLAN.

forbidden: Deregisters all the VLANs except VLAN 1 on the current port, and inhibits the creation and registration of any other VLAN on the current port.

normal: Allows both manual and dynamic creation, registration, and Deregistration of VLANs on the current port.

Description Use the **gvrp registration** command to configure the GVRP registration type on a port.

Use the **undo gvrp registration** command to restore the default GVRP registration type on a port.

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

Note that these commands can be operated only on trunk ports.

Related command: **display gvrp statistics**

Example # Configure the GVRP registration type on the port Ethernet2/0/1 to fixed.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet2/0/1
[SW7750-Ethernet2/0/1] gvrp registration fixed
```

16 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 the QinQ configuration of the current system, including the current status of VLAN-VPN and the VLAN ID of VLAN-VPN.

Example # Display the QinQ configuration of the current system.

```
<SW7750> display port vlan-vpn
Ethernet3/0/4
 VLAN-VPN status: enabled
 VLAN-VPN VLAN: 1
```

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 the QinQ function for a port.

Use the **undo vlan-vpn** command to disable the QinQ function for a port.

By default, the QinQ function is disabled.

With the QinQ function enabled, a received packet is tagged with the default VLAN tag of the receiving port no matter whether or not the packet already carries a VLAN tag. If the packet already carries a VLAN tag, the packet becomes a dual-tagged packet. Otherwise, the packet becomes a packet carrying the default VLAN tag of the port.

CAUTION:

- *The QinQ feature is unavailable if the port has the Voice VLAN feature enabled.*
- *After you enable the QinQ feature for a port, the Voice VLAN function is not available on the port.*
- *3C16863 and 3C16862 I/O Modules do not support the QinQ feature.*

Example # Enable the QinQ function for Ethernet2/0/1 port.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet 2/0/1
[SW7750-Ethernet2/0/1] vlan-vpn enable
```

vlan-vpn priority

Syntax **vlan-vpn priority** *inner-priority* **remark** *outer-priority*

undo vlan-vpn priority *inner-priority*

View Ethernet port view

Parameter *inner-priority*: Priority of the inner tag to be mapped, in the range of 0 to 7.

outer-priority: Priority of the outer tag obtained through mapping the priority of the inner tag, in the range of 0 to 7.

Description Use the **vlan-vpn priority** command to enable the inner-to-outer tag priority mapping for the specific port.

Use the **undo vlan-vpn priority** command to restore the default setting.

By default, inner-to-outer tag priority mapping is not configured for a port.

Example # Enable inner-to-outer tag priority mapping for Ethernet2/0/1. Map the inner tag priority 3 to outer tag priority 5.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet 2/0/1
[SW7750-Ethernet2/0/1] vlan-vpn priority 3 remark 5
```

17 SELECTIVE QINQ CONFIGURATION COMMANDS

You can implement traffic-based selective QinQ on a Switch 7750 by using ACLs and QoS techniques. Refer to "QoS Commands" on page 777.

double-vlan-id

Syntax **double-vlan-id inbound** *vlan-id-list* **outer-vid** *vlan-id*

undo double-vlan-id inbound { **all** | *vlan-id-list* } **outer-vid** *vlan-id*

View QinQ view

Parameter **inbound** *vlan-id-list*: Species one or more inner VLAN IDs as part of a match condition. You can provide up to 10 VLAN ID lists, by each of which you can specify an indiviual VLAN ID in the form of *vlan-id*, or a range of VLAN IDs in the form of *start-vlan-id* **to** *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID.

all: Species all packets.

outer-vid *vlan-id*: Specified an outer VLAN ID as part of a match condition.

Description Use the **double-vlan-id** command to define a match condition for outer tag replacement. The outer VLAN tag of every matched packet will be replaced with the VLAN tag specifed in the **vlan-vpn vid** command.

Use the **undo double-vlan-id** command to remove the configuration.

By default, no match condition is configured for outer tag replacement.

Related command: **vlan-vpn vid**.

- *The **double-vlan-id** command is to be used in conjunction with the **vlan-vpn vid** command.*
- *The **double-vlan-id** command cannot be used while the **vlan-vpn enable** and **raw-vlan-id inbound** commands are in effect on the port.*

Example # Configure outer tag replacement on Ethernet2/0/1 to replace the outer VLAN tag of packets with an inner VLAN ID in the range of 8 to 15 and an outer VLAN ID of 30 with the tag of VLAN 20. Specify Ethernet 2/0/5 as the uplink port and configure it to send packets without removing the outer VLAN tag.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet 2/0/1
[SW7750-Ethernet2/0/1] vlan-vpn vid 20 uplink Ethernet 2/0/5
[SW7750-Ethernet2/0/1-vid-20] double-vlan-id  inbound  8 to 15  outer-vid 30
```

raw-vlan-id inbound

Syntax **raw-vlan-id inbound** *vlan-id-list*

undo raw-vlan-id inbound { **all** | *vlan-id-list* }

View QinQ view

Parameter *vlan-id-list*: List of VLAN Ids. You need to provide this argument in the form of *vlan-id-list* = { *vlan-id* [**to** { *vlan-id* }] } & <1-10>, where & <1-10> means that you can provide up to ten VLAN Ids/VLAN ID lists.

all: Specifies the packets of all the VLANs.

Description Use the **raw-vlan-id inbound** command to specify a group of VLANs, single-tagged inbound packets of which are to be tagged with specified outer VLAN tags.

Use the **undo raw-vlan-id inbound** command to remove the configuration.

Note that the **raw-vlan-id inbound** command needs to be coupled by the **vlan-vpn vid** command.

Example # Configure the inbound packets of VLAN 8 through VLAN 15 received on Ethernet2/0/1 to be tagged with outer tag of VLAN 20. Specify Ethernet2/0/5 as the upstream port, and specify Ethernet2/0/5 to remove outer tags when it forwards packets.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet 2/0/1
[SW7750-Ethernet2/0/1] vlan-vpn vid 20 uplink Ethernet 2/0/5 untagged
[SW7750-Ethernet2/0/1-vid-20] raw-vlan-id inbound 8 to 15
```

vlan-vpn vid

Syntax **vlan-vpn vid** *vlan-id* **uplink** *interface-type interface-number* [**untagged**]

undo vlan-vpn vid *vlan-id*

View Ethernet port view

Parameter **vid** *vlan-id*: Specifies ID of the VLAN whose tag is to be inserted to matched packets as the outer VLAN tag.

uplink *interface-type interface-number*: Specifies the upstream port of the packets to be tagged with outer VLAN tags.

untagged: Sets whether to keep VLAN tags of the packets tagged with outer VLAN tags when they are forwarded on the upstream port.

Description

Use the **vlan-vpn vid** command to specify the VLAN whose tag is to be inserted to matched packets as the outer VLAN tag and specify the upstream port for these packets. You can use the **raw-vlan-id inbound** command to specify the outer VLAN tag for packets with the specified inner VLAN tags.

Use the **undo vlan-vpn vid** command to remove the configuration.

When the upstream port and the port where the selective QinQ configured are not on the same module, if the module where the upstream port resides is unplugged, this configuration is invisible. This configuration takes effect again when the unplugged module is plugged.

When the specified upstream port is available, the configuration of the **raw-vlan-id inbound** command remains even if the upstream port configuration or untagged attribute in this configuration is modified. When the upstream port is unavailable, the configuration of the **raw-vlan-id inbound** command is removed if this configuration is modified.

CAUTION: *A QinQ-enabled port and its corresponding upstream port cannot be added to the same aggregation group.*

- *Type-A I/O Modules do not support the selective QinQ feature. Type A I/O Modules include: 3C16860, 3C16861, LS81FS24A, 3C16858, 3C16859, and 32Gbps and 64Gbps Switch Fabrics.*
- *The 3C16863 and 3C16862 I/O Modules do not support the selective QinQ feature.*

Note that the **vlan-vpn vid** command needs to be coupled by the **raw-vlan-id inbound** command.

Example

Configure to use VLAN 20 tag as the outer VLAN tag of packets with the inner tag of VLAN 10 received on Ethernet2/0/1. Specify the upstream port as Ethernet2/0/5 and specify the upstream port to remove outer tags of the packets when forwarding the packets.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet 2/0/1
[SW7750-Ethernet2/0/1] vlan-vpn vid 20 uplink Ethernet 2/0/5 untagge
d
[SW7750-Ethernet2/0/1-vid-20] raw-vlan-id inbound 10
```

18 SHARED VLAN CONFIGURATION COMMANDS

display shared-vlan

Syntax **display shared-vlan**

View Any view

Parameter None

Description Use the **display shared-vlan** command to display the shared VLANs configured for all the I/O Modules and Fabrics in the system.

Example # Display the shared VLANs configured for all the I/O Modules and Fabrics in the system.

```
<SW7750> display shared-vlan
 shared-vlan 1 mainboard
 shared-vlan 3 slot 4
```

The fields above show that the shared VLAN configured in the current system include VLAN 1 on the Fabric and VLAN 3 on the I/O Module in slot 4.

shared-vlan mainboard

Syntax **shared-vlan** *vlan-id* **mainboard**

undo shared-vlan *vlan-id* **mainboard**

View System view

Parameter *vlan-id*: ID of the shared VLAN, in the range of 1 to 4,094.

Description Use the **shared-vlan mainboard** command to configure a shared VLAN on the Fabric. Use the **undo shared-vlan mainboard** command to remove the shared VLAN on the Fabric.

By default, no shared VLAN is configured on the Fabric.

- *For a Switch 7758 with two Fabrics equipped, the shared VLAN configured on the primary Fabric also takes effect on the secondary Fabric.*

- *You must specify an existing VLAN to be the shared VLAN. Otherwise, the system prompts configuration failure information.*

CAUTION: *The shared VLAN can destroy RRPP rings and disable the RRPP feature, and thus cause rings in the network. So make sure that the RRPP feature and the shared VLAN feature is not enabled on a switch at the same time.*

Example # Specify VLAN 10 to be a shared VLAN on the Fabric.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] shared-vlan 10 mainboard
```

shared-vlan slot

Syntax **shared-vlan** *vlan-id* **slot** *slot-number*

undo shared-vlan *vlan-id* **slot** *slot-number*

View System view

Parameter *vlan-id*: ID of the shared VLAN, in the range of 1 to 4,094.

Description Use the **shared-vlan slot** command to configure shared VLAN on the I/O Module. Use the **undo shared-vlan slot** command to remove the shared VLAN from the I/O Module.

By default, no shared VLAN is configured on the I/O Module.

You must specify an existing VLAN to be the shared VLAN. Otherwise, the system prompts configuration failure information.

CAUTION: *The shared VLAN can destroy RRPP rings and disable the RRPP feature, and thus cause rings in the network. So make sure that the RRPP feature and the shared VLAN feature is not enabled on a switch at the same time.*

Example # Specify VLAN 20 to be the shared VLAN on the I/O Module in slot 3.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] shared-vlan 20 slot 3
```

19 PORT BASIC CONFIGURATION COMMANDS

broadcast-suppression

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

undo broadcast-suppression

View Ethernet port view

Parameter *ratio*: Maximum ratio of the received broadcast traffic to the total bandwidth on an Ethernet port. The value ranges from 1 to 100 and defaults to 100. The smaller the ratio is, the less broadcast traffic is allowed.

bandwidth *bandwidth*: Specifies the maximum bandwidth of broadcast traffic received on the Ethernet port. For a 100 Mbps port, the *bandwidth* argument is in the range of 1 to 100 in Mbps; for a gigabit port, the *bandwidth* argument is in the range of 1 to 1000 in Mbps.

pps *pps*: Specifies the maximum number of broadcast packets allowed to be received per second on an Ethernet port (in pps).

- For a 100 Mbps Ethernet port, the *pps* argument is in the range of 0 to 148,810.
- For a Gigabit Ethernet port, the *pps* argument is in the range of 1,488,100.
- For a 10GE port, the *pps* argument is in the range of 0 to 14,881,000.

Description Use the **broadcast-suppression** command to limit broadcast traffic allowed to be received on each port (in system view) or on a specified port (in Ethernet port view).

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

When incoming broadcast traffic exceeds the broadcast traffic threshold you set, the system drops the packets exceeding the threshold to reduce the broadcast traffic ratio to the reasonable range, so as to keep normal network service.

By default, broadcast suppression is disabled.

Type-A I/O Modules, including 3C16860, 3C16861, LS81FS24A, 3C16858, and 3C16859, do not support enabling broadcast suppression on ports.

A port supports one way of broadcast suppression at the same time. If broadcast suppression has been configured for a port for multiple times, only the latest configuration takes effect.

Example # Allow incoming broadcast traffic to occupy at most 20% of the bandwidth on the port.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet 2/0/1
[SW7750-Ethernet2/0/1] broadcast-suppression 20
```

# Set the maximum number of broadcast packets that can be received per second by the Ethernet2/0/2 port to 1000 pps.

```
[SW7750-Ethernet2/0/2] broadcast-suppression pps 1000
```

copy configuration

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

View System view

Parameter *interface-type*: Port type.

interface-number: Port number.

source-agg-id: Source aggregation group number, in the range of 1 to 384. The port with the smallest port number in the aggregation group is used as the source port.

interface-list: Destination port list, *interface-list =interface-type interface-number* [**to** *interface-type interface-number*] &<1-10. &<1-10> means that you can input up to 10 ports/port ranges.

destination-agg-id: Destination aggregation group number, in the range of 1 to 384.

Description Use the **copy configuration** command to copy the configuration on a port to some other ports to keep consistent configuration on them.

Any aggregation group port you input in the destination port list will be removed from the list and the ***copy*** *command will not take effect on the port. If you want an aggregation group port to have the same configuration with the source port, you can specify the aggregation group of the port as the destination (with the destination-agg-id argument).*

Example # Copy the configuration of Ethernet3/01 to Ethernet3/0/2.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] copy configuration source Ethernet3/0/1 destination Ethernet3/0/2
 The operation will be invalid for some special port(s) in the destination port
list, such as aggregation port.
Copying VLAN configuration...
Copying Protocol based VLAN configuration...
Copying LACP configuration...
Copying QOS configuration...
Copying STP configuration...
Copying speed/duplex configuration...
Port configuration copy complete
```

description

Syntax **description** *text*

undo description

View Ethernet port view

Parameter *text*: Port description, a string of up to 80 characters.

Description Use the **description** command to set a port description string.

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

By default, no description is defined for a port.

Example # Set description string "lanswitch-interface" for the Ethernet2/0/1 port.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet2/0/1
[SW7750-Ethernet2/0/1] description lanswitch-interface
```

display brief interface

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

View Any view

Parameter *interface-type*: Port type.

interface-number: Port number.

|: Specifies to use a regular expression to describe the configuration information entries to be displayed.

begin: Each entry must begin with a specified character string.

include: Each entry must include a specified character string.

exclude: Each entry must not include a specified character string.

regular-expression: Regular expression, a string of 1 to 256 characters.

Description Use the **display brief interface** command to display the brief configuration information about one or all interfaces, including: interface type, link state, link rate, duplex mode, link type, default VLAN ID and port description string (only the first 33 characters are displayed).

This command is similar to the **display interface** command, but the information it displays is briefer.

Currently, for the port types other than Ethernet port, this command only displays the link state, and shows "--" in all other configuration information fields.

Related command: **display interface**.

Example # Display the brief configuration information about the Ethernet2/0/1 port.

```
<SW7750> display brief interface Ethernet2/0/1
Interface:
Eth  - Ethernet  GE   - GigabitEthernet
Loop - LoopBack  Vlan - Vlan-interface  M-E - M-Ethernet
Link:
spf -spoofing
Speed/Duplex:
A - auto-negotiation

Interface     Link   Speed  Duplex Type        PVID Description
-------------------------------------------------------------------------
Eth3/0/1      DOWN   A      A      access      1    abc
```

Table 26 Field descriptions of the display brief interface command

Field	Description
Interface	Port type
Link	Link state: UP or DOWN
Speed	Link rate
Duplex	Duplex mode
Type	Link type: access, hybrid or trunk
PVID	Default VLAN ID
Description	Port description string (only the first 33 characters are displayed)

display interface

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

View Any view

Parameter *interface-type*: Port type.

interface-number: Port number.

Description

Use the **display interface** command to display port configuration.

When using this command:

- If you specify neither port type nor port number, the command displays information about all ports.
- If you specify only port type, the command displays information about all ports of the specified type.
- If you specify both port type and port number, the command displays information about the specified port.

Example

Display the configuration information of the Ethernet2/0/1 port.

```
<SW7750> display interface Ethernet2/0/1
 Ethernet2/0/1 current state : DOWN
 IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 00e0-fc2c-3f11
 The Maximum Transmit Unit is 1500
 Media type is twisted pair, loopback not set
 Port hardware type is 100_BASE_TX
 Unknown-speed mode, unknown-duplex mode
 Link speed type is autonegotiation, link duplex type is autonegotiation
 Flow-control is not enabled
 The Maximum Frame Length is 1536
 Allow jumbo frame to pass
 Port monitor last value: 1
 PVID: 1
 Mdi type: auto
 Port link-type: access
  Tagged   VLAN ID : none
  Untagged VLAN ID : 1
 Last 300 seconds input:  0 packets/sec 0 bytes/sec
 Last 300 seconds output:  0 packets/sec 0 bytes/sec
 Input(total):  1150 packets, 149854 bytes
         542 broadcasts, 55 multicasts, - pauses
 Input(normal):  - packets, - bytes
         - broadcasts, - multicasts, - pauses
 Input:  - input errors, 0 runts, - giants,  0 throttles, 0 CRC
         0 frame,  - overruns, - aborts, - ignored, - parity errors
 Output(total): 1288 packets, 116919 bytes
         0 broadcasts, 886 multicasts, 0 pauses
 Output(normal): - packets, - bytes
         - broadcasts, - multicasts, - pauses
 Output: 0 output errors,  - underruns, - buffer failures
         0 aborts, 0 deferred, 0 collisions, 0 late collisions
         - lost carrier, - no carrier
Receive Packet Peak Value Info: 35 bytes/sec, happened at 09:24:56 06-19-2007
Transmit Packet Peak Value Info: 37 bytes/sec, happened at 09:25:01 06-19-2007
```

Table 27 Field descriptions of the display interface command

Field	Description
Ethernet2/0/1 current state	Enable/disable status of the current Ethernet port
IP Sending Frames' Format	Ethernet frame format
Hardware address	Port hardware address
The Maximum Transmit Unit	The maximum transmit unit (MTU)
Media type	Media type
Port hardware type	Port hardware type
Flow-control is enabled	Flow-control status of the port
The Maximum Frame Length	Maximum frame length allowed on the port

Table 27 Field descriptions of the display interface command

Field	Description
Allow jumbo frame to pass	Whether Jumbo frame is allowed on the port.
Port monitor last value: 5	Delay of reporting down state to the system for a port
PVID	Default VLAN ID of the port
Mdi type	Network cable type
Port link-type	Port link type
Tagged VLAN ID	Identify the VLANs whose packets will be forwarded with tags on the port.
Untagged VLAN ID	Identify the VLANs whose packets will be forwarded without tags on the port.
Last 300 seconds input: 0 packets/sec 0 bytes/sec Last 300 seconds output: 0 packets/sec 0 bytes/sec	Rate and number of incoming and outgoing packets in the last 300 seconds
Input(total): 1150 packets, 149854 bytes 542 broadcasts, 55 multicasts, - pauses Input(normal): - packets, - bytes - broadcasts, - multicasts, - pauses Input: - input errors, 0 runts, - giants, 0 throttles, 0 CRC 0 frame, - overruns, - aborts, - ignored, - parity errors	Statistics on the incoming packets and errors on the port The "-" indicates that the statistical item is not supported.
Output(total): 1288 packets, 116919 bytes 0 broadcasts, 886 multicasts, 0 pauses Output(normal): - packets, - bytes - broadcasts, - multicasts, - pauses Output: 0 output errors, - underruns, - buffer failures 0 aborts, 0 deferred, 0 collisions, 0 late collisions - lost carrier, - no carrier	Statistics on the outgoing packets and errors on the port The "-" indicates that the statistical item is not supported.
Receive Packet Peak Value Info	Peak incoming rate (in Bps) A port figures out the average incoming rate periodically. The Peak incoming rate displayed by the **display interface** command is the maximum average incoming rate ever figured out.
happened at	Time when the peak rate occurs
Transmit Packet Peak Value Info	Peak outgoing rate (in Bps) A port figures out the average outgoing rate periodically. The Peak outgoing rate displayed by the **display interface** command is the maximum average outgoing rate ever figured out.

display loopback-detection

Syntax **display loopback-detection** [**port-loopbacked**] [**|** { **begin** | **include** | **exclude** } *regular-expression*]

View Any view

Parameter **port-loopbacked**: Specifies to display the information of ports where loopback occurs.

|: Specifies to use a regular expression to display the details in the configuration information of an interface.

begin: Specifies the interface information to begin with a specific character/string.

include: Specifies the interface information to include a specific character/string.

exclude: Specifies the interface information to exclude a specific character/string.

regular-expression: Regular expression, a string containing 1 to 256 characters.

Description Use the **display loopback-detection** command to display the information related to the loopback detection function on the port.

Example # Display the information about loopback detection on the port and "40" is included in the interface information.

```
<SW7750> display loopback-detection | include 40
Loopback-detection interval time is 30 seconds
Interface                     detect    control      per-vlan  loopback-status
-------------------------------------------------------------------------
GigabitEthernet2/0/40      N        N            N        not-loop
Ethernet3/0/40             N        N            N        not-loop
```

Table 28 Field descriptions of the display loopback-detection command

Field	Description
Loopback-detection interval time	Interval of performing loopback detection
Interface	Interface name
detect	Whether loopback detection is enabled
control	Processing mode for the port where loopback is detected
per-vlan	Whether to perform loopback detection on all the VLANs on the port
loopback status	Whether loopback occurs on the current port

duplex

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

undo duplex

View Ethernet port view

Parameter **auto**: Sets the port to auto-negotiation mode.

full: Sets the port to full duplex mode.

half: Sets the port to half duplex mode.

Description Use the **duplex** command to set the duplex mode of the current port.

Use the **undo duplex** command to restore the default duplex mode, that is, auto-negotiation mode.

By default, the duplex mode of a port is in auto-negotiation mode.

Related command: **speed**.

Example # Set the duplex mode of Ethernet2/0/1 to full-duplex mode.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet2/0/1
[SW7750-Ethernet2/0/1] duplex full
```

enable log updown

Syntax **enable log updown**

undo enable log updown

View Ethernet port view

Parameter None

Description Use the **enable log updown** command to allow a port to output the Up/Down log information.

Use the **undo log enable updown** command to disable the port from outputting Up/Down log information.

By default, a port is allowed to output the Up/Down log information.

Example # By default, a port is allowed to output the Up/Down log information. Execute the **shutdown** command or the **undo shutdown** command on Ethernet2/0/1, and the system outputs the Up/Down log information of Ethernet2/0/1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet 2/0/1
[SW7750-Ethernet2/0/1] shutdown
%Sep  8 11:56:41 2006 3Com Switch 7765 (4-Slot Chassis) L2INF/5/PORT LINK STATUS CHANGE:
 Ethernet2/0/11: is DOWN
[SW7750-Ethernet2/0/1] undo shutdown
%Sep  8 11:57:00 2006 3Com Switch 7765 (4-Slot Chassis) L2INF/5/PORT LINK STATUS CHANGE:
 Ethernet2/0/11: is UP
```

# Disable Ethernet2/0/1 from outputting Up/Down log information, execute the **shutdown** command or the **undo shutdown** command on Ethernet2/0/1, and no Up/Down log information is output for Ethernet2/0/1.

```
[SW7750-Ethernet2/0/1] undo enable log updown
[SW7750-Ethernet2/0/1] shutdown
[SW7750-Ethernet2/0/1] undo shutdown
```

flow-control

Syntax **flow-control**

undo flow-control

View Ethernet port view

Parameter None

Description Use the **flow-control** command to enable flow control on the port so as to avoid packet loss during congestion.

Use the **undo flow-control** command to disable flow control on the port.

By default, flow control is disabled on a port.

Enable flow control on the port following the two steps

- *Enable flow control globally;*
- *Enable flow control on the port in Ethernet port view.*

Example # Enable flow control on the Ethernet2/0/1 port.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet2/0/1
[SW7750-Ethernet2/0/1] flow-control
```

flow-control enable

Syntax **flow-control enable**

undo flow-control disable

View System view

Parameter None

Description Use the **flow-control enable** command to enable flow control globally.

Use the **flow-control disable** command to disable flow control globally.

By default, flow control is disabled globally.

Example

Enable flow control globally.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] flow-control enable
```

flow interval

Syntax

flow-interval *interval*

undo flow-interval

View

Ethernet port view

Parameter

Interval: Interval (in seconds) to perform statistics on port information. This argument ranges from 5 to 300 (in step of 5) and is 300 by default.

Description

Use the **flow-interval** command to set the interval to perform statistics on port information.

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

By default, this interval is 300 seconds.

When you use the **display interface** *interface-type interface-number* command to display the information of a port, the system performs statistical analysis on the traffic flow passing through the port during the specified interval and displays the average rates in the interval. For example, if you set the interval to 100 seconds, the displayed information is as follows:

```
Last 100 seconds input:  0 packets/sec 0 bytes/sec
 Last 100 seconds output:  0 packets/sec 0 bytes/sec
```

Related command:

display interface.

Example

Set the interval to perform statistics on the Ethernet2/0/1 port to 100 seconds.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet 2/0/1
[SW7750-Ethernet2/0/1] flow-interval 100
```

hardspeedup

Syntax

hardspeedup enable

hardspeedup disable

View

System view

Parameter

None

Description

Use the **hardspeedup enable** command to enable command to enable the hardware speedup function inside the port.

Use the **hardspeedup disable** command to disable the hardware speedup function inside the port.

By default, the hardware speedup function inside the port is enabled.

- *The commands above are applicable to type-A I/O Modules only, including 3C16860, 3C16861, LS81FS24A, 3C16858, and 3C16859.*
- *The commands above are diagnostic, so you cannot use them at discretion.*

Example

Enable the hardware speedup function inside the port.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] hardspeedup enable
```

interface

Syntax

interface *interface-type interface-number*

View

System view

Parameter

interface-type: Port type, which can be Aux, Ethernet, GigabitEthernet, LoopBack, M-Ethernet, NULL, Tunnel or Vlan-interface.

interface-number: Port number, in the format of I/O Module slot number/subcard slot number/port number.

Table 29 Range of I/O Module slot number/subcard slot number

Description/ Device	Range of I/O Module number	Subcard slot number	Range of port number
S7704	0 to 3	0	Depending on the number of ports on the I/O Module you select
S7707	0 to 6	0	
S7708R	0 to 7	0	

Description

Use the **interface** command to enter Ethernet port view. To configure parameters for a port, you must enter the port view first.

Example

Enter Ethernet2/0/1 port view.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet2/0/1
[SW7750-Ethernet2/0/1]
```

jumboframe enable

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

undo jumboframe enable

View Ethernet port view

Parameter *jumboframe-value*: Size of the permitted jumbo frame, in the range of 1,536 to 9,216 in byte.

Description Use the **jumboframe enable** command to allow jumbo frames to pass through the current Ethernet port.

Use the **undo jumboframe enable** command to inhibit jumbo frames from passing through the current Ethernet port.

By default, jumbo frames that are larger than 1,518 bytes and smaller than 1,536 bytes are allowed to pass through the Ethernet port.

Example # Allow jumbo frames smaller than 1,536 bytes to pass through Ethernet2/0/1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet2/0/1
[SW7750-Ethernet2/0/1] jumboframe enable
```

loopback-detection enable

Syntax **loopback-detection enable**

undo loopback-detection enable

View Ethernet port view

Parameter None

Description Use the **loopback-detection enable** command to enable the loopback detection feature on the port.

Use the **undo loopback-detection enable** command to disable the loopback detection feature on the port.

By default, the loopback detection feature is disabled on the port.

Related command: **display loopback-detection**.

Example # Enable the loopback detection feature.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] loopback-detection enable
```

loopback-detection interval-time

Syntax **loopback-detection interval-time** *time*

undo loopback-detection interval-time

View System view

Parameter *time*: Interval for detecting external loopback on a port, in the range of 5 to 300 (in seconds). It is 30 seconds by default.

Description Use the **loopback-detection interval-time** command to set the interval for detecting external loopback on a port.

Use the **undo loopback-detection interval-time** command to restore the default interval.

Related command: **display loopback-detection**.

Example # Set the interval for detecting external loopback on a port to 10 seconds.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] loopback-detection interval-time 10
```

loopback-detection control

Syntax **loopback-detection control** { **block** | **nolearning** | **shutdown** }

undo loopback-detection control

View Ethernet port view

Parameter **block**: Specifies to block the port where loop is detected, that is, the port cannot receive or send any packets except BPDU packets. The system will periodically detect whether loopback still occurs on the port. If yes, the port will be blocked continuously. If not, and no other protocols (such as STP, LACP, DLDP) change the state of the port, the port will be restored to the state of sending and receiving packets normally.

nolearning: Specifies the port to continue forwarding packets after loopback is detected on it. However, the port will stop learning new MAC addresses. The system will periodically detect whether loopback still occurs on the port. If yes, the port keeps in the current state. If not, the port will be restored to the state of sending and receiving packets normally, and additionally the MAC address learning function will be also restored for the port.

shutdown: Specifies to disable the port after loopback is detected on the port.

Description Use the **loopback-detection control** command to set the processing mode for the port where loopback is detected.

Use the **undo loopback-detection control** command to cancel the defined processing mode for the port where loopback is detected.

By default, no processing mode is set for the port where loopback is detected.

Example # Specify the processing mode for the port where loopback is detected as **nolearning**.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet 2/0/1
[SW7750-Ethernet2/0/1] loopback-detection control nolearning
```

loopback-detection per-vlan enable

Syntax **loopback-detection per-vlan enable**

undo loopback-detection per-vlan enable

View Ethernet port view

Parameter None

Description Use the **loopback-detection per-vlan enable** command to enable loopback detection for all the VLANs on the current trunk port or hybrid port.

Use the **undo loopback-detection per-vlan enable** command to enable loopback detection for only the default VLAN on the current port.

By default, loopback detection is enabled for only the default VLAN of a trunk port or hybrid port.

Note that this command is not available to access ports.

Example # Enable loopback detection for all the VLANs on the trunk port Ethernet2/0/1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet 2/0/1
[SW7750-Ethernet2/0/1] port link-type trunk
[SW7750-Ethernet2/0/1] loopback-detection per-vlan enable
```

mdi

Syntax

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

undo mdi

View

Ethernet port view

Parameter

across: Specifies the network cable to be crossover network cable.

auto: Identifies the network cable type (crossover or straight through) automatically.

normal: Specifies the network cable to be straight through network cable.

Description

Use the **mdi** command to set the network types that can be identified by Ethernet ports.

Use the **undo mdi** command to restore the default network cable type that can be identified by Ethernet ports.

By default, the port identifies the network type automatically.

CAUTION: *The Switch 7750 supports the auto mode only. If another mode is specified, the system prompts "Operation not supported".*

Example

Specify Ethernet2/0/1 to identify the network cable type automatically.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet2/0/1
[SW7750-Ethernet2/0/1] mdi auto
```

multicast-suppression

Syntax

multicast-suppression { *ratio* | **bandwidth** { *mbps-value* | **kbps** *kbps-value* } | **pps** *max-pps* }

undo multicast-suppression

View

Ethernet port view

Parameter

ratio: Maximum ratio of received multicast traffic to the total bandwidth on the Ethernet port. The value ranges from 1 to 100 (in step of 1) and defaults to 100. The smaller the ratio is, the less multicast traffic is allowed to be received.

mbps-value: Maximum bandwidth (in Mbps) for receiving multicast traffic on an Ethernet port. The range of the *mbps-value* argument depends on the port type:

- 1 to 100 for 100 Mbps Ethernet ports;

- 1 to 1,000 Mbps for Gigabit Ethernet ports;
- 1 to 10,000 Mbps for 10 GE ports.

kbps *kbps-value*: Specifies the maximum bandwidth (in Kbps) for receiving multicast traffic, in the range of 64 to 1,024,000 in the step of 64.

max-pps: Maximum number of multicast packets allowed to be received per second on the Ethernet port (in pps). The range of the *max-pps* argument depends on the port type.

- 1 to 148,810 for 100 Mbps Ethernet ports;
- 1 to 1,488,100 for Gigabit Ethernet ports;
- 1 to 14,881,000 for 10 GE ports.

Description

Use the **multicast-suppression** command to limit multicast traffic allowed to be received on the current port.

Use the **undo multicast-suppression** command to restore the default multicast suppression setting on the current port.

When incoming multicast traffic on the port exceeds the multicast traffic threshold you set, the system drops the packets exceeding the threshold to reduce the multicast traffic ratio to the reasonable range, so as to keep normal network service.

By default, the switch does not suppress multicast traffic.

CAUTION: *Note that type-A I/O Modules (including 3C16860, 3C16861, LS81FS24A, 3C16858, 3C16859) do not support enabling multicast suppression on a port.*

Example

Allow the incoming multicast traffic on the Ethernet2/0/1 port to occupy at most 20% of the bandwidth on the port.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet 2/0/1
[SW7750-Ethernet2/0/1] multicast-suppression 20
```

# Set the maximum number of multicast packets that can be forwarded per second by the Ethernet2/0/2 port to 1000 pps.

```
[SW7750-Ethernet2/0/2] multicast-suppression pps 1000
```

port monitor last

Syntax

port monitor last [*value*]

undo port monitor last

View

Ethernet port view

Parameter *value*: Delay of reporting down state to the system, in the range of 0 to 60. When this argument is set to 0, the port will report its state as soon as it is brought down. The bigger this argument is, the longer delay it takes for a port to report its down state to the system.

Description Use the **port monitor last** command to set the delay of reporting down state to the system for the current port.

Use the **undo port monitor last** command to restore the delay of reporting down state to the system for the current port to the default value, which is related to the configuration performed in system view:

- If you have configured the global delay in stem view (refer to "port monitor last slot" on page 211 "port monitor last slot" on page 211 for details), the default delay will be the global delay.
- If no global delay is configured, the default delay is 1.

The delay of reporting down state to the system can be configured in either system view or Ethernet port view. If the delay is configured in both system view and Ethernet port view simultaneously, the configuration performed in Ethernet port view is given priority.

After the setting, you can use the **display interface** command to display the information about the field "Port monitor last value".

Example # Set the delay of reporting down state to the system to 5 for Ethernet2/0/1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet2/0/1
[SW7750-Ethernet2/0/1] port monitor last 5
```

port monitor last slot

Syntax **port monitor last** [**slot** *slot-number*] *value*

undo port monitor last [**slot** *slot-number*]

View System view

Parameter *slot-number*: Number of the slot where the I/O Module resides.

value: Delay of reporting down state to the system, in the range of 0 to 60. When this argument is set to 0, the port will report its state as soon as it is brought down. The bigger this argument is, the longer delay it takes for a port to report its down state to the system.

Description Use the **port monitor last** command to set the delay of reporting down state to the system for the ports of all the I/O Modules or the specified I/O Module.

Use the **undo port monitor last** command to restore the delay to the default value.

By default, the delay of reporting down state to the system is 1.

After the setting, you can use the **display interface** command to display the information about the field "Port monitor last value".

Example # Set the delay of report down state to the system to 10 for the ports on the I/O Module in slot 5.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] port monitor last slot 5 10
```

reset counters interface

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

View User view

Parameter *interface-type*: Port type.

interface-number: Port number.

Description Use the **reset counters interface** command to clear the statistics of the port, preparing for a new statistics collection.

- If you specify neither port type nor port number, the command clears statistics of all ports.
- If specify only port type, the command clears statistics of all ports of this type.
- If specify both port type and port number, the command clears statistics of the specified port.

Example # Clear the statistics of Ethernet2/0/1.

```
<SW7750> reset counters interface ethernet2/0/1
```

shutdown

Syntax **shutdown**

undo shutdown

View Ethernet port view

Parameter None

Description Use the **shutdown** command to disable an Ethernet port.

Use the **undo shutdown** command to enable an Ethernet port.

By default, an Ethernet port is enabled.

Example # Enable Ethernet2/0/1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet2/0/1
[SW7750-Ethernet2/0/1] undo shutdown
```

speed

Syntax **speed** { **10** | **100** | **1000** | **10000** | **auto** }

undo speed

View Ethernet port view

Parameter **10**: Specifies the port speed to 10 Mbps.

100: Specifies the port speed to 100 Mbps.

1000: Specifies the port speed to 1000 Mbps.

auto: Specifies the port speed to the auto-negotiation mode.

For ports of different types, the parameter prompts after you enter the ***speed*** *command are also different.*

Description Use the **speed** command to set the port speed.

Use the **undo speed** command to restore the port speed to the default setting.

By default, the port speed is in the auto-negotiation mode.

Example # Set the speed of Ethernet2/0/1 to 10 Mbps.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet 2/0/1
[SW7750-Ethernet2/0/1] speed 10
```

speed auto

Syntax **speed auto** [**10** | **100** | **1000**]*

View Ethernet port view

Parameter **10**: Configures 10 Mbps as an auto-negotiation speed of the port.

100: Configures 100 Mbps as an auto-negotiation speed of the port.

1000: Configures 1,000 Mbps as an auto-negotiation speed of the port.

Description Use the **speed auto** [**10** | **100** | **1000**]* command to configure auto-negotiation speed(s) for the current port.

By default, the port speed is auto-negotiated.

The last configuration will take effect if you configure the command for multiple times.

Example # Configure 10 Mbps and 1000 Mbps as the auto-negotiation speeds of Ethernet 2/0/1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet 2/0/1
[SW7750-Ethernet2/0/1] speed auto 10 1000
```

speedup

Syntax **speedup enable**

speedup disable

View System view

Parameter None

Description Use the **speedup enable** command to enable the hardware speedup function outside the port.

Use the **speedup disable** command to disable the hardware speedup function outside the port.

By default, the hardware speedup function outside the port is disabled.

- *The commands above are applicable to type-A I/O Modules only, including 3C16860, 3C16861, LS81FS24A, 3C16858, and 3C16859.*
- *The commands above are diagnostic, so you cannot use them at discretion.*

Example # Enable the hardware speedup function outside the port.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] speedup enable
```

unicast-suppression

Syntax **unicast-suppression** { *ratio* | **bandwidth** { *mbps-value* | **kbps** *kbps-value* } | **pps** *max-pps* }

undo unicast-suppression

View Ethernet port view

Parameter *ratio*: Maximum ratio of the received unknown unicast traffic to the total bandwidth on an Ethernet port. The value ranges from 1 to 100 in the step of 1 and defaults to 100. The smaller the ratio is, the less unknown unicast traffic is allowed.

mbps-value: Maximum bandwidth (in Mbps) for receiving unknown unicast traffic on an Ethernet port. The range of the *mbps-value* argument depends on the port type:

- 1 to 100 for 100 Mbps Ethernet ports;
- 1 to 1000 for 1000 Mbps Ethernet ports;
- 1 to 10,000 Mbps for 10 GE ports.

kbps *kbps-value*: Specifies the maximum bandwidth (in Kbps) for receiving unknown unicast traffic, in the range of 64 to 1,024,000 in the step of 64.

max-pps: Maximum number of unknown unicast packets allowed to be received per second on the Ethernet port (in pps). The range of the *max-pps* argument depends on the port type.

- 0 to 100 for 148810 Mbps Ethernet ports;
- 0 to 1000 for 1488100 Mbps Ethernet ports;
- 0 to 14881000 Mbps for 10 GE ports.

Description Use the **unicast-suppression** command to set the size of unknown unicast traffic allowed to be received on the current port.

Use the **undo unicast-suppression** command to restore the size of unknown unicast traffic allowed to be received on the current port.

When incoming unknown unicast traffic on the port exceeds the threshold you set, the system drops the packets exceeding the threshold to reduce the unknown unicast traffic ratio to the reasonable range, so as to keep normal network service.

This function is disabled by default.

⚠ ***CAUTION:*** *Type-A I/O Modules (including 3C16860, 3C16861, LS81FS24A, 3C16858, and 3C16859) do not support enabling unknown unicast suppression on a port.*

Example # Allow the incoming unknown unicast traffic on the Ethernet2/0/1 port to occupy at most 20% of the bandwidth on the port.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface ethernet 2/0/1
[SW7750-Ethernet2/0/1] unicast-suppression 20
```

# Set the maximum number of unknown unicast packets that can be forwarded per second by Ethernet2/0/2 to 1,000 pps.

```
[SW7750-Ethernet2/0/2] unicast-suppression pps 1000
```

virtual-cable-test

Syntax **virtual-cable-test**

View Ethernet port view

Parameter None

Description Use the **virtual-cable-test** command to enable the system to test the cable connected to a specific port and to display the results. The system can test these attributes of the cable:

- Cable status, including normal, abnormal, abnormal-open, abnormal-short and failure
- Cable length

- *If the cable is in normal state, the displayed information is* "-".
- *If the cable is in any other state, the displayed length value is the length from the port to the faulty point.*
- *Pair impedance mismatch*
- *Pair skew*
- *Pair swap*
- *Pair polarity*
- *Insertion loss*
- *Return loss*
- *Near-end crosstalk*

By default, the system does not test the cable connected to the Ethernet port.

- *The combo port does not support the **virtual-cable-test** command.*
- *The error for cable length tested through the **virtual-cable-test** command is ¬±5m.*

Example # Enable the system to test the cable connected to Ethernet2/0/1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet2/0/1
[SW7750-Ethernet0/1] virtual-cable-test
Cable status: abnormal(open), 7 metres
Pair Impedance mismatch: yes
Pair skew: 4294967294 ns
Pair swap: swap
Pair polarity: normal
Insertion loss: 7 db
Return loss: 7 db
Near-end crosstalk: 7 db
```

20 Link Aggregation Configuration Commands

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 the local system, including the system priority and the MAC address.

Example # Display the device ID of the local system.

```
<SW7750> display lacp system-id
 Actor System ID: 0x8000, 000f-e20f-0100
```

Table 30 Field descriptions of the **display lacp system-id** command

Field	Description
Actor System ID	Device ID of the local system, including the system priority and the system MAC address

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 range.

- If the **to** keyword is not specified, only one port is specified;
- If the **to** keyword is specified, multiple contiguous ports are specified;
- The *interface-type* argument represents the port type and the *interface-number* argument represents the port number.

Description Use the **display link-aggregation interface** command to display the link aggregation details about a specified port or port range, including:

- Link aggregation group ID of the specified port or port range

- Port priority, operation key and LACP status flag of the local end,
- Device ID, port number, port priority, operation key and protocol status flag and LACP packet statistics of the remote end

Note that, for a manual aggregation group, value 0 is displayed for all the above items of the remote end (which does not indicate the real information of the remote end), since information about the remote end cannot be obtained for a manual aggregation group.

Example # Display the link aggregation details on the specified port.

```
<SW7750> display link-aggregation interface ethernet2/0/1
Ethernet2/0/1:
   Attached AggID: 20
   Local:
     Port-Priority: 32768, Oper key: 2, Flag: 0x3d
   Remote:
     System ID: 0x8000, 000e-84a6-fb00
     Port Number: 2, Port-Priority: 32768 , Oper-key: 10, Flag: 0x3d
   Received LACP Packets: 8 packet(s), Illegal: 0 packet(s)
   Sent LACP Packets: 9 packet(s)
```

Table 31 Field descriptions of the **display link-aggregation interface** command

Field	Description
Attached AggID	ID of the aggregation group to which the specified port belongs
Local: Port-Priority: 32768, Oper key: 1, Flag: 0x00	Port priority, operation key and LACP status 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 number, port priority, operation key and LACP status flag of the remote end
Received LACP Packets: 0 packet(s), Illegal: 0 packet(s) Sent LACP Packets: 0 packet(s)	Statistics about LACP packets, including: the number of received LACP packets, the number of illegal LACP packets and the number of send LACP packets

display link-aggregation summary

Syntax **display link-aggregation summary**

View Any view

Parameter None

Description Use the **display link-aggregation summary** command to display summary information of all aggregation groups, including device ID of the local end, aggregation group ID, aggregation group type, device ID of the remote end, number of the selected ports, number of the unselected ports, load sharing type and master port number.

Example # Display summary information of all aggregation groups.

```
<SW7750> display link-aggregation summary
 Aggregation Group Type: D -- Dynamic, S -- Static, M -- Manual
Loadsharing Type: Shar - Loadsharing, NonS - Non-Loadsharing
Actor ID: 0x8000, 000f-e20f-ff04
  AL     AL  Partner ID           Select    Standby Share   Master
  ID     Type                     Ports Ports   Type        Port
-------------------------------------------------------------------
  1  D   0x8000, 000f-e20f-ff01 1       0       NonS        Ethernet2/0/1
  10     M   none                       1       0       NonS        Ethernet2/0/2
  20     S   0x8000, 000f-e20f-ff01 1       0       NonS        Ethernet2/0/3
```

Table 32 Field descriptions of the **display link-aggregation summary** command

Field	Description
Actor ID	Local device ID
AL ID	Aggregation group ID
AL Type	Aggregation group type: D (dynamic), S (static), or M (manual)
Partner ID	ID of the remote device
Select Ports	Number of the selected ports
Standby Ports	Number of standby ports
Share Type	Load sharing type: Shar (load-sharing), or NonS (non-load-sharing)
Master Port	Port with the smallest port number in the aggregation group

display link-aggregation verbose

Syntax **display link-aggregation verbose** [*agg-id*]

View Any view

Parameter *agg-id*: ID of the aggregation group to be displayed, which must be the ID of the existing aggregation group, in the range of 1 to 384.

Description Use the **display link-aggregation verbose** command to display the details about a specified aggregation group, including:

- Aggregation group ID, aggregation group type, load sharing type, aggregation group description string;
- Local end details: device ID, port number, port status, port priority, LACP flag, operation key and connection status;
- Remote end details: local port, remote port index, remote port priority, operation key, and device ID.

Note that, for a manual aggregation group, value 0 is displayed for all the above items of the remote end (which does not indicate the real information of the remote end), since information about the remote end cannot be obtained for a manual aggregation group.

Example # Display the details about aggregation group 1.

```
<SW7750> display link-aggregation verbose 1
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Aggregation ID: 1,  AggregationType: Static,   Loadsharing Type: NonS
Aggregation Description:
System ID: 0x8000, 000f-e218-d0d0
Port Status: S -- Selected,  T -- sTandby
Local:
    Port                    Status  Priority Flag Oper-Key Link-Status
--------------------------------------------------------------------------
    GigabitEthernet2/0/1    S       32768    0x7d 1        Up
    GigabitEthernet2/0/2    T       32768    0x45 2        Down
Remote:
    Actor                   Partner Priority Flag Oper-Key SystemID
--------------------------------------------------------------------------
GigabitEthernet2/0/1    0       32768    0x38 0        0x8000,0000-0000-0000
GigabitEthernet2/0/2    0       32768    0x30 0        0x8000,0000-0000-0000
```

Table 33 Field descriptions of the **display link-aggregation verbose** command

Field	Description
Aggregation ID	Aggregation group ID
AggregationType	Aggregation group type, including dynamic aggregation, static aggregation and manual aggregation
Loadsharing Type	Loadsharing type, including Loadsharing and Non-Loadsharing
Aggregation Description	Aggregation group description string
System ID	Local device ID
Port state	Port state
Local	Other information about the local end, including port number, port state, port priority, LACP flag, operation key and connection status
Remote	Detailed information about the remote end, including: local port number, remote port index, port priority, flag bit, operation key and device ID

hash

Syntax **hash** { **dstip** | **dstmac** | **ip** | **l4port** | **mac** | **srcip** | **srcmac** } { **ioboard slot** *slot-number* | **mainboard** }

undo hash { **dstip** | **dstmac** | **ip** | **l4port** | **mac** | **srcip** | **srcmac** } { **ioboard slot** *slot-number* | **mainboard** }

View System view

Parameter **dstip**: Specifies to use a destination IP address as the parameter of the HASH algorithm.

dstmac: Specifies to use a destination MAC address as the parameter of the HASH algorithm.

ip: Specifies to use the value obtained from the XOR operation performed between the source IP address and the destination IP address as the parameter of the HASH algorithm.

l4port: Specifies to use the port number of TCP or UDP as the parameter of the HASH algorithm.

mac: Specifies to use the value obtained from the XOR operation performed between the source MAC address and the destination MAC address as the parameter of the HASH algorithm.

srcip: Specifies to use a source IP address as the parameter of the HASH algorithm.

srcmac: Specifies to use a source MAC address as the parameter of the HASH algorithm.

ioboard: Enables configured parameter to be valid for I/O Modules only.

slot *slot-num*: Specifies a slot number of the I/O Module.

mainboard: Enables configured parameter to be valid for Fabrics only.

- *All the seven parameters are available on type-A I/O Modules including 3C16860, 3C16860, 3C16861, 3C16861, LS81FS24A, LS81FS24, 3C16858, 3C16858, 3C16859, and 3C16859.*
- *None of the above seven parameters are available on non-type-A I/O Modules.*
- *Only type-A I/O Modules support **l4port**.*

Description Use the **hash** command to configure parameters used by the HASH algorithm in link aggregation.

Use the **undo hash** command to cancel the configuration.

By default, type-A I/O Modules use four-tuple (**dstip**, **dstmac**, **srcip** and **srcmac**) as the parameters for HASH operation. I/O Modules other than type-A I/O Modules use **ip** as the parameter for HASH operation.

Example # For I/O Module 2, use the destination IP address as the parameter of the HASH algorithm.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] hash dstip ioboard slot 2
```

lacp enable

Syntax **lacp enable**

undo lacp enable

View Ethernet port view

Parameter None

Description Use the **lacp enable** command to enable the LACP protocol.

Use the **undo lacp enable** command to disable the LACP protocol.

Example # Enable the LACP protocol on Ethernet 2/0/1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet2/0/1
[SW7750-Ethernet2/0/1] 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, ranging from 0 to 65,535 and defaulting to 32,768.

Description Use the **lacp port-priority** command to set the priority of the current port.

Use the **undo lacp port-priority** command to restore the default port priority.

Example # Set the port priority to 64.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet2/0/1
[SW7750-Ethernet2/0/1] 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, ranging from 0 to 65,535 and defaulting to 32,768.

Description Use the **lacp system-priority** command to set the system priority.

Use the **undo lacp system-priority** command to restore the default system priority.

Example # Set the system priority to 64.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] lacp system-priority 64
```

link-aggregation

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

View System view

Parameter *interface-type*: Port type.

interface-num: Port number.

to: Specifies a series of contiguous ports.

both: Performs load sharing for both inbound traffic and outbound traffic on all member ports in the aggregation group.

Description Use the **link-aggregation** command to add a series of ports to a new manual aggregation group, to which the system assigns a new group number. The **link-aggregation group** *agg-id* **mode** command and the **port link-aggregation group** command can be used together to implement the function of the **link-aggregation** command.

By default:

- For IP packets, the system performs load sharing based on IP addresses;
- For non-IP packets, the system performs load sharing based on MAC addresses.

Example # Set up an aggregation group with Ethernet 2/0/1 to Ethernet 2/0/4 and perform load sharing for both inbound and outbound traffic of the aggregation group.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] link-aggregation ethernet2/0/1 to ethernet2/0/4 both
```

link-aggregation group description

Syntax **link-aggregation group** *agg-id* **description** *agg-name*

undo link-aggregation group *agg-id* **description**

View System view

Parameter *agg-id*: Aggregation group ID, in the range of 1 to 384.

agg-name: Aggregation group name, a string of 1 to 32 characters.

Description Use the **link-aggregation group description** command to set a description for an aggregation group.

Use the **undo link-aggregation group description** command to remove the description of the aggregation group.

Example # Set the description "office" for aggregation group 22.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] link-aggregation group 22 description office
```

link-aggregation group 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 384.

manual: Creates a manual aggregation group.

static: Creates a static aggregation group.

Description Use the **link-aggregation group mode** command to create a manual or static aggregation group.

Use the **undo link-aggregation group** command to remove an aggregation group.

Example # Create manual aggregation group 22

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] 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 384.

Description Use the **port link-aggregation group** command to add the current Ethernet port to a manual or static aggregation group.

Use the **undo port link-aggregation group** command to remove the current Ethernet port from the aggregation group.

Example # Add Ethernet 2/0/1 to aggregation group 22.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet2/0/1
[SW7750-Ethernet2/0/1] port link-aggregation group 22
```

reset lacp statistics

Syntax **reset lacp statistics** [**interface** *interface-type interface-number* [**to** *interface-type interface-number*]]

View User view

Parameter **interface** *interface-type interface-number* [**to** *interface-type interface-number*]: Specifies a port range.

- If the **to** keyword is not specified, only one port is specified;
- If the **to** keyword is specified, multiple contiguous ports are specified;
- The *interface-type* argument represents the port type and the *interface-number* argument represents the port number.

Description Use the **reset lacp statistics** command to clear LACP statistics on specified port(s), or on all ports if no port is specified.

Example # Clear LACP statistics on all Ethernet ports.

```
<SW7750> reset lacp statistics
```

21 PORT ISOLATION CONFIGURATION COMMANDS

description

Syntax **description** *text*

undo description

View Isolation group view

Parameter *text*: Description string for an isolation group, comprising 1 to 80 characters.

Description Use the **description** command to specify the description string for the current isolation group.

Use the **undo description** command to remove the description string for the current isolation group.

By default, no description string is specified for the isolation group.

Example # Specify "home" as the description string for isolation group 1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] port-isolate group 1
[SW7750-port-isolate-group1] description home
```

display isolate port

Syntax **display isolate port** [**group** *group-id*]

View Any view

Parameter *group-id*: ID of an isolation group, in the range 1 to 64.

Description Use the **display isolate port** command to display the configuration of a created isolation group, including:

- ID of the isolation group
- Description string for the isolation group
- Ports that the isolation group contains

Example # Display the configuration of isolation group 1.

```
<SW7750> display isolate port group 1
 Isolate group ID: 1
 Description: home
 Isolated port(s) in group 1:
             Ethernet2/0/2  Ethernet2/0/3  Ethernet2/0/4
```

port

Syntax **port** *interface-list*

undo port *interface-list*

View Isolation group view

Parameter *interface-list*: List of destination ports, expressed in the form of *interface-list* = *interface-type interface-number* [**to** *interface-type interface-number*] &<1-10>., where:

- The *interface-type* argument represents the type of the bound port;
- The *interface-number* argument represents the number of the bound port;
- The **to** keyword specifies a group of contiguous ports. The port number after the **to** keyword must be not smaller than that before the **to** keyword.
- &<1-10> means that you can provide up to 10 port indices/port index lists for this argument.

Description Use the **port** command to add the specified ports to an isolation group.

Use the **undo port** command to remove the specified ports from an isolation group.

By default, an isolation group contains no Ethernet port.

This command functions the same as the "port isolate group" on page 230 "port isolate group" on page 230 command except that Ethernet ports must be specified in this command.

Example # Add Ethernet2/0/2 to isolation group 1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] port-isolate group 1
[SW7750-port-isolate-group1] port Ethernet 2/0/2
```

port isolate group

Syntax **port isolate group** *group-id*

undo port isolate

View Ethernet port view

Parameter *group-id*: ID of an isolation group, in the range 1 to 64.

Description Use the **port isolate group** command to add the current Ethernet port to a created isolation group.

Use the **undo port isolate** command to remove the current Ethernet port from an isolation group.

By default, an isolation group contains no Ethernet port.

This command functions the same as the “port” on page 230 “port” on page 230 command except that Ethernet ports need not be specified in this command.

- *An Ethernet port belongs to only one port isolation group. If you add an Ethernet port to different isolation groups, the port belongs to only the latest isolation group to which the port is added.*
- *Currently, modules of Type A (3C16860, 3C16861, LS81FS24A, 3C16858, and 3C16859) do not support the Port Isolation feature.*

Example # Add Ethernet2/0/3 port to isolation group 1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet2/0/3
[SW7750- Ethernet2/0/3] port isolate group 1
```

port-isolate group

Syntax **port-isolate group** *group-id*

undo port-isolate group *group-id*

View System view

Parameter *group-id*: ID of an isolation group, in the range 1 to 64.

Description Use the **port-isolate group** command to create an isolation group.

Use the **undo port-isolate** command to remove the specified isolation group.

By default, an isolation group contains no Ethernet ports.

Example # Create isolation group 1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] port-isolate group 1
[SW7750-port-isolate-group1]
```

22 PORT SECURITY COMMANDS

Currently, A type modules (3C16860, 3C16860, 3C16861, 3C16861, LS81FS24A, LS81FS24, 3C16858, 3C16858, 3C16859, and 3C16859) do not support the port security feature.

display mac-address security

Syntax **display mac-address security** [**interface** *interface-type interface-number*] [**vlan** *vlan-id*] [**count**]

View Any view

Parameter *interface-type*: Port type.

interface-number: Port number.

vlan-id: VLAN ID, in the range of 1 to 4094.

count: Displays the number of security MAC addresses.

Description Use the **display mac-address security** command to display information about security MAC addresses. Each piece of information for a port includes: secure MAC address on the port, VLAN ID of the port, current MAC address state, port index, and MAC address aging time.

By checking the output of this command, you can verify the current configuration.

Example # Display the security MAC address configuration on GigabitEthernet 2/0/1 port.

```
<SW7750> display mac-address security interface GigabitEthernet 2/0/1
MAC ADDR         VLAN ID   STATE          PORT INDEX               AGING TIME(s)
0001-0001-0001  1        Security     GigabitEthernet2/0/1  NOAGED

  ---  1 mac address(es) found on port GigabitEthernet2/0/1 ---
```

display port-security

Syntax **display port-security** [**interface** *interface-list*]

View Any view

Parameter

interface-list: Ethernet port list, which can contain multiple Ethernet ports. The *interface-list* argument is in the format of { *interface-type interface-number* [**to** *interface-type interface-number*] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 port indexes/port index ranges in this argument.

Description

Use the **display port-security** command to display information about port security configuration (including global configuration, and configuration on specified or all ports).

By checking the output of this command, you can verify the current configuration.

CAUTION:

- *This command will display global and all ports' security configuration information if the interface-list argument is not specified.*
- *This command will display particular port's security configuration information if the interface-list argument is specified.*

Example

Display global and all ports' security configuration information.

```
<SW7750> display port-security
 Equipment port-security is enabled
 RALM logoff trap is Enabled
 Disableport Timeout: 20 s
 OUI value:
   Index is 2,  OUI value is 000100

 GigabitEthernet2/0/1 is link-down
   Port mode is noRestriction
   NeedtoKnow mode is disabled
   Intrusion mode is no action
   Max mac-address num is not configured
   Stored mac-address num is 0
   Authorization is permit

 GigabitEthernet2/0/2 is link-down
   Port mode is noRestriction
   NeedtoKnow mode is disabled
   Intrusion mode is no action
   Max mac-address num is not configured
   Stored mac-address num is 0
   Authorization is permit
```

(Any display that follows is omitted.)

Table 34 Field descriptions of the **display port-security** command

Field	Description
Equipment port security is enabled	Port security is enabled on the switch.
RALM logoff trap is Enabled	The sending of RALM authentication success trap messages is enabled.
Disableport Timeout: 100 s	The temporary port-disabling time is 100 seconds.
OUI value	The next line displays OUI value.

Table 34 Field descriptions of the **display port-security** command

Field	Description
GigabitEthernet2/0/1 is link-down	The link status of the port GigabitEthernet 2/0/1 is "down".
Port mode is noRestriction	The security mode of the port is normal.
NeedtoKnow mode is disabled	NTK is disabled on a port
Intrusion mode is no action	no action is taken when intrusion protection is triggered.
Max mac-address num is 100	The maximum number of MAC addresses allowed on the port is 100.
Stored mac-address num is 0	No MAC address is stored.
Authorization is permit	Authorization information delivered by the RADIUS server will be applied to the port.

mac-address security

Syntax

mac-address security *mac-address* **interface** *interface-type interface-number* **vlan** *vlan-id*

undo mac-address security *mac-address* [**interface** *interface-type interface-number*] **vlan** *vlan-id*

undo mac-address security { interface *interface-type interface-number* | **vlan** *vlan-id* }

View

System view

Parameter

mac-address: Security MAC address, in the H-H-H format.

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

vlan-id: VLAN ID of the security MAC address, ranging 1 to 4094.

Description

Use the **mac-address security** command to manually add a security MAC address to a port.

Use the **undo mac-address security** command to remove a security MAC address from a port.

By default, no security MAC address is configured.

You can manually add a security MAC address to a port only when port security is enabled globally and the ***port-security port-mode autolearn*** *command is configured on the port.*

Example

Add 0001-0001-0001 as a security MAC address to GigabitEthernet 2/0/1 in VLAN 1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] port-security enable
[SW7750] interface GigabitEthernet 2/0/1
[SW7750-GigabitEthernet2/0/1] port-security max-mac-count 100
```

```
[SW7750-GigabitEthernet2/0/1] port-security port-mode autolearn
[SW7750-GigabitEthernet2/0/1] quit
[SW7750] mac-address security 0001-0001-0001 interface GigabitEthernet 2/0/1 vlan 1
```

port-security enable

Syntax **port-security enable**

undo port-security enable

View System view

Parameter None

Description Use the **port-security enable** command to enable port security.

Use the **undo port-security enable** command to disable port security.

By default, port security is disabled.

⚠ ***CAUTION:*** *To avoid confliction, the following restrictions on 802.1x authentication and MAC address authentication occur after port security is enabled*

- *The access control mode (set by the* ***dot1x port-control*** *command) automatically changes to* ***auto****.*
- *The* ***dot1x****,* ***dot1x port-method****,* ***dot1x port-control*** *and* ***mac-authentication*** *commands cannot be used.*

Example # Enable port security.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] port-security enable
Notice: The port-control of 802.1x will be restricted to auto when port-security is enabled.
 Please wait... Done.
```

port-security intrusion-mode

Syntax **port-security intrusion-mode** { **disableport** | **disableport-temporarily** | **blockmac** }

undo port-security intrusion-mode

View Ethernet port view

Parameter **disableport**: Specifies to permanently disable the port.

disableport-temporarily: Specifies to temporarily disable the port, and enable the port after a pre-set time.

blockmac: Specifies to discard the packets with illegal source MAC addresses.

Description Use the **port-security intrusion-mode** command to set the action to be taken by the device when intrusion protection is triggered on the port.

Use the **undo port-security intrusion-mode** command to cancel the action setting.

By default, intrusion protection is not configured.

By checking the source MAC addresses in inbound data frames or the username and password in 802.1x authentication requests on a port, intrusion protection detects illegal packets (packets with illegal MAC address) or events and takes a pre-set action accordingly. The actions you can set include: disconnecting the port temporarily/permanently and blocking packets with invalid MAC addresses.

The following cases can trigger intrusion protection on a port

- *A packet with unknown source MAC address is received on the port while MAC address learning is disabled on the port.*
- *A packet with unknown source MAC address is received on the port while the amount of security MAC addresses on the port has reached the preset maximum number.*
- *The user fails the 802.1x or MAC address authentication.*

After executing the **intrusion-mode blockmac** command, you can only use the **display port-security** command to view blocked MAC addresses, which you cannot configure as static MAC addresses.

*If intrusion protection mode is set to **disableport-temporarily** on the port, the time set by the **port-security timer disableport** command determines how long the system temporarily disables the port when intrusion protection is triggered on the port.*

Example # Configure the switch to disable GigabitEthernet 2/0/1 when intrusion protection is triggered on the port.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] port-security enable
[SW7750] interface GigabitEthernet2/0/1
[SW7750-GigabitEthernet2/0/1] port-security intrusion-mode disableport
```

port-security authorization ignore

Syntax **port-security authorization ignore**

undo port-security authorization ignore

View Ethernet port view

Parameter None

Description Use the **port-security authorization ignore** command to configure the port to ignore the authorization information delivered by the RADIUS server.

Use the **undo port-security authorization ignore** command to restore the default configuration.

By default, the port uses (does not ignore) the authorization information delivered by the RADIUS server.

- With the **port-security authorization ignore** command executed, issuing the **display port-security** command will display "Authorization is ignore" in the output information.
- With the **undo port-security authorization ignore** command executed, issuing the **display port-security** command will display "Authorization is permit" in the output information.

Example # Configure GigabitEthernet 2/0/2 to ignore the authorization information delivered from the RADIUS server.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface GigabitEthernet2/0/2
[SW7750-GigabitEthernet2/0/2] port-security authorization ignore
```

port-security max-mac-count

Syntax **port-security max-mac-count** *count-value*

undo port-security max-mac-count

View Ethernet port view

Parameter *count-value*: Maximum number of MAC addresses allowed on the port, in the range of 1 to 1,024.

Description Use the **port-security max-mac-count** command to set the maximum number of MAC addresses allowed on the port.

Use the **undo port-security max-mac-count** command to cancel this limit.

By default, there is no limit on the number of MAC addresses allowed on the port.

Example # Set the maximum number of MAC addresses allowed on the port to 100.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] port-security enable
[SW7750] interface GigabitEthernet2/0/1
[SW7750-GigabitEthernet2/0/1] port-security max-mac-count 100
```

port-security ntk-mode

Syntax **port-security ntk-mode** { **ntkonly** | **ntk-withbroadcasts** | **ntk-withmulticasts** }

undo port-security ntk-mode

View Ethernet port view

Parameter **ntkonly**: Allows the port to transmit only unicast packets with successfully-authenticated destination MAC addresses.

ntk-withbroadcasts: Allows the port to transmit broadcast packets and unicast packets with successfully-authenticated destination MAC addresses.

ntk-withmulticasts: Allows the port to transmit multicast packets, broadcast packets and unicast packets with successfully-authenticated destination MAC addresses.

Description Use the **port-security ntk-mode** command to configure the NTK feature on the port.

Use the **undo port-security ntk-mode** command to restore the default setting.

Be default, NTK is disabled on a port, namely all frames are allowed to be sent.

By checking the destination MAC addresses of the data frames to be sent from a port, the NTK feature ensures that only successfully authenticated devices can obtain data frames from the port, thus preventing illegal devices from intercepting network data.

Example # Set the NTK feature to **ntk-withbroadcasts** on GigabitEthernet 2/0/1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] port-security enable
[SW7750] interface GigabitEthernet 2/0/1
[SW7750-GigabitEthernet2/0/1] port-security ntk-mode ntk-withbroadcasts
```

port-security oui

Syntax **port-security oui** *OUI-value* **index** *index-value*

undo port-security oui index *id-value*

View System view

Parameter *OUI-value*: OUI value. You can input a full MAC address (in hexadecimal format) for this argument and the system will calculate the OUI value from your input.

index-value: OUI index, ranging from 1 to 16.

The organizationally unique identifiers (OUIs) are assigned by IEEE to different manufacturers. Each OUI uniquely identifies an equipment manufacturer in the world and is the higher 24 bits of MAC address.

Description Use the **port-security oui** command to set an OUI value for authentication.

Use the **undo port-security oui** command to cancel the OUI value setting.

CAUTION:

- *The OUI value set by this command takes effect only when the security mode of the port is set to **userlogin-secure-oui** by the **port-security port-mode** command.*
- *You need only to input a full MAC address in hexadecimal format for the OUI-value argument in this command, and the system will automatically convert the address from hexadecimal format to binary format and then take the higher 24 bits of the resulting binary data as the OUI value.*

Related command: **port-security port-mode**.

Example # Set an OUI value by specifying the MAC address 000f-e200-0000, with an OUI index of 5.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] port-security oui 000f-e200-0000 index 5
```

port-security port-mode

Syntax **port-security port-mode** { **autolearn** | **mac-authentication** | **mac-else-userlogin-secure** | **mac-else-userlogin-secure-ext** | **secure** | **userlogin** | **userlogin-secure** | **userlogin-secure-ext** | **userlogin-secure-or-mac** | **userlogin-secure-or-mac-ext** | **userlogin-withoui** }

undo port-security port-mode

View Ethernet port view

Parameter **autolearn**: Sets the port security mode to **autoLearn**.

mac-authentication: Sets the port security mode to **macAddressWithRadius**.

mac-else-userlogin-secure: Sets the port security mode to **mac-else-userlogin-secure**.

mac-else-userlogin-secure-ext: Sets the port security mode to **mac-else-userlogin-secure-ext**.

secure: Sets the port security mode to **secure**.

userlogin: Sets the port security mode to **userLogin**.

userlogin-secure: Sets the port security mode to **userlogin-secure**.

userlogin-secure-ext: Sets the port security mode to **userlogin-secure-ext**.

userlogin-secure-or-mac: Sets the port security mode to **userlogin-secure-or-mac**.

userlogin-secure-or-mac-ext: Sets the port security mode to **userlogin-secure-or-mac-ext**.

userlogin-withoui: Sets the port security mode to **userlogin-secure-oui**.

Description

Use the **port-security port-mode** command to set the security mode of the port.

Use the **undo port-security port-mode** command to restore the port to the normal operating mode.

Port security defines various security modes that allow devices to learn legal source MAC addresses, in order for you to implement different network security management as needed. With port security, packets whose source MAC addresses cannot be learned by your switch in a security mode, or packets that fail to pass 802.1x authentication are considered illegal.

By default, no security mode is set on the port.

Example

Set the security mode on GigabitEthernet 2/0/1 to **userlogin**.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] port-security enable
[SW7750] interface GigabitEthernet2/0/1
[SW7750-GigabitEthernet2/0/1] port-security port-mode userlogin
```

port-security timer disableport

Syntax

port-security timer disableport *timer*

undo port-security timer disableport

View

System view

Parameter

timer: This argument ranges from 20 to 300 and defaults to 20 (in seconds).

Description

Use the **port-security timer disableport** command to set the time during which the system temporarily disables a port.

Use **undo port-security timer disableport** command restore the default time.

By default, the system disables a port for 20 seconds.

*After the **port-security intrusion-mode disableport-temporarily** command is executed on a port, the time set by the **port-security timer disableport** timer command determines how long the port can be temporarily disabled.*

Example # Set the time during which the system temporarily disables a port to 50 seconds.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] port-security timer disableport 50
```

port-security trap

Syntax **port-security trap** { **addresslearned** | **intrusion** | **dot1xlogon** | **dot1xlogoff** | **dot1xlogfailure** | **ralmlogon** | **ralmlogoff** | **ralmlogfailure** }

undo port-security trap { **addresslearned** | **intrusion** | **dot1xlogon** | **dot1xlogoff** | **dot1xlogfailure** | **ralmlogon** | **ralmlogoff** | **ralmlogfailure** }

View System view

Parameter **addresslearned**: Enables/disables the sending of MAC address learning trap messages.

intrusion: Enables/disables the sending of intrusion packet discovery trap messages.

dot1xlogon: Enables/disables the sending of 802.1x user logon trap messages.

dot1xlogoff: Enables/disables the sending of 802.1x user logoff trap messages.

dot1xlogfailure: Enables/disables the sending of 802.1x user authentication failure trap messages.

ralmlogon: Enables/disables the sending of RALM user logon trap messages.

ralmlogoff: Enables/disables the sending of RALM user logoff trap messages.

ralmlogfailure: Enables/disables the sending of RALM user authentication failure trap messages.

RADIUS authenticated login using MAC-address (RALM) refers to MAC address-based RADIUS authentication.

Description Use the **port-security trap** command to enable the sending of specified type(s) of trap messages.

Use the **undo port-security trap** command to disable the sending of specified type(s) of trap messages.

By default, the system disables the sending of any types of trap messages.

This command is based on the trap feature, which enables the switch to send trap messages when special data packets (generated by illegal intrusion, abnormal user logon/logoff, or other special activities) are passing through a port, so as to help the network administrator to monitor special activities.

When you use the **display port-security** command to display global information, the system will display which types of trap messages are allowed to send.

Related command: **display port-security**.

Example # Allow the sending of intrusion packet discovery trap messages.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] port-security trap intrusion
```

23 PORT BINDING COMMANDS

Currently, A type modules (3C16860, 3C16860, 3C16861, 3C16861, LS81FS24A, LS81FS24, 3C16858, 3C16858, 3C16859, and 3C16859) do not support the port binding feature.

am user-bind

Syntax

In system view:

am user-bind { **mac-addr** *mac-address* | **ip-addr** *ip-address* }* *interface-list*

undo am user-bind { **mac-addr** *mac-address* | **ip-addr** *ip-address* } *interface-list*

In Ethernet port view:

am user-bind { **mac-addr** *mac-address* | **ip-addr** *ip-address* }*

undo am user-bind { mac-addr *mac-address* | **ip-addr** *ip-address* }

View

System view/Ethernet port view

Parameter

mac-address: MAC address to be bound.

ip-address: IP address to be bound.

interface-list: Ethernet port list, *interface-list =interface-type interface-number* [**to** *interface-type interface-number*] &<1-10. &<1-10> means that you can input up to 10 ports/port ranges

Description

Use the **am user-bind** command to bind the MAC and IP addresses of a user with a specified port.

Use the **undo am user-bind** command to cancel the binding.

By default, the MAC and IP addresses of a user is not bound with any port.

- *Up to 100 MAC addresses and IP addresses can be bound to a port.*
- *A MAC/IP address cannot be bound to more than one port.*

Example

Bind the MAC address 000f-e200-5101 and IP address 10.1.1.1 (supposing they are MAC and IP addresses of a legal user) to GigabitEthernet 2/0/2 port.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] am user-bind mac-addr 000f-e200-5101 ip-addr 10.1.1.1 interface GigabitEthernet2/0/2
```

display am user-bind

Syntax **display am user-bind** [**interface** *interface-type interface-number* | **mac-addr** *mac-address* | **ip-addr** *ip-address*]

View Any view

Parameter **interface**: Displays binding information on a specified port.

interface-type: Port type.

interface-number: Port number.

mac-addr *mac-address* : Displays only the binding information of a specified MAC address.

ip-addr *ip-address* : Displays only the binding information of a specified IP address.

Description Use the **display am user-bind** command to display port binding information.

Example # Display the current system port binding information.

```
<SW7750> display am user-bind
Following address bind have been configured (* means that the rule is set by system):
  Mac                       IP                     Port
  000f-e200-5101          1.2.3.3               Ethernet2/0/2
  000f-e200-5102          2.3.2.3               Ethernet2/0/4
```

The above output displays that two port binding settings exist:

- MAC address 000f-e200-5101 and IP address 1.2.3.3 are bound with Ethernet 2/0/2.
- MAC address 000f-e200-5102 and IP address 2.3.2.3 are bound with Ethernet 2/0/4.

24 DLDP Configuration Commands

display dldp

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

View Any view

Parameter *interface-type*: Port type.

interface-number: Port number.

Description Use the **display dldp** command to display the DLDP configuration information of the device or the specified port.

Example # Display the DLDP configuration information of the device.

```
<SW7750> display dldp
 dldp interval 10
 dldp work-mode enhance
 dldp authentication-mode none
 dldp unidirectional-shutdown manual
 dldp delaydown-timer 1
 The port number with DLDP is 2.
interface GigabitEthernet2/0/1
 dldp port state : inactive
 dldp link state : down
 The neighbor number of the port is 0.
interface GigabitEthernet2/0/2
 dldp port state : advertisement
 dldp link state : up
 The neighbor number of the port is 1.
        neighbor mac address : 000f-e227-750d
        neighbor port index : 98
        neighbor state : two way
        neighbor aged time : 24
```

Table 35 Field descriptions of the **display dldp** command

Field	Description
dldp interval	Interval for sending DLDP advertisement packets
dldp work-mode	DLDP work mode
dldp authentication-mode	DLDP authentication mode
dldp unidirectional-shutdown	DLDP action to be performed on detecting a unidirectional link
dldp delaydown-timer	Setting of the DelayDown timer

Table 35 Field descriptions of the **display dldp** command

Field	Description
The port number with DLDP	Number of the DLDP-enabled ports on device
interface GigabitEthernet2/0/1	Port type and port number
dldp port state	DLDP state of a port
dldp link state	DLDP link state
The neighbor number of the port	Number of the neighbor ports
neighbor mac address	MAC address of a neighbor port
neighbor port index	Neighbor port index
neighbor state	Neighbor state (two way or unknown)
neighbor aged time	Neighbor aging time

dldp

Syntax **dldp** { **enable** | **disable** }

View System view, Ethernet port view

Parameter None

Description In system view:

Use the **dldp enable** command to enable DLDP globally on all optical ports of the switch.

Use the **dldp disable** command to disable DLDP globally on all optical ports of the switch.

In Ethernet port view:

Use the **dldp enable** command to enable DLDP on the current port.

Use the **dldp disable** command to disable DLDP on the current port.

The commands apply to both non-optical ports and optical ports.

By default, DLDP is disabled.

*When you use the **dldp enable/dldp disable** commands in system view to enable/disable DLDP globally on all optical ports of the switch, these commands are only valid for the existing optical ports on the device, however, they are not valid for those added subsequently.*

Example # Enable DLDP globally on all optical ports of the switch.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] dldp enable
 DLDP is enabled on all fiber ports.
```

dldp authentication-mode

Syntax

dldp authentication-mode { **none** | **simple** *simple-password* | **md5** *md5-password* }

undo dldp authentication-mode

View

System view

Parameter

none: Performs no authentication with the peer port.

simple: Sets the authentication mode with the peer port to plain text.

simple-password: Password for authentication with the peer port, a plaintext string in the range of 1 character to 16 characters.

md5: Specifies the mode of authentication with the peer port to MD5.

Description

Use the **dldp authentication-mode** command to set the DLDP authentication mode and password for the ports of the local and peer devices.

Use the **undo dldp authentication-mode** to cancel the DLDP authentication mode and password for the ports of the local and peer devices.

By default, authentication mode is **none**, that is, authentication is not performed.

Note that:

When you configure the DLDP authentication mode and authentication password, make sure the same DLDP authentication mode and password are set for the ports connecting the local and peer devices. Otherwise, DLDP authentication fails. DLDP cannot work when DLDP authentication fails.

Related command:

dldp unidirectional-shutdown.

Example

Enable DLDP on the ports connecting two devices. Plaintext authentication is performed with the password **password1**.

- Configure 3Com A:

```
<SW7750A> system-view
System View: return to User View with Ctrl+Z.
[SW7750A] dldp authentication-mode simple password1
```

- Configure 3Com B:

```
<SW7750B> system-view
System View: return to User View with Ctrl+Z.
[SW7750B] dldp authentication-mode simple password1
```

dldp interval

Syntax

dldp interval *integer*

undo dldp interval

View System view

Parameter *Integer*: Interval of sending DLDP packets, in the range of 1 seconds to 100 seconds. It is 5 seconds by default.

Description Use the **dldp interval** command to set the interval of sending advertisement packets when all the DLDP-enabled ports are in the Advertisement status.

Use the **undo dldp interval** command to restore the interval to the default value 5 seconds.

By default, the interval of sending advertisement packets is 5 seconds.

Note that:

- *The interval you define is applicable to all DLDP-enabled ports.*
- *The interval must be shorter than one-third of the STP convergence time. If too long an interval is set, an STP loop may occur before DLDP shuts down unidirectional links. On the contrary, if too short an interval is set, network traffic increases, and port bandwidth is reduced. Generally, the STP convergence time is 30 seconds.*
- *For the **dldp interval** integer command, make sure that the same interval for transmitting advertisement packets is set on the ports used to connected both devices; otherwise DLDP will not operate properly.*

Example # Set the interval of sending advertisement packets to 20 seconds for all the DLDP-enabled ports.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] dldp interval 20
```

dldp reset

Syntax **dldp reset**

View System view, Ethernet port view

Parameter None

Description In system view:

Use the **dldp reset** command to reset the DLDP status of all the ports disabled by DLDP.

In Ethernet port view:

Use the **dldp reset** command to reset the DLDP status of the current port disabled by DLDP.

After the **dldp reset** command is executed, the DLDP status of these ports changes from disable to active and DLDP restarts to probe the link status of the fiber cables or copper twisted pairs.

Related command: **dldp**, and **dldp unidirectional-shutdown**.

Example # Reset the DLDP status of all the ports disabled by DLDP.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] dldp reset
```

dldp unidirectional-shutdown

Syntax **dldp unidirectional-shutdown** { **auto** | **manual** }

undo dldp unidirectional-shutdown

View System view

Parameter **auto**: Disables the corresponding port automatically when DLDP detects a unidirectional link.

manual: Prompts the user to disable the corresponding port manually instead of disabling the port automatically when DLDP detects an unidirectional link. It stops the DLDP packet sending/receiving on the port at the same time.

Description Use the **dldp unidirectional-shutdown** command to set the DLDP handling mode when a unidirectional link is found.

Use the **dldp unidirectional-shutdown** command to restore the default setting.

By default, the handling mode of DLDP after unidirectional links are detected is **auto**.

Related command: **dldp work-mode**.

Example # Configure DLDP to automatically disable the corresponding port when a unidirectional link is found.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] dldp unidirectional-shutdown auto
```

dldp work-mode

Syntax **dldp work-mode** { **enhance** | **normal** }

undo dldp work-mode

View System view

Parameter **enhance**: Configures DLDP to work in enhanced mode. In this mode, DLDP probes actively whether neighbors exist when neighbor tables are aging.

normal: Configures DLDP to work in normal mode. In this mode, DLDP does not probe actively whether neighbors exist when neighbor tables are aging.

Description Use the **dldp work-mode** command to set the DLDP operating mode.

Use the **undo dldp work-mode** command to restore the default DLDP operating mode.

By default, DLDP works in normal mode.

Example # Configure DLDP to work in enhanced mode.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] dldp work-mode enhance
```

dldp delaydown-timer

Syntax **dldp delaydown-timer** *delaydown-time*

undo dldp delaydown-timer

View System view

Parameter *delaydown-time*: Delaydown timer to be set (in seconds). This argument ranges from 1 to 5. By default, the delaydown timer expires after 1 second it is triggered.

Description Use the **dldp delaydown-timer** command to set the delaydown timer.

Use the **undo dldp delaydown-timer** command to restore the default delaydown timer setting.

Example # Set the delaydown timer to 2 seconds.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] dldp delaydown-timer 2
```

25 MAC ADDRESS TABLE CONFIGURATION COMMANDS

This chapter describes the management of static and dynamic MAC address entries. For information on the management of multicast MAC address entries, refer to "Static Multicast MAC Address Table Configuration Commands" on page 523.

bridgemactocpu

Syntax **bridgemactocpu** { **enable** | **disable** }

View System view

Parameter **enable**: Enables the packets to be passed to the CPU for processing.

disable: Disables the packets from being passed to the CPU for processing.

Description Use the **bridgemactocpu** command to set whether the packets with destination MAC address as the bridge MAC address of the switch will be passed to the CPU for processing.

By default, the packets with destination MAC address as the bridge MAC address of the switch are not passed to the CPU for processing.

Example # Enable the packets with destination MAC address as the bridge MAC address of the switch to be passed to the CPU for processing.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] bridgemactocpu enable
```

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 display the aging time for the dynamic MAC address entries in the MAC address table.

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

Example # Display the aging time for the dynamic MAC address entries.

```
<SW7750> display mac-address aging-time
Mac address aging time: 300s
```

The output information indicates that the aging time for the dynamic MAC address entries is 300 seconds.

```
<SW7750> display mac-address aging-time
Mac address aging time: no-aging
```

The output information indicates that dynamic MAC address entries do not age out.

display mac-address

Syntax **display mac-address** [*display-option*]

View Any view

Parameter *display-option*: Option used to display specific MAC address table information, as described in Table 36.

Table 36 Description on the *display-option* argument

Value	Description
mac-address [**vlan** *vlan-id*]	Displays information about a specified MAC address entry.
{ **static** | **dynamic** } [**interface** *interface-type interface-number*] [**vlan** *vlan-id*] [**count**]	Displays information about dynamic or static address entries.
interface *interface-type interface-number* [**vlan** *vlan-id*] [**count**]	Displays information about the MAC address entries concerning a specified port.
vlan *vlan-id* [**count**]	Displays information about the MAC address entries concerning a specified VLAN.
count	Displays the total number of the MAC address entries maintained by the switch.

mac-address: MAC address.

static: Displays static MAC address entries. (A static MAC address entry does not age.)

dynamic: Displays dynamic MAC address entries. (A dynamic MAC address entry ages with time.)

interface-type: Port type.

interface-number: Port number.

vlan-id: VLAN ID. This argument ranges from 1 to 4094.

count: Displays only the total number of the MAC address entries.

Description

Use the **display mac-address** command to display information about MAC address entries in a MAC address table, including: MAC address, VLAN and port corresponding to the MAC address, the type (static or dynamic) of a MAC address entry, aging time and so on.

Example

Display the information about the MAC address 000f-e201-0101.

```
<SW7750> display mac-address 000f-e201-0101
MAC ADDR        VLAN ID    STATE            PORT INDEX             AGING TIME(s)
000f-e201-0101     1       Learned          Ethernet3/0/11    AGING
```

# Display the MAC address entries for the port Ethernet2/0/4.

```
<SW7750> display mac-address interface Ethernet 2/0/4
MAC ADDR        VLAN ID    STATE            PORT INDEX             AGING TIME(s)
00e0-0112-9a86     2       Config static     Ethernet2/0/4        NOAGED
000c-760a-172d     1       Learned          Ethernet2/0/4         AGING
000d-88f6-44c1     1       Learned          Ethernet2/0/4         AGING
000d-88f7-9f7d     1       Learned          Ethernet2/0/4         AGING
000d-88f7-b090     1       Learned          Ethernet2/0/4         AGING
000d-88f7-b094     1       Learned          Ethernet2/0/4         AGING
000d-88f8-4e88     1       Learned          Ethernet2/0/4         AGING

---  7 mac address(es) found on port Ethernet2/0/4 ---
```

# Display the total number of MAC address entries found in VLAN 2.

```
<SW7750> display mac-address vlan 2 count
 9 mac address(es) found in vlan 2
```

Table 37 Field descriptions of the **display mac-address** command

Field	Description
MAC ADDR	MAC address
VLAN ID	ID of the VLAN to which the network device identified by the MAC address belongs
STATE	The state of the MAC address. The value of this field can be "Static", "Learned", and so on.
PORT INDEX	Port index (including port type and port number)
AGING TIME(s)	Indicates whether a MAC address entry is aging

higig-port mac-learning disable

Syntax

higig-port mac-learning disable *slot-number*

undo higig-port mac-learning disable *slot-number*

View

System view

Parameter

slot-number: Number of the module slot for which MAC address learning on HiGig ports is to be enabled/disabled.

Description

Use the **higig-port mac-learning disable** command to disable the HiGig ports from learning MAC addresses.

Use the **undo higig-port mac-learning disable** command to enable the HiGig ports to learn MAC addresses.

By default, HiGig ports are enabled to learn MAC addresses.

The above-mentioned command is not available for the following modules: 3C16860, 3C16861, LS81FS24A, 3C16858, 3C16859, LS8M1PT4GB0, LS8M1PT8GB0, LS81PT4GA, and LS81PT8GA.

Example

Disable the HiGig ports on the module in slot 3 from learning MAC addresses.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] higig-port mac-learning disable 3
```

mac-address

Syntax

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

undo mac-address [*mac-address-attribute*]

View

System view

Parameter

static: Specifies that the MAC address entry to be added/updated is of static type.

dynamic: Specifies that the MAC address entry to be added/updated is of dynamic type.

mac-address: MAC address.

interface-type: Port type.

interface-number: Port number.

vlan-id: VLAN ID. This argument ranges from 1 to 4094.

mac-address-attribute: String used to specify the MAC address entries to be removed, as described in Table 38.

Table 38 Description on the *mac-address-attribute* argument

Value	Description
{ **static** | **dynamic** } **interface** *interface-type interface-number*	Removes the static or dynamic MAC address entries concerning a specified port.
{ **static** | **dynamic** } **vlan** *vlan-id*	Removes the static or dynamic MAC address entries concerning a specified VLAN.
{ **static** | **dynamic** } *mac-address* [**interface** *interface-type interface-number*] **vlan** *vlan-id*	Removes a specified static or dynamic MAC address entry.

Table 38 Description on the *mac-address-attribute* argument

Value	Description
interface *interface-type interface-number*	Removes all the MAC address entries concerning a specified port.
vlan *vlan-id*	Removes all the MAC address entries concerning a specified VLAN.
mac-address [**interface** *interface-type interface-number*] **vlan** *vlan-id*	Removes a specified MAC address entry.

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

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

If the MAC address you input in the **mac-address** command already exists in the MAC address table, the system will modify the attributes of the corresponding MAC address entry according to your settings in the command.

You can remove all MAC address entries (unicast MAC addresses only) concerning a specific port, or remove a specific type of MAC address entries, such as the addresses learnt by the system and dynamic or static MAC address entries configured.

Example # Configure a static MAC address entry with the following settings:

- MAC address: 000f-e201-0101
- Outbound port: Ethernet2/0/1 port
- Ethernet2/0/1 port belongs to VLAN 2.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] mac-address static 000f-e201-0101 interface Ethernet 2/0/1 vlan 2
```

mac-address learning synchronization

Syntax **mac-address learning synchronization**

undo mac-address learning synchronization

View System view

Parameter None

Description Use the **mac-address learning synchronization** command to enable MAC address learning synchronization between module chips.

Use the **undo mac-address learning synchronization** command to disable MAC address learning synchronization between module chips.

By default, MAC address learning synchronization between module chips is disabled.

Example # Enable MAC address learning synchronization between module chips.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] mac-address learning synchronization
```

mac-address mac-learning disable

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

undo mac-address mac-learning disable

View Ethernet port view

Parameter None

Description Use the **mac-address mac-learning disable** command to disable the current port from learning MAC addresses.

Use the **undo mac-address mac-learning disable** command to re-enable the current port to learn MAC addresses.

By default, the port is enabled to learn MAC addresses.

- *Do not use the* ***mac-address mac-learning disable*** *command together with any 802.1X-related command in Ethernet port view.*
- *Do not use the* ***mac-address mac-learning disable*** *command together with the* ***mac-address max-mac-count*** *command.*

Example # Disable the port Ethernet2/0/1 from learning MAC addresses.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet 2/0/1
[SW7750-Ethernet2/0/1] mac-address mac-learning disable
```

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 a port can learn. This argument ranges from 0 to 16384. A value of 0 disables the port from learning MAC addresses.

Description Use the **mac-address max-mac-count** command to set the maximum number of MAC addresses an Ethernet port can learn.

Use the **undo mac-address max-mac-count** command to cancel the limitation on the number of MAC addresses an Ethernet port can learn.

By default, the number of MAC addresses an Ethernet port can learn is not limited.

When you use the **mac-address max-mac-count** command, the port stops learning MAC addresses after the number of MAC addresses it learned reaches the value of the *count* argument you provided. You can use the **undo mac-address max-mac-count** command to cancel this limit so that the port can learn an unlimited number of MAC addresses, which is the default setting.

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

Example # Set the maximum number of MAC addresses Ethernet2/0/3 port can learn to 600.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet 2/0/3
[SW7750-Ethernet2/0/3] 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 (in seconds) for layer 2 dynamic MAC address entries. The *age* argument ranges from 10 to 1000000 and defaults to 300.

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

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

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

Set the aging time for dynamic MAC address entries as required but ensure that the aging time does not decrease the layer 2 packet forwarding performance of the switch.

- If the aging time is too short, the MAC address entries that are still valid may be removed. Upon receiving a packet destined for a MAC address that is already removed, the switch broadcasts the packet through all its ports in the VLAN which the packet belongs to. This decreases the operating performance of the switch.

- If the aging time is too long, MAC address entries may still exist even if they turn invalid. This causes the switch to be unable to update its MAC address table in time. In this case, the MAC address table cannot reflect the position changes of network devices in time.

Example # Set the aging time for MAC address entries to 500 seconds.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] mac-address timer aging 500
```

26 Centralized MAC Address Authentication Configuration Commands

display mac-authentication

Syntax **display mac-authentication** [**interface** *interface-list*]

View Any view

Parameter *interface-list*: List of Ethernet ports. You can specify multiple Ethernet ports by providing this argument in the form of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-10>, where &<1-10> means that you can provide up to 10 port indexes/port index ranges for this argument.

Description Use the **display mac-authentication** command to display global information about centralized MAC address authentication, including:

- The state of centralized MAC address authentication (enabled/disabled)
- Timer settings
- The number of online users
- The MAC addresses in quiet period
- MAC authentication information about each port

Example # Display the global information about centralized MAC address authentication.

```
<SW7750> display mac-authentication
 Mac address authentication is Enabled.
 Mac authentication re-authenticate is Disabled.
 Authentication mode is UsernameAsMacAddress
 Fixed username:mac
 Fixed password:not configured
          Offline detect period is 300s
          Quiet period is 60s.
          Server response timeout value is 100s
          Mac-reauthenticate period is 1800s.
          Max allowed user number is 4096
          Current user number amounts to 0
          Current domain: not configured, use default domain
Silent Mac User info:
          MAC ADDR             From Port               Port Index
GigabitEthernet2/0/1 is link-down
  MAC address authentication  is Disabled
  Authenticate success: 0, failed: 0
  Current online user number is 0
```

```
     MAC ADDR          Authenticate state            AuthIndex
......
```

Table 39 Field descriptions of the **display mac-authentication** command

Field	Description
Mac address authentication is Enabled	Centralized MAC address authentication is enabled.
Mac authentication re-authenticate is Disabled	Centralized MAC address re-authentication is disabled.
Authentication mode	Centralized MAC address authentication mode. The default is the MAC address mode.
Fixed username	User name used in the fixed mode, which defaults to mac.
Fixed password	Password used in the fixed mode, which is not configured by default.
Offline detect period	Offline detect timer, which sets the time interval to check whether a user goes offline and defaults to 300 seconds.
Quiet period	Quiet timer sets the quiet period. A switch goes through a quiet period if a user fails to pass the MAC address authentication. The default value is 60 seconds.
Server response timeout value	Server timeout timer, which sets the timeout time for the connection between a switch and the RADIUS server. By default, it is 100 seconds.
Mac-reauthenticate period	Re-authentication period timer
Max allowed user number	The maximum number of users supported by the switch.
Current user number amounts to	The current number of users
Current domain	The current used domain. It is not configured by default.
Silent Mac User info	The information about the silent user. When the user fails to pass MAC address authentication because of inputting error user name and password, the switch sets the user to be in quiet state. During quiet period, the switch does not process the authentication request of this user.
GigabitEthernet2/0/1 is link-down	The link connected to GigabitEthernet2/0/1 is down.
MAC address authentication is Disabled	MAC address authentication is disabled on GigabitEthernet2/0/1.
Authenticate success: 0, failed: 0	Statistics of the MAC address authentications performed on the port, including the numbers of successful and failed authentication operations.
Current online user number	The number of the users current access the network through the port
MAC ADDR	Peer MAC address

Table 39 Field descriptions of the **display mac-authentication** command

Field	Description
Authenticate state	The state of the users accessing the network through the port, which can be: ■ MAC_AUTHENTICATOR_CONNECTING: Connecting ■ MAC_AUTHENTICATOR_SUCCESS: Authentication passed ■ MAC_AUTHENTICATOR_FAILURE: Fail to pass authentication ■ MAC_AUTHENTICATOR_LOGOFF: Offline
AuthIndex	Index of the current MAC address with regard to the authentication port

mac-authentication

Syntax **mac-authentication**

undo mac-authentication

View System view, Ethernet port view

Parameter None

Description Use the **mac-authentication** command to enable centralized MAC address authentication globally or for a specified port.

Use the **undo mac-authentication** command to disable centralized MAC address authentication globally or for a specified port.

By default, centralized MAC address authentication is disabled both globally and for a port.

When being executed in system view, the **mac-authentication** command enables centralized MAC address authentication globally.

When being executed in Ethernet port view, the **mac-authentication** command enables centralized MAC address authentication for the current port.

You can configure the global or port-specific MAC address authentication-related attributes before or after you enable centralized MAC address authentication.

Example # Enable centralized MAC address authentication globally.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] mac-authentication
MAC authentication is enabled globally.
```

# Enable centralized MAC address authentication on Ethernet2/0/1.

```
[SW7750] interface Ethernet 2/0/1
[SW7750-Ethernet2/0/1] mac-authentication
MAC authentication is enabled on port Ethernet 2/0/1 already
```

mac-authentication interface

Syntax **mac-authentication interface** *interface-list*

undo mac-authentication interface *interface-list*

View System view

Parameter *interface-list*: List of Ethernet ports. You can specify multiple Ethernet ports by providing this argument in the form of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-10>, where &<1-10> means that you can provide up to 10 port indexes/port index ranges.

Description Use the **mac-authentication interface** command to enable the centralized MAC address authentication for specified ports.

Use the **undo mac-authentication interface** command to disable the centralized MAC address authentication on specified ports.

By default, centralized MAC address authentication is disabled on a port.

- *To make the centralized MAC address authentication configuration takes effect on a port, you need to enable the centralized MAC address authentication for the port after you enable centralized MAC address authentication globally.*
- *The configuration of the maximum number of learned MAC addresses (configured through the **mac-address max-mac-count** command) is unavailable for the ports with centralized MAC address authentication enabled. Similarly, the centralized MAC address authentication is unavailable for the ports with the maximum number of learned MAC addresses configured.*

Example # Enable centralized MAC address authentication for Ethernet2/0/1 port.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] mac-authentication interface Ethernet 2/0/1
```

mac-authentication authmode usernameasmacaddress

Syntax **mac-authentication authmode usernameasmacaddress** [**usernameformat** { **with-hyphen** | **without-hyphen** }]

undo mac-authentication authmode

View System view

Parameter

usernameformat: Specifies the input format of the username and password.

with-hyphen: Uses hyphened MAC addresses as usernames and passwords, 00-05-e0-1c-02-e3 for example.

without-hyphen: Uses MAC addresses without hyphens as usernames and passwords, 0005e01c02e3 for example.

Description

Use the **mac-authentication authmode usernameasmacaddress** command to specify the centralized MAC address authentication mode as MAC address.

Use the **undo mac-authentication authmode** command to restore the default centralized MAC address authentication mode.

By default, the MAC address mode is adopted for the centralized MAC address authentication.

Example

Specify centralized MAC address authentication mode as MAC address, using hyphened MAC addresses as the usernames and passwords.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] mac-authentication authmode usernameasmacaddress usernamefo
rmat with-hyphen
```

mac-authentication authmode usernamefixed

Syntax

mac-authentication authmode usernamefixed

undo mac-authentication authmode

View

System view

Parameter

None

Description

Use the **mac-authentication authmode usernamefixed** command to specify the centralized MAC address authentication mode as fixed mode.

Use the **undo mac-authentication authmode** command to restore the default centralized MAC address authentication mode.

By default, the MAC address mode is adopted.

Example

Specify centralized MAC address authentication mode as fixed mode.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] mac-authentication authmode usernamefixed
```

mac-authentication authpassword

Syntax **mac-authentication authpassword** *password*

undo mac-authentication authpassword

View System view

Parameter *password*: Password to be set, a string comprising 1 to 63 characters.

Description Use the **mac-authentication authpassword** command to set a password for centralized MAC address authentication when the fixed mode is adopted.

Use the **undo mac-authentication authpassword** command to cancel the configured password.

By default, no fixed password is configured.

Example # Set the password to mac.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] mac-authentication authpassword mac
```

mac-authentication authusername

Syntax **mac-authentication authusername** *username*

undo mac-authentication authusername

View System view

Parameter *username*: User name to be set, a string comprising 1 to 55 characters.

Description Use the **mac-authentication authusername** command to set a user name when the fixed mode is adopted.

Use the **undo mac-authentication authusername** command to restore the default user name.

By default, the user name used in MAC address authentication (in the fixed mode) is mac.

Example # Set the user name to vipuser for fixed mode.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] mac-authentication authusername vipuser
```

mac-authentication domain

Syntax **mac-authentication domain** *isp-name*

undo mac-authentication domain

View System view

Parameter *isp-name*: ISP domain name, a string comprising up to 24 characters. Note that this argument cannot be null and cannot contain these characters: "/", ":", "*", "?", "<", and ">".

Description Use the **mac-authentication domain** command to configure an ISP domain for centralized MAC address authentication.

Use the **undo mac-authentication domain** command to restore the default ISP domain for centralized MAC address authentication.

By default, the domain for centralized MAC address authentication is not configured.

Use the "default domain" as the ISP domain name.

Example # Configure the domain for centralized MAC address authentication to be Cams.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] mac-authentication domain Cams
```

mac-authentication re-authenticate enable

Syntax **mac-authentication re-authenticate enable**

undo mac-authentication re-authenticate enable

View System view

Parameter None

Description Use the **mac-authentication re-authenticate enable** command to enable the MAC address regular re-authentication function.

Use the **undo mac-authentication re-authenticate enable** command to disable the MAC address regular re-authentication function.

By default, MAC address regular re-authentication is disabled.

⚠ ***CAUTION:*** *You must enable MAC address authentication globally and on a port before you can enable the MAC address regular re-authentication function.*

Example # Enable the MAC address regular re-authentication function globally.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] mac-authentication re-authenticate enable
```

mac-authentication re-authenticate mac-address

Syntax **mac-authentication re-authenticate mac-address** *mac-address*

View System view

Parameter *mac-address*: All valid unicast MAC addresses.

Description Use the **mac-authentication re-authenticate mac-address** command to re-authenticate a specified MAC address that has already passed the MAC address authentication.

CAUTION:

- *For a user with the specified MAC address, each MAC address re-authentication configuration will trigger a re-authentication. If the re-authentication succeeds, the user will be authorized; otherwise, the user will be made offline.*
- *When you configure to re-authenticate a specified MAC address, if the MAC address has failed the MAC address authentication, the re-authentication operation will be ignored.*

Example # Configure to re-authenticate MAC address 000F-3D80-4433 which has passed the MAC address authentication.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] mac-authentication re-authenticate mac-address 000F-3D80-44
33
```

mac-authentication timer

Syntax **mac-authentication timer** { **offline-detect** *offline-detect-value* | **quiet** *quiet-value* | **server-timeout** *server-timeout-value* | **reauth-period** *reauth-period-value* }

undo mac-authentication timer { **offline-detect** | **quiet** | **server-timeout** | **reauth-period** }

View System view

Parameter *offline-detect-value*: Offline detect timer (in seconds) setting. This argument ranges from 1 to 65,535 and defaults to 300. The offline detect timer sets the time interval for a switch to test whether a user goes offline.

quiet-value: Quiet timer (in seconds) setting. This argument ranges from 1 to 3,600 and defaults to 60. After a user fails to pass the authentication performed by a switch, the switch quiets for a specific period (the quiet period) before it authenticates the user again.

server-timeout-value: Server timeout timer setting (in seconds). This argument ranges from 1 to 65,535 and defaults to 100. During authentication, the switch prohibits a user from accessing the network through the corresponding port if the connection between the switch and the RADIUS server times out.

reauth-period-value: Reauth-period timer. After a user passes the MAC address authentication, the switch will periodically request the server for re-authentication. This argument ranges from 1 to 1,000,000, in seconds. The default period is 1800 seconds.

Description

Use the **mac-authentication timer** command to configure the timers used in centralized MAC address authentication.

Use the **undo mac-authentication timer** command to restore a timer to its default setting.

Related command: **display mac-authentication**.

Example

Set the server timeout timer to 150 seconds.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] mac-authentication timer server-timeout 150
```

reset mac-authentication

Syntax

reset mac-authentication statistics [**interface** *interface-list*]

View

User view

Parameter

interface-list: List of Ethernet ports. You can specify multiple Ethernet ports by providing this argument in the form of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-10>, where *interface-type* is the port type, *interface-number* is the port number, and &<1-10> means you can provide up to 10 ports/port ranges.

Description

Use the **reset mac-authentication** command to clear the centralized MAC address authentication statistics. If you execute this command with the **interface** keyword specified, the centralized MAC address authentication statistics of the specified port is cleared. If the keyword is not specified, the command clears the global centralized MAC address authentication statistics.

Example

Clear the centralized MAC address authentication statistics of GigabitEthernet 2/0/1.

```
<SW7750> reset mac-authentication statistics interface GigabitEthern
et 2/0/1
```

27 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 settings of an MST (multiple spanning tree) region.

Configuring MST region-related parameters (especially the VLAN mapping table) result in spanning trees being regenerated. To reduce network topology jitter caused by the configuration, MSTP (multiple spanning tree protocol) does not regenerate spanning trees immediately after the configuration; it does this only after you activate the new MST region-related settings or enable MSTP, and then the new settings can really take effect.

This command causes the switch to operate with the new MST region-related settings you configured and spanning trees to be regenerated.

Related command: **instance**, **region-name**, **revision-level**, **vlan-mapping modulo**, and **check region-configuration**.

Example # Activate the MST region-related settings.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] stp region-configuration
[SW7750-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 display the current MST region configuration, including region name, revision level, and VLAN mapping table.

MSTP-enabled switches are in the same region only when they have the same MST region-related configuration. A switch cannot be in a respected region if any one of the above three MST region-related settings does not be consistent with that of another switch in the region.

You can use this command to find the MST region the switch currently belongs to or check to see whether or not the MST region-related configuration is correct.

Related command: **instance**, **region-name**, **revision-level**, **vlan-mapping modulo**, and **active region-configuration**.

Example # Display the MST region configuration of the current switch.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] stp region-configuration
[SW7750-mst-region] check region-configuration
Admin Configuration
   Format selector :0
   Region name     :00e0fc003900
   Revision level  :0

   Instance   Vlans Mapped
      0       1 to 9, 11 to 4094
     16       10
```

Table 40 Field descriptions of the **check region-configuration** command

Field	Description
Format selector	The selector specified by MSTP
Region name	The name of the MST region
Revision level	The revision level of the MST region
Instance Vlans Mapped	Spanning tree instance-to-VLAN mappings in the MST region

display stp

Syntax **display stp** [**instance** *instance-id*] [**interface** *interface-list* | **slot** *slot-number*] [**brief**]

View Any view

Parameter *instance-id*: ID of the spanning tree instance ranging from 0 to 16. A value of 0 specifies the common and internal spanning tree (CIST).

interface-list: Ethernet port list. You can specify multiple Ethernet ports by providing this argument in the form of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-10>, where

&<1-10> means that you can provide up to 10 port indexes/port index ranges for this argument.

Slot *slot-number*: Specifies a slot, the STP-related information about which is to be displayed.

brief: Displays only port state and protection measures taken on the port.

Description

Use the **display stp** command to display the state and statistical information about one or all spanning trees.

The state and statistical information about MSTP can be used to analyze and maintain the topology of a network. It also can be used to make MSTP operating properly.

- If neither spanning tree instance nor port list is specified, the command displays spanning tree information about all spanning tree instances on all ports in order of port number.
- If only a spanning tree instance is specified, the command displays information about the specified spanning tree instance on all ports in the order of the port number.
- If only a port list is specified, the command displays information about all spanning tree instances on these ports in the order of the port number.
- If both a spanning tree instance and a port list are specified, the command displays spanning tree information about the specified spanning tree instance and the specified ports in order of spanning tree instance ID.

MSTP state information includes:

- Global CIST parameters: Protocol operation mode, switch priority in the CIST instance, MAC address, Hello time, Max age, Forward delay, Max hops, the common root of the CIST, the external path cost for the switch to reach the CIST common root, region root, the internal path cost for the switch to reach the region root, CIST root port of the switch, the state of the BPDU (bridge protocol data unit) guard function (enabled or disabled), and the state of the digest snooping feature (enabled or disabled).
- CIST port parameters: Port protocol, port role, port priority, path cost, designated bridge, designated port, edge port/non-edge port, whether or not the link on the port is a point-to-point link, the maximum transmitting speed, type of the enabled guard function, state of the digest snooping feature (enabled or disabled), VLAN mappings, Hello time, Max age, Forward delay, Message-age time, and Remaining-hops.
- Global MSTI parameters: MSTI instance ID, bridge priority of the instance, region root, internal path cost, MSTI root port, and master bridge.
- MSTI port parameters: Port state, role, priority, path cost, designated bridge, designated port, and Remaining Hops.

The statistical information includes: the numbers of the TCN BPDUs, the configuration BPDUs, the RST BPDUs, and the MST BPDUs transmitted/received by each port.

Related command: **reset stp**.

Example # Display the state and statistical information about a spanning tree.

```
<SW7750> display stp instance 0 interface Ethernet 1/0/1 to Ethernet 1/0/4 brief
  MSTID      Port                  Role  STP State     Protection
   0        Ethernet1/0/1         ALTE  DISCARDING      LOOP
   0        Ethernet1/0/2         DESI  FORWARDING      NONE
   0        Ethernet1/0/3         DESI  FORWARDING      NONE
   0        Ethernet1/0/4         DESI  FORWARDING      NONE
```

Table 41 Field descriptions of the **display stp** command

Field	Description
MSTID	ID of a spanning tree instance in the MST region
Port	Port index
Role	Port role
STP State	STP state on the port, which can be forwarding and discarding.
Protection	Protection type of the port

display stp abnormalport

Syntax **display stp abnormalport**

View Any view

Parameter None

Description Use the **display stp abnormalport** command to display the ports that are blocked by STP guard functions.

Example # Display the ports that are blocked by STP guard functions.

```
<SW7750> display stp abnormalport
MSTID        Port                     Block Reason
--------- --------------------    -------------
  0          Ethernet1/0/20        Root-Protection
  1          Ethernet1/0/21        Loop-Protection
```

Table 42 Field descriptions of the **display stp abnormalport** command

Field	Description
MSTID	MST instance ID in the MST region
Port	Port number
Block Reason	The function blocking the port

display stp portdown

Syntax **display stp portdown**

View Any view

Parameter

None

Description

Use the **display stp portdown** command to display the ports that are shut down by STP guard functions.

Example

Display the ports that are shut down by STP guard functions.

```
<SW7750> display stp portdown
Port                  Down Reason
--------------------  ------------
Ethernet1/0/20        BPDU-Protection
```

Table 43 Field descriptions of the **display stp portdown** command

Field	Description
Port	Port number
Down Reason	The function shutting down 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 display the activated MST region configuration, including the region name, region revision level, and spanning tree instance-to-VLAN mappings configured for the switch.

Related command:

stp region-configuration.

Example

Display the activated MST region configuration.

```
<SW7750> display stp region-configuration
Oper Configuration
   Format selector :0
   Region name     :hello
   Revision level  :0

   Instance   Vlans Mapped
      0       21 to 4094
      1       1 to 10
      2       11 to 20
```

Table 44 Field descriptions of the **display stp region-configuration** command

Field	Description
Format selector	The selector specified by MSTP
Region name	The name of the MST region
Revision level	The revision level of the MST region
Instance Vlans Mapped	Spanning tree instance-to-VLAN mappings in the MST region

display stp root

Syntax **display stp root**

View Any view

Parameter None

Description Use the **display stp root** command to display information about the root ports in the MSTP region where the switch resides.

Example # Display information about the root ports in the MSTP region where the switch resides.

```
<SW7750> display stp root
  MSTID   Root Bridge ID        ExtPathCost  IntPathCost   Root Port
--------  ------------------- ------------  ------------- -----------
  0       32768.00e0-fc53-d908  0            200           Ethernet1/0/18
```

Table 45 Field descriptions of the **display stp root** command

Field	Description
MSTID	MST instance ID in the MST region
Root Bridge ID	ID of the root bridge
ExtPathCost	Cost of the external path from the switch to the root bridge
IntPathCost	Cost of the internal path from the switch to the root bridge
Root Port	Root port

display stp root

Syntax **display stp root**

View Any view

Parameter None

Description Use the **display stp root** command to display information about the root ports in the MSTP region where the switch resides.

Example # Display information about the root ports in the MSTP region where the switch resides.

```
<SW7750> display stp root
  MSTID   Root Bridge ID        ExtPathCost  IntPathCost   Root Port
--------  ------------------- ------------  ------------- -----------
  0       32768.00e0-fc53-d908  0            200           Ethernet1/0/18
```

Table 46 Field descriptions of the **display stp root** command

Field	Description
MSTID	MST instance ID in the MST region

Table 46 Field descriptions of the **display stp root** command

Field	Description
Root Bridge ID	ID of the root bridge
ExtPathCost	Cost of the external path from the switch to the root bridge
IntPathCost	Cost of the internal path from the switch to the root bridge
Root Port	Root port

instance

Syntax **instance** *instance-id* **vlan** *vlan-list*

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

View MST region view

Parameter *instance-id*: ID of a spanning tree instance ranging from 0 to 16. A value of 0 specifies the CIST.

vlan-list: List of VLANs. You need to provide this argument in the form of *vlan-list* = { *vlan-id* [**to** *vlan-id*] }&<1-10>, where &<1-10> means that you can provide up to 10 VLAN IDs/VLAN ID ranges for this argument. Normally, a VLAN ID can be a number ranging from 1 to 4094. VLANs with their IDs beyond this range (if the switch supports this kind VLAN IDs), such as VLAN 4095, VLAN 4096, can only be mapped to the CIST (spanning tree instance 0).

Description Use the **instance** command to map specified VLANs to a specified spanning tree instance.

Use the **undo instance** command to remove the mappings from the specified VLANs to the specified spanning tree instance and remap the specified VLANs to the CIST (spanning tree instance 0). If you specify no VLAN in the **undo instance** command, all VLANs that are mapped to the specified spanning tree instance are remapped to the CIST.

By default, all VLANs are mapped to the CIST.

VLAN-to-spanning tree instance mappings are recorded in the VLAN mapping table of an MSTP switch. So these two commands are actually used to manipulate the VLAN mapping table. You can add/remove a VLAN to/from the VLAN mapping table of a specific spanning tree instance by using these two commands.

Note that a VLAN cannot be mapped to multiple spanning tree instances at the same time. A VLAN-to-spanning tree instance mapping is automatically removed if you map the VLAN to another spanning tree instance.

Related command: **region-name**, **revision-level**, **vlan-mapping modulo**, **check region-configuration**, and **active region-configuration**.

Example # Map VLAN 2 to spanning tree instance 1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] stp region-configuration
[SW7750-mst-region] instance 1 vlan 2
```

region-name

Syntax **region-name** *name*

undo region-name

View MST region view

Parameter *name*: MST region name to be set for the switch, a string of 1 to 32 characters.

Description Use the **region-name** command to set an MST region name for a switch.

Use the **undo region-name** command to revert to the default MST region name.

The default MST region name of a switch is its MAC address.

MST region name, along with VLAN mapping table and MSTP revision level, determines the MST region which a switch belongs to.

Related command: **instance**, **revision-level**, **check region-configuration**, **vlan-mapping modulo**, and **active region-configuration**.

Example # Set the MST region name of the switch to "hello".

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] stp region-configuration
[SW7750-mst-region] region-name hello
```

reset stp

Syntax **reset stp** [**interface** *interface-list*]

View User view

Parameter *interface-list*: Ethernet port list. You can specify multiple Ethernet ports by providing this argument in the form of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-10>, where &<1-10> means that you can provide up to 10 port indexes/port index ranges for this argument.

Description Use the **reset stp** command to clear spanning tree-related statistics on Ethernet ports.

The spanning tree statistics include the numbers of the TCN BPDUs, configuration BPDUs, RST BPDUs, and MST BPDUs sent/received through one or more specified ports or all ports (note that STP BPDUs and TCN BPDUs are counted only for CISTs.)

This command clears the spanning tree-related statistics on specified ports if you specify the *interface-list* argument. If you do not specify the *interface-list* argument, this command clears the spanning tree-related statistics on all ports.

Related command: **display stp**.

Example # Clear the spanning tree-related statistics on ports Ethernet1/0/1 through Ethernet1/0/3.

```
<SW7750> reset stp interface Ethernet 1/0/1 to Ethernet 1/0/3
```

revision-level

Syntax **revision-level** *level*

undo revision-level

View MST region view

Parameter *level*: MSTP revision level to be set for the switch. This argument ranges from 0 to 75,535.

Description Use the **revision-level** command to set the MSTP revision level for a switch.

Use the **undo revision-level** command to revert to the default revision level.

By default, the MSTP revision level is 0.

MSTP revision level, along with MST region name and VLAN mapping table, determines the MST region which a switch belongs to.

Related command: **instance**, **region-name**, **check region-configuration**, **vlan-mapping modulo**, and **active region-configuration**.

Example # Set the MSTP revision level of the MST region to 5.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] stp region-configuration
[SW7750-mst-region] revision-level 5
```

stp

Syntax **stp** { **enable** | **disable** }

undo stp

View System view, Ethernet port view

Parameter **enable**: Enables MSTP globally or on a port.

disable: Disables MSTP globally or on a port.

Description Use the **stp** command to enable/disable MSTP globally or on a port.

Use the **undo stp** command to revert to the default MSTP state globally or on a port.

By default, MSTP is disabled globally and on a port.

By default, once MSTP is enabled globally, it is enabled on a port.

After MSTP is enabled, the actual operation mode, which can be STP-compatible mode, RSTP-compatible mode, and MSTP mode, is determined by the protocol mode configured by users. A switch becomes a transparent bridge if MSTP is disabled.

After being enabled, MSTP maintains spanning trees by processing configuration BPDUs of different VLANs. After being disabled, it stops maintaining spanning trees.

Related command: **stp mode**, and **stp interface**.

Example # Enable MSTP globally.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] stp enable
```

# Disable MSTP on Ethernet1/0/1 port.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface ethernet 1/0/1
[SW7750-Ethernet1/0/1] 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 guard function.

Use the **undo stp bpdu-protection** command to revert to the default state of the BPDU guard function.

By default, the BPDU guard function is disabled.

Normally, the access ports of the devices operating on the access layer directly connect to terminals (such as PCs) or file servers. These ports are usually configured as edge ports to achieve rapid transition. But they resume non-edge ports automatically upon receiving configuration BPDUs, which causes spanning trees regeneration and network topology jitter.

Normally, no configuration BPDU will reach edge ports. But malicious users can attack a network by sending configuration BPDUs deliberately to edge ports to cause network jitter. You can prevent this type of attacks by utilizing the BPDU guard function. With this function enabled on a switch, the switch shuts down the edge ports that receive configuration BPDUs and then reports these cases to the administrator. If a port is shut down, only the administrator can restore it.

Example # Enable the BPDU guard function.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] stp bpdu-protection
```

stp bridge-diameter

Syntax **stp bridge-diameter** *bridgenum*

undo stp bridge-diameter

View System view

Parameter *bridgenum*: Network diameter to be set for a switched network. This argument ranges from 2 to 7.

Description Use the **stp bridge-diameter** command to set the network diameter of a switched network. The network diameter of a switched network is represented by the maximum possible number of switches between any two terminals in a switched network.

Use the **undo stp bridge-diameter** command to revert to the default network diameter.

By default, the maximum number of switches between any two terminal devices in the switched network is 7.

After you configure the network diameter of a switched network, MSTP adjusts its Hello time, Forward delay, and Max age settings accordingly. With the network diameter set to 7 (the default), the three time-relate settings, Hello time, Forward delay, and Max age, are set to their defaults as well.

The **stp bridge-diameter** command only applies to CIST; it is invalid for MSTIs.

Related command: **stp timer forward-delay**, **stp timer hello**, and **stp timer max-age**.

Example # Set the network diameter to 5.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] stp bridge-diameter 5
```

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 the digest snooping feature.

Use the **undo stp config-digest-snooping** command to disable the digest snooping feature.

The digest snooping feature is disabled by default.

According to IEEE 802.1s, two connected switches can interwork with each other through MSTIs in an MST region only when the two switches have the same MST region-related configuration. With MSTP employed, interconnected switches determine whether or not they are in the same MST region by checking the configuration IDs of the BPDUs between them. (A configuration ID contains information such as region ID and configuration digest.)

As some partners' switches adopt proprietary spanning tree protocols, they cannot interwork with other switches in an MST region even if they are configured with the same MST region-related settings as other switches in the MST region.

This kind of problems can be overcome by implementing the digest snooping feature. If a switch port is connected to a partner's switch that has the same MST region-related settings but adopts a proprietary spanning tree protocol, you can enable digest snooping on the port. Then the switch regards the peer switch connected to the port as in the same region and records the configuration digests carried in the BPDUs received from the switch, which will be put in the BPDUs to be send to the peer switch.. In this way, the switch can interwork with the partners' switches in an MST region.

- *The digest snooping feature is needed only when your Switch 7750 is connected to partner's proprietary protocol-adopted switches.*
- *To enable the digest snooping feature successfully, you must first enable it on all the switch ports that connect to partner's proprietary protocol-adopted switches and then enable it globally.*

- *To enable the digest snooping feature, the interconnected switches must be configured with exactly the same MST settings.*
- *The digest snooping feature must be enabled on all the switch ports that connect to partners' proprietary protocol-adopted switches in the same MST region.*
- *With the digest snooping feature enabled, the VLAN-to-MSTI mapping cannot be modified.*
- *The digest snooping feature is not applicable to MST region edge ports.*

Example # Enable the digest snooping feature for Ethernet1/0/1 port.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet1/0/1
[SW7750-Ethernet1/0/1] stp config-digest-snooping
[SW7750-Ethernet1/0/1] quit
[SW7750]stp config-digest-snooping
```

stp cost

Syntax **stp** [**instance** *instance-id*] **cost** *cost*

undo stp [**instance** *instance-id*] **cost**

View Ethernet port view

Parameter *instance-id*: ID of a spanning tree instance ranging from 0 to 16. A value of 0 specifies the CIST.

cost: Path cost to be set for the port. This argument ranges from 1 to 200,000.

Description Use the **stp cost** command to set the path cost of the current port in a specified spanning tree instance.

Use the **undo stp cost** command to revert to the default path cost of the current port in the specified spanning tree instance.

By default, a switch automatically calculates the path costs of a port in different spanning tree instances based on a specified standard.

If you specify the *instance-id* argument to be 0 or do not specify this argument, the **stp cost** command sets the path cost of the port on CIST.

The path costs of a port in spanning tree instances affect the roles of the ports in the spanning tree instances. By configuring different path costs for the same port in different MSTIs, you can make flows of different VLANs traveling along different physical links, so as to achieve VLAN-based load balancing. Changing the path cost of a port in a spanning tree instance may change the role of the port in the instance and put it in state transition.

Related command: **stp interface cost**.

Example # Set the path cost of Ethernet1/0/3 port in spanning tree instance 2 to 200.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface ethernet1/0/3
[SW7750-Ethernet1/0/3] 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 Ethernet port as an edge port.

disable: Configures the current Ethernet 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 current Ethernet port to its default state.

By default, all Ethernet ports of a switch are non-edge ports.

An edge port is a port that is directly connected to a user terminal instead of another switch or a network segment. Rapid transition is applied to edge ports because, on these ports, no loops can be incurred by network topology changes. You can enable a port to transit to the forwarding state rapidly by setting it to an edge port. And you are recommended to configure the Ethernet ports directly connected to user terminals as edge ports to enable them to transit to the forwarding state rapidly.

Normally, configuration BPDUs cannot reach an edge port because the port is not connected to another switch. But when the BPDU guard function is disabled on an edge port, configuration BPDUs sent deliberately by a malicious user may reach the port. If an edge port receives a BPDU, it turns to a non-edge port.

Related command: **stp interface edged-port**.

CAUTION*: Among loop guard function, root guard function and edge port setting, only one can be valid on a port at one time.*

Example # Configure Ethernet1/0/1 port as a non-edge port.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface ethernet1/0/1
[SW7750-Ethernet1/0/1] stp edged-port disable
```

stp interface

Syntax **stp interface** *interface-list* { **enable** | **disable** }

View System view

Parameter *interface-list*: Ethernet port list. You can specify multiple Ethernet ports by providing this argument in the form of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-10>, where &<1-10> means that you can provide up to 10 port indexes/port index ranges for this argument.

enable: Enables MSTP on the specified ports.

disable: Disables MSTP on the specified ports.

Description Use the **stp interface** command to enable or disable MSTP on specified ports in system view.

By default, MSTP is enabled on the ports of a switch if MSTP is globally enabled on the switch, and is disabled on the ports if MSTP is globally disabled.

An MSTP-disabled port does not participate in any calculation of spanning tree and is always in forwarding state.

⚠ ***CAUTION:*** *Disabling MSTP on ports may result in loops.*

Related command: **stp mode**, **stp**.

Example # Enable MSTP on Ethernet1/0/1 port in system view.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] stp interface Ethernet 1/0/1 enable
```

stp interface config-digest-snooping

Syntax **stp interface** *interface-list* **config-digest-snooping**

undo stp interface *interface-list* **config-digest-snooping**

View System view

Parameter

interface-list: Ethernet port list. You can specify multiple Ethernet ports by providing this argument in the format of *interface-list* ={ *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-10>, where &<1-10> means that you can provide up to 10 port indexes/port index ranges for this argument.

Description

Use the **stp interface config-digest-snooping** command to enable the digest snooping feature.

Use the **undo stp interface config-digest-snooping** command to disable the digest snooping feature.

By default, the digest snooping feature is disabled.

According to IEEE 802.1s, two interconnected MSTP switches can interwork with each other through MSTIs in an MST region only when the two switches have the same MST region-related configuration. Interconnected MSTP switches determine whether or not they are in the same MST region by checking the configuration IDs of the BPDUs between them. (A configuration ID contains information such as region ID and configuration digest.)

As some partners' switches adopt proprietary spanning tree protocols, they cannot interwork with other switches in an MST region even if they are configured with the same MST region-related settings as other switches in the MST region.

This problem can be overcome by implementing the digest snooping feature. If a port on a Switch 7750 is connected to a partner's switch that has the same MST region-related settings as its own but adopts a proprietary spanning tree protocol, you can enable digest snooping on the port. Then the Switch 7750 regards the partner's switch as in the same region; it records the configuration digests carried in the BPDUs received from the partner's switch, and put them in the BPDUs to be send to the partner's switch. In this way, the Switch 7750es can interwork with the partners' switches in the same MST region.

- *The digest snooping feature is needed only when your Switch 7750 is connected to partner's proprietary protocol-adopted switches.*
- *To enable the digest snooping feature successfully, you must first enable it on all the ports of your Switch 7750 that are connected to partner's proprietary protocol-adopted switches and then enable it globally.*
- *To enable the digest snooping feature, the interconnected switches must be configured with exactly the same MST region-related configuration.*
- *The digest snooping feature must be enabled on all the ports of your Switch 7750 that are connected to partners' proprietary protocol-adopted switches in the same MST region.*
- *With the digest snooping feature enabled, the VLAN-to-MSTI mapping cannot be modified.*
- *The digest snooping feature is not applicable to MST region edge ports.*

Example

Enable the digest snooping feature on Ethernet1/0/1 port in system view.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] stp interface Ethernet 1/0/1 config-digest-snooping
```

stp interface 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. You can specify multiple Ethernet ports by providing this argument in the form of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-10>, where &<1-10> means that you can provide up to 10 port indexes/port index ranges for this argument.

instance-id: Spanning tree instance ID ranging from 0 to 16. A value of 0 specifies the CIST.

cost: Port path cost to be set. This argument ranges from 1 to 200,000,000.

Description Use the **stp interface cost** command to set the path cost(s) of the specified port(s) in a specified spanning tree instance in system view.

Use the **undo stp interface cost** command to revert to the default path cost(s) of the specified port(s) in the specified spanning tree instance in system view.

By default, a switch automatically calculates the path costs of a port in different spanning tree instances based on a specified standard.

If you specify the *instance-id* argument to be 0 or do not specify this argument, the **stp interface cost** command sets the path cost(s) of the specified port(s) in the CIST.

The path costs of a port in spanning tree instances affect the roles of the ports in the spanning tree instances. By configuring different path costs for the same port in different MSTIs, you can make flows of different VLANs traveling along different physical links, so as to achieve VLAN-based load balancing. Changing the path cost of a port in a spanning tree instance may change the role of the port in the instance and put it in state transition.

The default port path cost differs with port speed. Refer to Table 47 for details.

Related command: **stp cost**.

Example # Set the path cost of Ethernet1/0/3 port in spanning tree instance 2 to 400 in system view.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] stp instance 2 interface Ethernet 1/0/3 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. You can specify multiple Ethernet ports by providing this argument in the form of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-10>, where &<1-10> means that you can provide up to 10 port indexes/port index ranges for this argument.

enable: Configures the specified Ethernet ports to be edge ports.

disable: Configures the specified Ethernet ports to be non-edge ports.

Description

Use the **stp interface edged-port enable** command to configure the specified Ethernet port(s) as edge ports in system view.

Use the **stp interface edged-port disable** command to configure the specified Ethernet port(s) as non-edge ports in system view.

Use the **undo stp interface edged-port** command to restore the specified Ethernet port(s) to their default states.

By default, all Ethernet ports of a switch are non-edge ports.

An edge port is a port that is directly connected to a user terminal instead of another switch or a network segment. Rapid transition is applied to edge ports because, on these ports, no loops can be incurred by network topology changes. You can enable a port to transit to the forwarding state rapidly by setting it to an edge port. And you are recommended to configure the Ethernet ports directly connected to user terminals as edge ports to enable them to transit to the forwarding state rapidly.

Normally, configuration BPDUs cannot reach an edge port because the port is not connected to another switch. But when the BPDU guard function is disabled on an edge port, configuration BPDUs sent deliberately by a malicious user may reach the port. If an edge port receives a BPDU, it turns to a non-edge port.

Related command: **stp edged-port**.

CAUTION*: Among loop guard function, root guard function and edge port setting, only one can be valid on a port at one time.*

Example # Configure Ethernet1/0/3 port as an edge port in system view.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] stp interface Ethernet 1/0/3 edged-port enable
```

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. You can specify multiple Ethernet ports by providing this argument in the form of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-10>, where &<1-10> means that you can provide up to 10 port indexes/port index ranges for this argument.

Description Use the **stp interface loop-protection** command to enable the loop guard function in system view.

Use the **undo stp interface loop-protection** command to revert to the default state of the loop guard function in system view.

The loop guard function is disabled by default.

Related command: **stp loop-protection**.

⚠ ***CAUTION****: Among loop guard function, root guard function and edge port setting, only one can be valid on the same port.*

Example # Enable the loop guard function on Ethernet1/0/1 port.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] stp interface Ethernet 1/0/1 loop-protection
```

stp interface mcheck

Syntax **stp** [**interface** *interface-list*] **mcheck**

View System view

Parameter *interface-list*: Ethernet port list. You can specify multiple Ethernet ports by providing this argument in the form of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-10>, where &<1-10> means that you can provide up to 10 port indexes/port index ranges for this argument.

Description Use the **stp interface mcheck** command to perform the mCheck operation on specified port(s) in system view.

A port on an MSTP-enabled switch toggles to the STP-/RSTP-compatible mode automatically if an STP-/RSTP-enabled switch is connected to it. But when the STP-/RSTP-enabled switch is disconnected from the port, the port cannot toggle back to the MSTP mode automatically. In this case, you can force the port to toggle to the MSTP mode by performing the mCheck operation on the port.

Related command: **stp mcheck**, and **stp mode**.

Example # Perform the mCheck operation for Ethernet1/0/3 port in system view.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] stp interface Ethernet 1/0/3 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 the rapid transition feature on a specified port.

Use the **undo stp interface no-agreement-check** command to disable the rapid transition feature on a specified port.

The rapid transition feature is disabled on any port by default.

Some manufactures' switches adopt proprietary spanning tree protocols that are similar to RSTP in the way to implement rapid transition on designated ports. When a switch of this kind operates as the upstream switch of a Switch 7750 running MSTP, the upstream designated port fails to change their states rapidly.

The rapid transition feature is developed to avoid this case. When a Switch 7750 running MSTP is connected in the upstream direction to a manufacture's switch running proprietary spanning tree protocol, you can enable the rapid transition feature on the ports of the Switch 7750 operating as the downstream switch. Among these ports, those operating as the root ports will then send agreement packets to their upstream ports after they receive proposal packets from the upstream designated ports, instead of waiting for agreement packets from the upstream switch. This enables designated ports of the upstream switch to change their states rapidly.

Related command: **stp no-agreement-check**.

- *The rapid transition feature can be enabled on root ports or alternate ports only.*
- *If you configure the rapid transition feature on the designated port, the feature does not take effect on the port.*

Example # Enable the rapid transition feature for Ethernet1/0/1 port.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750]stp interface Ethernet1/0/1 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. You can specify multiple Ethernet ports by providing this argument in the form of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-10>, where &<1-10> means that you can provide up to 10 port indexes/port index ranges for this argument.

force-true: Specifies that the links connected to the specified Ethernet ports are point-to-point links.

force-false: Specifies that the links connected to the specified Ethernet ports are not point-to-point links.

auto: Specifies to automatically determine whether or not the links connected to the specified Ethernet ports are point-to-point links.

Description Use the **stp interface point-to-point** command to specify whether the links connected to the specified Ethernet ports are point-to-point links in system view.

Use the **undo stp interface point-to-point** command to restore the links connected to the specified ports to their default link types, which are automatically determined by MSTP.

If no keyword is specified in the **stp interface point-to-point** command, the **auto** keyword is used by default, and so MSTP automatically determines the types of the links connected to the specified ports.

The rapid transition feature is not applicable to ports on non-point-to-point links.

If an Ethernet port is the master port of an aggregated port or operates in full-duplex mode, the link connected to the port is a point-to-point link.

You are recommended to let MSTP automatically determine the link types.

These two commands only apply to CIST and MSTIs. If you configure the link to which a port is connected to be a point-to-point link (or a non-point-to-point link), the configuration applies to all spanning tree instances (that is, the port is configured to connect to a point-to-point link (or a non-point-to-point link) in all spanning tree instances). If the actual physical link is not a point-to-point link and you configure the link to which the port is connected to be a point-to-point link, loops may temporarily occur.

Related command: **stp point-to-point**.

Example # Configure the link connected to Ethernet1/0/3 port as a point-to-point link in system view.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] stp interface Ethernet 1/0/3 point-to-point force-true
```

stp interface 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. You can specify multiple Ethernet ports by providing this argument in the form of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-10>, where &<1-10> means that you can provide up to 10 port indexes/port index ranges for this argument.

instance-id: Spanning tree instance ID ranging from 0 to 16. A value of 0 specifies the CIST.

priority: Port priority to be set. This argument ranges from 0 to 240 and must be a multiple of 16 (such as 0, 16, and 32). The default port priority of a port in any spanning tree instance is 128.

Description Use the **stp interface port priority** command to set a port priority for the specified ports in the specified spanning tree instance.

Use the **undo stp interface port priority** command to restore the specified ports to the default port priority in the specified spanning tree instance.

If you specify the *instance-id* argument to be 0, these two commands apply to the port priorities on the CIST. The role a port plays in a spanning tree instance is determined by the port priority in the instance. A port on an MSTP-enabled switch can have different port priorities and play different roles in different MSTIs. This enables packets of different VLANs to be forwarded along different physical paths, so as to achieve load balancing by VLANs. Changing port priorities results in port roles being re-determined and may cause state transitions.

Related command: **stp port priority**.

Example # Set the port priority of Ethernet1/0/3 port (with regard to spanning tree instance 2) to 16.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] stp interface Ethernet 1/0/3 instance 2 port priority 16
```

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. You can specify multiple Ethernet ports by providing this argument in the form of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-10>, where &<1-10> means that you can provide up to 10 port indexes/port index ranges for this argument.

Description Use the **stp interface root-protection** command to enable the root guard function on specified port(s).

Use the **undo stp interface root-protection** command to restore the root guard function to the default state on specified port(s).

By default, the root guard function is disabled.

Configuration errors or attacks may result in configuration BPDUs with their priorities higher than that of a root bridge, which causes new root bridge to be elected and network topology jitter to occur. In this case, flows that should travel along high-speed links may be led to low-speed links, and network congestion may occur.

You can avoid this by utilizing the root guard function. Ports with this function enabled can only be kept as designated ports in all spanning tree instances. When a port of this type receives configuration BPDUs with higher priorities, it changes to Discarding state (rather than becomes a non-designated port) and stops forwarding packets (as if it is disconnected from the link). It resumes the normal state if it does not receive any configuration BPDUs with higher priorities for a specified period.

Related command: **stp root-protection**.

__CAUTION__: Among loop guard function, root guard function and edge port setting, only one can be valid on a port at one time.

Example # Enable the root guard function on Ethernet1/0/1 port.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] stp interface Ethernet 1/0/1 root-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. You can specify multiple Ethernet ports by providing this argument in the form of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-10>, where &<1-10> means that you can provide up to 10 port indexes/port index ranges for this argument.

packetnum: Also known as maximum transmitting speed, the maximum number of configuration BPDUs a port can send in each Hello time. This argument ranges from 1 to 255 and defaults to 3.

Description Use the **stp interface transmit-limit** command to set the maximum number of configuration BPDUs each specified port can send in each Hello time.

Use the **undo stp interface transmit-limit** command to revert to the default maximum number.

The larger the *packetnum* argument is, the more packets a port can transmit in each Hello time. Configure the *packetnum* argument to a proper value to limit the number of BPDUs a port can send in each Hello time to avoid MSTP from occupying too much network resources when network topology jitter occur.

Related command: **stp transmit-limit**.

Example # Set the maximum transmitting speed of Ethernet1/0/3 port to 5.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] stp interface Ethernet 1/0/3 transmit-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 the loop guard function on the current port.

Use the **undo stp loop-protection** command to restore the loop guard function to the default state on the current port.

By default, the loop guard function is disabled.

A switch maintains the states of the root port and other blocked ports by receiving and processing BPDUs from the upstream switch. These BPDUs may get lost because of network congestions and link failures. If a switch does not receive BPDUs from the upstream switch for a certain period, the switch selects a new root port; the original root port becomes a designated port; and the blocked ports transit to forwarding state. This may cause loops in the network.

The loop guard function suppresses loops. With this function enabled, if link congestions or link failures happen, a root port becomes a designated port, and the port state becomes discarding. The blocked port also becomes designated port and the port state becomes discarding (do not forward packets), and thereby loops can be prevented.

Example # Enable the loop guard function on Ethernet1/0/1 port.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet1/0/1
[SW7750-Ethernet1/0/1] stp loop-protection
```

stp max-hops

Syntax **stp max-hops** *hops*

undo stp max-hops

View System view

Parameter *hops*: Maximum hops to be set. This argument ranges from 1 to 40. The default maximum hops value of an MST region is 20.

Description Use the **stp max-hops** command to set the maximum hops for the MST region the current switch belongs to.

Use the **undo stp max-hops** command to revert to the default maximum hops.

The maximum hops values configured on the region roots of the CIST and MSTI in an MST region limit the size of the MST region.

A configuration BPDU contains a field that maintains the remaining hops of the configuration BPDU. And a switch discards the configuration BPDUs whose remaining hops are 0. After a configuration BPDU reaches a root bridge of a spanning tree in a MST region, the value of the remaining hops field in the configuration BPDU is decreased by 1 every time the configuration BPDU passes a switch. Such a mechanism disables the switches that are beyond the maximum hops from participating in spanning tree generation, and thus limits the size of an MST region.

With such a mechanism, the maximum hops configured on the switch operating as the root bridge of the CIST or an MSTI in a MST region becomes the network diameter of the spanning tree, which limits the size of the spanning tree in the current MST region. The switches that are not root bridges in the MST region adopt the maximum hops settings of their root bridges.

Example # Set the maximum hops of the current MST region to 35.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] stp max-hops 35
```

stp mcheck

Syntax **stp mcheck**

View Ethernet port view

Parameter None

Description Use the **stp mcheck** command to perform the mCheck operation on the current port.

When a port on an MSTP-enabled upstream switch connects with an STP enabled downstream switch, the port transits to the STP-compatible mode. But when the STP enabled downstream switch is then replaced by an MSTP-enabled switch, the port cannot automatically transit to the MSTP mode but remains in the STP-compatible mode. In this case, you can force the port to transit to the MSTP mode by performing the mCheck operation on the port.

Similarly, when a port on an RSTP-compatible upstream switch connects with an STP-enabled downstream switch, the port transits to the STP-compatible mode. But when the STP enabled downstream switch is then replaced by an MSTP-enabled switch, the port cannot automatically transit to the MSTP mode but remains in the STP-compatible mode. In this case, you can force the port to transit to the MSTP-compatible mode by performing the mCheck operation on the port.

Related command: **stp mode**, **stp interface mcheck**.

Example # Perform the mCheck operation for Ethernet1/0/1 port.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet1/0/1
[SW7750-Ethernet1/0/1] stp mcheck
```

stp mode

Syntax **stp mode** { **stp** | **rstp** | **mstp** }

undo stp mode

View System view

Parameter **stp**: Enables the STP-compatible mode.

mstp: Enables the MSTP mode.

rstp: Enables RSTP-compatible.

Description Use the **stp mode** command to set the MSTP operation mode.

Use the **undo stp mode** command to revert to the default MSTP operation mode.

By default, a switch operates in MSTP mode.

To make a switch compatible with STP/RSTP, MSTP provides following three operation modes:

STP-compatible mode, where a switch sends out STP BPDU packets

RSTP-compatible mode, where a switch sends out RSTP BPDU packets

MSTP mode, where a switch sends out MSTP BPDU packets

Related command: **stp mcheck**, **stp**, **stp interface**, and **stp interface mcheck**.

Example # Configure the switch to operate in STP-compatible mode.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] 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 the rapid transition feature for a port.

Use the **stp no-agreement-check** command to disable the rapid transition feature.

By default, the rapid transition feature is disabled on a port.

Some manufactures' switches adopt proprietary spanning tree protocols that are similar to RSTP in the way to implement rapid transition on designated ports. When a switch of this kind operates as the upstream switch of a Switch 7750 running MSTP, the upstream designated port fails to change their states rapidly.

The rapid transition feature aims to resolve this problem. When a Switch 7750 running MSTP is connected in the upstream direction to a manufacture's switch running proprietary spanning tree protocol, you can enable the rapid transition feature on the ports of the Switch 7750 operating as the downstream switch. Among these ports, those operating as the root ports will then send agreement packets to their upstream ports after they receive proposal packets from the upstream designated ports, instead of waiting for agreement packets from the upstream switch. This enables designated ports of the upstream switch to change their states rapidly.

Related command: **stp interface no-agreement-check**.

- *The rapid transition feature can be enabled on root ports or alternate ports only.*
- *If you configure the rapid transition feature on the designated port, the feature does not take effect on the port.*

Example # Enable the rapid transition feature for Ethernet1/0/1 port.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750]interface Ethernet1/0/1
[SW7750-Ethernet1/0/1]stp no-agreement-check
```

stp pathcost-standard

Syntax **stp pathcost-standard** { **dot1d-1998** | **dot1t** | **legacy** }

undo stp pathcost-standard

View System view

Parameter **dot1d-1998**: Uses the IEEE 802.1D-1998 standard to calculate the default path costs of ports.

dot1t: Uses the IEEE 802.1t standard to calculate the default path costs of ports.

legacy: Uses the proprietary standard to calculate the default path costs of ports.

Description Use the **stp pathcost-standard** command to set the standard to be used to calculate the default path costs of the links connected to the switch.

Use the **undo stp pathcost-standard** command to specify to use the default standard.

By default, a switch uses the IEEE 802.1t standard to calculate the default path costs of ports.

Table 47 Transmission speeds and the corresponding path costs

Transmission speed	Operation mode (half-/full-duplex)	802.1D-1998	IEEE 802.1t	Standard defined by Private
0	-	75,535	200,000,000	200,000
10 Mbps	Half-duplex/Full-duplex	100	200,000	2,000
	Aggregated link 2 ports	95	1,000,000	1,800
	Aggregated link 3 ports	95	666,666	1,600
	Aggregated link 4 ports	95	500,000	1,400
100 Mbps	Half-duplex/Full-duplex	19	200,000	200
	Aggregated link 2 ports	15	100,000	180
	Aggregated link 3 ports	15	66,666	160
	Aggregated link 4 ports	15	50,000	140
1,000 Mbps	Full-duplex	4	200,000	20
	Aggregated link 2 ports	3	10,000	18
	Aggregated link 3 ports	3	6,666	16
	Aggregated link 4 ports	3	5,000	14
10 Gbps	Full-duplex	2	200,000	2
	Aggregated link 2 ports	1	1,000	1
	Aggregated link 3 ports	1	666	1
	Aggregated link 4 ports	1	500	1

Normally, when a port operates in full-duplex mode, the corresponding path cost is slightly less than that when the port operates in half-duplex mode.

When calculating the path cost of an aggregated link, the 802.1D-1998 standard does not take the number of the ports on the aggregated link into account, whereas the 802.1T standard does. The following formula is used to calculate the path cost of an aggregated link:

Path cost = 200,000 / link transmission speed,

Where the link transmission speed is the sum of the speeds of the unblocked ports on the aggregated link, which is measured in 100 Kbps.

Example # Configure to use the IEEE 802.1D-1998 standard to calculate the default path costs of ports.note2

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] stp pathcost-standard dot1d-1998
```

# Configure to use the IEEE 802.1t standard to calculate the default path costs of ports.note2

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] stp pathcost-standard dot1t
```

stp point-to-point

Syntax **stp point-to-point** { **force-true** | **force-false** | **auto** }

undo stp point-to-point

View Ethernet port view

Parameter **force-true**: Specifies that the link connected to the current Ethernet port is a point-to-point link.

force-false: Specifies that the link connected to the current Ethernet port is not a point-to-point link.

auto: Specifies to automatically determine whether or not the link connected to the current Ethernet port is a point-to-point link.

Description Use the **stp point-to-point** command to specify whether the link connected to the current Ethernet port is a point-to-point link.

Use the **undo stp point-to-point** command to restore the link connected to the current Ethernet port to its default link type, which is automatically determined by MSTP.

If no keyword is specified in the **stp point-to-point** command, the **auto** keyword is used by default, and so MSTP automatically determines the type of the link connected to the current port.

The rapid transition feature is not applicable to ports on non-point-to-point links.

If an Ethernet port is the master port of an aggregation port or operates in full-duplex mode, the link connected to the port is a point-to-point link.

You are recommended to let MSTP automatically determine the link types of ports.

These two commands only apply to CISTs and MSTIs. If you configure the link to which a port is connected is a point-to-point link (or a non-point-to-point link), the configuration applies to all spanning tree instances (that is, the port is configured to connect to a point-to-point link [or a non-point-to-point link] in all spanning tree instances). If the actual physical link is not a point-to-point link and you configure the link to which the port is connected to be a point-to-point link, loops may temporarily occur.

Related command: **stp interface point-to-point**.

Example # Configure the link connected to Ethernet1/0/3 port as a point-to-point link.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet1/0/3
[SW7750-Ethernet1/0/3] 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-id*: Spanning tree instance ID ranging from 0 to 16. A value of 0 specifies the CIST.

port priority *priority*: Sets the port priority. The *priority* argument ranges from 0 to 240 and must be a multiple of 16 (such as 0, 16, and 32). The default port priority of a port in any spanning tree instance is 128.

Description Use the **stp port priority** command to set the port priority of the current port in the specified spanning tree instance.

Use the **undo stp port priority** command to restore the current port to the default port priority in the specified spanning tree instance.

If you specify the *instance-id* argument to be 0 or do not specify the argument, these two commands apply to the port priorities on the CIST. The role a port plays in a spanning tree instance is determined by the port priority in the instance. A port on a MSTP-enabled switch can have different port priorities and play different roles in different MSTIs. This enables packets of different VLANs to be forwarded along different physical paths, so as to achieve load balancing by VLANs. Changing port priorities result in port roles being re-determined and may cause state transitions.

Related command: **stp interface port priority**.

Example # Set the port priority of Ethernet1/0/3 port in spanning tree instance 2 to 16.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet1/0/3
[SW7750-Ethernet1/0/3] stp instance 2 port priority 16
```

stp portlog

Syntax **stp** [**instance** *instance-id*] **portlog**

undo stp [**instance** *instance-id*] **portlog**

View System view

Parameter **instance** *instance-id*: Specifies a spanning tree instance ID, ranging from 0 to 16. The value of 0 indicates the CIST.

Description Use the **stp portlog** command to enable log and trap message output for the ports of a specified instance.

Use the **undo stp portlog** command to disable this function.

By default, log and trap message output is disabled.

Executing the **stp portlog** command (without using the **instance** *instance-id* parameters) will enable log and trap message output for the ports of instance 0.

Example # Enable log and trap message output for the ports of instance 1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] stp instance 1 portlog
```

stp portlog all

Syntax **stp portlog all**

undo stp portlog all

View System view

Parameter None

Description Use the **stp portlog all** command to enable log and trap message output for the ports of all instances.

Use the **undo stp portlog all** command to disable this function.

By default, log and trap message output is disabled on the ports of all instances.

Example # Enable log and trap message output for the ports of all instances.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] stp portlog all
```

stp priority

Syntax

stp [**instance** *instance-id*] **priority** *priority*

undo stp [**instance** *instance-id*] **priority**

View

System view

Parameter

instance-id: Spanning tree instance ID ranging from 0 to 16. A value of 0 specifies the CIST.

priority: Switch priority to be set. This argument ranges from 0 to 61,440 and must be a multiple of 4,096 (such as 0, 4,096, and 8,192). There are totally 16 available switch priorities.

Description

Use the **stp priority** command to set the priority of the switch in the specified spanning tree instance.

Use the **undo stp priority** command to restore the switch to the default priority in the specified spanning tree instance.

The default priority of a switch is 32,768.

The priorities of switches are used for spanning tree generation. Switch priorities are spanning tree-specific. That is, you can set different priorities for the same switch in different spanning tree instances.

If you do not specify the *instance-id* argument, the two commands apply to the CIST.

Example

Set the priority of the switch in spanning tree instance 1 to 4,096.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] stp instance 1 priority 4096
```

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 revert to the default MST region-related settings.

MST region-related settings include: region name, revision level, and VLAN mapping table. The three MST region-related settings default to:

- MST region name: The first MAC address of the switch
- VLAN mapping table: All VLANs are mapped to the CIST.
- MSTP revision level: 0

And you can modify the three settings after entering MST region view by using the **stp region-configuration** command.

Example # Enter MST region view.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] stp region-configuration
[SW7750-mst-region]
```

stp root primary

Syntax **stp** [**instance** *instance-id*] **root primary** [**bridge-diameter** *bridgenum* [**hello-time** *centi-seconds*]]

undo stp [**instance** *instance-id*] **root**

View System view

Parameter *instance-id*: Spanning tree instance ID ranging from 0 to 16. A value of 0 specifies the CIST.

bridgenum: Network diameter of the specified spanning tree. This argument ranges from 2 to 7 and defaults to 7.

centi-seconds: Hello time (in centiseconds) of the specified spanning tree. This argument ranges from 100 to 1,000 and defaults to 200.

Description Use the **stp root primary** command to configure the current switch as the root bridge of a specified spanning tree instance.

Use the **undo stp root** command to cancel the current configuration.

By default, a switch is not configured as a root bridge.

If you do not specify the *instance-id* argument, these two commands apply to the CIST.

You can specify the current switch as the root bridge of a spanning tree instance regardless of the priority of the switch. You can also specify the network diameter of the switched network by using the **stp root primary** command. The switch will then figure out the following three time parameters: Hello time, Forward delay, and Max age. As the Hello time figured out by the network diameter is not always the optimal one, you can set it manually through the **hello-time** *centi-seconds* parameter. Normally, you are recommended to set the network diameter and leave the Forward delay and Max age parameters being automatically determined by the network diameter you set.

CAUTION:

- *You can configure only one root bridge for a spanning tree instance and can configure one or more secondary root bridges for a spanning tree instance. Configuring multiple root bridges for a spanning tree instance causes unpredictable spanning tree computing results.*
- *Once a switch is configured as the root bridge or a secondary root bridge, its priority cannot be modified.*

Example # Configure the current switch as the root bridge of spanning tree instance 1, setting the network diameter of the switched network to 4, and the Hello time to 500 centiseconds.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] stp instance 1 root primary bridge-diameter 4 hello-time 50
0
```

stp root secondary

Syntax **stp** [**instance** *instance-id*] **root secondary** [**bridge-diameter** *bridgenum*] [**hello-time** *centi-seconds*]]

undo stp [**instance** *instance-id*] **root**

View System view

Parameter *instance-id*: Spanning tree instance ID ranging from 0 to 16. A value of 0 specifies the CIST.

bridgenum: Network diameter of the specified spanning tree. This argument ranges from 2 to 7 and defaults to 7.

centi-seconds: Hello time in centiseconds of the specified spanning tree. This argument ranges from 100 to 1,000 and defaults to 200.

Description Use the **stp root secondary** command to configure the current switch as a secondary root bridge of a specified spanning tree instance.

Use the **undo stp root** command to cancel the current configuration.

By default, a switch does not operate as a secondary root bridge.

If you do not specify the *instance-id* argument, these two commands apply to the CIST.

You can configure one or more secondary root bridges for a spanning tree instance. If the switch operating as the root bridge fails or is turned off, the secondary root bridge with the least MAC address becomes the root bridge.

You can also specify the network diameter and the Hello time of the switch that you are configuring as a secondary root bridge. The switch will then figures out the other two time parameters: Forward delay and Max age. You can configure only one root bridge for a spanning tree instance but you can configure one or more secondary root bridges for a spanning tree instance. Once a switch is configured as the root bridge or a secondary root bridge, its priority cannot be modified.

Example

Configure the current switch as a secondary root bridge of spanning tree instance 4, setting the network diameter of the switched network to 5 and the Hello time to 300 centiseconds.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] stp instance 4 root secondary bridge-diameter 5 hello-time
300
```

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 the root guard function on the current port.

Use the **undo stp root-protection** command to restore the root guard function to the default state on the current port.

By default, the root guard function is disabled.

Configuration errors or attacks may result in configuration BPDUs with their priorities higher than that of a root bridge, which causes new root bridge to be elected and network topology jitter to occur. In this case, flows that are to travel along high-speed links may be led to low-speed links, and network congestion may occur.

You can avoid this by utilizing the root guard function. Ports with this function enabled can only be kept as designated ports in all spanning tree instances. When a port of this type receives configuration BPDUs with higher priorities, it changes to Discarding state (rather than becomes a non-designated port) and stops forwarding packets (as if it is disconnected from the link). It resumes the normal state if it does not receive any configuration BPDUs with higher priorities for a specified period.

Related command: **stp interface root-protection**.

Example # Enable the root guard function on Ethernet1/0/1 port.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet1/0/1
[SW7750-Ethernet1/0/1] 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 TC-BPDU attack guard function.

Use the **stp tc-protection disable** command to disable the TC-BPDU attack guard function.

By default, the TC-BPDU attack guard function is enabled. The operation of removing MAC address tables can be executed for up to six times within 10 seconds.

Normally, upon receiving a TC-BPDU, a switch removes its local MAC address table and then updates its ARP address table based on STP instances according to the updated MAC address table. If a malicious user forges TC-BPDUs to attack a switch, the switch will receive a large amount of TC-BPDUs in a short period, so that the switch will be busy in removing local MAC address tables and updating ARP address tables, which will affect STP calculation and occupy a large amount of network bandwidth. As a result, the CPU utilization stays high for the switch.

With the TC-BPDU attack guard function enabled, the switch performs the operation of removing its MAC address table once upon receiving a TC-BPDU, and triggers a timer with the period of 10 seconds at the same time. If the switch receives more TC-BPDUs within this period, the switch can perform the operation of removing MAC address tables for up to six times. Such a mechanism prevents the switch from removing MAC address tables frequently and the subsequent negative effect.

Example # Enable the TC-BPDU guard function on the switch.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] stp tc-protection enable
```

stp tc-protection threshold

Syntax **stp tc-protection threshold** *number*

undo stp tc-protection threshold

View System view

Parameter *number*: Upper threshold of the times for a switch to process TC-BPDUs within 10 seconds, in the range 1 to 255.

Description Use the **stp tc-protection threshold** command to set the upper threshold of the times for a switch to remove its MAC address table within 10 seconds.

Use the **undo stp tc-protection threshold** command to cancel the configuration.

Normally, upon receiving a TC-BPDU, a switch removes its local MAC address table and then updates the ARP address table based on STP instances according to the updated MAC address table. If a malicious user forges TC-BPDUs to attack a switch, the switch will receive a large amount of TC-BPDUs in a short period, so that the switch will be busy in removing local MAC address tables and updating ARP address tables, which will affect STP calculation and occupy a large amount of network bandwidth. As a result, the CPU utilization stays high for the switch.

With the TC-BPDU attack guard function enabled, the switch performs the operation of removing the local MAC address table only once after it receives a TC-BPDU, and triggers a timer with the period of 10 seconds at the same time. If the switch receives more TC-BPDUs within this period, the switch can perform the operation of removing MAC address entries for up to six times. Such a mechanism prevents the switch from removing MAC address tables frequently and the subsequent negative effect.

You can use the **stp tc-protection threshold** command to set the upper threshold of the times for a switch to remove its MAC address table in the period set by the timer. If the number of received TC-BPDUs is less than the specified upper threshold, the switch will remove its MAC address table upon receiving a TC-BPDU. If the number of received TC-BPDUs is more than the specified upper threshold, the switch will remove its MAC address table for the times equal to the specified upper threshold. For example, if you set the upper threshold for the times for the switch to remove its MAC address table to 100 in the specified period, while the switch receives 200 TC-BPDUs in the period. In this case, the switch removes its MAC address table for only 100 times within the period.

Example # Specify the switch to remove its MAC address table for up to five times within 10 seconds.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] stp tc-protection threshold 5
```

stp timer forward-delay

Syntax

stp timer forward-delay *centi-seconds*

undo stp timer forward-delay

View

System view

Parameter

centi-seconds: Forward delay in centiseconds to be set. This argument ranges from 400 to 3,000 and defaults to 1,500.

Description

Use the **stp timer forward-delay** command to set the Forward delay of the switch.

Use the **undo stp timer forward-delay** command to revert to the default Forward delay.

To prevent the occurrence of temporary loops, when a port changes its state from discarding to forwarding, it undergoes an intermediate state and waits for a specific period to synchronize with the remote switches. This state transition period is determined by the Forward delay configured on the root bridge.

The Forward delay setting configured on a root bridge applies to all switches operating in the same spanning tree instance.

As for the configuration of the three time-related parameters (that is, the Hello time, Forward delay, and Max age parameters), the following formulas must be met to prevent network jitter.

2 x (Forward delay - 1 second) >= Max age

Max age >= 2 x (Hello time + 1 second)

You are recommended to specify the network diameter of the switched network and the Hello time by using the **stp root primary** or **stp root secondary** command. After that, the three proper time-related parameters are automatically determined.

Related command:

stp timer hello, **stp timer max-age**, and **stp bridge-diameter**.

Example

Set the Forward delay to 2,000 centiseconds.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] stp timer forward-delay 2000
```

stp timer hello

Syntax

stp timer hello *centi-seconds*

undo stp timer hello

View System view

Parameter *centi-seconds*: Hello time in centiseconds to be set. This argument ranges from 100 to 1,000 and defaults to 200.

Description Use the **stp timer hello** command to set the Hello time of the switch.

Use the **undo stp timer hello** command to revert to the default Hello time.

A root bridge regularly sends out configuration BPDUs to maintain the existing spanning trees. The Hello time is used to set the sending interval. When a switch becomes a root bridge, it regularly sends BPDUs at the interval specified by the hello time you have configured on it. While, the other none-root-bridge switches listen to the BPDUs; if they do not receive a BPDU in a specific period, spanning trees will be regenerated.

As for the configuration of the three time-related parameters (that is, the Hello time, Forward delay, and Max age parameters), the following formulas must be met to prevent network jitter.

2 * (Forward delay - 1 second) >= Max age

Max age >= 2 * (Hello time + 1 second)

You are recommended to specify the network diameter of the switched network and the Hello time by using the **stp root primary** or **stp root secondary** command. After that, the three proper time-related parameters are automatically determined.

Related command: **stp timer forward-delay**, **stp timer max-age**, and **stp bridge-diameter**.

Example # Set the Hello time to 400 centiseconds.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] stp timer hello 400
```

stp timer max-age

Syntax **stp timer max-age** *centi-seconds*

undo stp timer max-age

View System view

Parameter *centi-seconds*: Max age in centiseconds to be set. This argument ranges from 600 to 4,000 and defaults to 2,000.

Description Use the **stp timer max-age** command to set the Max age of the switch.

Use the **undo stp timer max-age** command to revert to the default Max age.

MSTP is capable of detecting link problems and automatically restoring redundant links to forwarding state. In CIST, switches use the Max age parameter to judge whether or not a received configuration BPDU times out. And spanning trees will be regenerated if a configuration BPDU received by a port times out.

The Max age is meaningless to MSTIs. The Max age configured for the root bridge of the CIST applies to all switches operating on the CIST, including the root bridge.

As for the configuration of the three time-related parameters (that is, the Hello time, Forward delay, and Max age parameters), the following formulas must be met to prevent network jitter.

2 * (Forward delay - 1 second) >= Max age,

Max age >= 2 * (Hello time + 1 second).

You are recommended to specify the network diameter of the switched network and the Hello time parameter by using the **stp root primary** or **stp root secondary** command. After that, the three proper time-related parameters are automatically determined.

Related command: **stp timer forward-delay**, **stp timer hello**, and **stp bridge-diameter**.

Example # Set the Max age to 1,000 centiseconds.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] stp timer max-age 1000
```

stp timer-factor

Syntax **stp timer-factor** *number*

undo stp timer-factor

View System view

Parameter *number*: Hello time factor. This argument ranges from 1 to 20 and defaults to 3.

Description Use the **stp timer-factor** command to set the timeout time of MSTP protocol packets on a switch in the form of a multiple of the Hello time. For example, with the *number* argument set to 3, the timeout time is three times of the Hello time.

Use the **undo stp timer-factor** command to revert to the default Hello time factor.

A switch regularly sends protocol packets to its neighboring devices at the interval specified by the Hello time parameter to test the links. Normally, a switch regards its upstream switch faulty if the former does receive any protocol packets from the latter in a period three times of the Hello time and then initiates the spanning tree regeneration process.

Spanning trees may be regenerated even in a steady network if an upstream switch continues to be busy. You can configure the timeout time factor to a larger number to avoid this. Normally, the timeout time can be four (or more) times of the Hello time. For a steady network, the timeout time can be five to seven times of the Hello time.

Example # Set the Hello time factor to 7.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] stp timer-factor 7
```

stp transmit-limit

Syntax **stp transmit-limit** *packetnum*

undo stp transmit-limit

View Ethernet port view

Parameter *packetnum*: Maximum number of configuration BPDUs a port can transmit in each Hello time. This argument ranges from 1 to 255 and defaults to 5.

Description Use the **stp transmit-limit** command to set the maximum number of configuration BPDUs the current port can transmit in each Hello time.

Use the **undo stp transmit-limit** command to revert to the default maximum number.

A larger number configured by the **stp transmit-limit** command allows more configuration BPDUs can be transmitted in each Hello time, which may occupy more switch resources. So configure it to a proper value to avoid MSTP from occupying too many network resources.

Related command: **stp interface transmit-limit**.

Example # Set the maximum number of configuration BPDUs that can be transmitted by the Ethernet1/0/1 port in each Hello time to 15.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet1/0/1
[SW7750-Ethernet1/0/1] stp transmit-limit 15
```

vlan-mapping modulo

Syntax **vlan-mapping modulo** *modulo*

View MST region view

Parameter *modulo*: Modulo ranging from 1 to 16.

Description Use the **vlan-mapping modulo** command to map VLANs to specific spanning tree instances.

By default, all VLANs in a network are mapped to the CIST (spanning tree instance 0).

MSTP uses a VLAN mapping table to describe VLAN-to-spanning-tree-instance mappings. You can use this command to establish the VLAN mapping table and to map VLANs to specific spanning tree instances.

Note that a VLAN cannot be mapped to multiple different spanning tree instances at the same time. A VLAN-to-spanning-tree-instance mapping becomes invalid when you map the VLAN to another spanning tree instance.

*You can map VLANs to specific spanning tree instances quickly by using the **vlan-mapping modulo** modulo command. The ID of the spanning tree instance to which a VLAN is mapped can be figured out by using the following expression:*

(VLAN ID-1) % *modulo* + 1,

Where (VLAN ID-1) % *modulo* yields the module of (VLAN ID-1) with regards to *modulo*. For example, if you set the *modulo* argument to 16, then VLAN 1 is mapped to spanning tree instance 1, VLAN 2 is mapped to spanning tree instance 2, ..., VLAN 16 is mapped to spanning tree instance 16, VLAN 17 is mapped to spanning tree instance 1, and so on.

Related command: **check region-configuration**, **revision-level**, **region-name**, and **active region-configuration**.

Example # Map VLANs to spanning tree instances, with the modulo being 16.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] stp region-configuration
[SW7750-mst-region] vlan-mapping modulo 16
```

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 the BPDU Tunnel function for a switch.

Use the **undo vlan-vpn tunnel** command to disable the BPDU Tunnel function.

The BPDU Tunnel function enables BPDUs to be transparently transmitted between geographically dispersed user networks through specified VLAN VPNs in operator's networks, through which spanning trees can be generated across these user networks and are independent of those of the operator's network.

By default, the BPDU Tunnel function is disabled.

- *The BPDU Tunnel function can only be enabled on devices with STP employed.*
- *The BPDU Tunnel function can only be enabled on access ports.*
- *To enable the BPDU Tunnel function, make sure the links between operator's networks are trunk links.*
- *As the VLAN-VPN function is unavailable on ports with 802.1x, GVRP, GMRP, STP, or NTDP employed, the BPDU Tunnel function is not applicable to these ports.*

Example # Enable the BPDU Tunnel function for the switch.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] vlan-vpn tunnel
```

28 Routing Table Monitoring Commands

The words "router" covered in the following text represent routers in common sense and Ethernet switches running a routing protocol. To improve readability, this will not be mentioned again in this manual.

display ip routing-table

Syntax **display ip routing-table**

View Any view

Parameter None

Description Use the **display ip routing-table** command to display the routing table summary.

This command displays the summary of the routing table. Each line represents one route, containing destination address/mask length, protocol, preference, cost, next hop, and output interface.

This command displays only the currently used routes, that is, the optimal routes.

Example # Display the summary of the current routing table.

```
<SW7750> 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 Field descriptions of the **display ip routing-table** command

Field	Description
Destination/Mask	Destination address/mask length
Protocol	Routing protocol
Pre	Route preference

Table 48 Field descriptions of the **display ip routing-table** command

Field	Description
Cost	Route cost
Nexthop	Next hop address
Interface	Output interface, through which the data packets destined for the destination network segment are sent

display ip routing-table acl

Syntax **display ip routing-table acl** { *acl-number* | *acl-name* } [**verbose**]

View Any view

Parameter *acl-number*: Number of the number-identified ACL, in the range of 2,000 to 2,999.

acl-name: Name of the basic name-identified ACL.

verbose: Displays the detailed information about active and inactive routes filtered by the ACL rules if this keyword is provided; displays the brief information about the active routes filtered by the ACL rules.

Description Use the **display ip routing-table acl** command to display the routes filtered by the basic ACL rules.

This command is mainly used to trace and display the routing policies, that is, to display the routes filtered by the rules based on the input basic ACL numbers.

Example # Display the brief information about the active routes filtered by the basic ACL 2000.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] acl number 2000
[SW7750-acl-basic-2000] rule permit source 10.1.1.1 0.0.0.255
[SW7750-acl-basic-2000] rule deny source any
[SW7750-acl-basic-2000] display ip routing-table acl 2000
Routes matched by access-list 2000:
  Summary count: 2
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
```

Refer to Table 48 for the description on the displayed information above.

# Display the detailed information about the active and inactive routes filtered by the basic ACL 2000.

```
<SW7750> display ip routing-table acl 2000 verbose
Routes matched by access-list 2000:
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: #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 Field descriptions of the **display ip routing-table acl** command

Field	Description
Destination	Destination address
Mask	Mask
Protocol	Routing protocol that detects this route
Preference	Preference of the route
Nexthop	Address of the next hop
Interface	Outbound interface where packets to the destination network segment are forwarded.
Vlinkindex	Virtual link index

Table 49 Field descriptions of the **display ip routing-table acl** command

Field	Description	
State	Route state:	
	ActiveU	Active unicast routes
	Blackhole	Blackhole routes, which are similar to Reject routes except that blackhole routes do not send ICMP unreachable messages to the source end of the packet.
	Delete	The route is deleted.
	Gateway	Indirectly reachable routes
	Hidden	If you do not want to remove some routes that are not available temporarily for some reasons (such as the configured polices, the port being down), you can hide the route so as to restore it later.
	Holddown	Holddown is a route redistribution policy adopted by some distance-vector (D-V) routing protocols such as RIP. Through Holddown, a routing protocol can avoid the flooding of error routes and deliver route unreachable messages accurately. It redistributes 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 the interior gateway protocol (IGP).
	NoAdvise	NoAdvise routes are nor released when the routing protocol ad
	NotInstall	Generally, the route with the highest preference in a routing table is added to the core routing table and released. Comparatively, noninstall routes cannot be added to the core routing table, however, they may be released.
	Reject	Reject route do not distribute packets as other routes. Instead, the packet that selects a reject route will be dropped, and ICMP unreachable messages will be sent to the source end of the packet. Reject routes are generally used in network tests.
	Retain	When the routes in the core routing table are removed, the routes with the retain tag will not be removed. You can tag some static routes as retain routes so that they can continue to exist in the core routing table.
	Static	The static routes manually configured on the route are tagged as static routes, which will not be removed from the routing table if the router is restarted after the **save** command is executed.
	Unicast	Unicast routes
Age	The time that a route exists in the routing table, expressed in the form of hh:mm:ss.	
Cost	Route 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 notation.

mask: IP address mask, length in dotted decimal notation or expressed as an integer. It ranges from 0 to 32 when expressed as an integer.

longer-match: Specifies all the routes that lead to the destination address and match the specified mask. If you do not specify the *mask* argument, those that match the natural mask are specified.

verbose: With the **verbose** argument specified, this command displays the verbose information of both the active and inactive routes. Without the argument specified, this command only displays the summary of active routes.

Description

Use the **display ip routing-table** *ip-address* command to display the routing information of the specified destination address.

With different arguments provided, the command output is different. The following is the command output with different arguments provided:

- **display ip routing-table** *ip-address*

If the destination address *ip-address* corresponds to a route in the natural mask range, this command displays the route that is the longest match of the destination address *ip-address* and is active.

- **display ip routing-table** *ip-address mask*

This command only displays the routes exactly matching the specified destination address and mask.

- **display ip routing-table** *ip-address* **longer-match**

This command displays all destination address routes matching the specified destination address in the natural mask range.

- **display ip routing-table** *ip-address mask* **longer-match**

This command displays all destination address routes matching the specified destination address in the specified mask range.

Example

There is a corresponding route in the natural mask range. Display the summary.

```
<SW7750> display ip routing-table 169.0.0.0
Destination/Mask        Protocol    Pre Cost    Nexthop     Interface
169.0.0.0/16            Static  60  0       2.1.1.1     LoopBack1
```

For detailed description of the output information, see Table 48.

# There is no corresponding route (only the longest matching route is displayed) in the natural mask range. Display the summary.

```
<SW7750> display ip routing-table 169.253.0.0
Destination/Mask       Protocol   Pre     Cost   Nexthop    Interface
169.0.0.0/8            Static      60      0     2.1.1.1    LoopBack1
```

# There are corresponding routes in the natural mask range. Display detailed information.

```
<SW7750> 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:2
**Destination: 169.0.0.0        Mask: 255.0.0.0
        Protocol: #Static       Preference: 60
        *NextHop: 2.1.1.1          Interface: 2.1.1.1(LoopBack1)
        Vlinkindex: 0
        State: <Int ActiveU Static Unicast>
        Age: 3:47   Cost: 0/0   Tag: 0
**Destination: 169.0.0.0        Mask: 255.254.0.0
        Protocol: #Static       Preference: 60
        *NextHop: 2.1.1.1          Interface: 2.1.1.1(LoopBack1)
        Vlinkindex: 0
        State: <Int ActiveU Static Unicast>
        Age: 3:47   Cost: 0/0   Tag: 0
```

# There is no corresponding route in the natural mask range (only the longest matched route is displayed). Display the detailed information.

```
<SW7750> display ip routing-table 169.253.0.0 verbose
Routing Tables:
  Generate Default: no
  + = Active Route, - = Last Active, # = Both   * = Next hop in use
  Summary count:1
**Destination: 169.0.0.0        Mask: 255.0.0.0
        Protocol: #Static       Preference: 60
        *NextHop: 2.1.1.1          Interface: 2.1.1.1(LoopBack1)
        Vlinkindex: 0
        State: <Int ActiveU Static Unicast>
        Age: 3:47   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* and *ip-address2, mask2* determine one address range together. .*ip-address1* ANDed with *mask1* specifies the start of the range, while *ip-address2* ANDed with *mask2* specifies the end. This command displays the route in this address range.

mask1, mask2: IP address mask, length in dotted decimal notation or expressed as an integer. It ranges from 0 to 32 when expressed as an integer.

verbose: With the **verbose** argument provided, this command displays the verbose information of both active and inactive routes. Without this argument provided, this command displays the summary of active routes only.

Description

Use the **display ip routing-table** *ip-address1 ip-address2* command to display the route information in the specified destination address range.

Example

Display the routing information of destination addresses ranging from 1.1.1.0 to 2.2.2.0.

```
<SW7750>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: Name of the IP address prefix list, containing 1 to 19 characters.

verbose: Displays the detailed information about active and inactive routes filtered by the ACL rules if this keyword is provided; displays the brief information about the active routes filtered by the ACL rules.

Description

Use the **display ip routing-table ip-prefix** command to display the routes filtered based on the specified ip-prefix list.

This command is mainly used to track and display the routing policy. It displays the routes filtered by the rules based on the input ip-prefix list name.

If the specified ip-prefix list does not exist, with the **verbose** keyword provided, this command displays the detailed information about all active and inactive routes; without the **verbose** argument keyword, this command displays the brief information about all active routes only.

Example

Display the brief information about the active routes filtered by the IP-prefix list named abc2, which permits the route with a prefix of 10.1.1.0 and a mask length of 24 to 32.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] ip ip-prefix abc2 permit 10.1.1.0 24 less-equal 32
[SW7750] 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        DIRECT     0     0       10.1.1.2        Vlan-interface1
10.1.1.2/32        DIRECT     0     0       127.0.0.1       InLoopBack0
```

For detailed information about the displayed information above, please refer to Table 48.

# Display the detailed information about the active and inactive routes filtered by the ip-prefix list named abc2.

```
[SW7750] 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: #DIRECT       Preference: 0
        *NextHop: 10.1.1.2         Interface: 10.1.1.2(Vlan-interface1)
        Vlinkindex: 0
        State: <Int ActiveU Retain Unicast>
        Age: 3:23:44    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: 3:23:44    Cost: 0/0       Tag: 0
```

For detailed description on the displayed information above, refer to Table 49.

display ip routing-table protocol

Syntax **display ip routing-table protocol** *protocol* [**inactive** | **verbose**]

View Any view

Parameter *protocol*: You can provide one of the following values for this argument.

- **direct**: Displays direct-connect route information
- **static**: Displays 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.

inactive: With this argument provided, this command displays the inactive route information. Without this argument provided, this command displays both active and inactive route information.

verbose: With this argument provided, this command displays the verbose route information. Without this argument provided, this command displays route summary only.

Description Use the **display ip routing-table protocol** command to display the route information of a specific protocol.

Example # Display the summary of all direct-connect routes.

```
<SW7750> display ip routing-table protocol direct
DIRECT Routing tables:
  Summary count: 8
DIRECT Routing table status:<active>:
  Summary count: 7
Destination/Mask   Protocol Pre  Cost        Nexthop     Interface
10.5.1.0/24        DIRECT   0    0        10.5.1.5     Vlan-interface105
10.5.1.5/32        DIRECT   0    0       127.0.0.1     InLoopBack0
100.100.1.1/32     DIRECT   0    0       127.0.0.1     InLoopBack0
102.1.1.0/24       DIRECT   0    0       102.1.1.1     LoopBack1
102.1.1.1/32       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 table status:<inactive>:
  Summary count: 1
Destination/Mask   Protocol Pre  Cost        Nexthop       Interface
100.100.1.1/32     DIRECT   0    0           100.100.1.1   LoopBack0
```

# Display the static routing table.

```
<SW7750> 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
```

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 display the route information in a tree structure.

Example

```
<SW7750> display ip routing-table radix
Radix tree for INET (2) inodes 14 routes 10:

                   +--8+--{169.0.0.0
                   |  +-32+--{169.1.1.1
                +--0+
                |  |  +--8+--{127.0.0.0
                |  |  |  +-32+--{127.0.0.1
                |  +--1+
                |     |  +--8+--{2.0.0.0
                |     |  |     +-24+--{2.2.2.0
                |     |  |     |  +-32+--{2.2.2.2
                |     |  |  +-22+
                |     |  |     +-32+--{2.2.1.1
                |     +--6+
                |        +--8+--{1.0.0.0
                |           +-32+--{1.1.1.1
```

Table 50 Field descriptions 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 display the statistics information about routes.

The statistics information about routes includes the total number of routes, the number of routes added by protocols, the number of routes deleted by the protocols, the number of routes which are not deleted though they are with the *deleted* tag, the number of active routes, and the number of inactive routes.

Example # Display the statistics information about routes.

```
<SW7750> 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 Field descriptions of the **display ip routing-table statistics** command

Field	Description
Proto	Routing protocol. O_ASE stands for OSPF_ASE routes; O_NSSA stands for OSPF NSSA routes; AGGRE stands for aggregated routes.
route	Number of routes
active	Number of active routes

Table 51 Field descriptions of the **display ip routing-table statistics** command

Field	Description
added	Number of routes added after the router is rebooted or the routing table is cleared last time.
deleted	Number of routes deleted (Such routes will be freed in a period of time)
Total	Total number of the different kinds of routes.

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 display the verbose routing table information.

With the **verbose** argument provided, 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. Finally, the verbose description of each route will be output.

The **display ip routing-table verbose** command can display all current routes, including inactive routes and invalid routes.

Example # Display the verbose routing table information.

```
<SW7750> display ip routing-table verbose
Routing Tables:
  + = 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
```

Table 49 describes the meaning of route status and Table 52 shows the statistics information about the routing table.

Table 52 Field descriptions 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

reset ip routing-table statistics

Syntax **reset ip routing-table statistics protocol** { **all** | *protocol* }

View User view

Parameter **all**: Specifies all the protocols.

protocol: Protocol to be specified, which can be **BGP**, **DIRECT**, **ISIS**, **OSPF**, **OSPF-ASE**, **OSPF-NSSA**, **RIP**, or **STATIC**.

Description Use the **reset ip routing-table statistics** command to clear routing table statistics.

Example # Clear routing table statistics.

```
<SW7750> reset ip routing-table statistics protocol all
This will erase the specific routing counters information.
Are you sure?[Y/N]y
```

# Display routing table statistics. Now, all route statistics are cleared.

```
<SW7750> display ip routing-table statistics
Routing tables:
Proto      route      active     added      deleted
DIRECT     6          6          0          0
STATIC     0          0          0          0
BGP        0          0          0          0
RIP        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      6          6          0          0
```

29 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 static routes.

The system will request your confirmation before it deletes all the configured static routes.

Related command:

ip route-static and **display ip routing-table**.

Example

Delete all the static routes in the router.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] delete static-routes all
Are you sure to delete all the unicast static routes?[Y/N]y
```

ip route-static

Syntax

ip route-static *ip-address* { *mask* | *mask-length* } { *interface-type interface-number* | *next-hop* } [**preference** *preference-value*] [**reject** | **blackhole**]

undo ip route-static *ip-address* { *mask* | *mask-length* } [*interface-type interface-number* | *next-hop*] [**preference** *preference-value*]

View

System view

Parameter

ip-address: Destination IP address, in dotted decimal notation.

mask: Mask.

mask-length: Mask length. Since 1s in a 32-bit mask must be consecutive, a mask in dotted decimal notation can be replaced by *mask-length*, which is the number of the consecutive 1s in the mask.

interface-type interface-number: Next-hop outgoing interface to be specified. Currently, you can specify the next-hop outgoing interface as **NULL 0** only. The packets sent to a **null** interface, which is a virtual interface, will be discarded immediately. This can decrease the system load.

next-hop: Next hop IP address of the route, in dotted decimal notation.

preference-value: Preference level of the route, in the range from 1 to 255. The default preference is 60.

reject: Indicates an unreachable route. If a static route to a destination has the "**reject**" attribute, all the IP packets destined for this destination will be discarded.

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 all the IP packet addresses destined for this destination are dropped without the source host being notified.

Description Use the **ip route-static** command to configure a static route.

Use the **undo ip route-static** command to delete a manually configured static route.

By default, the system can obtain the subnet route directly connected to the router. When you configure a static route, if no preference is specified for the route, the preference defaults to 60, and if the route is not specified as **reject** or **blackhole**, the route will be reachable by default.

When configuring a static route, note the following points:

- If the destination IP address and the mask are both 0.0.0.0, what you are configuring is a default route. All the packets that fail to find a routing entry will be forwarded through this default route.
- You cannot configure an interface address of the local switch as the next hop address of a static route.
- You can configure a different preference to implement flexible route management policy.

Related command: **display ip routing-table**, **ip route-static default-preference**, **ip route-static default-preference**.

Example # Configure the next hop of the default route as 129.102.0.2.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ip route-static 0.0.0.0 0.0.0.0 129.102.0.2
```

ip route-static default-preference

Syntax **ip route-static default-preference** *default-preference-value*

undo ip route-static default-preference

View System view

Parameter *default-preference-value*: Default precedence of the static routes, in the range of 1 to 255. It is 60 by default.

Description Use the **ip route-static default-preference** command to set the default precedence of the static routes.

Use the **undo ip route-static default-preference** command to restore the default precedence to the default value.

If a static route is configured without the specified precedence, its precedence is set to the default precedence value.

Related command: **display ip routing-table**, and **ip route-static**.

Example # Set the default precedence of static routes to 120.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] ip route-static default-preference 120
```

30 RIP CONFIGURATION COMMANDS

The word "router" covered in the following text represent routers in common sense and Ethernet switches running a routing protocol. To improve readability, this will not be mentioned again in this manual.

checkzero

Syntax **checkzero**

undo checkzero

View RIP view

Parameter None

Description Use the **checkzero** command to enable zero field check of RIP-1 packets.

Use the **undo checkzero** command to disable zero field check.

By default, RIP-1 performs zero field check.

According to the protocol (RFC 1058) specifications, some fields in RIP-1 packets must be zero and these fields are called zero fields. You can use the **checkzero** command to enable/disable zero field check of RIP-1 packets. When zero field check is enabled, if an incoming RIP-1 packet has a non-zero zero field, the packet will be rejected.

This command does not apply to RIP-2 packets because they have no zero fields.

Example # Disable zero field check on RIP-1 packets.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] rip
[SW7750-rip] undo checkzero
```

default cost

Syntax **default cost** *value*

undo default cost

View RIP view

Parameter *value*: Default routing cost to be set, ranging from 1 to 16. It is 1 by default.

Description Use the **default cost** command to set the default routing cost of imported routes.

Use the **undo default cost** command to restore the default value.

If no routing cost is specified when you use the **import-route** command to import routes from another routing protocol, the routes will be imported with the default routing cost specified with the **default cost** command.

Related command: **import-route**.

Example # Set the default routing cost of the routes imported from other routing protocols to 3.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] rip
[SW7750-rip] default cost 3
```

display rip

Syntax **display rip**

View Any view

Parameter None

Description Use the **display rip** command to display the current RIP operation state and RIP configuration.

Example # Display the current RIP operation state and configuration.

```
<SW7750> display rip
RIP is running
    Checkzero is on        Default cost : 1
    Summary is on          Preference : 100
    Traffic-share-across-interface is off
    Period update timer : 30
    Timeout timer : 180
    Garbage-collection timer : 120
    No peer router
    Network :
    10.0.0.0
```

Table 53 Field descriptions of the **display rip** command

Field	Description
RIP is running	RIP is active.

Table 53 Field descriptions of the **display rip** command

Field	Description
Checkzero is on	Zero field checking is enabled.
Default cost : 1	The default route cost is 1
Summary is on	Routes are aggregated automatically
Preference : 100	The preference of RIP is 100
Traffic-share-across-interface is off	Traffic is shared across equivalent routes.
Period update timer : 30	Settings of the three timers of RIP
Timeout timer : 180	
Garbage-collection timer : 120	
No peer router	No destination address of a transmission is specified
Network :10.0.0.0	RIP is enabled on network segment 10.0.0.0

display rip routing

Syntax **display rip routing**

View Any view

Parameter None

Description Use the **display rip routing** command to display RIP routing information.

Example # Display RIP routing table information.

```
<SW7750> display rip routing
                    RIP routing table: public net
A = Active      I = Inactive      G=Garbage collection

Destination/Mask   Cost NextHop         Age     SourceGateway   Att
6.0.0.0/8          1    10.153.25.22    4s      10.153.25.22    A
```

Table 54 Field descriptions of the **display rip routing** command

Field	Description
Destination/Mask	Destination address/Mask
Cost	Cost
NextHop	Net hop address
Age	The time that a route exists in the routing table, namely, the aging time
SourceGateway	Gateway originating the route
Att	Attribute value, which may be one of the three following values: A Active routes I Inactive routes G Unreachable route in the state of garbage collection. If garbage collection times out, and the unreachable route does not receive update messages from the same neighbor, the route will be removed from the routing table completely.

filter-policy export

Syntax **filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [*protocol* [*process-id*] | **interface** *interface-type interface-number*]

filter-policy route-policy *route-policy-name* **export**

undo filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [*protocol* [*process-id*] | **interface** *interface-type interface-number*]

undo filter-policy route-policy *route-policy-name* **export**

View RIP view

Parameter *acl-number*: Number of the basic or advanced ACL used to filter routing information by destination address, in the range of 2,000 to 3,999.

ip-prefix-name: Name of the address ip-prefix list used to filter routing information by destination address, containing 1 to 19 characters.

route-policy-name: Name of the routing policy used to filter routing information, containing 1 to 19 characters. A routing policy can enable RIP to determine which routes are to be sent/received based on such fields as acl/cost/interface/ip/ip-prefix/tag.

protocol: Routing protocol whose routing information is to be filtered. Currently, this can be **bgp**, **direct**, **isis**, **ospf**, **ospf-ase**, **ospf-nssa** or **static**.

process-id: Routing protocol process ID, in the range of 1 to 65535. This argument is valid only when the protocol is **ospf**.

interface: Interface where the routes to be advertised will be filtered.

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

Description Use the **filter-policy export** command to enable RIP to filter the routing information to be advertised.

Use the **undo filter-policy export** command to cancel the filtering of the routing information to be advertised.

By default, RIP does not filter routing information before advertising.

Related command: **acl**, **filter-policy import**, **ip ip-prefix**.

Example # Configure to filter route information by ACL 2000 before the information is advertised.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] rip
[SW7750-rip] filter-policy 2000 export
```

filter-policy import

Syntax **filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* [**gateway** *ip-prefix-name*] | **gateway** *ip-prefix-name* } **import** [**interface** *interface-type interface-number*]

filter-policy route-policy *route-policy-name* **import**

undo filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name* [**gateway** *ip-prefix-name*] | **gateway** *ip-prefix-name* } **import** [**interface** *interface-type interface-number*]

undo filter-policy route-policy *route-policy-name* **import**

View RIP view

Parameter *acl-number:* Number of the ACL used to filter routing information by destination address, in the range of 2,000 to 3,999.

ip-prefix-name: Name of the address prefix list used to filter routing information by destination address, containing 1 to 19 characters.

gateway *ip-prefix-name:* Name of the address prefix list used to filter routing information by the address of the neighbor router advertising the information, containing 1 to 19 characters.

route-policy-name: Name of the routing policy used to filter routing information, containing 1 to 19 characters. A routing policy can enable RIP to determine which routes are to be sent/received based on such fields as acl/cost/interface/ip/ip-prefix/tag.

interface *interface-type interface-number*: Filters routes on the specified interface. The *interface-type* argument represents the interface type and the *interface-number* argument represents the interface number.

Description Use the **filter-policy gateway import** command to enable RIP to filter received routing information by a specified address so that the routing information advertised by the address can pass the filter.

Use the **undo filter-policy gateway import** command to disable the above filtering.

Use the **filter-policy import** command to filter the received routing information.

Use the **undo filter-policy import** command to disable the above filtering.

You can control the range of routes received by RIP by specifying an ACL, ip-prefix list and routing policies.

Related command: **acl**, **filter-policy export**, **ip ip-prefix**.

Example # Configure to filter incoming routing information by acl 2000.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] rip
[SW7750-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 enable RIP to accept host routes.

Use the **undo host-route** command to reject host routes.

By default, RIP accepts host routes.

In some special cases, RIP receives a great number of host routes from the same network segment. These routes are of little help to path searching and occupy a lot of resources. In this case, the **undo host-route** command can be used to reject host routes.

Example # Enable RIP to reject host routes.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] rip
[SW7750-rip] undo host-route
```

import-route

Syntax **import-route** *protocol* [*process-id* | **allow-ibgp**] [**cost** *value* | **route-policy** *route-policy-name*]*

undo import-route *protocol* [*process-id*]

View RIP view

Parameter *protocol*: Redistributes routes from the protocol, which can be **direct**, **ospf**, **ospf-ase**, **ospf-nssa**, **static**, **isis** or **bgp**.

process-id: Redistributes routes from the process of the protocol.

allow-ibgp: Redistributes iBGP routes.

value: Cost value of redistributed routes, in the range of 1 to 16.

route-policy *route-policy-name*: Redistributes only the routes matching the conditions of the specified route-policy. The Name of a routing policy contains 1 to 19 characters.

Description Use the **import-route** command to redistribute routes from another routing protocol into RIP.

Use the **undo import-route** command to disable route redistribution from another routing protocol.

By default, RIP does not redistribute routes from other protocols.

The **import-route** command is used to import the routes of another protocol with a specified cost. RIP regards the imported routes as its own routes and transmits them with the specified cost. This command can greatly enhance the capability of RIP to obtain routes, thereby improving RIP performance.

If the **cost** *value* is not specified, routes will be imported with the default routing cost (set by the **default cost** command, ranging from 1 to 16). If the cost of an imported route is 16, RIP marks the route as HOLD DOWN (however, the route can still be used to forward packets), and continues to announce the route with this cost to other routers running RIP until the Garbage Collection timer times out (the timeout time defaults to 120 seconds).

Related command: **default cost**.

Note that:

*The **import-route bgp** command redistributes only eBGP routes, while the **import-route bgp** allow-i**bgp** command redistributes both iBGP and eBGP routes. Because the redistributed iBGP routes have the AS-PATH attribute removed, routing loops may occur. Therefore, use the allow-i**bgp** keyword with caution.*

Example # Import static routes with the cost of 4.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] rip
[SW7750-rip] import-route static cost 4
```

# Set the default cost and import OSPF routes with the default cost.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] rip
[SW7750-rip] default cost 3
[SW7750-rip] import-route ospf
```

network

Syntax **network** *network-address*

undo network *network-address*

View RIP view

Parameter *network-address*: Address of the network for which RIP is enabled/disabled. It can be the IP network address of any interface.

Description Use the **network** command to enable RIP on a specified interface.

Use the **undo network** command to disable RIP on the interface.

By default, RIP is disabled on any interface.

After a RIP routing process is started, it is disabled on any interface. To enable RIP routing on an interface, you must use the **network** command.

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 **network** 129.102.0.0.

Related command: **rip work**.

Example # Enable RIP on the interface with the network address 129.102.0.0.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] rip
[SW7750-rip] network 129.102.0.0
```

peer

Syntax **peer** *ip-address*

undo peer *ip-address*

View RIP view

Parameter *ip-address*: IP address of the interface on the peer router with which routing information needs to be exchanged, in dotted decimal notation.

Description Use the **peer** command to configure the destination address of the peer device with which routing information should be exchanged in unicast mode.

Use the **undo peer** command to cancel a unicast address.

By default, RIP does not send packets to any address in unicast mode.

This command is used to for non-broadcast networks to which protocol packets cannot be sent in broadcast mode. And you are not recommended to use this command in normal situation.

Example # Specify a unicast destination address of 202.38.165.1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] rip
[SW7750-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 preferences of routing protocols will finally determine which routing algorithm's routes will be selected as the optimal routes in the IP routing table. You can use this command to modify the RIP preference manually.

Example # Specify the RIP preference as 20.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] rip
[SW7750-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 the parameters of RIP, you can use this command to restore the default setting.

Example # Reset the RIP system configuration.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] rip
[SW7750-rip] reset
% Reset RIP's configuration and restart RIP? [Y/N]y
```

rip

Syntax **rip**

undo rip

View System view

Parameter None

Description Use the **rip** command to enable RIP and enter RIP view.

Use the **undo rip** command to disable RIP.

By default, the system does not run RIP.

RIP must be enabled before you can enter the RIP view and configure various RIP global parameters. You can, however, configure the interface-based parameters regardless of whether RIP is enabled.

Note that the interface parameters configured previously would be invalid when RIP is disabled.

Example # Enable RIP and enter RIP view.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] rip
[SW7750-rip]
```

rip authentication-mode

Syntax **rip authentication-mode** { **simple** *password* | **md5** { **rfc2453** *key-string* | **rfc2082** *key-string key-id* } }

undo rip authentication-mode

View Interface view

Parameter **simple**: Specifies to use simple text authentication mode.

password: Simple text authentication key, containing 1 to 16 characters.

md5: Specifies to use MD5 cipher text authentication mode.

rfc2453: Specifies that MD5 cipher text authentication packets will use a packet format (IETF standard) stipulated by RFC2453.

rfc2082: Specifies that MD5 cipher text authentication packets will use a packet format stipulated by RFC2082.

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 you use the **display current-configuration** command. You can also input the MD5 *key* in a cipher text form with a length of 24 characters.

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 RIP-2 authentication mode.

RIP-1 does not authenticate packets. Generally RIP authenticates packets in two modes: plaintext authentication and MD5 ciphertext authentication. There are two packet formats in the MD5 ciphertext authentication: one format conforms to RFC 2453 and the other format is described in RFC 2082. Routers support both formats. You can select any format as required.

Related command: **rip version**.

Example

Specify the interface Vlan-interface 10 to use the **simple** authentication with the authentication key of aaa.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 10
[SW7750-Vlan-interface10] rip version 2
[SW7750-Vlan-interface10] rip authentication-mode simple aaa
```

# Specify Vlan-interface 10 to use the MD5 cipher text authentication, with the authentication key of aaa and the packet format of **rfc2453.**

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 10
[SW7750-Vlan-interface10] rip version 2
[SW7750-Vlan-interface10] rip authentication-mode md5 rfc2453 aaa
```

rip input

Syntax

rip input

undo rip input

View Interface view

Parameter None

Description Use the **rip input** command to enable an interface to receive RIP packets.

Use the **undo rip input** command to disable an interface from receiving RIP packets.

By default, all interfaces, except loopback interfaces, can receive RIP packets.

This command is used in cooperation with another 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 # Configure the interface Vlan-interface 10 not to receive RIP packets.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750]interface Vlan-interface 10
[SW7750-Vlan-interface10] undo rip input
```

rip metricin

Syntax **rip metricin** *value*

undo rip metricin

View Interface view

Parameter *value*: Additional route metric added when receiving a RIP route, 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 RIP routes received on an interface.

Use the **undo rip metricin** command to restore the default value of this additional route metric.

Related command: **rip metricout**.

Example # Set the additional route metric added to RIP routes received on Vlan-interface 10 to 2.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
```

```
[SW7750] interface Vlan-interface 10
[SW7750-Vlan-interface10] rip metricin 2
```

rip metricout

Syntax

rip metricout *value*

undo rip metricout

View

Interface view

Parameter

value: Additional route metric added when transmitting a RIP route, ranging from 1 to 16. By default, the value is 1.

Description

Use the **rip metricout** command to configure the additional route metric added to the RIP routes to be transmitted on an interface.

Use the **undo rip metricout** command to restore the default value of this additional route metric.

*The **rip metricout** configuration only applies to the RIP routes learnt by the router and those generated by the router itself. It does not apply to any route imported to RIP by any other routing protocol.*

Related command:

rip metricin.

Example

Set the additional route metric added to the RIP routes to be transmitted on Vlan-interface 10 to 2.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 10
[SW7750-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 enable an interface to transmit RIP packets.

Use the **undo rip output** command to disable an interface from transmitting RIP packets.

By default, all interfaces except loopback interfaces are enabled to transmit RIP packets to the external.

This command is used in cooperation with another 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 from transmitting RIP packets.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 10
[SW7750-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 the **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 avoiding route loop. Only in some special cases does split horizon need to be disabled to ensure the correct execution of the protocol. So, disable split horizon only when necessary.

Example # Specify the interface Vlan-interface 10 not to use split horizon when processing RIP packets.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 10
[SW7750-Vlan-interface10] undo rip split-horizon
```

rip version

Syntax **rip version** { **1** | **2** [**broadcast** | **multicast**] }

undo rip version

View Interface view

Parameter **1**: Specifies the version of RIP packets on the interface to RIP-1.

2: Specifies the version of RIP packets on the interface to RIP-2.

broadcast: Transmission mode of RIP-2 packets is broadcast.

multicast: Transmission mode of RIP-2 packets is multicast.

Description Use the **rip version** command to specify the version of RIP packets on an interface.

Use the **undo rip version** command to restore the default 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 receives and transmits RIP-2 broadcast packets, receives RIP-1 broadcast 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 broadcast packets.

Example # Configure the interface Vlan-interface 10 as RIP-2 broadcast mode.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 10
[SW7750-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 RIP to transmit and receive RIP packets on an interface.

Use the **undo rip work** command to disable RIP from transmitting and receiving RIP packets on an interface.

By default, RIP is enabled from transmitting and receiving RIP packets on an interface.

This command is used in cooperation with **rip input**, **rip output** and **network** commands.

Related command:

network, **rip input**, **rip output**.

Example

Disable RIP from transmitting and receiving RIP packets on the interface Vlan-interface 10.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 10
[SW7750-Vlan-interface10] undo rip work
```

summary

Syntax

summary

undo summary

View

RIP view

Parameter

None

Description

Use the **summary** command to enable RIP-2 automatic route aggregation.

Use the **undo summary** command to disable RIP-2 automatic route aggregation.

By default, RIP-2 route aggregation is enabled.

Route aggregation can be used 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 aggregation function can be disabled with the **undo summary** command when it is necessary to broadcast subnet routes.

RIP-1 does not support subnet mask. Forwarding subnet routes may cause ambiguity. Therefore, RIP-1always uses route aggregation.

Related command:

rip version.

Example

Set RIP version on the interface Vlan-interface 10 as RIP-2 and disable route aggregation.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 10
[SW7750-Vlan-interface10] rip version 2
[SW7750-Vlan-interface10] quit
[SW7750] rip
[SW7750-rip] undo summary
```

timers

Syntax **timers** { **update** *update-timer* | **timeout** *timeout-timer* } *

undo timers { **update** | **timeout** } *

View RIP view

Parameter *update-timer*: Value of the Period Update timer, ranging from 1 to 3,600 seconds. By default, it is 30 seconds.

timeout-timer: Value of the Timeout timer, ranging from 1 to 3,600 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 Period Update, Timeout, and Garbage-collection timers are 30 seconds, 180 seconds, and 120 seconds, respectively.

Generally, it is regarded that the value of the Garbage-collection timer is fixed at four times that of the Period Update timer. Adjusting the Period Update timer will affect the Garbage-collection timer.

The modification of RIP timers is validated immediately.

Related command: **display rip**.

Example # Set the values of the Period Update timer and the Timeout timer of RIP to 10 seconds and 30 seconds respectively.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] rip
[SW7750-rip] timers update 10 timeout 30
```

traffic-share-across-interface

Syntax **traffic-share-across-interface**

undo traffic-share-across-interface

View RIP view

Parameter None

Description Use the **traffic-share-across-interface** command to enable traffic sharing across RIP interfaces, so as to distribute traffic evenly over equal-cost routes across the interfaces on a router.

Use the **undo traffic-share-across-interface** command to cancel traffic sharing.

By default, traffic sharing across RIP interfaces is disabled.

In the case the number of equal-cost routes reaches the upper limit:

With this function enabled, the newly learned equal-cost routes replace existing ones in the routing table.

With this function disabled, the router determines whether the aging time of the equal-cost route with the longest aging time has reached the threshold. If yes, the router replaces this route with the equal-cost route newly learned; otherwise, the router drops the equal-cost route newly learned.

Example # Enable traffic sharing across RIP interfaces.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] rip
[SW7750-rip] traffic-share-across-interface
```

31 OSPF CONFIGURATION COMMANDS

The words "router" covered in the following text represent routers in common sense and Ethernet switches running a routing protocol. To improve readability, this will not be mentioned again in this manual.

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: Specifies to advertise the aggregated route that match a specific IP address and mask.

not-advertise: Specifies not to advertise the aggregated route that match a specific IP address and mask.

Description Use the **abr-summary** command to enable route aggregation on an area border router (ABR).

Use the **undo abr-summary** command to disable route aggregation on an ABR.

By default, an ABR does not aggregate routes.

This command is applicable to ABRs only and is used for route aggregation in an area. It allows the ABR to transmit an aggregated route to other areas.

Route aggregation means that routing information is processed by an ABR, which transmits only one route to other areas for each network segment configured with route aggregation. You can configure multiple aggregation routes in an area so that OSPF can aggregate multiple network segments.

Example # Aggregate the routes in the two network segments, 36.42.10.0 and 36.42.110.0, in OSPF area 1 into one summary route 36.42.0.0 and transmit it to other areas.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
```

```
[SW7750] ospf 1
[SW7750-ospf-1] area 1
[SW7750-ospf-1-area-0.0.0.1] network 36.42.10.0 0.0.0.255
[SW7750-ospf-1-area-0.0.0.1] network 36.42.110.0 0.0.0.255
[SW7750-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 an OSPF area, which can be a decimal integer (ranging from 0 to 4294967295) or in the form of an IP address.

Description Use the **area** command to enter OSPF area view.

Use the **undo area** command to cancel the specified area.

Example # Enter OSPF area 0 view.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ospf 1
[SW7750-ospf-1] area 0
[SW7750-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*: IP address to be matched, in dotted decimal notation.

mask: IP address mask, in dotted decimal notation.

not-advertise: Specifies not to advertise the aggregated route matching the specified IP address and mask. If this argument is not provided, the aggregated route will be advertised.

tag *value*: Tag value, which is mainly used to control route advertisement via route-policy. It ranges from 0 to 4294967295 and defaults to 1.

Description Use the **asbr-summary** command to configure the aggregation of imported routes by OSPF.

Use the **undo asbr-summary** command to cancel the aggregation.

By default, imported routes are not aggregated.

After the aggregation of imported routes is configured, if the local router is an autonomous system border router (ASBR), this command aggregates the imported Type-5 LSAs in the aggregation address range. If an NSSA is configured, this command also aggregates the imported Type-7 LSAs in the summary address range.

If the local router acts as both an ABR and a transit router in the NSSA, this command aggregates Type-5 LSAs transformed from Type-7 LSAs. If the router is not the router in the NSSA, the aggregation is disabled.

Related command: **display ospf asbr-summary**.

Example # Set aggregation of routes imported by the router 3Com.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ospf 1
[SW7750-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.

Use the **ospf authentication-mode simple** command to configure a simple text authentication key.

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.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ospf 1
[SW7750-ospf-1] area 0
```

# Specify the OSPF area 0 to support MD5 cipher text authentication.

```
[SW7750-ospf-1-area-0.0.0.0] authentication-mode md5
```

default cost

Syntax **default cost** *value*

undo default cost

View OSPF view

Parameter *value:* Default routing cost of 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 routing cost of external routes to its default value.

Since OSPF can import external routing information and propagate the information to the entire autonomous system, routing cost of external routes can influence route selection and calculation. Therefore, 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.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ospf 1
[SW7750-ospf-1] default cost 10
```

default interval

Syntax **default interval** *seconds*

undo default interval

View OSPF view

Parameter *seconds*: Default interval, in seconds, of importing external routes. It ranges from 1 to 2147483647 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 of importing external routes.

OSPF can import external routing information and propagate it to the entire autonomous system. However, importing routes too often greatly affects the performance of the device. Therefore, 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.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ospf 1
[SW7750-ospf-1] default interval 10
```

default limit

Syntax **default limit** *routes*

undo default limit

View OSPF view

Parameter *routes:* Default limit on the number of external routes imported in a unit time. It ranges from 200 to 2147483647 and defaults to1000.

Description Use the **default limit** command to configure the default limit on the number of routes imported by OSPF in a unit time.

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 many external routes at a time greatly affects the performance of the device. Therefore, it is necessary to limit the number of external routes imported during each import interval.

Related command: **default interval**.

Example # Specify the default limit on the number of external routes imported by OSPF in each import interval as 200.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
```

```
[SW7750] ospf 1
[SW7750-ospf-1] default limit 200
```

default tag

Syntax **default tag** *tag*

undo default tag

View OSPF view

Parameter *tag*: Default tag, in the range of 0 to 4,294,967,295, which is 1 by default.

Description Use the **default tag** command to configure the default tag of OSPF when it imports an external route.

Use the **undo default tag** command to restore the default tag of OSPF when it imports the external route.

When OSPF imports a route found by another routing protocol 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 of OSPF imported external route of the autonomous system as 10.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ospf 1
[SW7750-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. You can use the command described in this section to specify the default type when external routes are imported.

Related command: **default tag**.

Example # Configure OSPF to import external routes of type 1 by default.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ospf 1
[SW7750-ospf-1] default type 1
```

default-cost

Syntax **default-cost** *value*

undo default-cost

View OSPF Area view

Parameter *value*: Cost value of the default route transmitted by OSPF to the STUB or NSSA area. It ranges from 0 to 16,777,214 and defaults to 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 default cost of the default route transmitted by OSPF to the STUB or NSSA area.

This command only applies to an ABR in a STUB area or NSSA area.

To configure a STUB area, you need to use the **stub** and **default-cost** commands.

You must use the **stub** command on all the routers connected to a STUB area to configure the area with the STUB attribute.

Use the **default-cost** command to configure the cost of the default route transmitted by an ABR to the STUB area or NSSA area.

Related command: **stub**, **nssa**.

Example # Set area 1 as the STUB area and the cost of the default route transmitted to this STUB area to 60.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
```

```
[SW7750] ospf 1
[SW7750-ospf-1] area 1
[SW7750-ospf-1-area-0.0.0.1] network 20.0.0.0 0.255.255.255
[SW7750-ospf-1-area-0.0.0.1] stub
[SW7750-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**: Generates an ase lsa describing the default route and advertises it if the local router is not configured with the default route. If this keyword is not provided, the local router must be configured with the default route before it can import the ase lsa, which generates the default route.

cost *value*: Specifies the cost value of this ase lsa. The value of *value* ranges from 0 to 16777214 and defaults to 1.

type *type-value:* Specifies the cost type of this ase lsa. The value of *type-value* ranges from 1 to 2 and defaults 2.

route-policy *route-policy-name:* If the default route matches the route-policy specified by *route-policy-name*, the route-policy will affect the value in ase lsa. The *route-policy-name* argument is a string of 1 to 19 characters.

Description Use the **default-route-advertise** command to import the default route to OSPF route area.

Use the **undo default-route-advertise** command to cancel the import of the default route.

By default, OSPF does not import the default route.

The **import-route** command cannot import the default route. To import the default route to the route area, the **default-route-advertise** command must be used. If the local router is not configured with the default route, the keyword **always** should be specified so that ase lsa of the default route is generated.

Related command: **import-route**.

Example # The ase lsa of the default route is generated only if the local router has the default route.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ospf 1
[SW7750-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.

```
[SW7750-ospf-1] default-route-advertise always
```

display ospf abr-asbr

Syntax **display ospf** [*process-id*] **abr-asbr**

View Any view

Parameter *process-id*: OSPF Process ID, in the range of 1 to 65,535. If you do not specify a process ID, this command applies to all current OSPF processes.

Description Use the **display ospf abr-asbr** command to display the information about the ABR and ASBR of OSPF.

Example # Display the information about the OSPF ABRs and ASBRs.

```
<SW7750> display ospf abr-asbr
                   OSPF Process 1 with Router ID 1.1.1.1
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 55 Field descriptions of the **display ospf abr-asbr** command

Field	Description
Destination	Router ID of the ABR or ASBR
Area	Area where the router is connected to the ASBR
Cost	Routing overhead value of the route
Nexthop	Nexthop address to the destination
Interface	Local output interface

display ospf asbr-summary

Syntax **display ospf** [*process-id*] **asbr-summary** [*ip-address mask*]

View Any view

Parameter *process-id*: OSPF Process ID, in the range of 1 to 65,535. If you do not specify a process ID, this command applies to all current OSPF processes.

ip-address: Matched IP address, in dotted decimal notation.

mask: IP address mask, in dotted decimal notation.

Description Use the **display ospf asbr-summary** command to display the summary information of OSPF imported route.

If you do not specify an IP address or mask, 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.

```
<SW7750> display ospf asbr-summary
```

OSPF Process 1 with Router ID 10.1.1.1

```
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 56 Field descriptions of the **display ospf asbr-summary** command.

Field	Description	
net	Destination network segment	
mask	Mask	
tag	Tag	
status	Status information, which takes one of the following 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*: OSPF Process ID, in the range of 1 to 65,535. If you do not specify a process ID, this command applies to all current OSPF processes.

Description Use the **display ospf brief** command to display brief OSPF information.

Example # Display brief OSPF information.

```
<SW7750> display ospf brief
                 OSPF Process 1 with Router ID 10.1.1.1
                        OSPF Protocol Information

 RouterID: 10.1.1.1
 Spf-schedule-interval: 5
 Routing preference: Inter/Intra: 10 External: 150
 Default ASE parameters: Metric: 1 Tag: 1 Type: 2
 SPF computation count: 163
 Area Count: 1    Nssa Area Count: 0

 Area 0.0.0.0:
   Authtype: none   Flags: <>
   SPF scheduled: <Router Net Intra>
   Interface: 110.1.1.1 (Vlan-interface110)
     Cost: 11 State: DR    Type: Broadcast
     Priority: 11
     Designated Router: 110.1.1.1
     Backup Designated Router: 110.1.1.2
     Timers: Hello 10, Dead 40, Poll 40, Retransmit 5, Transmit Delay 1
```

Table 57 Field descriptions of the **display ospf brief** command

Field	Description	
RouterID	Router ID of the router	
spf-schedule-interval	Interval of SPF schedule	
Authtype	Authentication type of OSPF	
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	Name of interface belonging to this area	
Cost	Cost of routes	
State	State information	
Type	Network type of OSPF interface/the first type refers to the type of the imported external route	
Priority	Priority	
Designated Router	IP address of designated router (DR)	
Backup Designated Router	IP address of backup designated router (BDR)	
Timers	OSPF timers, defined 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*: OSPF Process ID, in the range of 1 to 65,535. If you do not specify a process ID, this command applies to all current OSPF processes.

Description Use the **display ospf cumulative** command to display cumulative OSPF statistics.

Example # Display cumulative OSPF statistics.

```
<SW7750> display ospf cumulative
                 OSPF Process 1 with Router ID 10.1.1.1
                               Cumulations

  IO Statistics
             Type        Input     Output
            Hello         6271       9241
   DB Description         9659       9915
   Link-State Req          419       1426
Link-State Update        30190      51723
   Link-State Ack        13642      22262
  ASE: 6231 Checksum Sum: C3D40E0
  LSAs originated by this router
  Router: 141  Net: 5
  LSAs Originated: 146  LSAs Received: 161905

  Area 0.0.0.0:
    Neighbors: 4  Interfaces: 5
    Spf: 163  Checksum Sum 3C60A5F8
    rtr: 105 net: 187 sumasb: 0 sumnet: 30500

  Routing Table:
    Intra Area: 8  Inter Area: 0  ASE: 5
```

Table 58 Field descriptions 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

Table 58 Field descriptions of the **display ospf cumulative** command

Field		Description
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*: OSPF Process ID, in the range of 1 to 65,535. If you do not specify a process ID, this command applies to all current OSPF processes.

Description Use the **display ospf error** command to display OSPF error information.

Example # Display the OSPF error information.

```
<SW7750> 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: HELLO: NBMA neighbor unknown      0: DD: neighbor state low
   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
   0: LS UPD: LSA length wrong
```

Table 59 Field descriptions 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

Table 59 Field descriptions of the **display ospf error** command

Field	Description
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
HELLO: router id confusion	Hello packet: Router ID confusion
HELLO: virtual neighbor unknown	Hello packet: unknown virtual neighbor
HELLO: NBMA neighbor unknown	Hello packet: unknown NBMA neighbor
DD: neighbor state low	Database description (DD) packet: asynchronous neighbor state
DD: unknown LSA type	DD packet: unknown LSA type
DD: router id confusion	DD packet: router id unidentifiable
DD: extern option mismatch	DD packet: external route flag error
LS ACK: neighbor state low	Link state acknowledgment (LS ACK) packet: asynchronous neighbor state
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: asynchronous neighbor state
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: asynchronous neighbor state
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
LS UPD: LSA length wrong	Link state update packet: LSA length error

display ospf interface

Syntax **display ospf** [*process-id*] **interface** [**verbose |** *interface-type interface-number* [**verbose**]]

View Any view

Parameter *process-id*: OSPF Process ID, in the range of 1 to 65,535. If you do not specify a process ID, this command applies to all current OSPF processes.

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

verbose: Specifies to display detailed OSPF interface information.

Description Use the **display ospf interface** command to display the OSPF interface information. With the **verbose** keyword specified, detailed OSPF interface information will be displayed.

Example # Display the OSPF interface information of Vlan-interface1.

```
<SW7750> 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 40, Retransmit 5, Transmit Delay 1
```

Table 60 Field descriptions 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	
Priority	Priority of DR for interface election	
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, defined 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**] [*ip-address* **| verbose**] [**originate-router** *ip-address* | **self-originate**]]

View Any view

Parameter *process-id*: OSPF Process ID, in the range of 1 to 65,535. If you do not specify a process ID, this command applies to all current OSPF processes.

area-id: OSPF area ID, which can be a decimal integer (ranging from 0 to 4294967295) or in the form of an IP address.

brief: Displays brief database statistics.

asbr: Displays the database summary about Type-4 LSAs (summary-Asbr-LSAs) advertised by ASBR routers.

ase: Displays the database summary about the Type-5 LSAs (AS-external-LSAs). This argument is unavailable if you have provided a value for *area-id*.

network: Displays the database summary about the Type-2 LSAs (network-LSAs).

nssa: Displays the database summary about the Type-7 LSAs (NSSA-external-LSAs).

router: Displays the database summary about the Type-1 LSAs (router-LSAs).

summary: Displays the database summary about the Type-3 LSAs (summary-net-LSAs).

ip-address: Link state identifier (in the form of an IP address).

originate-router *ip-address*: Specifies the Router ID of the router advertising the LSAs.

verbose: Specifies to display detailed information about the LSAs in the database.

self-originate: Displays the database information about the LSAs generated by the local router (self-originate LSAs).

Description Use the **display ospf lsdb** command to display the database information about OSPF connection state. With the **verbose** keyword specified, detailed information about the specific type of LSAs in the OSPF connection state database will be displayed.

Example # Display the database information about OSPF connection state.

```
<SW7750> display ospf lsdb
                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 61 Field descriptions 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 that advertises the LSA
Age	Age of the LSA
Len	Length of the LSA
Sequence	Sequence number of the LSA
Metric	Cost from the router that advertises the LSA to LSA destination
Where	Location of the LSA

```
<SW7750> 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 62 Field descriptions 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 that advertises the LSA
ls age	Age of the LSA
len	Length of the LSA

Table 62 Field descriptions of the **display ospf lsdb ase** command

Field	Description
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*: OSPF Process ID, in the range of 1 to 65,535. If you do not specify a process ID, this command applies to all current OSPF processes.

Description Use the **display ospf nexthop** command to display the OSPF next-hop information.

Example # Display the OSPF next-hop information.

```
<SW7750> display ospf nexthop
                OSPF Process 1 with Router ID 2.2.2.2

Next hops:
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 63 Field descriptions 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, namely, number of routes using the next hop
Intf Addr	IP address of the interface to the next hop
Intf Name	Interface to the next hop
nexthop	Next hop

display ospf peer

Syntax **display ospf** [*process-id*] **peer** [**brief** | **statistics**]

View Any view

Parameter *process-id*: OSPF Process ID, in the range of 1 to 65,535. If you do not specify a process ID, this command applies to all current OSPF processes.

Description Use the **display ospf peer** command to display the information about OSPF peer.

Use the **display ospf peer brief** command to display the brief information, including router ID, interface, and state, about every OSPF peer.

Use the **display ospf peer statistics** command to display the statistics of every OSPF peer, namely, the number of peers in various states in every area.

Example # Display the information about OSPF peer.

```
<SW7750> display ospf peer
                OSPF Process 1 with Router ID 1.1.1.1
                                Neighbors
Area 0.0.0.0 interface 10.153.17.88(Vlan-interface1)’s neighbor(s)
  RouterID: 2.2.2.2         Address: 10.153.17.89
        State: Full  Mode: Nbr is Master  Priority: 1
        DR: 10.153.17.89  BDR: 10.153.17.88
        Dead timer expires in 31s
        Neighbor has been up for 01:14:14
```

Table 64 Field descriptions of the **display ospf peer** command

Field	Description
RouterID	Router ID of neighbor router
Address	Address of the interface, through which neighbor router communicates with the router
State	State of adjacency relation
Mode	Master/Slave mode formed by negotiation in exchanging DD packet
Priority	Priority of DR/BDR for neighbor election
DR	IP address of the interface of elected DR
BDR	IP address of the interface of elected BDR
Dead timer expires in 31s	If no hello packet is received from the peer within this interval, the peer will be considered to be invalid.
Neighbor has been up for 01:14:14	Time of neighbor connection

# Display OSPF peer statistics.

```
<SW7750> display ospf peer statistics
                OSPF Process 1 with Router ID 1.1.1.1
                                Neighbor Statistics
Area ID      Down Attempt Init 2-Way ExStart Exchange Loading Full Total
0.0.0.0      0    0       0    0    0       0        0        1    1
0.0.0.1      0    0       0    0    0       0        0        1    1
Total        0    0       0    0    0       0        0        2    2
```

Table 65 Field descriptions of the **display ospf peer statistics** command

Field	Description
Area ID	Area ID

Table 65 Field descriptions of the **display ospf peer statistics** command

Field	Description
Down	Initial state for OSPF to establish neighbor relation, which indicates that OSPF router does not receive the message from a certain neighbor router within a period of time
Attempt	It is enabled in an NBMA environment, such as Frame Relay, X.25 or ATM. It indicates that OSPF router does not receive the message from a certain neighbor router within a period of time, but still attempts to send Hello packet to the adjacent routers for their communications with a lower frequency.
Init	It indicates that OSPF router has received Hello packet from a neighbor router, but its IP address is not contained in the Hello packet. Therefore, a two-way communication between them has not been established.
2-Way	It indicates that a two-way communication between OSPF router and neighbor router has been established. DR and BDR can be selected in this state (or higher state).
ExStart	In this state, the router determines the sequence number of initial database description (DD) packet used for data exchange, so that it can obtain the latest link state information
Exchange	It indicates that OSPF router sends DD packet to its neighbor routers to exchange link state information
Loading	In this state, OSPF router requests neighbor routers based on the updated link state information from neighbor routers and its expired information, and waits for response from neighbor routers
Full	It indicates that database synchronization between the routers that have established neighbor relation has been completed, and their link state databases have been consistent

display ospf request-queue

Syntax **display ospf** [*process-id*] **request-queue**

View Any view

Parameter *process-id*: OSPF Process ID, in the range of 1 to 65,535. If you do not specify a process ID, this command applies to all current OSPF processes.

Description Use the **display ospf request-queue** command to display the information about the OSPF request-queue.

Example # Display the information about the OSPF request-queue.

```
<SW7750> display ospf request-queue
                OSPF Process 1 with Router ID 1.1.1.1
                              Request List

  The Router’s Neighbor is
  RouterID:  10.1.1.1       Address: 120.1.1.1
  Interface: 120.1.1.2      Area: 0.0.0.0
  Request list:
  LSID:151.14.83.0      AdvRouter:5.4.0.0  Sequence:8000002a  Age:545
  LSID:151.10.91.0      AdvRouter:5.4.0.0  Sequence:8000002a  Age:545
```

Table 66 Field descriptions 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	Area number of OSPF
LSID	Link State ID of the LSA
AdvRouter	Router ID of the router that advertised the LSA
Sequence	Sequence number of the LSA, used to discover old and repeated LSAs
Age	Age of the LSA

display ospf retrans-queue

Syntax **display ospf** [*process-id*] **retrans-queue**

View Any view

Parameter *process-id*: OSPF Process ID. If you do not specify a process ID, this command applies to all current OSPF processes.

Description Use the **display ospf retrans-queue** command to display the information about the OSPF retransmission queue.

Example # Display the information about the OSPF retransmission queue.

```
<SW7750> 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 67 Field descriptions 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	Area number of OSPF
Type	Type of the LSA
LSID	Link State ID of the LSA
AdvRouter	Router ID of the router that advertises the LSA

display ospf routing

Syntax **display ospf** [*process-id*] **routing**

View Any view

Parameter *process-id*: OSPF Process ID, in the range of 1 to 65,535. If you do not specify a process ID, this command applies to all current OSPF processes.

Description Use the **display ospf routing** command to display the information about OSPF routing table.

Example # Display OSPF routing information.

```
<SW7750> 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         0.0.0.0
10.10.0.0/16              1  Stub 10.10.0.1        3.3.3.3         0.0.0.0

Total Nets: 2
  Intra Area: 2  Inter Area: 0  ASE: 0  NSSA: 0
```

Table 68 Field descriptions 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	ID of the router that advertises the route
Area	Area ID
Intra Area	Number of intra-area routes
Inter Area	Number of inter-area routes
ASE	Number of external routes
NSSA	Number of NSSA routes

display ospf vlink

Syntax **display ospf** [*process-id*] **vlink**

View Any view

Parameter *process-id*: OSPF Process ID, in the range of 1 to 65,535. If you do not specify a process ID, this command applies to all current OSPF processes.

Description Use the **display ospf vlink** command to display the information about OSPF virtual links.

Example # Display OSPF virtual link information.

```
<SW7750> 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 69 Field descriptions of the **display ospf vlink** command

Field	Description	
Virtual-link Neighbor-id	Router ID of virtual-link neighbor router	
State	State	
Interface	IP address of 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, or NSSA area	
Timers	OSPF timers, defined 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	

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 OSPF view

Parameter *acl-number*: Basic or advanced ACL number, in the range of 2,000 to 3,999.

ip-prefix-name: Name of the address prefix list, containing 1 to 19 characters.

protocol: Routing protocol advertising the routing information. At present, it can be **direct**, **rip**, **bgp, isis** or **static**.

Description Use the **filter-policy export** command to enable the ASBR routers to filter the external routes imported to OSPF. This command is applicable only to ASBR routers

Use the **undo filter-policy export** command to cancel the filtering rule configured.

By default, OSPF does not receive routes advertised by the other routing protocols.

- *The* ***filter-policy export*** *command take effect on only the routes imported to the local device through the* ***import-route*** *command. If the* ***filter-policy*** *__export__ command is configured while the __import-route__ command is not configured to import other external routes (including OSPF routes in different processes), the __filter-policy export__ command does not take effect.*

- *If the protocol argument is not specified in the __filter-policy export__ command, this command takes effect on all the routes imported to the local device through the __import-route__ command.*

Related command: **acl**, **ip ip-prefix**.

Example # Configure OSPF to advertise only the routing information permitted by acl 2000.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] acl number 2000
[SW7750-acl-basic-2000] rule permit source 11.0.0.0  0.255.255.255
[SW7750-acl-basic-2000] rule deny source any
[SW7750-ospf-1] filter-policy 2000 export
```

filter-policy import

Syntax **filter-policy** { *acl-number* **|** **ip-prefix** *ip-prefix-name* **|** **gateway** *prefix-list-name* } **import**

undo filter-policy { *acl-number* **|** **ip-prefix** *ip-prefix-name* **|** **gateway** *ip-prefix-name* } **import**

View OSPF view

Parameter *acl-number*: 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, containing 1 to 19 characters.

gateway *ip-prefix-name:* Specifies the name of the address prefix list used for filtering the addresses of the neighbor routers advertising the routing information.

Description Use the **filter-policy import** command to configure the OSPF rules for 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. You can use the **filter-policy** command to set the filtering conditions for the routing information to be received. Only the routing information passing the filter can be received.

The **filter-policy import** command filters the routes calculated by OSPF. Only the routes passing the filter can be added to the routing table. The routes can be filtered based on next hop and destination address.

OSPF is a dynamic routing protocol based on link state, with routing information hidden in LSAs. Therefore, OSPF cannot filter any advertised or received LSA. This command is used much less in OSPF than in distance-vector routing protocols.

Example # Filter the received routing information according to the rule defined by ACL 2000.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] acl number 2000
[SW7750-acl-basic-2000] rule permit source 20.0.0.0  0.255.255.255
[SW7750-acl-basic-2000] rule deny source any
[SW7750-ospf-1] filter-policy 2000 import
```

import-route

Syntax **import-route** *protocol* [*process-id* | **allow-ibgp**] [**cost** *value* | **type** *value* | **tag** *value* | **route-policy** *route-policy-name*]*

undo import-route *protocol* [*process- id*]

View OSPF view

Parameter *protocol*: Redistributes routes from the protocol, which can be **direct**, **rip**, **bgp, isis**, **static**, **ospf**, **ospf-ase** and **ospf-nssa**.

process-id: Redistributes routes from the process of the protocol.

allow-ibgp: Redistributes iBGP routes.

route-policy *route-policy-name*: Redistributes only the routes matching the conditions of the specified route-policy. The Name of a routing policy contains 1 to 19 characters.

cost *value*: Specifies the cost of redistributed routes, in the range of 0 to 16,777,214.

type *value*: Specifies the cost type of redistributed routes. The value ranges from 1 to 2.

tag *value*: Specifies the tag of redistributed routes.

Description Use the **import-route** command to redistribute routes from another routing protocol.

Use the **undo import-route** command to disable route redistribution from another routing protocol.

By default, RIP does not redistribute routes from other protocols.

- *The **import-route bgp** command redistributes only eBGP routes, while the **import-route bgp allow-ibgp** command redistributes both iBGP and eBGP routes. Because the redistributed iBGP routes have the AS-PATH attribute removed, routing loops may occur. Therefore, use the **allow-ibgp** keyword with caution.*
- *You are recommended to configure the route type, cost and tag together in one command. When you configure them individually, the new configuration will overwrite the old configuration.*

By default, the routing information of other protocols is not imported.

Example # Configure to import RIP routes as type-2 routes, with the route tag of 33 and the route cost of 50.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ospf 1
[SW7750-ospf-1] import-route rip type 2 tag 33 cost 50
```

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, represented in dotted decimal notation.

ip-mask: IP address wildcard shielded text (similar to the complement of the IP address mask).

Description Use the **network** command to enable an interface to run the OSPF protocol.

Use the **undo network** command to disable an interface from running OSPF.

By default, the interface does not belong to any area.

To run OSPF on an interface, the master IP address of this interface must be in the range of the network segment specified by this command. If only the slave 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 master 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 reside) as 6.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ospf 1
[SW7750-ospf-1] area 6
[SW7750-ospf-1-area-0.0.0.6] network 10.110.36.0 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 the default route to the NSSA area.

no-import-route: Specifies not to import route to the NSSA area.

no-summary: An ABR is disabled from transmitting summary_net LSAs to the NSSA area.

Description Use the **nssa** command to configure an OSPF area as an NSSA area.

Use the **undo nssa** command to cancel the function.

By default, no NSSA area is configured.

For all the routers connected to the NSSA area, the **nssa** command must be used to configure the area as the NSSA attribute.

The **default-route-advertise** argument is used to generate the default type-7 LSA. No matter whether the route 0.0.0.0 exists in the routing table on the ABR, the type-7 LSA default route will always be generated. The type-7 LSA default route is generated only when the route 0.0.0.0 exists in the routing table on the ASBR.

On the ASBR, if the **no-import-route** argument is provided, the external route imported by OSPF with the **import-route** command will not be advertised to NSSA area.

Example # Configure area 1 as NSSA area.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ospf 1
[SW7750-ospf-1] area 1
[SW7750-ospf-1-area-0.0.0.1] network 36.0.0.0 0.255.255.255
[SW7750-ospf-1-area-0.0.0.1] nssa
```

ospf

Syntax **ospf** [*process-id* [**router-id** *router-id*]]

undo ospf [*process-id*]

View System view

Parameter *process-id:* OSPF Process ID, ranging from 1 to 65,535. By default, the process ID is 1. *process-id* is locally significant.

router-id: Router ID used by an OSPF process, represented in dotted decimal notation.

Description Use the **ospf** command to enable OSPF

Use the **undo ospf** command to disable OSPF

After OSPF is enabled, you can perform the related configuration in OSPF view.

By default, the system does not run OSPF.

Related command: **network**.

Example # Enable OSPF.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] router id 10.110.1.8
[SW7750] ospf
[SW7750-ospf-1]
```

# Enable the running of the OSPF protocol with process ID specified as 120.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] router id 10.110.1.8
[SW7750] ospf 120
[SW7750-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:* Uses plain text authentication. The *password* argument is a string of up to eight characters.

key-id: ID of the authentication key in MD5 authentication mode, ranging from 1 to 255.

key: MD5 authentication key. If it is input in a plain text form, MD5 *key* is a string of 1 to 16 characters. It is displayed in a cipher text form with 24 characters in length when the **display current-configuration** command is executed. Inputting the MD5 *key* in a cipher text form with 24 characters in length 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 the OSPF packets.

The passwords for authentication keys of the routers on the same network segment must be identical. In addition, you need to use the **authentication-mode** command to set the authentication type of the area, so as to validate the configuration.

Related command:

authentication-mode.

Example

Configure area 1 where the network segment 131.119.0.0 of interface Vlan-interface 10 resides to support MD5 cipher text authentication. Set the authentication key identifier to 15 and the authentication key to abc.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ospf 1
[SW7750-ospf-1] area 1
[SW7750-ospf-1-area-0.0.0.1] network 131.119.0.0 0.0.255.255
[SW7750-ospf-1-area-0.0.0.1] authentication-mode md5
[SW7750-Vlan-interface10] ospf authentication-mode md5 15 abc
```

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 the cost for running OSPF on the interface.

Use the **undo ospf cost** command to restore the default costs.

For the switch, the default cost for running OSPF protocol on a VLAN interface is 1.

Example # Specify the cost spent when an interface runs OSPF as 33.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 10
[SW7750-Vlan-interface10] ospf cost 33
```

ospf dr-priority

Syntax **ospf dr-priority** *dr-priority-value*

undo ospf dr-priority

View Interface view

Parameter *dr-priority-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 preferred when the election conflict occurs.

Example # Set the priority of the interface Vlan-interface 10 to 8 during DR election.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 10
[SW7750-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*: OSPF Process ID. It ranges from 1 to 65535 and defaults to 1.

Description Use the **ospf mib-binding** command to bind MIB operation to the specified OSPF process.

Use the **undo ospf mib-binding** command to restore the default settings.

When OSPF enables the first process, OSPF always binds MIB operation to this process. You can use this command to bind MIB operation to another OSPF process.

To cancel the binding, use the **undo ospf mib-binding** command. OSPF will automatically re-bind MIB operation to the first process that it enables.

By default, MIB operation is bound to the OSPF process enabled first.

Example # Bind MIB operation to OSPF process 100.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ospf mib-binding 100
```

# Bind MIB operation to OSPF process 200.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ospf mib-binding 200
```

# Cancel the binding of MIB operation.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] 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 sending DD packets. That is, 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. You can use this command to configure the specified interface manually to write the MTU value area in DD packets when sending DD packets. That is, the actual MTU value of the interface is written in.

Example # Configure interface Vlan-interface 3 to write MTU value area when sending DD packets.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 3
[SW7750-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 point-to-multipoint.

p2p: Changes the interface network type to point-to-point.

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.

OSPF divides networks into four types based on link layer protocol:

- Broadcast: If Ethernet or FDDI is adopted, OSPF defaults the network type to broadcast.
- Non-Broadcast Multi-access (**nbma**): If Frame Relay, ATM, HDLC or X.25 is adopted, OSPF defaults the network type to NBMA.
- Point-to-Multipoint (**p2mp**): OSPF will not default the network type of any link layer protocol to **p2mp**. The general undertaking is to change a partially connected NBMA network to **p2mp** network if the NBMA network is not fully-meshed.
- Point-to-point (**p2p**): If PPP, LAPB or POS is adopted, OSPF defaults the network type to **p2p**.

If there is any router not supporting multicast addresses on a broadcast network, the network type of the interface can be changed to NBMA. Alternatively, the network type of the interface can be changed from NBMA to broadcast.

For a non-broadcast multi-accessible network to be of NBMA type, any two routers in the network must be directly reachable to each other through a virtual circuit. In other words, the network must be fully-meshed.

For a network not meeting this condition, the network type of the interface must be changed to point-to-multipoint. In this way, routing information can be exchanged between two routers not directly reachable to each other through another router that is directly reachable to the two routers.

If only two routers run OSPF in the same network segment, the network type of the interface can also be changed to point-to-point.

Note that you must use the **peer** command to configure the peer if the network type of the interface is NBMA or manually changed to NBMA with the **ospf network-type** command.

Related command: **ospf dr-priority**.

Example # Set the interface Vlan-interface 10 to NBMA type.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 10
[SW7750-Vlan-interface10] ospf network-type nbma
```

ospf timer dead

Syntax **ospf timer dead** *seconds*

undo ospf timer dead

View Interface view

Parameter *seconds:* Dead interval of the OSPF neighbor. It is in seconds and ranges from 1 to 65,535.

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 is 40 seconds for the OSPF peers of **p2p** and **broadcast** interfaces and is 120 seconds for those of **p2mp** and **nbma** interfaces.

The dead interval of OSPF peers means that, within this interval, if no Hello message is received from the peer, the peer will be considered to be invalid. The value of **dead** *seconds* should be at least four times of that of the **Hello** *seconds*. The **dead** *seconds* for the routers on the same network segment must be identical.

Related command: **ospf timer hello**.

Example # Set the peer dead interval on the interface Vlan-interface 10 to 80 seconds.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 10
[SW7750-Vlan-interface10] ospf timer dead 80
```

ospf timer hello

Syntax **ospf timer hello** *seconds*

undo ospf timer hello

View Interface view

Parameter *seconds*: Interval, in seconds, at which an interface transmits hello packet. It ranges from 1 to 255.

Description Use the **ospf timer hello** command to configure the interval for transmitting Hello messages 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 **p2p** or **broadcast** type to transmit Hello messages, and 30 seconds for an interface of **p2mp** or **nbma** type.

Related command: **ospf timer dead**.

Example # Configure the interval of transmitting Hello messages on the interface Vlan-interface 10 to 20 seconds.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 10
[SW7750-Vlan-interface10] ospf timer hello 20
```

ospf timer poll

Syntax **ospf timer poll** *seconds*

undo ospf timer poll

View Interface view

Parameter *seconds*: Poll Hello interval in seconds. It ranges from 1 to 65,535 and defaults to 40.

Description Use the **ospf timer poll** command to configure the poll Hello packet interval on NBMA and **p2mp** network.

Use the **undo ospf timer poll** command to restore the default poll interval.

On an NBMA or **p2mp** network, if a neighbor becomes invalid, Hello packet will be transmitted at the interval of **poll** *seconds*. You can configure the **poll** *seconds* to specify how often the interface transmits Hello packet before it establishes adjacency with the adjacent router. Poll seconds should be no less than 3 times of Hello.

Example # Configure to transmit poll Hello packet through interface Vlan-interface 20 every 120 seconds.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 20
[SW7750-Vlan-interface20] ospf timer poll 120
```

ospf timer retransmit

Syntax **ospf timer retransmit** *interval*

undo ospf timer retransmit

View Interface view

Parameter *interval:* Interval, in seconds, for retransmitting LSA on an interface. It ranges from 1 to 3600 and defaults to 5.

Description Use the **ospf timer retransmit** command to configure the interval for LSA retransmission on an interface.

Use the **undo ospf timer retransmit** command to restore the default interval value for LSA retransmission 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 retransmission interval, this LSA will be retransmitted.

The LSA retransmit between adjacent routers should not be set too short; otherwise, unexpected retransmission will occur (See RFC2328).

Example # Specify the retransmit for LSA transmission between the interface Vlan-interface 10 and the adjacent routers to 12 seconds.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 10
[SW7750-Vlan-interface10] ospf timer retransmit 12
```

ospf trans-delay

Syntax **ospf trans-delay** *seconds*

undo ospf trans-delay

View Interface view

Parameter *seconds*: LSA transmission delay on an interface. It ranges from 1 to 3,600 and defaults to 1 (in seconds).

Description Use the **ospf trans-delay** command to configure the LSA transmission delay on an interface.

Use the **undo ospf trans-delay** command to restore the default LSA transmission delay on an interface.

LSA ages in the "link state database" (LSDB) of the router as time goes by (1 added every second), but it does 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.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 10
[SW7750-Vlan-interface10] ospf trans-delay 3
```

peer

Syntax **peer** *ip-address* [**dr-priority** *dr-priority-value*]

undo peer *ip-address*

View OSPF view

Parameter *ip-address:* IP address of the peer, represented in dotted decimal notation.

dr-priority-value: Value of the corresponding priority of a neighbor in the NBMA network. It ranges from 0 to 255 and defaults to 1.

Description Use the **peer** command to configure the IP address of the neighbor router and specify DR priority on an NBMA network.

Use the **undo peer** command to cancel this configuration.

Example # Configure the IP address of the neighbor router as 10.1.1.1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ospf 1
[SW7750-ospf-1] peer 10.1.1.1
```

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 the highest preference selected for forwarding IP packets.

Example # Specify the preference of an imported external route of the AS as 160.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ospf 1
[SW7750-ospf-1] preference ase 160
```

protocol multicast-mac enable

Syntax **protocol multicast-mac enable**

undo protocol multicast-mac enable

View System view

Parameter None

Description Use the **protocol multicast-mac enable** command to enable protocol multicast MAC address delivery.

Use the **undo protocol multicast-mac enable** command to disable protocol multicast MAC address delivery.

By default, protocol multicast MAC address delivery is enabled.

If OSPF is configured when Layer 2/Layer 3 multicast function is enabled in the system, the system will multicast the broadcast routing protocol packets because the broadcast MAC address and multicast MAC address used by the delivered OSPF routing protocol are the same. This makes broadcast packets unable to reach the destination host and adversely affects the running of the routing protocol.

You can disable the protocol multicast MAC address delivery function so that the system correctly forwards OSPF multicast packets, thus ensuring the normal running of the routing protocol.

- *Disable protocol multicast MAC address delivery (with the **undo protocol multicast-mac enable** command) if you are configuring OSPF with Layer 2/Layer 3 multicast function enabled in the system.*
- *You do not need to disable protocol multicast MAC address delivery if the system is enabled with OSPF only.*

Example # Disable protocol multicast MAC address delivery in the system.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750]undo protocol multicast-mac enable
```

reset ospf

Syntax **reset ospf** [**statistics**] { **all** | *process-id* }

View User view

Parameter **all**: Resets all OSPF processes.

process-id: OSPF Process ID, ranging from 1 to 65535. If this argument is not specified, all OSPF processes will be reset.

statistics: Resets OSPF statistics.

Description Use the **reset ospf all** command to reset all OSPF processes.

Use the **reset ospf** *process-id* command to reset the specified OSPF process and clear the statistics.

After you use this command to reset an OSPF process:

- Invalid LSA is cleared immediately before LSA times out.

- A new Router ID takes effect if the Router ID changes.
- DR and BDR are re-elected conveniently.
- OSPF configuration before the restart will not lose.

After this command is issued, the system will prompt you to confirm whether to re-enable OSPF.

Example # Reset all the OSPF processes.

```
<SW7750> reset ospf all
```

# Reset OSPF process 200.

```
<SW7750> reset ospf 200
```

router id

Syntax **router id** *router-id*

undo router id

View System view

Parameter *router-id*: Router ID, in dotted decimal notation, in the range of 0 to 255.

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.

When the router ID is configured manually, the IDs of any two routers cannot be same in the autonomous system. Thus, you can select the IP address of an interface as the ID of this router.

Related command: **ospf**.

A modified router ID takes effect only after OSPF is re-enabled.

Example # Set the router ID to 10.1.1.3.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] router id 10.1.1.3
```

silent-interface

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

undo silent-interface *interface-type interface-number*

View

OSPF view

Parameter

interface-type interface-number: Interface number.

Description

Use the **silent-interface** command to disable an interface from transmitting OSPF packet.

Use the **undo silent-interface** command to restore the default setting.

By default, the interface is enabled to transmit OSPF packet.

To prevent the router on some network from receiving the OSPF routing information, you can use this command to disable this interface from transmitting OSPF packet. On the switch, this command can be used to enable/disable OSPF packet transmission through the specified VLAN interface.

Example

Disable interface Vlan-interface 20 from transmitting OSPF packet.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ospf 1
[SW7750-ospf-1] silent-interface Vlan-interface 20
```

snmp-agent trap enable ospf

Syntax

snmp-agent trap enable ospf [*process-id*] [**ifstatechange** | **iftxretransmit** | **ifrxbadpkt** | **ifcfgerror** | **virifstatechange** | **nbrstatechange** | **virnbrstatechange** | **virifcfgerror** | **ifauthfail** | **virifauthfail** | **virifrxbadpkt** | **viriftxretransmit** | **originatelsa** | **maxagelsa** | **lsdboverflow** | **lsdbapproachoverflow**]*

undo snmp-agent trap enable ospf [*process-id*] [**ifstatechange** | **iftxretransmit** | **ifcfgerror** |**virifstatechange** | **nbrstatechange** | **virnbrstatechange** | **virifcfgerror** | **ifauthfail** | **virifauthfail** | **ifrxbadpkt** | **virifrxbadpkt** | **viriftxretransmit** | **originatelsa** | **maxagelsa** | **lsdboverflow** | **lsdbapproachoverflow**]*

View

System view

Parameter

process-id: OSPF Process ID, in the range of 1 to 65,535. If you do not specify a process ID, this command applies to all current OSPF processes.

ifstatechange, **virifstatechange**, **nbrstatechange**, **virnbrstatechange**, **ifcfgerror**, **virifcfgerror**, **ifauthfail**, **virifauthfail**, **ifrxbadpkt**, **iftxretransmit**, **virifrxbadpkt, viriftxretransmit**, **originatelsa**, **maxagelsa, lsdboverflow**, and **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 does not apply 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 “SNMP Configuration Commands” on page 877.

Example # Enable the TRAP function for OSPF process 100.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] 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, in seconds. It ranges from 1 to 10 and defaults to 5.

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. Adjusting SPF calculation interval restrains frequent network changes, which may occupy too many bandwidth resources and router resources.

Example # Set the OSPF route calculation interval of 3Com to 6 seconds.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ospf 1
[SW7750-ospf-1] spf-schedule-interval 6
```

stub

Syntax **stub** [**no-summary**]

undo stub

View OSPF Area view

Parameter **no-summary**: Disables an ABR from transmitting Summary LSAs to the STUB area.

Description Use the **stub** command to configure the type of an OSPF area as "stub".

Use the **undo stub** command to cancel the settings.

By default, no area is set to be the STUB area.

If the router is an ABR, it will send a default route to the connected stub area . Use the **default-cost** command to configure the default route cost. In addition, you can specify the **no-summary** argument in the **stub** command to disable the receiving of type-3 LSAs by the stub area connected to the ABR.

Related command: **default-cost**.

Example # Set the type of OSPF area 1 to STUB.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ospf 1
[SW7750-ospf-1] area 1
[SW7750-ospf-1-area-0.0.0.1] stub
```

vlink-peer

Syntax **vlink-peer** *router-id* [**hello** *seconds* | **retransmit** *seconds* | **trans-delay** *seconds* | **dead** *seconds* | **simple** *password* | **md5** *keyid key*]*

undo vlink-peer *router-id*

View OSPF Area view

Parameter *route-id*: Router ID of virtual link peer.

hello *seconds*: Specifies the interval, in seconds, at which the router transmits hello packet. It ranges from 1 to 8192 and defaults to 10. This value must equal the **hello** *seconds* value of the router virtually linked to the interface.

retransmit *seconds:* Specifies the interval, in seconds, for retransmitting the LSA packets on an interface. It ranges from 1 to 3600 and defaults to 5.

trans-delay *seconds:* Specifies the delay, in seconds, for transmitting LSA packets on an interface. It ranges from 1 to 3600 and defaults to 1.

dead *seconds*: Specifies the interval, in seconds, of death timer. It ranges from 1 to 8192 and defaults to 40. This value must equal the **dead** *seconds* of the router virtually linked to it and must be at least four times of the hello *seconds*.

simple *password:* Specifies the simple text authentication password, which contains up to eight characters, of the interface. This value must equal the authentication key of the virtually linked peer.

keyid: MD5 authentication key ID. It ranges from 1 to 255. It must be equal to the authentication key ID of the virtually linked peer.

key: MD5 authentication key. If you use simple text authentication key, you can input a string containing 1 to 16 characters. When you use the **display current-configuration** command to display system information, the MD5 authentication key is displayed in the form of cipher text with a length of 24 characters. Inputting the *key* in the form of cipher text with a length of 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, an OSPF area must be connected to the backbone network. You can use the **vlink-peer** command to keep the connectivity. Virtual link can be regarded as a common interface that uses OSPF because the principle for configuring the parameters such as hello, retransmit, and trans-delay on it is similar.

Note that, when configuring virtual link authentication, you use the **authentication-mode** command to specify the authentication mode as MD5 cipher text or simple text on the backbone network.

Related command:

authentication-mode, **display ospf peer**.

Example

Create a virtual link to 10.110.0.3 and use the MD5 cipher authentication mode.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ospf 1
[SW7750-ospf-1] area 10.0.0.0
[SW7750-ospf-1-area-10.0.0.0] vlink-peer 10.110.0.3 md5 3 345
```

32 INTEGRATED IS-IS CONFIGURATION COMMANDS

The router in this document refers to a generic router and an Ethernet switch running routing protocols.

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**: Specifies to send the password in plain text.

md5: Specifies to send the password encrypted with MD5.

password: Specifies the password to be set. For the **simple** authentication mode, the *password* must be plain text. For the **md5** authentication mode, the password can be either plain text or ciphertext, and the result depends on the input. A plain password can be a string no longer than 16 bytes, such as user918. A cipher password must be a ciphertext of 24 bytes, such as (TT8F]Y5SQ=^Q‘MAF4<1!!.

ip: Specifies the system to check the configuration for the corresponding field of IP in LSP.

osi: Specifies the system to check the configuration for the corresponding field of OSI in LSP.

Whether a password should use the **ip** keyword or the **osi** keyword is not affected by the actual network environment.

Description Use the **area-authentication-mode** command to configure IS-IS to authenticate the packets (LSP, CSNP and PSNP) received from level-1 route using the predefined mode and password.

Use the **undo area-authentication-mode** command to disable IS-IS from authenticating the received packets above.

The system will neither authenticate the packets received from level-1 route nor check its password by default.

We can use this command to clear all leve-1 routing packets not compatible with the area authentication password set by the command. And at the same time, we also instruct the system to follow a specific mode to insert the area authentication password in all the level-1 routing packets sent from the local node.

Related command: **reset isis all**, **domain-authentication-mode**, and **isis authentication-mode**.

Example # Set the area authentication password to hello, and the authentication mode to simple.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] isis
[SW7750-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**: Specifies to receive and send narrow packets only.

wide: Specifies to receive and send wide packets only.

compatible: Specifies to receive or send both wide and narrow packets.

narrow-compatible: Specifies to receive both narrow and wide packets, but send only narrow packets.

wide-compatible: Specifies to receive both narrow and wide packets, but send only wide packets.

relax-spf-metric: Specifies to allow receiving routes with cost bigger than 1,024. If this keyword is not configured, any route with cost larger than 1,024 will be dropped. This configuration is only available when the **compatible** keyword or when the **narrow-compatible** keyword is provided.

Description Use the **cost-style** command to set the cost style of packets received or sent by IS-IS router.

Use the **undo cost-style** command to restore the default cost style.

Only narrow packets can be received and sent by default.

Related command: **isis cost**.

Example # Set the router to send only narrow packets, but receive both narrow and wide ones.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] isis
[SW7750-isis] cost-style narrow-compatible
```

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 the specified route-policy, which is a string containing 1 to 19 characters.

Description Use the **default-route-advertise** command to enable the L1 and L2 routers to generate default routes.

Use the **undo default-route-advertise** command to disable the function.

By default, L2 routers generate default routes.

This command can be executed on L1 routers or L2 routers. Defaults routes are generated in L2 LSP by default. Carrying out the **apply isis level-1** command in routing policy view will generate default routes in L1 LSP. Carrying out the **apply isis level-2** command in routing policy view will generate default routes in L2 LSP. Carrying out the **apply isis level-1-2** command in routing policy will generate default routes in L1 LSP and L2 LSP respectively.

Example # Configure the current router to generate default route in LSP.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750-isis] default-route-advertise
```

display isis brief

Syntax display isis brief

View Any view

Parameter None

Description Use the **display isis brief** command to display the brief information about IS-IS.

Example # Display the brief information about IS-IS.

```
<SW7750> display isis brief
                ISIS  Protocol Brief Information:
```

```
System protocol supported by IS-IS:  none
Is-level:  level-1-2
Cost-style:  narrow
Preference:  15
CLNS Preference:  15
Timers:
     spf-delay-interval:  5000
     spf-slice-size:  0
     lsp-max-age:  1200
     lsp-refresh:  900
     interval between SPFs:  level-1  10
                             level-2  10
```

display isis interface

Syntax **display isis interface** [**verbose**]

View Any view

Parameter **verbose**: Displays the detailed information about the interface.

Description Use the **display isis interface** command to view the information about the IS-IS-enabled interfaces.

The information displayed by this command includes the interface name, interface IP address, interface link state and so on. Besides all the information displayed by the **display isis interface** command, the **display isis interface verbose** command will display the IS-IS configuration information related to the interface, such as CSNP packets broadcast intervals, Hello packets broadcast intervals and the number of invalid Hello packets.

Example # Display the information about the IS-IS-enabled interface.

```
<SW7750> 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   No/No
```

# Display the detailed information about the IS-IS-enabled interface.

```
<SW7750> 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    No/No
  Secondary IP Address        :
  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**] | [*lsp-id* | **local**] | **verbose**]*

View Any view

Parameter **l1**, **level-1**: Specifies level-1 routing connection state database.

l2, **level-2**: Specifies level-2 routing connection state database.

lsp-id: LSP ID of the network-entity-title.

local: Specifies to display LSP information generated locally.

verbose: Specifies to display the detailed information of link state database.

Description Use the **display isis lsdb** command to display IS-IS link state database.

Example # Display a piece of LSP information.

```
<SW7750> 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 display the mesh-group of IS-IS.

You can use this command to view the mesh-group configuration of the current routing interface.

Example # Configure the IS-IS-enabled Vlan-interface 10 and Vlan-interface 20 of the router to belong to mesh group 100.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750-Vlan-interface10] isis mesh-group 100
[SW7750-Vlan-interface10] interface Vlan-interface 20
[SW7750-Vlan-interface20] isis mesh-group 100
```

# Display the configuration information of the IS-IS mesh group.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750-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**: Displays the area address advertised in a neighbor's Hello packet when this keyword is provided; displays only the brief information if this keyword is not specified.

Description Use the **display isis peer** command to display the information of the IS-IS neighbor.

Besides all the information displayed by the **display isis peer** command, the **display isis peer verbose** command will display the neighbor's area address, holdtime of Up state and the IP address of the directly-connected interface.

Example # Display the detailed information about IS-IS neighbors.

```
<SW7750> display isis peer verbose
System ID      Interface          Circuit ID        State HoldTime Type Pri
0000.0000.6502 Vlan-interface1000 0000.0000.6502.02 Up  8s       L1   64
  Area Address:  01  IP Address: 7.7.7.7   Period: 01:51:13

System ID      Interface          Circuit ID        State HoldTime Type Pri
0000.0000.6502 Vlan-interface1001 0001.0000.6506.02 Up  24s      L1   64
  Area Address:  01  IP Address: 6.6.6.6   Period: 00:53:50
```

# Display the information about IS-IS neighbors.

```
<SW7750> display isis peer
System ID      Interface          Circuit ID        State HoldTime Type Pri
0000.0000.6502 Vlan-interface1000 0000.0000.6502.02 Up 9s        L1   64
0000.0000.6502 Vlan-interface1001 0001.0000.6506.02 Up 24s       L1   64
```

display isis route

Syntax **display isis route** { **clns | ip** }

View Any view

Parameter **ip**: Displays IP-based IS-IS routing information.

clns: Displays OSI-based IS-IS routing information.

Description Use the **display isis route** command to display the IS-IS routing information.

Example # Display the output information of the **display isis ip route** command.

```
<SW7750> display isis route
                  ISIS IP Level - 2 Routing 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
--------------------------------------------------------------------------
D 111.1.0.0/16       10               Direct          Vlan-interface111  R/L/-
D 170.1.1.0/24       10               Direct          Vlan-interface170  R/L/-
I 131.1.0.0/16       20               111.1.1.1       Vlan-interface111  R/-/-
I 133.1.0.0/16       20               111.1.1.1       Vlan-interface111  R/-/-
I 135.1.0.0/16       20               111.1.1.1       Vlan-interface111  R/-/-
D 145.1.0.0/16       10               Direct          Vlan-interface145  R/L/-
```

display isis spf-log

Syntax **display isis spf-log**

View Any view

Parameter None

Description Use the **display isis spf-log** command to display the log record of IS-IS SPF calculation.

Example # Display the log record of IS-IS SPF calculation.

```
<SW7750> display isis spf-log
Details of Level 2 SPF Run:
 -------------------------------------------------------------------------------
      Trig.Event                    No.Of Nodes     Duration(ms)     StartTime
    IS_SPFTRIG_NEWADJ               2               74               0:10:55
    IS_SPFTRIG_NEWADJ               2               670              0:10:24
    IS_SPFTRIG_NEWADJ               2               23               0:10:2
    IS_SPFTRIG_NEWADJ               2               30               0:9:32
    IS_SPFTRIG_NEWADJ               2               34               0:9:1
    IS_SPFTRIG_NEWADJ               2               111              0:7:59
    IS_SPFTRIG_NEWADJ               2               302              0:25:1
    IS_SPFTRIG_NEWADJ               2               60               0:24:30
    IS_SPFTRIG_NEWADJ               2               232              0:20:31
    IS_SPFTRIG_NEWADJ               2               42               0:19:58
    IS_SPFTRIG_NEWADJ               2               37               0:19:32
    IS_SPFTRIG_NEWADJ               2               34               0:19:0
    IS_SPFTRIG_CIRC_UP              2               633              0:18:51
    IS_SPFTRIG_NEWADJ               2               78               0:17:59
    IS_SPFTRIG_ADJDOWN              0               -59863           0:15:7
    IS_SPFTRIG_NEWADJ               2               30               0:15:3
    IS_SPFTRIG_NEWADJ               2               32               0:14:2
    IS_SPFTRIG_NEWADJ               2               202              0:13:34
    IS_SPFTRIG_CIRC_DOWN            2               215              0:12:17
    IS_SPFTRIG_CIRC_UP              2               27               0:12:7
```

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: Specifies to send the password in plain text.

md5: Specifies to send the password after encrypted with MD5.

password: Specifies the password to be set. For the **simple** authentication mode, the *password* must be plain text. For **md5** authentication mode, the password can be either plain text or ciphertext, and the result depends on the input. A plain password can be a string no longer than 16 bytes, such as user918. A cipher password must be a ciphertext of 24 bytes, such as _(TT8F]Y5SQ=^Q‘MAF4<1!!.

ip: Specifies the system to check the configuration for the corresponding field of IP in LSP.

osi: Specifies the system to check the configuration for the corresponding field of OSI in LSP.

Whether a password should use the **ip** keyword or the **osi** keyword is not affected by the actual network environment.

Description

Use the **domain-authentication-mode** command to configure IS-IS routing domain to authenticate the received level-2 packets (LSP, CSNP and PSNP) using the predefined mode and password.

Use the **undo domain-authentication-mode** command to disable IS-IS from authenticating the received packets above.

The system will neither authenticate the received level-2 routing packet nor check its password by default.

You can use this command to clear all leve-2 routing packets not matching the domain-authentication password set by the command. At the same time, we also instruct the system to follow a specific mode to insert the area-authentication password in all the level-2 routing packets sent from the local node.

Related command:

area-authentication-mode, and **isis authentication-mode**.

Example

Use the simple mode and set the password to abc to authenticate level-2 routing packets.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] isis
[SW7750-isis] domain-authentication-mode simple abc
```

filter-policy export

Syntax **filter-policy** *acl-number* **export** [*protocol*]

undo filter-policy *acl-number* **export** [*protocol*]

View IS-IS view

Parameter *acl-number*: ACL number in the range of 2,000 to 3,999.

protocol: Protocol used to advertise routing information, including **direct**, **static**, **rip**, **bgp**, **ospf**, **ospf-ase**, **ospf-nssa** currently.

Description Use the **filter-policy export** command to enable IS-IS to filter the routes advertised by other routing protocols.

Use the **undo filter-policy export** command to disable the configured filter rules.

IS-IS does not filter the routes advertised by other routing protocols by default.

- *The **filter-policy export** command takes effect only on the routes imported through the **import-route** command. If the **filter-policy export** command is configured while the **import-route** command is not configured to import other non-IS-IS routes, the **filter-policy export** command does not take effect.*
- *If the protocol argument is not provided in the **filter-policy export** command, the command takes effect on all the routes imported to the local device using the **import-route** command.*

Related command: **filter-policy import**.

Example # Use ACL 2000 to filter the routes imported through IS-IS.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] isis
[SW7750-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*: ACL number in the range of 2,000 to 3,999.

Description

Use the **filter-policy import** command to enable IS-IS to filter the received routes.

Use the **undo filter-policy import** command to disable IS-IS from filtering the received routes.

IS-IS does not filter the received routes by default.

In some circumstances, only the routing information satisfying certain conditions will be received. You can configure the filtering condition by setting the filter-policy parameters.

Related command:

filter-policy export.

Example

Use ACL 2000 to filter the received routes.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] isis
[SW7750-isis] filter-policy 2000 import
```

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 set IS-IS to drop the LSP when it detects LSP checksum errors.

Use the **undo ignore-lsp-checksum-error** command to set IS-IS to ignore LSP checksum errors.

IS-IS ignores LSP checksum errors by default.

When the local IS-IS receives a LSP packet, it will check the LSP packet and compare the checksum calculated with that in the LSP packet. By default, the LSP packets will not be dropped even if the checksum is wrong. You can use the **ignore-lsp-checksum-error** to configure IS-IS to drop the LSP packet in case of checksum error.

Example

Configure IS-IS to drop the LSP packet in case of checksum error.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] isis
[SW7750-isis] ignore-lsp-checksum-error
```

import-route

Syntax **import-route** *protocol* [**allow-ibgp**] [**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:* Redistributes routes from the routing protocol, which can be **direct**, **static**, **rip**, **bgp**, **ospf**, **ospf-ase**, or **ospf-nssa**.

value: Cost of the imported route, in the range of 0 to 63.

allow-ibgp: Redistributes iBGP routes.

type: Specifies the type of the routing cost. If it is **internal**, then it is a route within an area; if it is **external**, it is a route between areas. The type is **internal** by default.

level-1: Redistributes routes to Level-1 routing table.

level-2: Redistributes routes to Level-2 routing table. If no level is specified, the routes are imported to level-2 routing table by default.

level-1-2: Redistributes routes to Level-1 and level-2 routing tables.

route-policy *route-policy-name*: Redistributes only routes satisfying the matching conditions of the designated route-policy. The *route-policy-name* argument is a string containing 1 to 19 characters.

Description Use the **import-route** command to enable IS-IS to filter the imported routes.

Use the **undo import-route** command to disable IS-IS from importing other protocols' routing information.

IS-IS does not import other protocols' routing information by default.

IS-IS takes all the routes imported to the routing domain as external routes, which describe how to select a routes to a destination outside of the routing domain.

Note that:

*The **import-route bgp** command redistributes only eBGP routes, while the **import-route bgp allow-ibgp** command redistributes both iBGP and eBGP routes. Because the redistributed iBGP routes have the AS-PATH attribute removed, routing loops may occur. Therefore, use the **allow-ibgp** keyword with caution.*

Related command: **import-route isis level-2 into level-1**.

Example # Import a static route with the cost of 15.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] isis
[SW7750-isis] import-route static 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

View IS-IS view

Parameter *acl-number*: ACL number in the range of 2000 to 3999. It can be either basic ACLs or advanced ACLs.

Description Use the **import-route isis level-2 into level-1** command to import the routing information of Level-2 area to Level-1 area.

Use the **undo import-route isis level-2 into level-1** command to disable this function.

By using the filter policy to filter the routes during the route penetration from Level-2 to Level-1, you call advertise in the Level-1 area only those routes that have passed the filter.

The routing information in Level-2 area will not be advertised in Level-1 area by default.

Related command: **import-route**.

Example # Set the router to penetrate routes from Level-2 to Level-1 through ACL.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] isis
[SW7750-isis] import-route isis level-2 into level-1 acl 2100
```

isis

Syntax **isis** [*tag*]

undo isis [*tag*]

View System view

Parameter *tag*: Name of an IS-IS routing process, consisting of no more than 128 characters. Its length can be 0, that is, the *tag* argument can be null.

Description Use the **isis** command to start a corresponding IS-IS routing process and enter the IS-IS view.

Use the **undo isis** command to delete the specified IS-IS routing process.

IS-IS routing processes are disabled by default.

Before running IS-IS protocol normally, you must first use the **isis** command to enable IS-IS process, then use the **network-entity** command to configure a network entity title (NET) for the router, and then use the **isis enable** command to enable each interface that need to run the IS-IS process.

Only one IS-IS routing process can be enabled on a router.

Related command: **isis enable**, and **network-entity**.

Example # Start the IS-IS routing process, with the system ID as 0000.0000.0002, and area ID as 01.0001.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] isis
[SW7750-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 Interface view

Parameter **simple**: Specifies to send the password in plain text.

md5: Specifies to send the password in ciphertext.

password: Specifies a password. For **simple** authentication mode, the *password* must be plain text. For **md5** authentication mode, the password can be either plain text or ciphertext, and the result depends on the input. A plain password can be a string no longer than 16 bytes, such as user918. A cipher password must be a ciphertext of 24 bytes, such as _(TT8F]Y5SQ=^Q‘MAF4<1!!.

level-1: Specifies to set a password for L1.

level-2: Specifies to set a password for L2.

ip: Specifies the system to check the configuration for the corresponding field of IP in LSP.

osi: Specifies the system to check the configuration for the corresponding field of OSI in LSP.

Whether a password should use the **ip** keyword or the **osi** keyword is not affected by the actual network environment.

Description Use the **isis authentication-mode** command to authenticate the IS-IS hello packets of the specified level using the specified authentication mode and password on the IS-IS interface.

Use the **undo isis authentication-mode** command to disable the authentication and remove the password.

There is no password or authentication by default.

If there is no other parameter but the password, then only level-1 and osi are available.

Related command: **area-authentication-mode**, and **domain-authentication-mode**.

Example # Set the plain password as tangshi for Level-1 adjacency on Vlan-interface 10.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 10
[SW7750-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**: Specifies to set up only level-1 adjacency for the interface.

level-1-2: Specifies to set up level-1-2 adjacency for the interface.

level-2: Specifies to set up only level-2 adjacency for the interface.

Description Use the **isis circuit-level** command to set link adjacency for the level-1-2 router.

Use the **undo isis circuit-level** command to resume the default configuration of link adjacency for the level-1-2 router.

An interface can be configured level-1-2 adjacency by default.

This command is only available for a level-1-2 router. If the local host is level-1-2 router and it need to set up some adjacency (**level-1** or **level-2**) with a peer router, then you can use this command to prescribe the local interface to receive and send only the hello packets. An interface can receive and send only one type of hello packet on a point-to-point link. You can use this command to reduce the router's processing time to save bandwidth.

Related command: **is-level**.

Example # Set the level-1 attributes for Vlan-interface 10 to prohibit sending and receiving level-2 Hello packets when the interface is connected to a non-backbone router within the same area.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 10
[SW7750-Vlan-interface10] isis enable
[SW7750-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 value for corresponding SPF calculation, in the range of 0 to 63. It is 10 by default.

level-1: Indicates the link cost corresponding to Level-1 layer.

level-2: Indicates the link cost corresponding to Level-2 layer.

Description Use the **isis cost** command to set the interface link cost for SPF calculation.

Use the **undo isis cost** command to resume the default link cost value.

If neither level-1 nor level-2 is assigned in the configuration, then both **level-1** and **level-2** are configured by default.

You are recommended to configure a proper link cost for each interface; otherwise, the link cost for IS-IS route calculation may not reflect the correct cost.

Example # Set the Level-2 link cost to 5 for Vlan-interface10.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 10
[SW7750] interface Vlan-interface 10
[SW7750-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*: Specifies the priority for selecting DIS, ranging from 0 to 127, with the default as 64.

level-1: Specifies the priority for selecting level-1 DIS.

level-2: Specifies the priority for selecting level-2 DIS.

If neither level-1 nor level-2 is specified in this command, then the level-1 and level-2 priority is configured by default.

Description Use the **isis dis-priority** command to specify the priority for selecting corresponding DIS.

Use the **undo isis dis-priority** command to resume the default priority.

Unlike DR of OSPF, there is no backup DIS for IS-IS and the router with 0 priority can also select DIS.

Related command: **area-authentication-mode**, and **domain-authentication-mode**.

Example # Configure the priority as 127 for Vlan-interface 10.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 10
[SW7750-Vlan-interface10] isis dis-priority 127 level-2
```

isis enable

Syntax **isis enable** [**clns** | **ip**] [*tag*]

undo isis enable [**clns** | **ip**] [*tag*]

View Interface view

Parameter *tag*: Name assigned to the IS-IS routing process when the **isis** command is executed in system view. If this argument is not specified, it is null.

clns: Specifies to enable IS-IS routing processes based on OSI protocol stack on the interface.

ip: Specifies to enable IS-IS routing processes based on TCP/IP protocol stack on the interface. By default, IS-IS routing processes based on TCP/IP protocol stack are enabled.

Description Use the **isis enable** command to enable the corresponding IS-IS routing process for the interface.

Use the **undo isis enable** command to disable this configuration.

The interface does not enable the IS-IS routing process by default.

Before running IS-IS protocol normally, you must use the **isis** command to enable IS-IS process, and use the **network-entity** command to configure a network entity title (NET) for the router, and then use the **isis enable** command to enable each interface that need to run the IS-IS process.

Related command: **isis**, and **network-entity**.

Example # Enable the IS-IS routing process on Vlan-interface 10.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] isis abc
[SW7750-isis] network-entity 10.0001.1010.1020.1030.00
[SW7750] interface Vlan-interface 10
[SW7750-Vlan-interface10] isis enable abc
```

isis mesh-group

Syntax **isis mesh-group** { *mesh-group-number* | **mesh-blocked** }

undo isis mesh-group

View Interface view

Parameter *mesh-group-number*: Mesh group number, ranging from 1 to 4,294,967,295.

mesh-blocked: After this parameter is configured, the interface will be blocked to 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 an interface from a mesh group.

An interface is not in any mesh group and can flood LSP normally by default.

For an interface not in a mesh group, it follows the normal process to flood the received LSP to other interfaces. For the NBMA network with high connectivity and multiple point-to-point links, this will cause repeated LSP flooding and bandwidth waste.

After an interface is added to a mesh group, it will only flood a received LSP to interfaces not belonging to the same mesh group.

When you add an interface to a mesh group or block the interface, make sure to retain some redundancy so that a link failure will not affect the normal LSP packet flooding.

Example # Add the IS-IS-enabled Vlan-interface 20 to mesh-group 3.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750-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*: Interval in seconds of sending CSNP packets over broadcast network, ranging from 1 to 65,535, with the default as 10 seconds.

level-1: Specifies the Level-1 time interval for sending CSNP packets.

level-2: Specifies the Level-2 time interval for sending CSNP packets.

If neither the **level-1** keyword nor the **level-2** keyword is specified, both the level-1 interval and the level-2 interval are set.

Description Use the **isis timer csnp** command to specify the time interval for sending CSNP packet over broadcast network.

Use the **undo isis timer csnp** command to resume the default value of 10 seconds.

This command only applies to the DIS router, which sends CSNP packets periodically. Besides, DIS is separated to Level-1 and Level-2, and their time intervals should be configured respectively.

Example # Configure Level-2 CSNP packets to be sent every 15 seconds over Vlan-interface 10.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 10
[SW7750-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: Interval in seconds for sending Hello packets, ranging from 3 to 255, with the default as 10 seconds.

level-1: Specifies the time interval for sending Level-1 Hello packets.

level-2: Specifies the time interval for sending Level-2 Hello packets.

If neither the **level-1** keyword nor the **level-2** keyword is specified, both the level-1 interval and the level-2 interval are set.

Description

Use the **isis timer hello** command to specify the time interval for sending the corresponding level Hello packets.

Use the **undo isis timer hello** command to resume the default value of 10 seconds.

The hello time interval must be configured respectively for the Level-1 and Level-2 packets on a broadcast network, because these two types of hello packets are sent separately. A point-to-point link does not require this. The shorter the time interval is, the more system resources will be occupied to send Hello packets, so you should configure a proper time interval depending on the specific requirements.

Related command:

isis timer holding-multiplier.

Example

Configure Level-2 Hello packets to be sent every 20 seconds over Vlan-interface 10.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 10
[SW7750-Vlan-interface10] isis timer hello 20 level-2
```

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 invalid Hello packets of an IS-IS neighbor, in the range of 3 to 1,000.

level-1: Specifies the number of invalid Hello packets of a Level-1 IS-IS neighbor.

level-2: Specifies the number of invalid Hello packets of a Level-2 IS-IS neighbor.

If neither the **level-1** keyword nor the **level-2** keyword is specified, the command takes effect on both level-1 and level-2 IS-IS neighbors.

Description

Use the **isis timer holding-multiplier** command to configure the number of invalid Hello packets for an IS-IS neighbor. When a specified number of Hello packets are not received from a neighbor, the neighbor will be considered as invalid.

Use the **undo isis timer holding-multiplier** command to resume the default configuration.

The number of invalid Hello packets is three by default.

You can configure the time intervals of Hello packets separately for Level-1 and Level-2 peers. But for point-to-point link, as there is only one kind of Hello packet, so you need not specify Level-1 or Level-2.

In fact, the number of invalid Hello packets is used to configure Holddown time. If a router receives no Hello packet from peer router within Holddown time, it will take the peer router as invalid. Depending on the interface configuration, the Holddown time can be configured differently for different routers within an area. You can adjust the Holddown time by changing either the time interval for sending Hello packets or the number of invalid Hello packets.

Related command: **isis timer hello**.

Example

Configure the number of Level-2 Hello packets signifying peer invalid as 5 for Vlan-interface, that is, if no Hello packet is received from the interface within 5 Hello packet time intervals, the IS-IS peer is considered as invalid.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 10
[SW7750-Vlan-interface10] isis timer holding-multiplier 5
```

isis timer lsp

Syntax

isis timer lsp *time*

undo isis timer lsp

View

Interface view

Parameter

time: Minimum time interval in millisecond for sending link-state packets, ranging from 1 to 1000, with the default as 33 milliseconds.

Description

Use the **isis timer lsp** command to configure the time interval for sending link-state packets over interface.

Use the **undo isis timer lsp** command to resume the default configuration.

Related command: **isis timer retransmit**.

Example

Configure the time interval as 500 milliseconds for Vlan-interface 10 to send LSP.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 10
[SW7750-Vlan-interface10] isis timer lsp 500
```

isis timer retransmit

Syntax **isis timer retransmit** *seconds*

undo isis timer retransmit

View Interface view

Parameter *seconds*: Interval in seconds for retransmitting LSP packets, ranging from 1 to 300, with the default as 5 seconds.

Description Use the **isis timer retransmit** command to configure the time interval for retransmitting LSP packets over point-to-point link.

Use the **undo isis timer retransmit** command to resume the default configuration.

You should be careful when configuring this parameter to avoid unnecessary retransmission.

You need not use this command over a broadcast link, because a LAP packet requires response from the peer only over a point-to-point link, but not over a broadcast link,

Related command: **isis timer lsp**.

Example # Configure the time interval as 10 seconds for Vlan-interface 10 to retransmit LSP.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z..
[SW7750] interface Vlan-interface 10
[SW7750-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**: Indicates the router works in Level-1, which means it only calculates routes within the area, and maintains L1 LSDB.

level-1-2: Indicates the router works in Level-1-2, which means it calculates routes and maintains LSDB for both L1 and L2.

level-2: Indicates the router works in Level-2, which means it calculates LSP switching and routes and maintains LSDB for L2 only.

Description Use the **is-level** command to configure IS-IS router type.

Use the **undo is-level** command to resume the default configuration.

The configuration is **level-1-2** by default.

It is recommended to configure system level when you configure IS-IS.

You can configure all the routers as either Level-1 or Level-2 if there is only one area, because there is no need for all routers to maintain two identical databases at the same time. You are advised to configure all routers as Level-2 in IP network so as to facilitate extending later.

Related command: **isis circuit-level**.

Example # Configure the current route to work in Level-1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] isis
[SW7750-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 enable the IS-IS adjacency state change output.

Use the **undo log-peer-change** command to disable the output.

The output is disabled by default.

When the adjacency state output is enabled, the IS-IS adjacency state change will be sent to the configuration terminal.

Example # Enable the IS-IS adjacency state change output on the current router.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
```

```
[SW7750] isis
[SW7750-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 specify IS-IS to adopt the MD5 algorithm compatible with other manufacturers.

Use the **undo md5-compatible** command to specify IS-IS to adopt the default MD5 algorithm.

By default, IS-IS adopt the private MD5 algorithm.

This command must be configured when the switch needs to perform IS-IS MD5 authentication with the devices of others manufacturers.

Example # Specify IS-IS to adopt the MD5 algorithm compatible with other manufacturers.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] isis
[SW7750-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*: Network entity title in the form of X...X.XXXX....XXXX.00, with the 12 "X" in the middle as system ID of the router, the last "00" as the SEL and the "X...X" in the front as the area address.

Description Use the **network-entity** command to configure the network entity title (NET) for an IS-IS routing process.

Use the **undo network-entity** command to delete a NET.

There is no NET by default.

A NET is a network service access point (NSAP), and it is in the range of 8 to 20 bytes for IS-IS.

A NET has three parts: The first part is area ID, which ranges from 1 to 13 bytes. The routes of the same area have the same area ID. The second part is the router's system ID of 6 bytes, which is unique within the whole area and backbone area. The third part is SEL, the ending byte with the value of 00. You need to configure only 1 NET for a router. When repartitioning an area, such as merging or splitting, you can reconfigure the router to ensure correct and continuous routing.

Related command: **isis**, and **isis enable**.

Example # Specify the NET as 10.0001.1010.1020.1030.00, of which 10.0001 is the area ID and 1010.1020.1030 is the system ID.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] isis
[SW7750-isis] network-entity 10.0001.1010.1020.1030.00
```

preference

Syntax **preference** [**clns | ip**] *value*

undo preference [**clns | ip**]

View IS-IS view

Parameter *value*: Preference value in the range of 1 to 255. It is 15 by default.

clns: Specifies IS-IS routing preference based on OSI protocol stack, in the range of 1 to 255. It is IP-based preference by default.

ip: Specifies IS-IS routing preference based on TCP/IP protocol stack, in the range of 1 to 255. By default, IS-IS routing preference based on TCP/IP protocol stack is used.

Description Use the **preference** command to configure IS-IS protocol preference.

Use the **undo preference** command to resume the default IS-IS protocol preference.

When a router runs multiple dynamic routing protocols at the same time, the system will configure a preference for each routing protocol. If several protocols find routes to the same destination, the one with the highest preference dominates.

Example # Configure the preference of IS-IS protocol as 25.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
```

```
[SW7750] isis
[SW7750-isis] preference 25
```

reset isis all

Syntax **reset isis all**

View User view

Parameter None

Description Use the **reset isis all** command to clear all ISIS data structure information.

The IS-IS data information will not be cleared by default.

This command is used when a LSP need to be updated immediately. For example, after performing the **area-authentication-mode** and **domain-authentication-mode** commands, if the router still has some old LSPs, you can use this command to clear these LSPs.

Related command: **area-authentication-mode**, and **domain-authentication-mode**.

Example # Clear all IS-IS data structure.

```
<SW7750> reset isis all
```

reset isis peer

Syntax **reset isis peer** *system-id*

View User view

Parameter *system-id*: System ID for an IS-IS peer, containing 12 to 32 characters.

Description Use the **reset isis peer** command to clear the data information of a specific IS-IS peer.

The IS-IS peer is not cleared by default.

This command is used when you need to re-establish a specific peer.

Example # Clear the IS-IS peer with system ID as 0000.0c11.1111.

```
<SW7750> 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 clear overload flag.

No overload flag is set by default.

When the overload flag is set for a router, the routes calculated by the router will be ignored by other routes when they calculate SPF. (But the routes directly connected to the router will not be ignored.)

When a router is set overload flag, other routers will not transmit the packets that should be forwarded by the router.

Example # Set overload flag on the current router.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] isis
[SW7750-isis] set-overload
```

silent-interface

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

undo silent-interface *interface-type interface-number*

View IS-IS view

Parameter *interface-type interface-number*: Interface index.

Description Use the **silent-interface** command to prohibit IS-IS packet sending on the specified interface.

Use the **undo silent-interface** command to permit IS-IS packet sending on the specified interface.

By default, IS-IS packet sending is permitted on all interfaces.

The **silent-interface** command just suppresses IS-IS packet sending. However, these IS-IS packets can still be sent on other interfaces.

Example # Prohibit IS-IS packet sending on Vlan-interface 3.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
```

```
[SW7750] isis
[SW7750-isis] silent-interface Vlan-interface 3
```

spf-delay-interval

Syntax **spf-delay-interval** *number*

undo spf-delay-interval

View IS-IS view

Parameter *number*: Interval of releasing CPU during routing calculation, in the range of 1,000 routes to 50,000 routes. It is 5,000 routes by default.

Description Use the **spf-delay-interval** command to set the interval of releasing CPU during SPF calculation.

Use the **undo spf-delay-interval** command to restore the default value.

When there are two many routes in the routing table, you can use this command to release CPU automatically after a certain number of routes are processed in order to prevent the SPF calculation from occupying the system resources for a long time to affect the response of the console. The unprocessed routes are to be processed in one second.

You can adjust the *number* argument according to the size of the routing table. If the **spf-slice-size** command is configured at the same time, the SPF calculation will be paused if the SPF calculation matches any of the setting.

By default, CPU is released when every 5,000 routes are processed.

Related command: **spf-slice-size**.

Example # Set IS-IS to release CPU when every 3,000 routes are processed.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] isis
[SW7750-isis] spf-delay-interval 3000
```

spf-slice-size

Syntax **spf-slice-size** *seconds*

undo spf-slice-size

View IS-IS view

Parameter *seconds*: Duration time in milliseconds during SPF calculation, ranging from 150 to 50,000. A calculation is ended when the duration time is reached or exceeded. If the *second* argument is set to 0, then the SPF calculation will continue until it finishes. It is 0 by default.

Description Use the **spf-slice-size** command to configure whether the SPF routing calculation is fragmented and the duration time for each fragment.

Use the **undo spf-slice-size** command to resume the default configuration.

When there are too many routes in the routing table, you can use this command to fragment the SPF calculation to avoid taking up the system resources for too long. You are not recommended to change the default configuration.

If the **spf-delay-interval** command is configured at the same time, the SPF calculation will be paused if the SPF calculation matches any of the setting.

Related command: **spf-delay-interval**.

Example # Set SPF duration time to one second.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] isis
[SW7750-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*: Address range to generate summarized routes, in dotted decimal notation.

mask: Mask of an aggregate route, in dotted decimal notation.

level-1: Specifies to summarize only the routes imported to level-1 area.

level-1-2: Specifies to summarize all the routes imported to level-1 area and backbone area.

level-2: Specifies to summarize only the routes imported to backbone area.

If none of the **level-1** keyword, **level-2** keyword, and **level-1-2** keyword is specified, the routes imported to backbone area are summarized.

Description Use the **summary** command to configure IS-IS to generate summarized routes.

Use the **undo summary** command to disable summary.

No route is summarized by default.

You can summarize the routes having the same next hop into one to reduce the routing table size, as well as the LSP and LSDB generated by the router. It is possible to summarize native IS-IS routes and imported routes. After summarization, the route cost is the minimum cost of those summarized routes.

Example # Set an aggregate route 202.0.0.0/8.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] isis
[SW7750-isis] summary 202.0.0.0 255.0.0.0
```

timer lsp-max-age

Syntax **timer lsp-max-age** *second*s

undo timer lsp-max-age

View IS-IS view

Parameter *seconds*: Maximum valid time of a LSP, in the range of 1 to 65,535 in seconds. It is 1,200 seconds by default.

Description Use the **timer lsp-max-age** command to set the maximum valid time of the LSPs generated on the current router.

Use the **undo timer lsp-max-age** command to restore the default setting.

When the router generates system LSPs, the LSPs are generated with the maximum valid time in them. When a LSP is received by other routers, the maximum valid time will be smaller and smaller. If the maximum valid time decreases to 0, this LSP will be removed from LSDB.

Related command: **timer lsp-refresh**.

Example # Set the maximum valid time of the LSPs generated by the current system to 25 minutes, namely, 1,500 seconds.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] isis
[SW7750-isis] timer lsp-max-age 1500
```

timer lsp-refresh

Syntax **timer lsp-refresh** *second*s

undo timer lsp-refresh

View IS-IS view

Parameter *seconds*: LSP updating period in seconds, ranging from 1 to 65,535. It is 900 seconds by default.

Description Use the **timer lsp-refresh** command to set LSP updating period.

Use the **undo timer lsp-refresh** to resume the default configuration.

You can keep LSP in synchronization for the whole area with this mechanism.

Related command: **timer lsp-max-age**.

Example # Set the updating period to 1,500 seconds for the current system LSP.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] isis
[SW7750-isis] timer lsp-refresh 1500
```

timer spf

Syntax **timer spf** *seconds* [**level-1** | **level-2**]

undo timer spf [**level-1** | **level-2**]

View IS-IS view

Parameter *seconds*: Maximum time interval (in seconds) for SPF calculation, ranging from 1 to 120, with the default as 10.

level-1: Specifies to set the time interval for only Level-1 SPF calculation.

level-2: Specifies to set the time interval for only Level-2 SPF calculation.

If neither the **level-1** keyword nor the **level-2** keyword is specified, the interval of both level-1 SPF calculation and the level-2 SPF calculation are set.

Description Use the **timer spf** command to set the time interval for SPF calculation.

Use the **undo timer spf** command to resume the default configuration.

In the IS-IS protocol, the short path must be calculated again when the LSDB changes. If the SPF calculation is performed frequently, plenty of system resources will be occupied and the router efficiency will be affected. Comparatively, performing SPF calculation periodically can improve the efficiency. You can set the time interval of performing SPF calculation as required.

Example # Set the time interval of performing SPF calculation to three seconds.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] isis
[SW7750-isis] timer spf 3
```

33 BGP Configuration Commands

Routers in this manual refer to common routers or Ethernet switches that run routing protocols, unless otherwise specified.

For the commands for defining routing policies in BGP, see Chapter 34 "IP Routing Policy Configuration Commands" on page 469.

aggregate

Syntax **aggregate** *ip-address mask* [**as-set** | **attribute-policy** *route-policy-name* | **detail-suppressed** | **origin-policy** *route-policy-name* | **suppress-policy** *route-policy-name*]*

undo aggregate *ip-address mask* [**as-set** | **attribute-policy** *route-policy-name* | **detail-suppressed** | **origin-policy** *route-policy-name* | **suppress-policy** *route-policy-name*]*

View BGP view/BGP multicast address family view

Parameter *ip-address*: Address of the aggregated route.

mask: Network mask of the aggregated route.

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.

origin-policy *route-policy-name*: Selects the original routes used for aggregation.

attribute-policy *route-policy-name:* Sets the attributes of the aggregated route. The length of *route-policy-name* parameter ranges from 1 to 16 character string.

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 70 Description on keywords of the **aggregate** command

keywords	Description
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 frequent change of routes may lead to route vibration.
detail-suppressed	This keyword does not establish 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	This keyword is used to select only the specific routes in accordance with the route-policy to create an aggregated route.
attribute-policy	This keyword is used to set attributes of the aggregated route. The same work can be done by using peer route-policy, etc.

Example # Create an aggregated route in BGP routing table.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] bgp 100
[SW7750-bgp] aggregate 192.213.0.0 255.255.0.0
```

bgp

Syntax **bgp** *as-number*

undo bgp [*as-number*]

View System view

Parameter *as-number*: Specified local AS number, in the range of 1 to 65,535.

Description Use the **bgp** command to enable BGP and enter the BGP view.

Use the **undo bgp** command to disable BGP.

By default, the BGP is disabled.

This command is used to enable/disable BGP and specify the local AS number of BGP.

Example # Enable BGP.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] bgp 100
[SW7750-bgp]
```

balance

Syntax **balance** *num*

undo balance

View BGP view

Parameter *num*: Number of BGP routes used for load balance. This argument ranges from 1 to 4. Value 1 means the system does not adopt load balance.

Description Use the **balance** command to configure BGP load balance.

Use the **undo balance** command to cancel the load balance configuration.

By default, the system does not adopt BGP load balance.

Example # Configure BGP load balance.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] bgp 100
[SW7750-bgp] balance  2
```

compare-different-as-med

Syntax **compare-different-as-med**

undo compare-different-as-med

View BGP view/BGP multicast address family view

Parameter None

Description Use the **compare-different-as-med** command to enable comparison of MED values from different AS neighboring routes when determining the best route.

Use the **undo compare-different-as-med** command to disable the comparison.

By default, it is not allowed 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 a smaller MED can be selected as the final route.

Do not use this command unless it is determined that the same IGP and routing selection mode are adopted by different autonomous systems.

Example # Enable comparison of MED values from different AS neighboring routes.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] bgp 100
[SW7750-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 65,535.

Description Use the **confederation id** command to configure confederation identifier.

Use the **undo confederation id** command to cancel the BGP confederation specified by the *as-number* argument.

By default, no confederation ID is 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. The following gives an example of the configuration of AS 41.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] bgp 41
[SW7750-bgp] confederation id 9
[SW7750-bgp] confederation peer-as 38 39 40
[SW7750-bgp] group Confed38 external
[SW7750-bgp] peer Confed38 as-number 38
[SW7750-bgp] peer 10.1.1.1 group Confed 38
[SW7750-bgp] group Remote98 external
[SW7750-bgp] peer Remote98 as-number 98
[SW7750-bgp] peer 200.1.1.1 group Remote98
```

confederation nonstandard

Syntax **confederation** { **nonstandard | standard1965** | **standard3065** }

undo confederation { **nonstandard | standard1965** | **standard3065** }

View BGP view.

Parameter None

Description Use the **confederation** { **nonstandard | standard1965** | **standard3065** } command to configure the standard type of confederation.

Use the **undo confederation** { **nonstandard | standard1965** | **standard3065** } command to cancel the configuration.

By default, the configured confederations are in compliance with RFC1965.

For the communication with nonstandard devices, you must execute the **confederation nonstandard** command on all the 3Com routers in the confederation.

Related command: **confederation id** and **confederation peer-as**.

Example # AS100 contains routers following nonstandard, which is composed of two sub-ASs, 64000 and 65000.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] bgp 64000
[SW7750-bgp] confederation id 100
[SW7750-bgp] confederation peer-as 65000
[SW7750-bgp] confederation nonstandard
```

confederation peer-as

Syntax **confederation peer-as** *as-number-list*

undo confederation peer-as [*as-number-list*]

View BGP view

Parameter *as-number-list:* List of sub-AS numbers. A maximum of 32 sub-ASs can be configured for a confederation in the command.

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 using 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** and **confederation id**.

Example # Configure the confederation contains AS 2001 and 2002.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] bgp 100
[SW7750-bgp] confederation peer-as 2000 2001
```

dampening

Syntax **dampening** [*half-life-reachable half-life-unreachable reuse suppress ceiling*] [**route-policy** *route-policy-name*]

undo dampening

View BGP view

Parameter *half-life-reachable*: Semi-dampening of a reachable route, in the range of 1 to 45 minutes. The default value is 15 minutes.

half-life-unreachable: Semi-dampening of an unreachable, in the range of 1 to 45 minutes. The default value is 15 minutes.

reuse: Threshold, in seconds, for disabling route suppression. When the penalty value is below this threshold, the route will be reused. The range is 1 to 20,000. The default value is 750.

suppress: Threshold, in seconds, for enabling route suppression. When the penalty value is above the threshold, the route is suppressed. The range is 1 to 20,000. The default value is 2,000.

ceiling: Upper penalty threshold in seconds, that is, the penalty value stops increasing when it reaches the upper threshold. The range is 1001 to 20,000. The default value is 16,000.

route-policy-name: Name of a route policy, in the range of 1 to 19 characters.

If no value is specified for the arguments, their default values will take effect. The *half-life-reachable, half-life-unreachable, reuse, suppres*s, and *ceiling* arguments are independent of each other.. Therefore, if you specify a value for any of these arguments, you must specify a value for all the others.

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 bgp dampening**, **reset bgp flap-info**, **display bgp routing-table dampened**, and **display bgp routing-table flap-info**.

Example # Configure BGP route dampening parameters.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] bgp 100
[SW7750-bgp] dampening 15 15 1000 2000 10000
```

default local-preference

Syntax **default local-preference** *value*

undo default local-preference

View BGP view/BGP multicast address family 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 default local preference.

Use the **undo default local-preference** command to restore the default value.

Configuring different local preferences will affect BGP routing selection.

Example

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] bgp 100
[SW7750-bgp] default local-preference 180
```

default med

Syntax **default med** *med-value*

undo default med

View BGP view/BGP multicast address family view

Parameter *med-value*: Specified MED value, in the range of 0 to 4294967295. The default *med-value* is "0".

Description Use the **default med** command to configure the default MED value of the system.

Use the **undo default med** command to restore the default MED value of the system.

The multi-exit discriminator (MED) is an external route metric. Different from the local preference, the MED is exchanged between autonomous systems. After the MED enters an autonomous system, it will not be sent out of this autonomous system. The MED attribute is used to select the optimal route, that is, the route with a smaller MED value is selected. When a router running the BGP obtains routes with the same destination address but different next hops through different external peers, the route selection will be based on the MED value. In the case that all other conditions are the same, the system first selects the route with the smaller MED value as an external route of the autonomous system.

Example # Set the MED value to "25"..

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750-bgp] default med 25
```

display bgp group

Syntax **display bgp** [**multicast**] **group** [*group-name*]

View Any view

Parameter **multicast**: Specifies multicast address family.

group-name: Name of a peer group, a string of 1 to 47 alphanumeric characters.

Description Use the **display bgp group** command to view the information of peer groups.

Example # Display the information of the peer group aaa.

```
<SW7750> 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
    no import policy route-policy
    no import policy filter-policy
    no import policy acl
    no import policy ip-prefix
    no default route produce
```

Table 71 Description on fields of the **display bgp group** command

Field	Description
Group	Name of peer group
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
default route produce	Whether or not to advertise default routing information

display bgp network

Syntax **display bgp** [**multicast**] **network**

View Any view

Parameter **multicast**: Specifies multicast address family.

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.

```
<SW7750> display bgp network
           Network             Mask          Route-policy
  ---------------------------------------------------------
         168.10.24.0      255.255.255.0        None
         10.0.0.0         255.0.0.0            None
```

Table 72 Description on 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.

```
<SW7750> display bgp paths 500
Id  Hash-index References Aggregator Origin As-Path
---------------------------------------------------
153 80         100        <null>      IGP   500 {500,400,600}
```

Table 73 Description on fields of the **display bgp paths** command

Field	Description
Id	Value of sequence number
Hash-Index	Value of Hash-index
References	Number of routes with reference
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** [**multicast**] **peer** [*ip-address* [**verbose**]]

display bgp [**multicast**] **peer** [**verbose**]

View Any view

Parameter **multicast**: Specifies multicast address family.

ip-address: IP address of the peer to be displayed, in dotted decimal notation.

verbose: Displays detailed information of the specified peer.

Description Use the **display bgp peer** command to display the information about the specified BGP peer.

Example # Display detailed information of the peer 10.110.25.20.

```
<SW7750> display bgp peer 10.110.25.20 verbose
         Peer: 10.110.25.20 Local: Unspecified
         Type: External
         State: Idle     Flags: <Idled>
         Last State: NoState     Last Event: NoEvent
         Last Error: None
         Options: <>

  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 74 Description on fields of the **display bgp peer** 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 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** [**multicast**] **routing-table** [*ip-address* [*mask*]]

View Any view

Parameter **multicast**: Specifies multicast address family.

ip-address: Destination of the network, in dotted decimal notation.

mask: Mask of the network.

Description Use the **display bgp routing-table** command to display all the BGP routing information.

Example # Display all the BGP routing information.

```
<SW7750> display bgp routing-table
Flags:   # - valid       ^ - active      I - internal
         D - damped      H - history     S - aggregate suppressed

    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

  Routes total: 10
```

Table 75 Description on fields of the **display bgp routing-table** command

Field	Description
Flags	Status code: # - valid (valid route) ^ - active (selected optimal route) I - internal (IBGP route) D - damped (attenuation dampened) H - history (history record) S - aggregate suppressed (aggregation suppressed)
Dest/Mask	Destination address/mask
Next Hop	IP address of the next hop
Med	Value of the MULTI_EXIT_DISC attribute, which ranges from 0 to 4294967295
Local-Pref	Local preference, which ranges from 0 to 4294967295
Origin	Origin attribute of a route, which indicates that the route updates its origin relative to the route originating it from the AS. It has three optional values: IGP The route is inside the AS. BGP treats the aggregation route and the route defined by the **network** command inside AS, and the 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 a route, which records all AS areas that the route passes to void route loop.

display bgp 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, in the range of 1 to 199.

multicast: Specifies multicast address family.

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 as-path-acl 1.

```
<SW7750> display bgp routing-table as-path-acl 1
Flags:   # - valid       ^ - active      I - internal
```

```
         D - damped      H - history     S - aggregate suppressed

  Dest/Mask         Next-Hop      Med     Local-pref   Origin    As-path
--------------------------------------------------------------------
#^ 1.1.1.0/24         10.10.10.1    0                   IGP      200
#^ 1.1.2.0/24         10.10.10.1    0                   IGP      200
#^ 1.1.3.0/24         10.10.10.1    0                   IGP      200
#^ 2.2.3.0/24         10.10.10.1    0                   INC      200
#^ 4.4.4.0/24         10.10.10.1    0                   INC      200
#^ 9.9.9.0/24         10.10.10.1    0                   INC      200
#^ 10.10.10.0/24      10.10.10.1    0                   IGP      200
#^  22.1.0.0/16       200.1.7.2     100                 INC      200
#   88.1.0.0/16   60     0.0.0.0                           IGP
```

Table 76 Description on 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
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** [**multicast**] **routing-table cidr**

View Any view

Parameter **multicast**: Specifies multicast address family.

Description Use the **display bgp routing-table cidr** command to view the routing information about the non-natural mask (namely the classless inter-domain routing, CIDR).

Example # Display BGP CIDR routing information.

```
<SW7750> display bgp routing-table cidr
Flags:   # - valid       ^ - active      I - internal
         D - damped      H - history     S - aggregate suppressed


    Dest/Mask         Next-Hop     Med     Local-pref   Origin    As-path
--------------------------------------------------------------------------
```

```
#^  22.1.0.0/16       200.1.7.2    30       100          INC      200
#   88.1.0.0/16       0.0.0.0      30                    IGP
```

For detailed description of the fields in the output information, see Table 75.

display bgp routing-table community

Syntax **display bgp** [**multicast**] **routing-table community** [*aa:nn*]&<1-13> [**no-export-subconfed** | **no-advertise** | **no-export**]* [**whole-match**]

View Any view

Parameter **multicast**: Specifies multicast address family.

aa:nn: Community number. &<1-13> means that you need to provide at least one and can provide up to 13 community numbers.

no-export-subconfed: Specifies not to export a route to the outside of the local AS or to other sub-ASs in the confederation after the route is received.

no-advertise: Specifies not to advertise a route to other BGP peers after the route is received.

no-export: Specifies not to export a route to the outside of the local AS after the route is received. If the confederation is used, the router cannot be exported to the outside of the confederation, but can be exported to other sub-ASs in the confederation.

whole-match: Displays 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.

```
<SW7750> display bgp routing-table community 11:22
Flags:   # - valid       ^ - active      I - internal
         D - damped      H - history     S - aggregate suppressed


    Dest/Mask       Next-Hop     Med     Local-pref   Origin    As-path
-------------------------------------------------------------------
#^   1.0.0.0/8      172.10.0.2            100          IGP
#^   2.0.0.0/8      172.10.0.2            100          IGP
```

For detailed description of the fields in the output information, see Table 75.

display bgp routing-table community-list

Syntax **display bgp** [**multicast**] **routing-table community-list** *community-list-number* [**whole-match**]

View Any view

Parameter **multicast**: Specifies multicast address family.

community-list-number: Community list number, in the range of 1 to 999.

whole-match: Displays 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.

```
<SW7750> display bgp routing-table community-list 1
Flags:   # - valid       ^ - active      I - internal
         D - damped      H - history     S - aggregate suppressed

Destination/Mask    Next-hop        Med     Local-Pref   Origin  As-Path
-------------------------------------------------------------------
    1.1.1.0/24      10.10.10.1      0                    IGP      200
    1.1.2.0/24      10.10.10.1      0                    IGP      200
    1.1.3.0/24      10.10.10.1      0                    IGP      200
    2.2.3.0/24      10.10.10.1      0                    INC      200
    4.4.4.0/24      10.10.10.1      0                    INC      200
    9.9.9.0/24      10.10.10.1      0                    INC      200
    10.10.10.0/24   10.10.10.2      0                    IGP
    10.10.10.0/24   10.10.10.1      0                    IGP      200
```

For detailed description of the fields in the output information, see Table 75.

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 display BGP dampened routes.

Example # Display BGP dampened routes.

```
<SW7750> display bgp routing-table dampened
Flags:   # - valid       ^ - active      I - internal
         D - damped      H - history     S - aggregate suppressed

Dest/Mask             Source    Damping-limit   Origin   As-path
-----------------------------------------------------------------
#D  11.1.0.0        133.1.1.2      1:20:00       IGP      200
```

Table 77 Field descriptions of the **display bgp routing-table dampened** command

Field	Description
Flags	Status code: # - valid (valid route) ^ - active (optimal route selected) I - internal (IBGP route) D - damped H - history S - aggregate suppressed B - balance (load balance)
#D	Valid and dampened route
Dest/Mask	The route to this network segment is dampened.
Source	Next hop of the route
Damping-limit	Time when damping is invalid, that is, time when the route can be reused.
Origin	The ORIGIN attribute of the route, which indicates the routing update origination of the route relative to the AS the route sourced from. It can be one of the three value: IGP This is an AS interior route. BGP regards both aggregated routes and routes defined by the **network** command as AS interior routes and set their origin type to IGP. EGP This route is learned from EGP (exterior gateway protocol). INC INCOMPLETE: indicates the route is obtained from an unknown source (that is, learned from a different source). BGP set the origin of the routes imported from other IGP protocols to INCOMPLETE
As-path	AS_PATH attribute of the route, which records all the ASs the route passes through and can be used to avoid route ring.

display bgp routing-table different-origin-as

Syntax **Display bgp [multicast] routing-table different-origin-as**

View Any view

Parameter **multicast**: Specifies multicast address family.

Description Use the **display bgp routing-table different-origin-as** command to display routes that have different source autonomous systems.

Example # Display the routes that have different source ASs.

```
<SW7750> display bgp routing-table different-origin-as
Flags:   # - valid       ^ - active      I - internal
         D - damped      H - history     S - aggregate suppressed


Destination/Mask     Next-hop       Med       Local-Pref  Origin   As-Path
------------------------------------------------------------------------
   10.10.10.0/24      10.10.10.2    0                     IGP
   10.10.10.0/24      10.10.10.1    0                     IGP      200
```

For detailed description of the fields in the output information, see Table 75.

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*: Route flap-info matching AS path regular expression.

acl-number: Number of the specified AS path to be matched, in the range of 1 to 199.

network-address: Network IP address related to the flap-info to be shown

mask: Network mask, in dotted decimal notation.

longer-match: Displays the flap-info of the route that has a mask longer than that specified by the *network-address mask* argument.

Description Use the **display bgp routing-table flap-info** command to display BGP flap-info.

Example # Display BGP flap-info.

```
<SW7750> display bgp routing-table flap-info
Flags:   # - valid       ^ - active      I - internal
         D - damped      H - history     S - aggregate suppressed

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 78 Description on fields of the **display bgp routing-table flap-info** command

Field	Description
Flags	State flags: # - valid (valid) ^ - active (selected) D - damped (discarded) H - history (history) I - internal (interior gateway protocol) S - aggregate suppressed (suppressed) B - balance (load balance)
#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.

Table 78 Description on fields of the **display bgp routing-table flap-info** command

Field	Description
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
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** [**multicast**] **routing-table peer** *ip-address* { **advertised** | **received** } [*network-address* [*mask*] | **statistic**]

View Any view

Parameter **multicast**: Specifies multicast address family.

ip -address: Specifies the peer to be displayed, in dotted decimal notation.

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, in dotted decimal notation.

statistic: Specifies to display the 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.

Example # Display the routing information advertised by BGP peer 1.1.1.2.

```
<SW7750> display bgp routing table peer 1.1.1.2 advertised
Dest/Mask          Next-hop       Med        Local-pref  Origin As-path
-------------------------------------------------------------------------
Appendant Flags: @ - Queued
 1.1.1.0/24         1.1.1.1        0           100         INC
```

Here, Appendant Flags indicates the appended flag, @ the route to be sent, ! the reachable route, and ~ to cancel route. For detailed description of the fields in the output information, see Table 75.

display bgp routing-table regular-expression

Syntax **display bgp** [**multicast**] **routing-table regular-expression** *as-regular-expression*

View Any view

Parameter **multicast**: Specifies multicast address family.

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 ^200$.

```
<SW7750> display bgp routing-table regular-expression ^200$
Flags:   # - valid       ^ - active      I - internal
         D - damped      H - history     S - aggregate suppressed


Dest/Mask       Next-hop         Med    Local-Pref  Origin AS-Path
---------------------------------------------------------------------
 1.1.1.0/24      10.10.10.1       0                  IGP   200
 1.1.2.0/24      10.10.10.1       0                  IGP   200
 1.1.3.0/24      10.10.10.1       0                  IGP   200
 2.2.3.0/24      10.10.10.1       0                  INC   200
 4.4.4.0/24      10.10.10.1       0                  IGP   200
 9.9.9.0/24      10.10.10.1       0                  INC   200
 10.10.10.0/24   10.10.10.1       0                  IGP   200
```

For detailed description of the fields in the output information, see Table 75.

display bgp routing-table statistic

Syntax **display bgp** [**multicast**] **routing-table statistic**

View Any view

Parameter **multicast**: Specifies multicast address family.

Description Use the **display bgp routing-table statistic** command to view the statistics of BGP routing information.

Example # Display the statistics of BGP routing information.

```
<SW7750> display bgp routing-table statistic
  Routes total: 4
```

filter-policy export

Syntax **filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [*protoco*l [*process-id*]]

undo filter-policy { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [*protoco*l [*process-id*]]

View BGP view/BGP multicast address family view

Parameter *acl-number*: Number of IP access control list.

ip-prefix-name: Name of ip prefix list, containing 1 to 19 characters.

protocol: Routing protocol, specifying a protocol whose routing information is filtered. Currently, the routing protocols includes **direct**, **ospf**, **ospf-ase**, **ospf-nssa**, **rip**, **isis,** and **static**.

process-id: Routing protocol process ID, in the range of 1 to 65,535. This argument is available only when the protocol is **ospf**, **ospf-ase**, or **ospf-nssa**.

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, filtration to the received routing information is not configured.

If a value is specified for the *protocol* argument, only the imported route generated by the specified protocol is filtered and the imported routes generated by other protocols are not affected. If no value is specified for the *protocol* argument, the imported route generated by any protocol will be filtered.

Example # Use ACL 2000 to filter the routing information advertised by BGP.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] bgp 100
[SW7750-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/BGP multicast address family view

Parameter *acl-number*: Number of IP access control list, in the range of 2000 to 3999.

ip-prefix-name: Name of address prefix list, containing 1 to 19 characters.

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 all imported BGP routes.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] bgp 100
[SW7750-bgp] filter-policy 2000 import
```

group

Syntax **group** *group-name* [**internal | external**]

undo group *group-name*

View BGP view

Parameter *group-name*: Name of the peer group, an alphanumeric string of 1 to 47 characters. It means only locally.

internal: Creates an IBGP peer group.

external: Creates an EBGP peer group, including other sub-ASs in the confederation.

Description Use the **group** *group-name* command to configure a peer group.

Use the **undo group** *group-name* command to cancel the configuration.

If no parameter is specified with the **group** command, an IBGP peer group is created.

The basic configurations of members in a peer group must be the same as those of the peer group. The BGP peer cannot exist independently, and it must belong to a peer group. Therefore, when configuring a BGP peer, create a peer group first and then add the BGP peer to the group.

Routing update policies of peer members must be the same as those of the peer group. However, entry policies can be different.

Example

Create a BGP group named test.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] bgp 100
[SW7750-bgp] group test
```

import-route

Syntax

import-route *protocol* [*process-id*] [**med** *med-value* **|** **route-policy** *route-policy-name*]*

undo import-route *protocol* [*process-id*]

View

BGP view/BGP multicast address family view

Parameter

protocol: Redistributes routes from the routing protocol, which can be **direct**, **ospf, ospf-ase**, **ospf-nssa**, **rip**, **isis** or **static** at present.

process-id: Specific process ID, in the range of 1 to 65,535. This argument is valid only when the *protocol* argument is **ospf**, **ospf-ase**, or **ospf-nssa**.

med *med-value*: MED value of redistributed routes, in the range of 0 to 4294967295.

Route-policy-name: Name of a route policy used for filtering redistributed routes, containing 1 to 19 characters.

Description

Use the **import-route** command to enable route redistribution from another routing protocol.

Use the **undo import-route** command to disable route redistribution from another routing protocol.

By default, no route redistribution is configured.

Example

Redistribute routes from RIP.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] bgp 100
[SW7750-bgp] import-route rip
```

ipv4-family

Syntax **ipv4-family multicast**

undo ipv4-family multicast

View BGP view

Description Use the **ipv4-family multicast** command to enter IPv4 multicast address family view.

Use the **undo ipv4-family multicast** command to remove all the configuration performed in IPv4 multicast address family view.

Example # Enter IPv4 multicast address family view.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] bgp 100
[SW7750-bgp] ipv4-family multicast
[SW7750-bgp-af-mul]
```

network

Syntax **network** *network-address* [*mask*] [**route-policy** *route-policy-name*]

undo network *network-address* [*mask*] [**route-policy** *route-policy-name*]

View BGP view/BGP multicast address family view

Parameter *network-address*: IP address of the destination network segment, in dotted decimal notation.

mask: Subnet mask, in dotted decimal notation.

route-policy-name: Route policy used for the advertised route, containing 1 to 19 characters.

Description Use the **network** command to advertise the network segment route to the BGP routing table.

Use the **undo network** command to cancel the existing configuration.

By default, the BGP does not advertise any network segment routes.

Example # Advertise routes to the network segment 10.0.0.0/16.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] bgp 100
[SW7750-bgp] network 10.0.0.0 255.255.0.0
```

peer advertise-community

Syntax **peer** *group-name* **advertise-community**

undo peer *group-name* **advertise-community**

View BGP view/BGP multicast address family view

Parameter *group-name*: Name of a peer group, containing 1 to 47 characters.

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: **ip community-list** and **apply community**.

Example # Transmit the community attribute to the peer group named test.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] bgp 100
[SW7750-bgp] peer test advertise-community
```

peer allow-as-loop

Syntax **peer** { *group-name* | *ip-address* } **allow-as-loop** [*number*]

undo peer { *group-name* | *ip-address* } **allow-as-loop**

View BGP view/BGP multicast address family view

Parameter *group-name:* Name of a peer group, containing 1 to 47 characters.

ip-address: IP address of the peer, in dotted decimal notation.

number: Times of repeating the local AS number, in the range of 1 to 10.

Description Use the **peer allow-as-loop** command to allow the local AS number to appear in the AS_Path attribute of the received route and configure the repeated times.

Use the **undo peer allow-as-loop** command to cancel the function.

Related command: **display current-configuration**, **display bgp routing-table peer**, and **display bgp routing-table group**.

Example # Set the times of repeating the local AS that learns routes from 1.1.1.1 to 2.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] bgp 100
[SW7750-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 a peer group, containing 1 to 47 characters.

as-number: AS number of the peer or peer group, in the range of 1 to 65,535.

Description Use the **peer as-number** command to configure the AS number of a peer group.

Use the **undo peer as-number** command to delete the AS number of a peer group.

By default, no AS number is configured for a peer group.

Example # Set the AS number for the peer named test to 100.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] bgp 100
[SW7750-bgp] peer test as-number 100
```

peer as-path-acl export

Syntax **peer** { *group-name* | *ip-address* } **as-path-acl** *acl-number* **export**

undo peer { *group-name* | *ip-address* } **as-path-acl** *acl-number* **export**

View BGP view/BGP multicast address family view

Parameter *group-name*: Name of the peer group, containing 1 to 47 characters.

ip-address: IP address of a peer.

acl-number: AS path ACL number, in the range of 1 to 199.

export: Specifies to filter the 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, no AS path ACL is configured for a peer group.

You can use the **peer as-path-acl export** command on a peer group. In the **peer as-path-acl export** command, the *acl-number* argument is the AS path list number. It is configured by using the **ip as-path-acl command**, instead of the **acl** command.

Related command: **peer as-path-acl import** and **ip as-path-acl**.

Example # Filter routes exported to the peer group (named test) based on AS path ACL 1.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] bgp 100
[SW7750-bgp] peer test as-path-acl 1 export
```

peer as-path-acl import

Syntax **peer** { *group-name* | *ip-address* } **as-path-acl** *acl-number* **import**

undo peer { *group-name* | *ip-address* } **as-path-acl** *acl-number* **import**

View BGP view/BGP multicast address family view

Parameter *group-name*: Name of the peer group, containing 1 to 47 characters.

ip-address: IP address of the peer, in dotted decimal notation.

acl-number: AS path list number, in the range of 1 to 199.

import: Applies the AS path list in filtering the 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.

Related command: **peer as-path-acl export** and **ip as-path-acl**

Example # Apply AS path ACL 1 in the peer group named test to filter BGP received routes.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] bgp 100
[SW7750-bgp] peer test as-path-acl 1 import
```

peer connect-interface

Syntax **peer** { *group-name* | *ip-address* } **connect-interface** *interface-type interface-number*

undo peer { *group-name* | *ip-address* } **connect-interface**

View BGP view

Parameter *group-name*: Name of the peer group, containing 1 to 47 characters.

ip-address: IP address of the peer, in dotted decimal notation.

interface-type interface-num: Interface type and 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 interface directly connected to the peer as the source interface of route update packets.

Generally, BGP uses the optimal source interface for route update packets. In order for the system to be able to send route update packets in the case that this interface is faulty, you can configure the loopback interface as the source interface of route update packets.

Example # Specify the source interface that sends route update packets to the peer group named test as Loopback 0.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] bgp 100
[SW7750-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:* Name of the peer group, containing 1 to 47 characters.

Description Use the **peer default-route-advertise** command to send the default route to the peer group.

Use the **undo peer default-route-advertise** command to cancel the sending of the default route to the peer group.

By default, the default route is not sent to the peer group.

For this command, no default route needs to exist in the routing table. A default route is sent unconditionally to a peer/peer group with the next hop as itself.

Example # Configure a peer group named test to generate a default route.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] bgp 100
[SW7750-bgp] peer test default-route-advertise
```

peer description

Syntax **peer** { *group-name* | *ip-address* } **description** *description-text*

undo peer { *group-name* | *ip-address* } **description**

View BGP view

Parameter *group-name*: Name of the peer group, containing 1 to 47 characters.

ip-address: IP address of the peer, in dotted decimal notation.

description-text: Description information configured, , containing 1 to 79 characters.

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, no description information is configured for peers/peer group.

You need to create a peer group before you can configure the description of the peer group.

Related command: **display current-configuration**, **display bgp peer**, and **display bgp routing-table group**.

Example # Configure the description information of an existing peer group named group1 as ISP1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] bgp 100
[SW7750-bgp] peer group1 description ISP1
```

peer ebgp-max-hop

Syntax

peer *group-name* **ebgp-max-hop** [*hop-count*]

undo peer *group-name* **ebgp-max-hop**

View

BGP view

Parameter

group-name: Name of the peer group, containing 1 to 47 characters.

hop-count: Maximum hop value, in the range of 1 to 255. By default, the value is 64.

Description

Use the **peer ebgp-max-hop** command 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, it is not allowed to establish any EBGP connection with a peer on an indirectly connected network.

By setting *hop-count*, you can also configure the maximum hop value of an EBGP connection.

Example

Allow the establishment of an EBGP connection with the peer group named test indirectly connected.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] bgp 100
[SW7750-bgp] peer test ebgp-max-hop
```

peer enable

Syntax

peer { *group-name* **|** *ip-address* } **enable**

undo peer { *group-name* **|** *ip-address* } **enable**

View

BGP view/BGP multicast address family view

Parameter

group-name: Name of the peer group, containing 1 to 47 characters.

ip-address: IP address of the peer, in dotted decimal notation.

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 18.10.0.9. After the configuration, the local router does not exchange BGP routing information with the peer 18.10.0.9..

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] bgp 100
[SW7750-bgp] peer 18.10.0.9 group group1
[SW7750-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/BGP multicast address family view

Parameter *group-name*: Name of the peer group, containing 1 to 47 characters.

acl-number: Basic or advanced ACL number, ranging from 2000 to 3999.

export: Applies a filtering policy on advertised routes. It applies to a peer group only.

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).

You can configure the **peer filter-policy export** command on a peer group only.

Related command: **acl** and **peer filter-policy import**.

Example # Configure to filter the routes advertised by the peer group named test by using ACL 2000..

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] bgp 100
[SW7750-bgp] peer test filter-policy 2000 export
```

peer filter-policy import

Syntax **peer** { *group-name* | *ip-address* } **filter-policy** *acl-number* **import**

undo peer { *group-name* | *ip-address* } **filter-policy** *acl-number* **import**

View BGP view/BGP multicast address family view

Parameter *group-name*: Name of the peer group, containing 1 to 47 characters.

ip-address: IP address of the peer, in dotted decimal notation.

acl-number: Basic or advanced ACL number, ranging from 2000 to 3999.

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: **peer filter-policy export**, **ip as-path-acl**, **peer as-path-acl export** and **peer as-path-acl import**.

Example # Set the filter-policy list of a peer group named test.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] bgp 100
[SW7750-bgp] peer test filter-policy 2000 import
```

peer group

Syntax **peer** *ip-address* **group** *group-name* [**as-number** *as-number*]

undo peer *ip-address*

View BGP view/BGP multicast address family view

Parameter *group-name*: Name of the peer group, containing 1 to 47 characters.

ip-address: IP address of the peer, in dotted decimal notation.

as-number: Peer AS number of the peer/peer group, in the range of 1 to 65,535.

Description Use the **peer group** command to add a peer to the existing peer group.

Use the **undo peer** *ip-address* command to delete a peer.

When adding a peer to a EBGP peer group without AS number, you should also specify the peer's AS number. While adding a peer to a IBGP peer group or to a EBGP peer group with AS number, you need not specify the AS number for the peer.

Example # Add a peer to the peer group test.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] bgp 100
[SW7750-bgp] group test external
[SW7750-bgp] peer test as-number 2004
[SW7750-bgp] peer 10.1.1.1 group test
```

peer ip-prefix export

Syntax **peer** *group-name* **ip-prefix** *ip-prefix-name* **export**

undo peer *group-name* **ip-prefix** *ip-prefix-name* **export**

View BGP view/BGP multicast address family view

Parameter *group-name*: Name of peer group, containing 1 to 47 characters.

ip-prefix-name: Name of the specified **ip-prefix**, containing 1 to 19 characters.

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.

Related command: **ip ip-prefix**, **peer ip-prefix import**.

Example # Configure the route filtering policy of the peer group based on the ip-prefix 1.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] bgp 100
[SW7750-bgp] peer group1 ip-prefix list1 export
```

peer ip-prefix import

Syntax **peer** { *group-name* | *ip-addess* } **ip-prefix** *ip-prefix-name* **import**

undo peer { *group-name* | *ip-addess* } **ip-prefix** *ip-prefix-name* **import**

View BGP view/BGP multicast address family view

Parameter *group-name*: Name of peer group, containing 1 to 47 characters.

ip-address: IP address of the peer, in dotted decimal notation.

ip-prefix-name: Name of the specified **ip-prefix**, containing 1 to 19 characters.

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.

Related command: **ip ip-prefix**, **peer ip-prefix export**.

Example # Configure the route filtering policy of the peer group based on the ip-prefix 1.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] bgp 100
[SW7750-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*: Name of the peer group, containing 1 to 47 characters.

Description Use the **peer next-hop-local** command to configure the peer group to take its own address as the next hop when routes are advertised to the peer group..

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.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] bgp 100
[SW7750-bgp] peer test next-hop-local
```

peer password

Syntax **peer** { *group-name* | *ip-address* } **password** { **cipher** | **simple** } *password*

undo peer { *group-name* | *ip-address* } **password**

View BGP view

Parameter *group-name*: Name of the peer group, containing 1 to 47 characters.

ip-address: IP address of the peer, in dotted decimal notation.

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.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] bgp 100
[SW7750-bgp] peer 10.1.100.2 password simple abc
```

# Perform the similar configuration on the peer.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] bgp 100
[SW7750-bgp] peer 10.1.100.1 password simple abc
```

peer public-as-only

Syntax **peer** *group-name* **public-as-only**

undo peer *group-name* **public-as-only**

View BGP view/BGP multicast address family view

Parameter *group-name*: Name of a peer group, containing 1 to 47 characters.

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 group named test.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] bgp 100
[SW7750-bgp] peer test public-as-only
```

peer reflect-client

Syntax **peer** *group-name* **reflect-client**

undo peer *group-name* **reflect-client**

View BGP view/BGP multicast address family view

Parameter *group-name*: Name of peer group, containing 1 to 47 characters.

Description Use the **peer reflect-client** command to configure the local device as a route reflector and configure a peer/peer group as the route reflector client.

Use the **undo peer reflect-client** command to cancel the existing configuration.

By default, no route reflector or client is configured.

This command only applies to peer group.

Related command: **reflect between-clients**, **reflector cluster-id**.

Example # Configure the peer group "test" as the route reflector client.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] bgp 100
[SW7750-bgp] peer test reflect-client
```

peer route-limit

Syntax **peer** { *group-name* | *ip-address* } **route-limit** *prefix-number* [[**alert-only** | **reconnect** *reconnect-time*] | *percentage-value*] *

undo peer { *group-name* | *ip-address* } **route-limit**

View BGP view

Parameter *group-name*: Name of peer group, containing 1 to 47 characters.

ip-address: IP address of the peer, in dotted decimal notation.

prefix-number: Number of the route prefixes to be received by the router, in the range of 1 to 262,144. If the number of route prefixes received from the specified peer/peer group exceeds the value of *prefix-numb*er, the router is automatically disconnected from the specified peer/peer group.

alert-only: Specifies to only print alert information and maintain the connection between the router and the specified peer/peer group if the number of route prefixes received from the peer/peer group exceeds *prefix-numb*er.

reconnect *reconnect-time*: Sets the interval at which the router reconnects to the specified peer/peer group. *reconnect-time* is the interval, in seconds, at which the router reconnects to the specified peer/peer group. The value of this argument ranges from 1 to 65,535, with no default.

percentage-value: Threshold value for the router to send a notification (that is, the router sends a notification when the percentage of the number of route prefixes received to *prefix-numb*er reaches *percentage-value*). It ranges from 1 to 100 and defaults to 75.

Description Use the **peer route-limit** command to set a limit on the number of route prefixes to be received from the specified peer/peer group.

Use the **undo peer route-limit** command to cancel the configuration.

By default, there is no limit on the number of route prefixes to be received from a peer/peer group.

Example # With peer 100.1.1.1 not configured, limit the number of route prefixes to be received from peer 100.1.1.1 to 10,000

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] bgp 100
[SW7750-bgp]peer 100.1.1.1 route-limit 10000
  Warning: No such peer
```

# With peer 100.1.1.1 configured, limit the number of route prefixes to be received from peer 100.1.1.1 to 10,000.

```
[SW7750-bgp]peer 100.1.1.1 route-limit 10000
```

# Limit the number of route prefixes to be received from the peer group named external to 10,000, specifying to print alert information when the number of route prefixes received from external reaches 10,000 and to print notification information when this number reaches 8,000.

```
[SW7750-bgp]peer external route-limit 10000 alert-only 80
```

# Limit the number of route prefixes to be received from the peer group named external to 10,000, specifying to reconnect the router to external every 120 seconds and to print notification information when the number of route prefixes received from external reaches 8,000.

```
[SW7750-bgp]peer external route-limit 10000 reconnect 120 80
```

# Limit the number of route prefixes to be received from the peer group named external to 10,000, specifying to print notification information when this number reaches 8,000.

```
[SW7750-bgp]peer external route-limit 10000 80
```

# Cancel the limit on the number of route prefixes to be received from peer 100.1.1.1.

```
[SW7750-bgp]undo peer 100.1.1.1 route-limit
```

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, containing 1 to 47 characters.

route-policy-name: The specified Route-policy. The length of *route-policy-name* parameter ranges from 1 to 19 character string.

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 advertised from the peer group named test.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] bgp 100
[SW7750-bgp] peer test route-policy test-policy export
```

peer route-policy import

Syntax

peer { *group-name* | *ip-address* } **route-policy** *route-policy-name* **import**

undo peer { *group-name* | *ip-address* } **route-policy** *route-policy-name* **import**

View

BGP view

Parameter

group-name: Name of peer group, containing 1 to 47 characters.

ip-address: IP address of the peer, in dotted decimal notation.

route-policy-name: Specified Route-policy. The length of *route-policy-name* parameter ranges from 1 to 19 character string.

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 ingress routing policy configured for the peer is higher than that 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/peer group test.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] bgp 100
[SW7750-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: Peer group name, containing 1 to 47 characters.

seconds: Minimum interval at which UPDATE packets are sent. It is in the range of 0 to 600 seconds. By default, the advertisement interval is 5 seconds for internal peer group and 30 seconds for external peer group.

Description

Use the **peer route-update-interval** command to configure the interval at which the same route update packet is sent to the peer group. .

Use the **undo peer route-update-interval** command to restore the default interval.

Example

Configure the interval of the BGP peer group "test" sending the route update packet as 10 seconds.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] bgp 100
[SW7750-bgp] peer test route-update-interval 10
```

peer timer

Syntax

peer { *group-name* | *ip-address* } **timer keep-alive** *keepalive-interval* **hold** *holdtime-interval*

undo peer { *group-name* | *ip-address* } **timer**

View

BGP view

Parameter

group-name: Name of peer group, containing 1 to 47 characters.

ip-address: IP address of the peer.

Keepalive-interval: Keepalive timer in seconds. It is in the range of 1 to 65,535 and defaults to 60 seconds.

Holdtime-interval: Holdtime timer in seconds. It is in the range of 3 to 65,535 and defaults to 180 seconds.

Description

Use the **peer timer** command to configure the Keepalive and holdtime timers for a peer/peer group.

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

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".

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] bgp 100
[SW7750-bgp] peer test timer keep-alive 60 hold 180
```

preference

Syntax **preference** *ebgp-value ibgp-value local-value*

undo preference

View BGP view/BGP multicast address family view

Parameter *ebgp-value*: Preference value for EBGP. It is in the range of 1 to 256 and defaults to 256.

ibgp-value: Preference value for IBGP routes. It is in the range of 1 to 256 and defaults to 256.

local-value: Preference value for locally-originated routes. It is in the range of 1 to 256 and defaults to 130.

Description Use the **preference** command to set preference values for. routes learned from external peers, routes learned from internal peers, and local-originated routes.

Use the **undo preference** command to restore the default preference values.

Example # Set the preferences of EBGP, IBGP and locally generated routes to 170.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] bgp 100
[SW7750-bgp] preference 170 170 170
```

reflect between-clients

Syntax **reflect between-clients**

undo reflect between-clients

View BGP view/BGP multicast address family 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 a route reflector is configured, it reflects the route of a client to another client.

By default, the clients of a route reflector are not fully interconnected and the route is reflected from a client to another client by default via the route reflector. If the clients are fully interconnected, you do not need to configure route reflection.

Related command: **reflector cluster-id**, and **peer reflect-client**.

Example # Disable the reflection between clients.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] bgp 100
[SW7750-bgp] undo reflect between-clients
```

reflector cluster-id

Syntax **reflector cluster-id** *cluster-id*

undo reflector cluster-id

View BGP view

Parameter *cluster-id:* Cluster ID of the route reflector, an integer number ranging from 1 to 4,294,967,295, or an IP address in dotted decimal notation.

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.

Generally, there is only one route reflector in a cluster. In this case, Router ID of the route reflector is used to identify the cluster. Setting multiple route reflectors enhances network stability. If multiple route reflectors are in a cluster, use this command to configure the same cluster ID for all the route reflectors to prevent route loop.

Related command: **reflect between-clients**, and **peer reflect-client**.

Example # A local router is one of the route reflectors in a cluster. Set the cluster ID of the route reflector as 80.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] bgp 100
[SW7750-bgp] reflector cluster-id 80
```

refresh bgp

Syntax **refresh bgp** { **all** | *ip-address* | **group** *group-name* } [**multicast**] { **import** | **export** }

View User view

Parameter

all: Refreshes all peers.

ip-address: Refreshes connection with a BGP peer with the specified IP address in dotted decimal notation.

group-name: Peer group name, containing 1 to 47 characters.

multicast: Specifies multicast address family.

import: Sends a ROUTE-REFRESH packet to the peer, requesting the peer to refresh the routes.

export: Refreshes routes advertised to the peers.

Description

Use the **refresh bgp** command to manually refresh BGP connections. Refreshing BGP connections can refresh the BGP routing table without interruption any BGP connection and apply a new policy.

After a BGP connection is created, only incremental routes are sent. However, in some cases, such as when BGP routing policy changes, the peer needs to re-advertise .routes or to be resent routes so that the routes are filtered again according to the new policy.

Example

Refresh all BGP connections.

```
<SW7750> refresh bgp all import
```

reset bgp

Syntax

reset bgp { **all** | *ip-address* | **group** *group-name* }

View

User view

Parameter

all: Resets all the connections with BGP.

ip-address: Resets connection with a specified BGP peer.

group *group-name*: Resets the connection with a specified peer group.

Description

Use the **reset bgp** *ip-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.

Use the **reset bgp group** *group-name* command to reset the BGP connection with a specified peer group.

After a BGP routing policy or protocol configuration changes, resetting the BGP connection will make the new configured policy take effect immediately.

Example # After using the **timer** command to configure new Keepalive and Holdtime intervals, you can reset all BGP connections for the new configuration to take effects immediately.

```
<SW7750> reset bgp all
```

reset bgp dampening

Syntax **reset bgp dampening** [*network-address* [*mask*]]

View User view

Parameter *network-address*: IP address of a network segment, in dotted decimal notation.

mask: Network mask, in dotted decimal notation.

Description Use the **reset bgp dampening** command to reset the flapping attenuation information of a route and release the suppression of a suppressed route.

Related command: **dampening**, and **display bgp routing-table dampened**.

Example # Reset the route attenuation information of the specified route.

```
<SW7750> reset bgp dampening 20.1.0.0 255.255.0.0
```

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 consistent with a specified filter list. The range of the parameter *acl-number* is 1 to 199.

network-address: Resets the flap-info of a record at this IP address.

mask: Network mask, in dotted decimal notation.

Description Use the **reset bgp flap-info** command to reset the flap info of a route.

If no value is specified, the flap info of all routes will be reset.

Related command: **dampening**.

Example # Reset the flap-info of all the routes that go through filter list 1.

```
<SW7750> reset bgp flap-info as-path-acl 1
```

router id

Syntax **router id** *router-id*

undo router id

View System view

Parameter *router-id*: Router ID, in dotted decimal notation.

Description Use the **router id** command to configure the ID of a BGP router.

Use the **undo router id** command to cancel the router ID that has been set.

Example # Set the router ID to 10.1.1.3.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] router id 10.1.1.3
```

summary

Syntax **summary**

undo summary

View BGP view/BGP multicast address family view

Parameter None

Description Use the **summary** command to configure auto aggregation of sub-network routes.

Use the **undo summary** command to disable it.

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.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] bgp 100
[SW7750-bgp] summary
```

timer

Syntax **timer keep-alive** *keepalive-interval* **hold** *holdtime-interval*

undo timer

View BGP view

Parameter *keepalive-interval:* Set the interval time value for keepalive time. The range is 1 to 65,535. By default, its value is 60 seconds.

holdtime-interval: Set the interval time value for hold time. The range is 3 to 65,535. By default, its value is 180 seconds.

Description Use the **timer** command to configure the Keep-alive and Hold-time timer of BGP.

Use **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 30 seconds and Hold-time timer as 90 seconds.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] bgp 100
[SW7750-bgp] timer keepalive 120 hold 360
```

undo synchronization

Syntax **undo synchronization**

View BGP view

Parameter None

Description Use the **undo synchronization** command to cancel the synchronization of BGP and IGP.

By default, BGP does not synchronize with IGP.

If the local BGP is not set synchronous with the IGP and the next hop of the learned BGP route is reachable, the local BGP will add this BGP route into its routing table immediately after it learns the route, rather than waiting till the IGP also learns the route.

This command means BGP does not synchronize with IGP in the current system. You need not configure it because the the Switch 7750 Family does not support the synchronization of BGP and IGP.

Example # Cancel the synchronization of BGP and IGP.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] bgp 100
[SW7750-bgp] undo synchronization
```

34 IP ROUTING POLICY CONFIGURATION COMMANDS

The word "router" covered in the following text represent routers in common sense and Ethernet switches running a routing protocol. To improve readability, this will not be mentioned again in this manual.

apply as-path

Syntax **apply as-path** *as-number-list*

undo apply as-path

View Route policy view

Parameter *as-number-list*: AS number list, in the form of a*s-number*&<1-10>. Here, a*s-number* is an AS number, which ranges from 1 to 65,535, and &<1-10> means you can input 1 to 10 AS numbers in one command.

Description Use the **apply as-path** command to add AS number before original AS path in Router-policy.

Use the **undo apply as-path** command to remove the added AS number.

By default, AS number is not set.

If the Route-policy matching conditions are met, AS attributes of the transmission route will be changed by the **apply as-path** command. A maximum of ten AS numbers can be added.

Example # Add AS number 200 before the original AS path

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750]route-policy 10 permit node 10
[SW7750-route-policy] apply as-path 200
```

apply community

Syntax **apply community** { **none** | [*aa:nn*] &<1-13> [**no-export-subconfed** | **no-export** | **no-advertise**]* [**additive**] }

undo apply community

View Route policy view

Parameter **none**: No community attribute

aa:nn: Community number. The value ranges of aa and nn are both from 1 to 65,535. &<1-13> means that you need to provide at least one and can provide up to 13 community numbers.

no-export-subconfed: Specifies not to send matching routes out of sub-autonomous system.

no-advertise: Specifies not to send matching routes to any peer entities.

no-export: Specifies not to send routes out of sub-autonomous system or federation but to send to the other sub-autonomous systems in the federation.

additive: Additive community attributes

Description Use the **apply community** command to set BGP community attributes in Route-policy.

Use the **undo apply community** command to cancel the BGP community attribute setting .

By default, BGP community attributes are not set.

If the Route-policy matching conditions are met, BGP community attributes will be changed by the **apply community** command.

Related command: **ip community-list**, **if-match community**, **route-policy** and **display bgp routing-table community**.

Example # Create a Route-policy named setcommunity and set its node sequence number as 16 and matching mode as permit. Enter route policy view and set matching conditions and execute attribute change command

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] route-policy setcommunity permit node 16
[SW7750-route-policy] if-match as-path 8
[SW7750-route-policy] apply community no-export
```

apply cost

Syntax **apply cost** *value*

undo apply cost

View Route policy view

Parameter

value: Route cost value of route information. The value ranges from 0 to 4294967295.

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 statement.

By default, no apply statement is defined.

An apply statement of Route-policy sets the cost of the routes passing the filtering.

Related command:

if-match interface, **if-match { acl | ip-prefix }**, **if-match ip next-hop**, **if-match cost**, **if-match tag**, **route-policy**, **apply ip next-hop**, **apply local-preference**, **apply origin**, and **apply tag**.

Example

Define an apply statement. When it is used for setting route information attribute, it sets the route cost value of route information as 120.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750]route-policy policy_10 permit node 12
[SW7750-route-policy] apply cost 120
```

apply cost-type

Syntax

apply cost-type [**internal** | **external**]

undo apply cost-type

View

Route policy view

Parameter

internal: Used in BGP, indicates that the IGP cost will be used as the BGP MED value when BGP peer entity advertises routes to the EBGP peer entity. This keyword is used only for IS-IS (representing that IS-IS interior cost will be used) and is invalid for other protocols.

External: This keyword is used only for IS-IS and is invalid for other protocols.

Description

Use the **apply cost-type** command to set the routing cost type of routing information.

Use the **undo apply cost-type** command to cancel the setting argument.

By default, routing cost is not set.

Example

Set IGP cost as the BGP MED value.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
```

```
[SW7750]route-policy 10 permit node 10
[SW7750-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:* IP address of next hop, in dotted decimal notation.

Description Use the **apply ip next-hop** command to set the IP address of next hop.

Use the **undo apply ip next-hop** command to cancel the setting argument.

By default, no next hop is defined.

An apply statement of Route-policy sets the next hop of the filtered packets.

Related command: **if-match interface**, **if-match { acl | ip-prefix }**, **if-match ip next-hop**, **if-match cost**, **if-match tag**, **route-policy**, **apply local-preference**, **apply cost**, **apply origin** and **apply tag**.

Example # Define an apply statement to set the next hop in the routing information to 193.1.1.8.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750]route-policy 10 permit node 10
[SW7750-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**: Imports routes to level-1 area.

level-2: Imports routes to level-2 area.

level-1-2: Imports routes to both level-1 area and level-2 area.

Description Use the **apply isis** command to define an apply clause to import routing information into the IS-IS area(s) at specified level(s).

Use the command to cancel the clause setting.

By default, no **apply** clause is defined.

Related command: **if-match interface**, **if-match { acl | ip-prefix }**, **if-match ip next-hop**, **if-match cost**, **if-match tag**, **route-policy**, **apply cost**, **apply origin** and **apply tag**.

Example # Define an apply clause to import routes to level-2 area.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750]route-policy 10 permit node 10
[SW7750-route-policy] apply isis level-2
```

apply local-preference

Syntax **apply local-preference** *local-preference*

undo apply local-preference

View Route policy view

Parameter *local-preference:* local preference, ranging from 0 to 4294967295.

Description Use the **apply local-preference** command to set local preference for routing information.

Use the **undo apply local-preference** command to cancel the apply statement setting.

Related command: **if-match interface**, **if-match { acl | ip-prefix }**, **if-match ip next-hop**, **if-match cost**, **if-match tag**, **route-policy**, **apply ip next-hop**, **apply local-preference**, **apply origin** and **apply tag**.

Example # Define an apply statement to set local preference for the routing information to 130.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750]route-policy 10 permit node 10
[SW7750-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: Specifies that BGP routing information source is internal route

egp: Specifies that BGP routing information source is external route

as-number: Specifies autonomous system number of external routes. The value ranges from 1 to 65,535.

incomplete: Specifies that BGP routing information source is unknown.

Description

Use the **apply origin** command to set BGP routing information source.

Use the **undo apply origin** command to cancel the apply statement setting.

Related command:

if-match interface, **if-match { acl | ip-prefix }**, **if-match ip next-hop**, **if-match cost**, **if-match tag**, **route-policy**, **apply ip next-hop**, **apply local-preference**, **apply cost** and **apply tag**.

Example

Define an apply statement to specify that the BGP routing information source is igp.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750]route-policy 10 permit node 10
[SW7750-route-policy] apply origin igp
```

apply tag

Syntax

apply tag *value*

undo apply tag

View

Route policy view

Parameter

value: Tag value of route information. The value ranges from 0 to 4294967295.

Description

Use the **apply tag** command to configure to set the tag area of RIP or OSPF route information.

Use the **undo apply tag** command to cancel the apply statement.

Related command:

if-match interface, **if-match { acl | ip-prefix }**, **if-match ip next-hop**, **if-match cost**, **if-match tag**, **route-policy**, **apply ip next-hop**, **apply local-preference**, **apply cost**, and **apply origin**.

Example

Define an apply statement. When it is used for setting route information attribute, it sets the tag area of route information as 100.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750]route-policy policy_10 permit node 12
[SW7750-route-policy] apply tag 100
```

display ip ip-prefix

Syntax **display ip ip-prefix** [*ip-prefix-name*]

View Any view

Parameter *ip-prefix-name*: Name of the address prefix list to be displayed, containing 1 to 19 characters.

Description Use the **display ip ip-prefix** command to display an address prefix list.

Related command: **ip ip-prefix**.

Example # Display the information about the address prefix list named p1.

```
<SW7750> display ip ip-prefix p1
name                 index   conditions  ip-prefix / mask    GE  LE
p1                   10      permit      10.1.0.0/16         17  18
```

Table 79 Field descriptions 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*: Name of the route-policy to be displayed, containing 1 to 19 characters.

Description Use the **display route-policy** command to display the configured Route-policy.

If you do not specify a route policy name, this command displays all route-policies configured.

Related command: **route-policy**.

Example # Display the information about Route-policy named policy1.

```
<SW7750> display route-policy policy1
Route-policy : policy1
```

```
Permit 10 : if-match (prefixlist) p1
            apply cost 100
            matched : 0     denied : 0
```

Table 80 Field descriptions of the **display route-policy** command

Field	Description	
Route-policy	Name of ip-prefix	
Permit 10	Information about the route-policy with the mode configured as permit and the node as 10:	
	if-match (prefixlist) p1	if-match statement configured
	apply cost 100	Apply routing cost 100 to the routes matching the conditions defined by if-match statement
	matched	Number of routes matching the conditions set by if-match statement
	denied	Number of routes not matching the conditions set by if-match statement

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*: Number of the ACL used for filter

ip-prefix-name: Name of the prefix address list used for filter, containing 1 to 19 characters.

Description Use the **if-match** { **acl** | **ip-prefix** } command to configure a rule for the route-policy and specify an matching IP address range.

Use the **undo if-match** { **acl** | **ip-prefix** } command to cancel the setting of the rule.

The **if-match** { **acl** | **ip-prefix** } command implements a filter by referencing an ACL or a prefix address list.

Related command: **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**, and **apply tag**.

Example # Define an if-match statement. When the statement is used for filtering route information, the route information filtered by route destination address through address prefix list p1 is permitted to pass the if-match statement.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] route-policy policy_10 permit node 12
```

```
  %New sequence of this list
[SW7750-route-policy] if-match ip-prefix p1
```

if-match as-path

Syntax **if-match as-path** *as-path-number*

undo if-match as-path

View Route policy view

Parameter *as-path-number:* AS path number, ranging from 1 to 199.

Description Use the **if-match as-path** command to match the AS path field of BGP routing information.

Use the **undo if-match as-path** command to cancel the AS path field matching.

By default, AS regular expression is not set for matching in Route-policy.

An if-match statement of Route-policy sets AS path attributes as matching conditions to filter BGP routing information.

Example # Create as-path 2, which permits the routing information of AS 200 and AS 300. Then create a Route-policy named test, and define an if-match statement quoting the definitions of as-path 2 for node 10 of the Route-policy.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ip as-path-acl 2 permit 200:300
[SW7750] route-policy test permit node 10
[SW7750-route-policy] if-match as-path 2
```

if-match community

Syntax **if-match community** { *basic-community-list-number* [**whole-match**] | *adv-community-list-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, which means that all communities and only these communities must be displayed.

Description Use the **if-match community** command to match community attributes of BGP routing information.

Use the **undo if-match community** command to cancel community attribute matching settings.

Be default, community attributes are not set for matching.

An if-match statement of Route-policy sets community attributes as matching conditions to filter BGP routing information.

Related command: **route-policy** and **ip community-list**.

Example # Create community-list 1, which permits routing information of AS 100 and AS 200. Then create a Route-policy named test and define an if-match statement quoting the definitions of community-list 1 for node 10 of the Route-policy.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ip community-list 1 permit 100:200
[SW7750] route-policy test permit node 10
[SW7750-route-policy] if-match community 1
```

if-match cost

Syntax **if-match cost** *value*

undo if-match cost

View Route policy view

Parameter *value*: Route cost value, ranging from 0 to 4,294,967,295.

Description Use the **if-match cost** command to configure one of the match rules of the route-policy to match the cost of routing information.

Use the **undo if-match cost** command to cancel the configuration of the match rule.

By default, no if-match statement is defined.

An if-match statement of the route-policy specifies the route cost of the routing information meeting the condition.

Related command: **if-match interface**, **if-match { acl | ip-prefix }**, **if-match ip next-hop**, **if-match tag**, **route-policy**, **apply ip next-hop**, **apply cost**, **apply local-preference**, **apply origin**, and **apply tag**.

Example # Define an if-match statement and allow the routing information with a routing cost of 8 to pass this if-match statement.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] route-policy policy permit node 1
  %New sequence of this list
[SW7750-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*: Interface type.

interface-number: Interface number.

Description Use the **if-match interface** command to configure to match the route whose next hop is the designated interface.

Use the **undo if-match interface** command to cancel the setting of matching condition.

By default, no if-match statement is defined.

As an if-match statement of route-policy, it matches the corresponding interface of route next hop when filtering route.

Related command: **if-match { acl | 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**, and **apply tag**.

Example # Define an if-match statement to match the route whose next hop interface is Vlan-interface 1

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] route-policy policy permit node 1
  %New sequence of this list
[SW7750-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: Number of the ACL used for filter. It ranges from 2,000 to 2,999.

ip-prefix-name: Name of the prefix address list used for filter.

Description

Use the **if-match ip next-hop** command to configure one of the match rules of route-policy on the next hop address of the routing information.

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.

By default, no if-match statement is defined.

An if-match statement of route-policy is used to specify the next hop matching the routing information when filtering the routes. It performs filter by referencing an ACL or an address prefix list.

Related command:

if-match interface, **if-match { acl | ip-prefix }**, **if-match cost**, **if-match tag**, **route-policy**, **apply ip next-hop**, **apply cost**, **apply local-preference**, **apply origin**, and **apply tag**.

Example

Define an if-match statement. It permits the routing information whose route next hop address filtered through prefix address list p1 to pass this if-match statement.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] route-policy policy permit node 1
  %New sequence of this list
[SW7750-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: Tag field value, ranging from 0 to 4,294,967,295.

Description

Use the **if-match tag** command to configure to match the tag field of route information.

Use the **undo if-match tag** command to cancel the existing matching rules.

Related command:

if-match interface, **if-match { acl | ip-prefix }**, **if-match ip next-hop**, **if-match cost**, **route-policy**, **apply ip next-hop**, **apply cost**, **apply local-preference**, **apply origin**, and **apply tag**.

Example

Define an if-match statement to permit the OSPF route information whose tag value is 8 to pass the if-match statement.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] route-policy policy permit node 1
  %New sequence of this list
[SW7750-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: AS path list number, ranging from 1 to 199.

as-regular-expression: AS path regular expression

Description

Use the **ip as-path-acl** command to configure an AS regular expression.

Use the **undo ip as-path-acl** command to cancel the defined regular expression.

The defined AS path list can be used in BGP policy.

Related command:

peer as-path-acl export, **peer as-path-acl import** and **display bgp routing-table as-path-acl**.

Example

Configure an AS path list

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ip as-path-acl 10 permit 200,300
```

ip community-list

Syntax

ip community-list *basic-comm-list-number* { **permit** | **deny** } [*aa:nn*] &<1-12> [**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: Basic community list number, ranging from 1 to 99.

adv-comm-list-number: Advanced community list number, ranging from 100 to 199.

permit: Specifies to allow access to matching conditions.

deny: Specifies to deny access to matching conditions.

aa:nn: Community number. The value ranges of aa and nn are both from 1 to 65,535. &<1-12> means that you need to provide at least one and can provide up to 12 community numbers.

internet: Specifies to advertise all routes.

no-export-subconfed: Specifies not to send matching routes out of sub-autonomous system.

no-advertise: Specifies not to send matching routes to any peer entities.

no-export: Specifies not to send routes out of sub-autonomous system or federation but to send to the other sub-autonomous systems in the federation.

comm-regular-expression: Community attribute in regular expression.

Description Use the **ip community-list** command to set a BGP community list.

Use the **undo ip community-list** command to cancel the community list settings.

The defined community list can be used in BGP policy.

Related command: **apply community**, **display bgp routing-table community-list**.

Example # Define a community list, and specify not to send the routes with the community attributes out of the local autonomous system.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] 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:* Name of address prefix list, containing 1 to 19 characters. It identifies an address prefix list uniquely.

index-number: Identifier of 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. If the permit mode is specified and the IP address to be filtered is in the ip-prefix range specified by the item, the item is filtered through and the next item is not tested. If the IP address to be filtered is not in the ip-prefix range specified by the item, the next item is tested

deny: Specifies the match mode of the defined address prefix list items as deny mode. If the deny mode is specified and the IP address to be filtered is in the ip-prefix range specified by the item, the item is not filtered through and the next item is not tested; otherwise, the next item is tested.

network: IP address prefix range (IP address). If it is specified as 0.0.0.0 0, all the IP addresses are matched.

len: IP address prefix range (mask length). If it is specified as 0.0.0.0 0, all the IP addresses are matched.

greater-equal, less-equal: 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 "greater 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.

An 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". That is, passing an item means filtering through this address prefix list. Not filtering through any item means not filtering through 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 matches the default route only.

Example

Define an ip-prefix named p1 to permit only the routes whose mask lengths are 17 or 18 on network segment 10.0.192.0 8 to pass.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ip ip-prefix p1 permit 10.0.192.0 8 greater-equal 17 less-e
qual 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*: Name of the Route-policy, containing 1 to 19 characters. It identifies a Route-policy uniquely.

permit: Specifies the match mode of the defined Route-policy node as permit mode. When a route entry meets all the if-match statements of the node, the entry is permitted to filter through the node and the apply statement of the node will be performed. If a route entry does not meet the if-match statement of the node, the next node of the route-policy will be tested.

deny: Specifies the match mode of the defined Route-policy node as deny mode. When a route entry meets all the if-match statements of the node, the entry is prohibited from filtering through the node and the next node will not be tested.

node: Specifies the node of the route policy.

node-number: Index of the node in the route-policy. When this route-policy is used for routing information filter, the node with smaller *node-number* will be tested first.

Description Use the **route-policy** command to enter the Route-policy view.

Use the **undo route-policy** command to delete the created Route-policy.

By default, no Route-policy is defined.

Route-policy is used for route information filter or route policy. A Route-policy comprises some nodes and each node comprises some if-match statements and apply statements.

An if-match statement defines the match rules of this node. An apply statement defines the actions after filtering through this node. The filtering relationship between the if-match statements of the node is "and". That is, all if-match statements of the node must be met.

The filtering relation between Route-policy nodes is "OR". That is, filtering through one node means filtering through this Route-policy. If the information does not filter through any node, it cannot filter through this Route-policy.

Related command: **if-match interface**, **if-match { acl | ip-prefix }**, **if-match ip next-hop**, **if-match cost**, **if-match tag**, **apply ip next-hop**, **apply local-preference**, **apply cost**, **apply origin**, and **apply tag**.

Example # Configure Route-policy policy_10, with the node number of 12 and the match mode of permit, and enter Route policy view.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750]route-policy policy_10 permit node 12
  %New sequence of this list
[SW7750-route-policy]
```

35 Route Capacity Configuration Commands

The word "router" covered in the following text represent routers in common sense and Ethernet switches running a routing protocol. To improve readability, this will not be mentioned again in this manual.

display memory

Syntax **display memory** [**slot** *slot_number*]

View Any view

Parameter *slot_number*: Number of the slot whose route capacity information is displayed.

Description Use the **display memory** command to display the memory setting.

Example # Display the current memory setting of the switch.

```
<SW7750> display memory
System Total Memory(bytes): 203563008
Total Used Memory(bytes): 77852012
Used Rate: 38%
```

The following table shows describes the fields of the command:

Table 81 Field descriptions of the **display memory** command

Field	Description
System Total Memory(bytes)	Free memory size, in bytes, of the switch
Total Used Memory(bytes)	Occupied memory size, in bytes, of the switch
Used Rate	Memory occupation rate

display memory limit

Syntax **display memory limit**

View Any view

Parameter None

Description Use the **display memory limit** command to display the memory setting and state information related to route capacity.

This command displays the current memory limit configuration, free memory, and state information about connections, such as times of disconnection, times of reconnection, and whether the current state is normal.

Example # Display the current memory setting and state information.

```
<SW7750>display memory limit
Current memory limit configuration information:
  system memory safety: 40 (MBytes)
  system memory limit: 30 (MBytes)
  auto-establish enabled

Free Memory: 111571652 (Bytes)

The state information about connection:
  The times of disconnect: 0
  The times of reconnect: 0
  The current state: Normal
```

The information displayed by this command includes Ethernet switch memory limit, size of free memory, times of disconnection, times of reconnection, and the current state.

The following table describes the fields of the command:

Table 82 Field descriptions of the **display memory limit** command

Field	Description
system memory safety	Safety value of the switch memory.
system memory limit	Lower limit of the switch memory.
auto-establish enabled	Automatic connection restoration is enabled (If automatic connection restoration is disabled, "auto-establish disabled" is displayed).
Free Memory	Size of the current free memory in bytes
The times of disconnect: 0	The times of the disconnection of the routing protocol is 0.
The times of reconnect: 0	The times of reconnection of the routing protocol is 0.
The current state: Normal	The current state is normal (If the current state is emergent, "Exigence" is displayed).

memory auto-establish disable

Syntax **memory auto-establish disable**

View System view

Parameter None

Description Use the **memory auto-establish disable** command to disable the automatic restoration of routing protocol connection (even if the free memory recovers to a safety value).

By default, when the free memory of the switch recovers to a safety value, connections of all the routing protocols will always recover (when the free memory of the switch decreases to a lower limit, the connection will be disconnected forcibly).

After this command is used, connections of all the routing protocols will not recover when the free memory of the switch recovers to a safety value. In this case, you need to restart the routing protocol to recover the connections.

Use this command with caution.

Related command: **memory auto-establish enable**, **memory { safety | limit }***, **display memory limit**.

Example # Disable automatic restoration of the routing protocol connections when the free memory of the current switch recovers.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] memory auto-establish disable
```

memory auto-establish enable

Syntax **memory auto-establish enable**

View System view

Parameter None

Description Use the **memory auto-establish enable** command to enable automatic restoration of routing protocol connections when the free memory of the switch recovers to the specified value.

Use the **memory auto-establish disable** command to disable this function.

By default, when the free memory of the switch recovers to a safety value, connections of all the routing protocols will always recover (when the free memory of the switch decreases to a lower limit, the connection will be disconnected forcibly).

By default, this function is enabled.

Related command: **memory auto-establish disable**, **memory { safety | limit }***, **display memory limit**.

Example # Enable automatic restoration of the connections of all the routing protocols when the free memory of the current switch recovers..

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] memory auto-establish enable
```

memory { safety | limit }*

Syntax **memory** { **safety** *safety-value* | **limit** *limit-value* }*

undo memory [**safety** | **limit**]

View System view

Parameter *safety-value*: Safety free memory of the switch , in Mbytes. Its value range depends on the free memory of the current switch. The default is 40.

limit-value: Lower limit of the switch free memory, in Mbytes. Its value range depends on the free memory of the current switch. The default is 30.

Description Use the **memory limit** *limit-value* command to configure the lower limit of the switch free memory.

When the free memory of the switch is less than this limit, all the routing protocol connections will be disconnected forcibly. The *limit-value* argument in the command must be less than the current free memory safety value; otherwise, the configuration will fail.

Use the **memory safety** *safety-value* command to configure the safety value of the switch free memory.

If you use the **memory auto-establish enable** command (the default configuration), the routing protocol connection that is forcibly disconnected automatically recovers when the free memory of the switch reaches this value. The *safety-value* argument in the command must be greater than the current free memory lower limit; otherwise, the configuration will fail.

Use the **memory safety** *safety-value* **limit** *limit-value* command to change both the safety value and lower limit of the switch free memory. The value of *safety-value* must be greater than that of *limit-value*; otherwise, the configuration will fail.

Use the **undo memory** command to restore the default safety value and lower limit of the switch free memory.

Related command: **memory auto-establish disable**, **memory auto-establish enable**, and **display memory limit**.

Example # Set the lower limit of the switch free memory to 2 MB and the safety value to 4 MB.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] memory safety 4 limit 2
```

36 GMRP CONFIGURATION COMMANDS

Ethernet switches serve as routers when an IP multicast protocol is running on them. The routers mentioned here refer to common routers and Layer 3 Ethernet switches running an IP multicast protocol.

display gmrp statistics

Syntax **display gmrp statistics** [**interface** *interface-list*]

View Any view

Parameter **interface** *interface-list*: Specifies Ethernet port list, expressed as *interface-list*={ *interface-type interface-number* [**to** { *interface-type interface-number* }] }&<1-10>.

Description Use the **display gmrp statistics** command to view the statistics information about GMRP.

This command is used for displaying the statistics information about GMRP, including the list of ports with GMRP enabled, GMRP status information, GMRP failed registrations and last origin of GMRP packet data unit (PDU).

If an interface is specified, the system displays the GMRP statistics information of the specified interface.

Example # Display the statistics information about GMRP on Ethernet 2/0/1.

```
<SW7750> display gmrp statistics interface Ethernet 2/0/1
GMRP statistics on port Ethernet2/0/1
Gmrp Status             : Enabled
Gmrp Running               :Yes
Gmrp Failed Registrations  : 0
Gmrp Last Pdu Origin       : 0000-0000-0000
```

display gmrp status

Syntax **display gmrp status**

View Any view

Parameter None

Description

Use the **display gmrp status** command to view the status of global GMRP.

Example

Display the status of global GMRP.

```
<SW7750> display gmrp status
GMRP is enabled
```

gmrp

Syntax

gmrp

undo gmrp

View

System view, Ethernet port view

Parameter

None

Description

Use the **gmrp** command to enable GMRP globally or enable GMRP on a port.

Use the **undo gmrp** command to disable GMRP globally or disable GMRP on a port..

By default, GMRP is disabled globally and on each port.

Executed in system view, this command will enable the global GMRP. After performing this command in Ethernet port view, GMRP will be enabled on a port.

Before enabling GMRP on a port, you shall enable GMRP globally.

Related command:

display gmrp status, **display gmrp statistics**.

Example

Enable GMRP globally.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] gmrp
GMRP is enabled globally.
```

37 IGMP SNOOPING CONFIGURATION COMMANDS

Ethernet switches serve as routers when an IP multicast protocol is running on them. The routers mentioned here refer to common routers and Layer 3 Ethernet switches where the IP multicast protocol is running.

display igmp-snooping configuration

Syntax **display igmp-snooping configuration**

View Any view

Parameter None

Description Use the **display igmp-snooping configuration** command to display IGMP Snooping configuration information.

When IGMP Snooping is enabled on the switch, this command displays the following information: IGMP Snooping status, aging time of the router port, query response timeout time, and aging time of multicast member ports.

Related command: **igmp-snooping**.

Example # Display IGMP Snooping configuration information on the switch.

```
<SW7750> display igmp-snooping configuration
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).
```

The above information shows: IGMP Snooping is enabled, the aging time of the router port is 105 seconds, the query response timeout time is one second, and the aging time of multicast member ports is 260 seconds.

display igmp-snooping group

Syntax **display igmp-snooping group** [**vlan** *vlan-id*]

View Any view

Parameter *vlan-id*: ID of the specified VLAN.

Description

Use the **display igmp-snooping group** command to display information about the IP and MAC multicast groups under one specified VLAN (with **vlan** *vlan-id*) or all VLANs (without **vlan** *vlan-id*).

This command displays the following information: VLAN ID, router port, IP multicast group address, member ports included in the IP multicast group, MAC multicast group, MAC multicast group address, and member ports included in the MAC multicast group.

Example

Display information about the multicast groups under VLAN 2.

```
<SW7750> display igmp-snooping group vlan 2
Total 1 IP Group(s).
  Total 1 MAC Group(s).

  Vlan(id):2.
    Total 1 IP Group(s).
    Total 1 MAC Group(s).
    Static router port(s):
    Dynamic router port(s):
    IP group(s):the following ip group(s) match to one mac group.
        IP group address:225.1.1.1
        Host port(s):GigabitEthernet2/0/1
    MAC group(s):
        MAC group address:0100-5e01-0101
        Host port(s):GigabitEthernet2/0/1
```

The information above means:

- Multicast groups exist in VLAN 2.
- The address of the IP multicast group is 255.1.1.1.

display igmp-snooping statistics

Syntax **display igmp-snooping statistics**

View Any view

Parameter None

Description

Use the **display igmp-snooping statistics** command to display IGMP Snooping message statistics.

This command displays the following information: the numbers of the IGMP general query messages, IGMP group-specific query messages, IGMP V1 report messages, IGMP V2 report messages, IGMP leave messages and error IGMP messages received, and the number of the IGMP group-specific query messages sent.

Related command: **igmp-snooping**.

Example # Display IGMP Snooping message statistics.

```
<SW7750> display igmp-snooping statistics
Received IGMP general query packet(s) number:0.
Received IGMP specific query packet(s) number:0.
Received IGMP V1 report packet(s) number:0.
Received IGMP V2 report packet(s) number:0.
Received IGMP leave packet(s) number:0.
Received error IGMP packet(s) number:0.
Sent IGMP specific query packet(s) number:0.
```

The information above shows that IGMP receives:

- zero IGMP general query packets
- zero IGMP specific query packets
- zero IGMP V1 report packets
- zero IGMP V2 report packets
- zero IGMP leave packets
- zero IGMP error packets

IGMP Snooping sends:

- zero IGMP specific query packets

display multicast-vlan

Syntax **display multicast-vlan** [*vlan-id*]

View Any view

Parameter *vlan-id*: ID of the specified VLAN.

Description Use the **display multicast-vlan** command to display the configuration of the multicast VLAN.

If the *vlan-id* argument is not provided when the command is executed, the configuration information about all the VLANs in the network is displayed.

Example # Display the configuration of multicast VLAN 2.

```
<SW7750> display multicast-vlan 2
multicast vlan 2’s subvlan list:
   Vlan 1024
```

The information above means:

- VLAN 2 exists
- VLAN 1024 is the subvlan of VLAN 2

igmp-snooping

Syntax **igmp-snooping** { **enable** | **disable** }

View System view

Parameter **enable**: Enables the IGMP Snooping feature.

disable: Disables the IGMP Snooping feature.

Description Use the **igmp-snooping enable** command to enable the IGMP Snooping feature.

Use the **igmp-snooping disable** command to disable the IGMP Snooping feature.

By default, the IGMP Snooping feature is disabled.

Example # Enable the IGMP Snooping feature on the switch.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] igmp-snooping enable
Enable IGMP-Snooping ok.
```

igmp-snooping fast-leave

Syntax **igmp-snooping fast-leave** [**vlan** *vlan-list*]

undo igmp-snooping fast-leave [**vlan** *vlan-list*]

View System view, Ethernet port view

Parameter *vlan-list:* Multiple VLANs in the form of vlan-list = { *vlan-id* [to *vlan-id*] } & < 1-10 >. The *vlan-id* argument is the ID of the VLAN, in the range of 1 to 4,094. &<1-10> means that you can provide the argument repeatedly for up to ten times.

Description Use the **igmp-snooping fast-leave** command to enable IGMP fast leave processing.

Use the **undo igmp-snooping fast-leave** command to cancel the configuration.

By default, IGMP fast leave processing is disabled.

Normally, when receiving an IGMP Leave message, IGMP Snooping does not immediately remove the port from the multicast group, but sends a group-specific query message. If no response is received in a given period, it then removes the port from the multicast group.

If this command is executed, when receiving an IGMP Leave packet, IGMP Snooping removes the port from the multicast group directly. When the port has only one user, enabling IGMP fast leave processing can save bandwidth.

- *This feature is effective for IGMP-V2-enabled clients.*
- *When this feature is enabled, if one of the multiple users on a port leaves, the multicast services for the other users in the same multicast group may be interrupted.*

Example # Enable IGMP fast leave processing on Ethernet 2/0/1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet 2/0/1
[SW7750-Ethernet2/0/1] igmp-snooping fast-leave
```

igmp-snooping general-query source-ip

Syntax **igmp-snooping general-query source-ip** { **current-interface |** *ip-address* }

undo igmp-snooping general-query source-ip

View VLAN view

Parameters **current-interface**: Configures to use the IP address of the virtual interface of the current VLAN as the source IP address of IGMP general queries.

ip-address: Specifies a source IP address for IGMP general queries.

Description Use the **igmp-snooping general-query** command to configure the source IP address of IGMP general queries.

Use the **undo igmp-snooping general-query source-ip** command to restore the system default.

This command can take effect only if the IGMP Snooping querier function is enabled on the switch.

By default, the Layer 2 multicast switch sends general query messages with the source IP address of 0.0.0.0.

Examples # Configure the Layer 2 multicast switch to send general query messages with the source IP address 2.2.2.2 in VLAN 3.

```
<SW7750> system-view
System view, return to user view with Ctrl+Z.
[SW7750] igmp-snooping enable
[SW7750] vlan 3
[SW7750-vlan3] igmp-snooping enable
[SW7750-vlan3] igmp-snooping querier
[SW7750-vlan3] igmp-snooping general-query source-ip 2.2.2.2
```

igmp-snooping group-limit

Syntax **igmp-snooping group-limit** *limit* [**vlan** *vlan-list* [**overflow-replace**] || **overflow-replace**]

undo igmp-snooping group-limit [**vlan** *vlan-list*]

View Ethernet port view

Parameter *limit*: Maximum number of multicast groups the port can join, in the range of 1 to 256.

overflow-replace: Permits the new multicast group to replace the previous multicast group. If this keyword is not specified in the specific VLAN, all the previous multicast groups are replaced by default. If this keyword is specified in the specific VLAN, the multicast group with the lowest IP address is replaced preferentially.

vlan-list: List of VLANs. You need to provide this argument in the form of *vlan-list* = { *vlan-id* [**to** *vlan-id*] }&<1-10>, where &<1-10> means that you can provide up to 10 VLAN IDs/VLAN ID ranges for this argument. Normally, a VLAN ID can be a number ranging from 1 to 4,094.

Description Use the **igmp-snooping group-limit** command to define the maximum number of multicast groups the port can join.

Use the **undo igmp-snooping group-limit** command to restore the default setting.

By default, the number of multicast groups on a port is 256

Example # Allow the Ethernet 2/0/1 port to join at most 200 multicast groups.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet 2/0/1
[SW7750-Ethernet2/0/1] igmp-snooping group-limit 200
```

igmp-snooping group-policy

Syntax **igmp-snooping group-policy** *acl-number* [**vlan** *vlan-list*]

undo igmp-snooping group-policy [**vlan** *vlan-list*]

View System view, Ethernet port view

Parameter *acl-number*: Basic ACL number, in the range of 2000 to 2999.

vlan-id: ID of the VLAN for the Ethernet port, in the range of 1 to 4094.

Description

Use the **igmp-snooping group-policy** command to configure an IGMP Snooping filtering ACL.

Use the **undo igmp-snooping group-policy** command to remove the IGMP Snooping filtering ACL.

By default, no IGMP Snooping filtering ACL is configured.

You can configure multicast filtering ACLs globally or on the switch ports connected to user ends so as to use the IGMP Snooping filter function to limit the multicast streams that the users can access. With this function, you can treat different VoD users in different ways by allowing them to access the multicast streams in different multicast groups.

In practice, when a user orders a multicast program, an IGMP host report message is generated. When the message arrives at the switch, the switch examines the multicast filtering ACL configured on the access port to determine if the port can join the corresponding multicast group or not. If yes, it adds the port to the forward port list of the multicast group. If not, it drops the IGMP host report message and does not forward the corresponding data stream to the port. In this way, you can control the multicast streams that users can access.

An ACL rule defines a multicast address or a multicast address range (for example 224.0.0.1 to 239.255.255.255) and is used to.

- Allow the port(s) to join only the multicast group(s) defined in the rule by a permit statement.
- Inhibit the port(s) from joining the multicast group(s) defined in the rule by a deny statement.

- *One port can belong to multiple VLANs. But for each VLAN on the port, you can configure only one ACL.*
- *If the port does not belong to the specified VLAN, the filter ACL you configured does not take effect on the port.*
- *If no ACL rule is configured in the command, the system will reject the multicast packets from all the multicast groups.*

Example

Configure ACL 2000 to allow users under port Ethernet 2/0/1 to access the multicast streams in groups 225.0.0.0 to 225.255.255.255.

- Configure ACL 2000.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] acl number 2000
[SW7750-acl-basic-2000] rule permit source 225.0.0.0 0.255.255.255
[SW7750-acl-basic-2000] quit
```

- Create VLAN 2 and add Ethernet 2/0/1 port to VLAN 2.

```
[SW7750] vlan 2
[SW7750-vlan2] port Ethernet 2/0/1
Gigabit[SW7750-vlan2] quit
```

- Configure ACL 2000 on Ethernet 2/0/1 to allow this VLAN 2 port to join only the IGMP multicast groups defined in the rule of ACL 2000.

```
[SW7750] interface Ethernet 2/0/1
[SW7750-Ethernet2/0/1] igmp-snooping group-policy 2000 vlan 2
[SW7750-Ethernet2/0/1] quit
```

# Configure ACL 2001 to allow users under Ethernet 2/0/2 to access the multicast streams in any groups except groups 225.0.0.0 to 225.0.0.255.

- Configure ACL 2001.

```
[SW7750] acl number 2001
[SW7750-acl-basic-2001] rule deny source 225.0.0.0 0.0.0.255
[SW7750-acl-basic-2001] rule permit source any
[SW7750-acl-basic-2001] quit
```

- Create VLAN 2 and add Ethernet 2/0/2 to VLAN 2.

```
[SW7750] vlan 2
[SW7750-vlan2] port Ethernet 2/0/2
[SW7750-vlan2] quit
```

- Configure ACL 2001 on Ethernet 2/0/2 to allow this VLAN 2 port to join any IGMP multicast groups except those defined in the deny rule of ACL 2001.

```
[SW7750] interface Ethernet 2/0/2
[SW7750-Ethernet2/0/2] igmp-snooping group-policy 2001 vlan 2
```

igmp-snooping host-aging-time

Syntax **igmp-snooping host-aging-time** *seconds*

undo igmp-snooping host-aging-time

View System view

Parameter *seconds*: Aging time of multicast member ports, in the range of 200 to 1000 in seconds.

Description Use the **igmp-snooping host-aging-time** command to configure the aging time of multicast member port.

Use the **undo igmp-snooping host-aging-time** command to restore the default aging time.

By default, the aging time of multicast member ports is 260 seconds.

The aging time of multicast member ports determines the refresh frequency of multicast group members. In an environment where multicast group members change frequently, a relatively shorter aging time is required.

Related command: **igmp-snooping**.

Example # Set the aging time of multicast member ports to 300 seconds.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] 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: Query response timeout time, in the range of 1 to 25 in seconds.

Description

Use the **igmp-snooping max-response-time** command to configure the query response timeout time.

Use the **undo igmp-snooping max-response-time** command to restore the default timeout time.

By default, the query response timeout time is 10 seconds.

The maximum response time you configured determines how long the switch can wait for a response to an IGMP Snooping query message.

Related command:

igmp-snooping, **igmp-snooping router-aging-time**.

Example

Set the query response timeout time to 15 seconds.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] igmp-snooping max-response-time 15
```

igmp-snooping querier

Syntax

igmp-snooping querier

undo igmp-snooping querier

View

VLAN view

Parameters

None

Description

Use the **igmp-snooping querier** command to enable the IGMP Snooping querier feature in the current VLAN of the Layer 2 multicast switch.

Use the **undo igmp-snooping querier** command to disable the IGMP Snooping querier feature in the current VLAN of the Layer 2 multicast switch.

By default, the IGMP Snooping querier feature of the Layer 2 multicast switch is disabled.

Examples # Enable the IGMP Snooping feature in VLAN 3.

```
<SW7750> system-view
System view, return to user view with Ctrl+Z.
[SW7750] igmp-snooping enable
[SW7750] vlan 3
[SW7750-vlan3] igmp-snooping enable
[SW7750-vlan3] igmp-snooping querier
```

igmp-snooping query-interval

Syntax **igmp-snooping query-interval** *seconds*

undo igmp-snooping query-interval

View VLAN view

Parameters *seconds*: Interval for the Layer 2 multicast switch to send general queries, ranging from 1 to 300, in seconds.

Description Use the **igmp-snooping query-interval** command to configure the interval between IGMP general queries sent by the Layer 2 switch.

Use the **undo igmp-snooping query-interval** command to restore the interval to the default value.

By default, the Layer 2 multicast switch sends general queries at the interval of 60 seconds.

These commands are effective only after the IGMP Snooping querier feature is enabled. The configured query interval must be longer than the maximum response time for general queries.

Examples # Configure the Layer 2 multicast switch to send general queries at the interval of 100 seconds in VLAN 3.

```
<SW7750> system-view
System view, return to user view with Ctrl+Z.
[SW7750] igmp-snooping enable
[SW7750] vlan 3
[SW7750-vlan3] igmp-snooping enable
[SW7750-vlan3] igmp-snooping querier
[SW7750-vlan3] igmp-snooping query-interval 100
```

igmp-snooping report-aggregation

Syntax **igmp-snooping report-aggregation**

View System view

Parameter None

Description Use the **igmp-snooping report-aggregation** command to enable suppression on Layer 2 multicast IGMP report packets. In the IGMP-snooping-enabled VLAN, only one IGMP report packet is sent to the upstream router port in an interval.

Use the **undo igmp-snooping report-aggregation** command to disable suppression on Layer 2 multicast IGMP report packets.

By default, suppression on IGMP report packets is disabled.

- *IGMP snooping must be enabled globally before the suppression on IGMP report packets is enabled.*
- *If IGMP snooping is disabled globally, the suppression on IGMP report packets is disabled simultaneously.*

Example # Enable suppression on Layer 2 multicast IGMP report packets on the switch.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] igmp-snooping enable
[SW7750] igmp-snooping report-aggregation
```

igmp-snooping router-aging-time

Syntax **igmp-snooping router-aging-time** *seconds*

undo igmp-snooping router-aging-time

View System view

Parameter *seconds*: Aging time of the router port, in the range of 1 to 1000 in seconds.

Description Use the **igmp-snooping router-aging-time** command to configure the aging time of the router port.

Use the **undo igmp-snooping router-aging-time** command to restore the default aging time.

By default, the aging time of the router port is 105 seconds.

The router port here refers to the port connecting the Layer 2 switch to the router. The Layer 2 switch receives IGMP general query messages from the router through this port. The aging time of the router port should be a value about 2.5 times of the general query interval.

Related command: **igmp-snooping max-response-time**, **igmp-snooping**.

Example # Set the aging time of the router port to 500 seconds.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] igmp-snooping router-aging-time 500
```

igmp-snooping version

Syntax **igmp-snooping version** *version-number*

undo igmp-snooping version

View VLAN view

Parameters *version-number*: IGMP version, in the range of 2 to 3 and defaulting to 2.

Description Use the **igmp-snooping version** command to configure the IGMP Snooping version in the current VLAN.

Use the **undo igmp-snooping version** command to restore the default IGMP Snooping version.

Examples # Set IGMP Snooping version to version 3 in VLAN 100.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] igmp-snooping enable
Enable IGMP-Snooping ok.
[SW7750] vlan 100
[SW7750-vlan100] igmp-snooping enable
[SW7750-vlan100] igmp-snooping version 3
```

igmp host-join port

Syntax **igmp host-join** *group-address* [**source-ip** *source-address*] **port** *interface-list*

undo igmp host-join *group-address* [**source-ip** *source-address*] **port** *interface-list*

View VLAN interface view

Parameters *group-address*: Address of the multicast group that the simulated host will join.

source-address: Address of the multicast source that the simulated host will join. This parameter is valid only when IGMPv3 Snooping is enabled in the VLAN.

port: Specifies one or more ports.

interface-list: Forwarding port list, in the form of *interface-list* = { *interface-type interface-number* [**to** { *interface-type interface-number* }] } &<1-10>. For their meanings and value ranges, see **interface** on page 205.

Description

Use the **igmp host-join port** command to enable simulated joining on the specified port(s) in VLAN interface view.

Use the **undo igmp host-join port** command to remove the configuration.

By default, simulated joining is disabled.

Examples

Configure Ethernet 2/0/1 in the VLAN corresponding to VLAN-interface 10 as a simulated host member of multicast group 225.0.0.1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 10
[SW7750-Vlan-interface10] igmp host-join 225.0.0.1 port Ethernet 2/0/1
```

igmp host-join

Syntax

igmp host-join *group-address* [**source-ip** *source-address*] **vlan** *vlan-id*

undo igmp host-join *group-address* [**source-ip** *source-address*] **vlan** *vlan-id*

View

Ethernet port view

Parameters

group-address: Address of the multicast group the simulated host is to join.

source-address: Address of the multicast source the simulated host is to join. This parameter is valid only when IGMPv3 Snooping is enabled in a VLAN.

vlan-id: ID of the VLAN to which the port belongs, in the range of 1 to 4094.

Description

Use the **igmp host-join** command to configure the current port as a simulated multicast group member host.

Use the **undo igmp host-join** command to remove the current port as a simulated multicast group member host.

CAUTION:

- *Before configuring a simulated host, enable IGMP Snooping in VLAN view first.*
- *The current port must belong to the specified VLAN; otherwise this configuration does not take effect.*

Examples

Configure Ethernet 2/0/1 as a simulated host for multicast source 1.1.1.1 and multicast group 225.0.0.1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750]igmp-snooping enable
  Enable IGMP-Snooping ok.
[SW7750]vlan 1
[SW7750-vlan1]igmp-snooping enable
[SW7750-vlan1]igmp-snooping version 3
[SW7750-vlan1]quit
[SW7750] interface Ethernet 2/0/1
[SW7750-Ethernet 2/0/1] igmp host-join 225.0.0.1 source-ip 1.1.1.1 vlan 10
```

multicast-vlan enable

Syntax **multicast-vlan enable**

undo multicast-vlan enable

View VLAN view

Parameter None

Description Use the **multicast-vlan enable** command to configure the current VLAN as a multicast VLAN.

Use the **undo multicast-vlan enable** command to disable the current VLAN from being a multicast VLAN.

By default, the multicast VLAN feature is disabled.

CAUTION:

- *You can configure up to 5 multicast VLANs for the device.*
- *A multicast VLAN cannot be configured as a multicast sub-VLAN.*
- *A multicast sub-VLAN cannot be configured as a multicast VLAN.*
- *A multicast sub-VLAN cannot be configured as the sub-VLAN of other multicast VLANs.*
- *One multicast sub-VLAN is corresponding to only one multicast VLAN.*
- *If multicast routing is enabled on a VLAN interface, the corresponding VLAN cannot be configured as a multicast VLAN.*

Example # Configure VLAN 2 as a multicast VLAN.

```
<SW7750> system-view
Enter system view, return to user view with Ctrl+Z
[SW7750] igmp-snooping enable
[SW7750] vlan 2
[SW7750-vlan2] multicast-vlan enable
```

multicast-vlan subvlan

Syntax **multicast-vlan** *vlan-id* **subvlan** *vlan-list*

undo multicast-vlan *vlan-id* **subvlan** *vlan-list*

View System view

Parameter *vlan-id*: ID of the specified VLAN.

vlan-list: Multiple VLANs in the form of vlan-list = { *vlan-id* [to *vlan-id*] } & < 1-10 >. The *vlan-id* argument is the ID of the VLAN, in the range of 1 to 4,094.

&<1-10> means that you can provide the argument repeatedly for up to ten times.

Description Use the **multicast-vlan subvlan** command to configure one or multiple VLANs as the sub-VLAN(s) of the multicast VLAN.

Use the **undo multicast-vlan subvlan** command to cancel the sub-VLANs of the multicast VLAN.

By default, no sub-VLAN is configured for a multicast VLAN.

CAUTION:

- *A multicast VLAN cannot be configured as a multicast sub-VLAN.*
- *A multicast sub-VLAN cannot be configured as a multicast VLAN.*
- *A multicast sub-VLAN cannot be configured as the sub-VLAN of other multicast VLANs.*
- *One multicast sub-VLAN is corresponding to only one multicast VLAN.*
- *If multicast routing is enabled on a VLAN interface, the corresponding VLAN cannot be configured as a multicast VLAN.*

Example # Configure VLAN 2 to VLAN 5 as the sub-VLANs of the multicast VLAN 10.

```
<SW7750> system-view
Enter system view, return to user view with Ctrl+Z
[SW7750] igmp-snooping enable
[SW7750] vlan 10
[SW7750-vlan10] igmp-snooping enable
[SW7750-vlan10] multicast-vlan enable
[SW7750-vlan10] quit
[SW7750] multicast-vlan 10 subvlan 2 to 5
```

reset igmp-snooping statistics

Syntax **reset igmp-snooping statistics**

View User view

Parameter None

Description Use the **reset igmp-snooping statistics** command to clear IGMP Snooping statistics.

Related command: **igmp-snooping**.

Example # Clear IGMP Snooping statistics.

```
<SW7750> reset igmp-snooping statistics
```

38 Common IP Multicast Configuration Commands

display mpm forwarding-table

Syntax

display mpm forwarding-table [*group-address* | *source-address*]

View

Any view

Parameter

group-address: Multicast group address to specify a multicast group, in the range of 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 display the information about multicast forwarding tables containing port information.

Only the (S, G) entry is displayed when the group address or source address is specified. Otherwise, the command displays all the entries.

If you want to query the information about multicast forwarding tables without port information, you can use the **display multicast forwarding-table** command.

Example

Query the information about the multicast forwarding table containing port information.

```
<SW7750> display mpm forwarding-table
Multicast Forwarding Cache Table
Total 1 entry(entries)

00001. (120.0.0.2, 225.0.0.2)
 iif Vlan-interface1200
 1 oif(s):
  Vlan-interface32
   GigabitEthernet3/0/19
Total 1 entry(entries) Listed
```

Table 83 describes the fields in the displayed information above:

Table 83 Field descriptions of the **display mpm forwarding-table** command

Field	Description
Multicast Forwarding Cache Table	Multicast forwarding table
Total 1 entry(entries)	Total number of entries
00001	Serial number of an entry

Table 83 Field descriptions of the **display mpm forwarding-table** command

Field	Description
(120.0.0.2, 225.0.0.2)	(S, G), namely, (source address, group address)
iif Vlan-interface1200	The ingress VLAN of the multicast forwarding table is VLAN 1200.
1 oif(s):	There is one egress VLAN in the multicast forwarding table.
Vlan-interface32 GigabitEthernet3/0/19...	The outgoing interface is VLAN-interface 32, with the outgoing port of GigabitEthernet 3/0/19.
Total 1 entry(entries) Listed	One (S, G) entry is listed.

display mpm group

Syntax **display mpm group** [**vlan** *vlan-id* [*ip-address*]]

View Any view

Parameter **vlan** *vlan-id*: Displays the VLAN where the multicast group information lies. If this keyword is not specified, the command displays the multicast group information in all VLANs.

ip-address: IP address of the multicast group to be displayed.

Description Use the **display mpm group** command to display the information about the IP multicast groups and MAC multicast groups in the specified VLAN or all the VLANs on the switch.

The displayed information includes:

- VLAN identifier
- Router port
- Address of the IP multicast group
- Member ports in the IP multicast group
- MAC multicast group
- Address of the MAC multicast group
- Member ports in the MAC multicast group

CAUTION:

- *The fields of this command are similar to those of the* ***display igmp group*** *command, except that the information of the specific ports is added.*
- *The fields of this command are the same as those of the* ***display igmp-snooping group*** *command except that the displayed VLANs are of different attributes.*
- *The* ***display igmp-snooping group*** *command displays the information about ports joining in layer-2 multicast groups in IGMP-snooping-enabled VLANs,*

*while the **display mpm group** command displays the information about ports joining in layer-3 multicast groups in IGMP-enabled VLANs.*

Example # Display the information about multicast groups in VLAN 1200.

```
<SW7750> display mpm group vlan 1200
  Total 1 IP Group(s).
  Total 1 MAC Group(s).
  Vlan(id):1200
    Total 1 IP Group(s).
    Total 1 MAC Group(s).
    Static router port(s):
    Dynamic router port(s):
    IP group(s):the following ip group(s) match to one mac group.
        IP group address:225.0.0.1
        Host port(s):Ethernet2/0/1
    MAC group(s):
        MAC group address:0100-5e00-0001
        Host port(s):Ethernet2/0/1
```

Table 84 Field descriptions of the **display mpm group** command

Field	Description
Vlan(id):1200.	The information about the multicast groups in VLAN 1200 is displayed.
Static router port(s):	Static router ports
Dynamic router port(s):	Dynamic router ports
IP group(s):the following ip group(s) match to one mac group	IP multicast groups corresponding to the same MAC multicast group
IP group address:225.0.0.1	Address of the IP multicast group: 225.0.0.1
Host port(s): Ethernet2/0/1	Member ports of an IP multicast group: Ethernet 2/0/1
MAC group(s)	MAC multicast group(s)
MAC group address:0100-5e00-0001	MAC multicast group address: 0100-5e00-0001
Host port(s): Ethernet2/0/1	Member ports of a MAC multicast group: Ethernet 2/0/1

display multicast forwarding-table

Syntax **display multicast forwarding-table** [*group-address* [**mask** { *group-mask* | *mask-length* }] | *source-address* [**mask** { *group-mask* | *mask-length* }] | **incoming-interface** { *interface-type interface-number*] **register** }]*

View Any view

Parameter *group-address*: Address of the specified multicast group, in the range of 224.0.0.0 to 239.255.255.255.

source-address: Unicast IP address of the multicast source.

incoming-interface: Incoming interface of the specified multicast forwarding entry.

register: Registration VLAN interface of the PIM-SM protocol.

Description Use the **display multicast forwarding-table** command to display the information about MAC forwarding tables.

Related command: **display multicast routing-table**.

Example # Display the information about MAC forwarding tables.

```
<SW7750> display multicast forwarding-table
Multicast Forwarding Cache Table
Total 1 entry: 0 entry created by IP, 1 entry created by protocol

00001. (10.0.0.4, 225.1.1.1), iif Vlan-interface2, 0 oifs,
     Protocol Create
     Matched 122 pkts(183000 bytes), Wrong If 0 pkts
     Forwarded 122 pkts(183000 bytes)

Total 1 entry Listed
```

Table 85 describes the displayed information above.

Table 85 Field descriptions of the **display multicast forwarding-table** command

Field	Description
Multicast Forwarding Cache Table	Multicast forwarding table
Total 1 entries	Total number of entries
00001	Serial number of an entry
(10.0.0.4, 225.1.1.1)	(s,g)
iif Vlan-interface2, 0 oifs	The incoming interface of the multicast forwarding table is Vlan-interface 2, and the multicast forwarding table does not have an outgoing interface.
Matched 122 pkts(183000 bytes), Wrong If 0 pkts	122 packets which are 183,000 bytes in all match the (s, g) entry, and 0 wrong packets match with the (s, g) entry.
Forwarded 122 pkts(183000 bytes)	122 packets which are 183,000 bytes in all are forwarded.

display multicast routing-table

Syntax **display multicast routing-table** [*group-address* [**mask** { *mask* | *mask-length* }] | *source-address* [**mask** { *mask* | *mask-length* }] | **incoming-interface** { *interface-type interface-number* | **register** }]*

View Any view

Parameter *group-address*: Multicast group address to specify a multicast group and display the routing table information corresponding to this group, in the range of 224.0.0.0 to 239.255.255.255.

source-address: Unicast IP address of the multicast source.

incoming-interface: Specifies the incoming interface of the multicast routing entry.

register: Registration interface of PIM-SM.

Description Use the **display multicast routing**-**table** command to display the information about the IP multicast routing table.

This command is used to display the information about the multicast routing table, while the **display multicast forwarding**-**table** command is used to display the information about the multicast forwarding table.

Example # View the information in the multicast routing table.

```
<SW7750> 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:
    1 oifs
      Vlan-interface2(2.2.2.4)

(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 following table describes the fields in the displayed information.

Table 86 Field descriptions of the **display multicast routing-table** command

Field	Description
Multicast Routing Table	Multicast routing table
Total 3 entries	There are 3 entries in all in the multicast routing table.
(4.4.4.4, 224.2.149.17)	(S, G) of the multicast routing table
Uptime: 00:15:16, Timeout in 272 sec Upstream interface: Vlan-interface1(4.4.4.6) Downstream interface list: 1 oifs Vlan-interface2(2.2.2.4)	The entry is up for 15 minutes and 16 seconds, and it times out in 272 seconds. The IP address of the upstream interface is 4.4.4.6. Downstream interface list: The IP address of the downstream interface is 2.2.2.4.
Matched 3 entries	Three entries match the configuration.

display multicast-source-deny

Syntax

display multicast-source-deny [**interface** *interface-type* [*interface-number*]]

View

Any view

Parameter

interface-type: Port type.

interface-number: Port number.

Description

Use the **display multicast-source-deny** command to display the configuration information about the multicast source port check.

When you use this command to display the information,

- If you specify neither the port type nor the port number, the multicast source port check information about all the ports on the switch is displayed.
- If you specify the port type only, the multicast source port check information about all ports of this type is displayed.
- If you specify both the port type and the port number, the multicast source port check information about the specified port is displayed.

Example

# Display the multicast source port suppression state of Ethernet 2/0/1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] display multicast-source-deny Ethernet 2/0/1
```

# Display the multicast source port suppression state of all the 100M Ethernet ports.

```
[SW7750] display multicast-source-deny interface Ethernet
```

multicast route-limit

Syntax

multicast route-limit *limit*

undo multicast route-limit

View

System view

Parameter

limit: Limit on the capacity of the multicast routing table, in the range of 0 to 1,024.

Description

Use the **multicast route-limit** command to limit the capacity of the multicast routing table. The router will drop the protocols and packets of the new (S, G).

Use the **undo multicast route-limit** command to restore the default limit on the capacity of the multicast routing table.

The limit on the capacity of the multicast routing table is 1024 by default.

If the number of existing routing entries exceeds the value to be configured when you configure this command, the existing entries in the routing table will not be removed. Instead, the system will prompt that the number of existing routing entries is more than the limit to be configured.

If you execute this command again, the new configuration will overlap the former configuration.

Example # Set the limit on the capacity of the multicast routing table to 100.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] multicast route-limit 100
```

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 the IP multicast routing feature.

Use the **undo multicast routing-enable** command to disable the IP multicast routing feature.

The IP multicast routing feature is disabled by default.

Example # Enable the IP multicast routing feature.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] multicast routing-enable
```

multicast static-router-port

Syntax **multicast static-router-port** *interface-type interface-number*

undo multicast static-router-port *interface-type interface-number*

View VLAN view

Parameter *interface-type*: Port type.

interface-number: Port number.

Description Use the **multicast static-router-port** command to specify the Ethernet port as the static router port of the current VLAN.

Use the **undo multicast static-router-port** command to disable the static router port configuration.

By default, no static router port is configured for the VLAN.

CAUTION:

- *Up to 256 static router ports can be configured in a system.*
- *Reflection ports cannot be configured as static router ports.*
- *A port in a multicast sub-VLAN cannot be configured as a static router port.*

Example # Configure Ethernet 2/0/1 in VLAN 2 as a static router port.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] vlan 2
[SW7750-vlan2] multicast static-router-port Ethernet 2/0/1
```

multicast static-router-port vlan

Syntax **multicast static-router-port vlan** *vlan-id*

undo multicast static-router-port vlan *vlan-id*

View Ethernet port view

Parameter *vlan-id*: ID of the specified VLAN, in the range of 1 to 4,094.

Description Use the **multicast static-router-port vlan** command to specify the current port in the VLAN as a static router port.

Use the **undo multicast static-router-port vlan** command to disable the static router port configuration.

By default, an Ethernet port is not specified as a static router port.

CAUTION:

- *Up to 256 static router ports can be configured in a system.*
- *Reflection ports cannot be configured as static router ports.*
- *A port in a multicast sub-VLAN cannot be configured as a static router port.*

Example # Configure Ethernet 2/0/1 in VLAN 2 as a static router port.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
```

```
[SW7750] interface Ethernet 2/0/1
[SW7750-Ethernet2/0/1] multicast static-router-port vlan 2
```

multicast wrongif-holdtime

Syntax

multicast wrongif-holdtime *seconds*

undo multicast wrongif-holdtime

View

System view

Parameter

seconds: Holdtime to prevent wrongif packets from being reported to the CPU, in the range of 0 to 300 seconds. During the configuration, if the *seconds* argument is less than 15, the system sets the holdtime to 15; if the *seconds* argument is more than 15, the system sets the holdtime to the multiples of 15 according to the user-defined range. For example, if you set the *seconds* argument to 14, the system sets the holdtime to 15; if you set the *seconds* argument to 16, the system sets the holdtime to 30; if you set the *seconds* argument to 31, the system sets the holdtime to 45, and so on.

Description

Use the **multicast wrongif-holdtime** command to set the holdtime to prevent wrongif packets from being reported to the CPU.

Use the **undo multicast wrongif-holdtime** command to restore the default holdtime.

By default, the holdtime to prevent wrongif packets from being reported to the CPU is 15 seconds.

When the switch receives a multicast packet, the switch will search the multicast forwarding entry according to the source address and destination address of the packet. If the matching forwarding entry is found and the packet is received on the right ingress of the forwarding entry, the packet will be forwarded according to the forwarding entry. If the packet is not received on the right ingress of the forwarding entry, the packet is regarded as a wrongif packet. The wrongif packet will be reported to the CPU.

In some network, many wrongif packets will be reported to the CPU of the switch, thus aggravating the workload of the switch. In this case, you can configure the holdtime of wrongif packets, so that the wrongif packets will be dropped instead of being forwarded to the CPU of the switch, and the CPU will be prevented from being stricken by too many packets.

In the configured holdtime, wrongif packets are not reported to the CPU, so that the CPU can be prevented from being stricken by too many multicast packets.

Example

Set the holdtime of wrongif packets to 60 seconds.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] multicast wrongif-holdtime 60
```

multicast-source-deny enable interface

Syntax **multicast-source-deny enable** [**interface** *interface-list*]

undo multicast-source-deny enable [**interface** *interface-list*]

View System view

Parameter *interface-list*: Specifies Ethernet port list, expressed in the form of *interface-list* = { { *interface-type interface-num* | *interface-name* } [**to** { *interface-type interface-num* | *interface-name* }] }&<1-10>. The *interface-number* argument refers to one single Ethernet port, expressed in the form of *interface-number* = { *interface-type interface-number* | *interface-name* }, where the *interface-type* argument refers to the port type, the *interface-number* argument refers to the port number, and the *interface-name* argument refers to the port name. For meanings and value ranges of *interface-type*, *interface-number* and *interface-name*, refer to "interface" on page 205.

Description Use the **multicast-source-deny enable** command to enable the multicast source port suppression feature.

Use the **undo multicast-source-deny enable** command to restore the default setting.

By default, the multicast source port suppression feature is disabled on all the ports.

The multicast source port suppression feature can filter multicast packets on the unauthorized multicast source port in order to avoid the case that the user connected to the port sets the multicast server privately.

In the system view, if the *interface-list* argument is not specified, the multicast source port suppression feature is enabled globally, that is, the feature is enabled on all the ports of the switch; if the *interface-list* argument is specified, the multicast source port suppression feature is enabled on the specified ports. In Ethernet port view, the *interface-list* argument cannot be specified in the command and you can use the command to enable the multicast source port suppression feature on the current port only.

⚠ ***CAUTION:*** *The multicast source port suppression feature is not supported on the following I/O Modules: 3C16860, 3C16861, LS81FS24A, 3C16859, and 3C16858.*

Example # Enable the multicast source port suppression feature on Ethernet 2/0/1 and Ethernet 2/0/2.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] multicast-source-deny enable interface Ethernet 2/0/1 to Ethernet 2/0/2
```

multicast-source-deny enable

Syntax

multicast-source-deny enable

undo multicast-source-deny enable

View

Ethernet port view

Parameter

None

Description

Use the **multicast-source-deny enable** command to enable multicast source port suppression.

Use the **undo multicast-source-deny enable** command to restore multicast source port suppression to the default settings.

By default, the multicast source port suppression feature is disabled on a port.

The multicast source port suppression feature can filter multicast packets on the unauthorized multicast source port in order to avoid the case that the user connected to the port sets the multicast server privately.

⚠ ***CAUTION:*** *The multicast source port suppression feature is not supported on the following I/O Modules: 3C16860, 3C16861, LS81FS24A, 3C16859, and 3C16858.*

Example

Enable the multicast source port suppression feature on Ethernet 2/0/1.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet 2/0/1
[SW7750-Ethernet2/0/1] multicast-source-deny enable
```

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** *interface-type interface-number* } * }

View

User view

Parameter

statistics: Clears the statistics information about MFC forwarding entries if this keyword is specified. Otherwise, MFC forwarding entries will be cleared.

all: Refers to all MFC forwarding entries.

group-address: Specifies the group address.

group-mask: Specifies the mask of the group address.

group-mask-length: Specifies the mask length of the group address.

source-address: Specifies the source address.

source-mask: Specifies the mask of the source address.

source-mask-length: Specifies the mask length of the source address.

incoming-**interface**: Specifies the incoming interface of the forwarding entry.

interface-type interface-number: VLAN interface type and VLAN interface number.

Description Use the **reset multicast forwarding**-**table** command to clear MFC forwarding entries or the statistics information about MFC forwarding entries.

The order of the *group-address* argument and the *source-address* argument can be turned over. However, you must input valid group addresses and source addresses. Otherwise, the system prompts error.

Related command: **reset pim routing-table**, **reset multicast routing-table**, and **reset multicast forwarding-table**.

Example # Clear the forwarding entries whose group address is 225.5.4.3 in the MFC forwarding table.

```
<SW7750> reset multicast forwarding-table 225.5.4.3
```

# Clear the statistics information about the forwarding entries whose group address is 225.5.4.3 in the MFC forwarding table.

```
<SW7750> 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** *interface-type interface-num*ber } * }

View User view

Parameter **all**: All routing entries in the multicast core routing table.

group-address: Specifies the group address.

group-mask: Specifies the mask of the group address.

group-mask-length: Specifies the mask length of the group address.

source-address: Specifies the source address.

source-mask: Specifies the mask of the source address.

source-mask-length: Specifies the mask length of the source address.

incoming-interface: Specifies the incoming interface of the routing entry.

interface-type interface-number: VLAN interface type and VLAN interface number.

Description

Use the **reset multicast routing-table** command to clear the routing entries in the multicast core routing table and remove the corresponding forwarding entries in the MFC forwarding table.

The order of the *group-address* argument and the *source-address* argument can be turned over. However, you must input valid group addresses and source addresses. Otherwise, the system prompts error.

Related command:

reset pim routing-table, **reset multicast forwarding-table** and **display multicast forwarding-table**.

Example

Clear the routing entries whose group address is 225.5.4.3 from the multicast core routing table.

```
<SW7750> reset multicast routing-table 225.5.4.3
```

39 Static Multicast MAC Address Table Configuration Commands

display mac-address multicast

Syntax

display mac-address multicast [**count**]

View

Any view

Parameter

count: Number of MAC entries.

Description

Use the **display mac-address multicast static** command to display the multicast MAC address entry/entries configured on the switch.

Executing this command with the **count** keyword will display the information about the number of multicast MAC address entries configured on the switch.

Example

Display all the multicast MAC address entries manually added in VLAN 1.

```
<SW7750> display mac-address multicast count
1 mac address(es) found
```

mac-address multicast interface

Syntax

mac-address multicast *mac-address* **interface** *interface-list* **vlan** *vlan-id*

undo mac-address multicast [*mac-address* [**interface** *interface-list*] **vlan** *vlan-id*]

View

System view

Parameter

mac-address: Multicast MAC address.

vlan-id: VLAN ID.

interface-list: Forwarding port list, in the format of { { *interface-type interface-num* } [**to** { *interface-type interface-num* }] }&<1-10>. Where, *interface-type* is a port type, *interface-number* is a port number (refer to **interface** on page 205), **to** is used to specify a port range, and &<1-10> represents you can totally specify up to 10 ports and port ranges.

Description

Use the **mac-address multicast** command to manually add a multicast MAC address entry.

Use the **undo mac-address multicast** command to remove a multicast MAC address entry.

Each multicast MAC address entry contains: multicast address, forward port, VLAN ID, and so on.

Related command: **display mac-address multicast**.

Example # Add a multicast MAC address entry, with the multicast address being 0100-5e0a-0805, the forwarding port being Ethernet 2/0/1, and the native VLAN being VLAN 1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] mac-address multicast 0100-5e0a-0805 interface Ethernet 2/0/1 vlan 1
```

40 IGMP CONFIGURATION COMMANDS

When running IP multicast protocols, Ethernet switches also provide the functions of switches. We use routers in this manual to stand for not only the common routers but also the layer 3 Ethernet switches running IP multicast protocols.

display igmp group

Syntax **display igmp group** [*group-address* | **interface** *interface-type interface-number*]

View Any view

Parameter *group-address*: Address of the multicast group.

interface-type interface-number: VLAN interface type and VLAN interface number of the router which are used to specify a VLAN interface. .

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 displayed information contains the multicast groups which are joined by the downstream hosts through IGMP or through command line.

Related command: **igmp host-join**.

Example # View the member information of multicast group in the system.

```
<SW7750> 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 87 Output description of the display igmp group command

Field	Description
Group address	Multicast group address
Last Reporter	The last host reporting to join in the multicast group
Uptime	Time passed since multicast group is discovered (hh: mm: ss).

Table 87 Output description of the display igmp group command

Field	Description
Expires	Specifies when the member will be removed from the multicast group (hh: mm: ss).

display igmp interface

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

View Any view

Parameter *interface-type interface-number*: VLAN interface type and VLAN interface number of the router which are used to specify a VLAN interface. If this argument is not specified, the information about all the VLAN interfaces where IGMP is running is displayed.

Description Use the **display igmp interface** command to view the IGMP configuration and running information on a VLAN interface.

Example # View the IGMP configuration and running information of all VLAN interfaces.

```
<SW7750> 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 256
  No IGMP group reported
```

Table 88 Field descriptions of the **display igmp interface** command

Field	Description
IGMP version	IGMP version
query interval	Interval of general query
querier timeout	Timeout time of the querier
max query response time	Maximum time of response to query
robust count	IGMP robust count, that is, the times of sending IGMP group-specific query packets before the IGMP querier receives the IGMP leave packet from the host
startup query interval	The startup interval of IGMP to send query packets
last member query interval	The interval of sending IGMP group-specific query packets when the IGMP querier receives the IGMP leave packets from the host
query timeout	Query timeout in IGMP version 1

Table 88 Field descriptions of the **display igmp interface** command

Field	Description
Policy to accept IGMP reports	The filtering policy of the IGMP multicast group to control the access to IP multicast groups
Querier for IGMP	IGMP querier
IGMP group limit	Limit on the number of IGMP groups added to the VLAN interface. The router does not process new IGMP packets when the number of IGMP packet exceeds the limit

igmp enable

Syntax **igmp enable**

undo igmp enable

View VLAN interface view

Parameter None

Description Use **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 a VLAN interface. .

These commands do not take effect until the multicast routing feature is enabled. After this configuration, start to configure other IGMP features.

Related command: **multicast routing-enable**.

Example # Enable IGMP on Vlan-interface 10.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 10
[SW7750-Vlan-interface10] igmp enable
```

igmp group-limit

Syntax **igmp group-limit** *limit*

undo igmp group-limit

View VLAN interface view

Parameter *limit*: Quantity of multicast groups, in the range of 0 to 256.

Description Use the **igmp group-limit** command to limit the number of multicast groups on an interface. The router does not process new packets when number of IGMP groups exceeds the limit.

Use the **undo igmp group-limit** command to restore the default setting.

By default, 256 IGMP groups are added to a VLAN interface.

The new configuration overwrites the old one if you run the command for a second time.

CAUTION:

- *New groups cannot be added when the number of IGMP multicast groups has exceeded the configured limit.*
- *If the number of existing multicast groups on the interface is more than the configured limit, the system will remove some old groups automatically to satisfy the configured limit.*

Example # Limit the maximum number of IGMP groups on Vlan-interface10 to 100.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 10
[SW7750-Vlan-interface10] igmp group-limit 100
```

igmp group-policy

Syntax **igmp group-policy** *acl-number* [**1** | **2** | **port** *interface-list*]

undo igmp group-policy [**port** *interface-list*]

View VLAN interface view

Parameter *acl-number*: Number of the basic IP access control list number, defining a multicast group range. The value ranges from 2000 to 2999.

1: IGMP version 1.

2: IGMP version 2. If IGMP version is not specified, version 2 will be used by default.

port: Limits the IGMP packets passing the port and matching with the ACL rules.

interface-list: Forwarding port list in the form of *interface-list* = { *interface-type interface-number* [**to** { *interface-type interface-number* }] }&<1-10>. The *interface-type* argument refers to the port type, and the *interface-number* argument refers to the port number. For the meanings and ranges of the two arguments, refer to “interface” on page 205.

Description Use the **igmp group-policy** command to set the filter of multicast groups on the VLAN interface to control the access to IP multicast groups.

Use **undo igmp group-policy** command to remove the filter configured.

By default, no filter is configured, that is, a host can join any multicast group.

If you do not want the hosts on the network that the VLAN interface is on to join some multicast groups and receive packets from the multicast groups to use this command to limit the range of the multicast groups serviced by the VLAN interface.

Related command: **igmp host-join**.

CAUTION: Ethernet ports must belong to the igmp-group-policy-enabled VLAN interfaces only.

Example # Configure the access-list 2000.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] acl number 2000
[SW7750-acl-basic-2000] rule permit source 225.0.0.0 0.255.255.255
[SW7750-acl-basic-2000] quit
```

# Configure that only the hosts matching ACL 2000 rules on VLAN-interface10 can be added to the multicast group whose IGMP version is specified to 2.

```
[SW7750-vlan-interface10] igmp group-policy 2000 2
```

igmp group-policy vlan

Syntax **igmp group-policy** *acl-number* **vlan** *vlan-id*

undo igmp group-policy vlan *vlan-id*

View Port view

Parameter *acl-number*: Number of the basic IP access control list number, defining a multicast group range. The value ranges from 2000 to 2999.

vlan-id: Specifies the ID for the VLAN to which the port belongs.

Description Use the **igmp group-policy vlan** command to set the filter of multicast groups on a port to control the access to the IP multicast groups.

Use the **undo igmp group-policy vlan** command to remove the configured filter.

By default, no filter is configured, that is, a host can join any multicast group.

This command has the same function with the **igmp group-policy** command. Note that the configured port must belong to the specified VLAN, and the IGMP protocol must be enabled on this port; otherwise, the configuration does not function.

Related command: **igmp group-policy**, **igmp host-join vlan**, and **igmp host-join port**.

Example # Configure that only the hosts matching ACL 2000 rules on Ethernet 2/0/1 in VLAN-interface 10 can be added to the multicast group.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 10
[SW7750-Vlan-interface10] igmp enable
[SW7750-Vlan-interface10] quit
[SW7750] interface Ethernet 2/0/1
[SW7750-Ethernet2/0/1] port access vlan 10
[SW7750-Ethernet2/0/1] igmp group-policy 2000 vlan 10
```

igmp host-join port

Syntax **igmp host-join** *group-address* **port** *interface-list*

undo igmp host-join *group-address* **port** *interface-list*

View VLAN interface view

Parameter *group-address*: Multicast address of the multicast group that an interface will join.

port: Specifies the port in the VLAN interface.

interface-list: Forwarding port list in the form of *interface-list* = { *interface-type interface-number* [**to** { *interface-type interface-number* }] }&<1-10>. The *interface-type* argument refers to the port type, and the *interface-number* argument refers to the port number. For the meanings and ranges of the two arguments, refer to "interface" on page 205.

Description Use the **igmp host-join port** command to configure simulated joining in VLAN interface view.

Use **undo igmp host-join port** command to restore the default.

By default, VLAN interfaces of a switch do not belong to any multicast group.

Related command: **igmp group-policy**.

Example # Add port Ethernet 2/0/1 in VLAN 10 to the multicast group 225.0.0.1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 10
[SW7750-Vlan-interface10] igmp host-join 225.0.0.1 port Ethernet 2/0
/1
```

igmp host-join vlan

Syntax **igmp host-join** *group-address* **vlan** *vlan-id*

undo igmp host-join *group-address* **vlan** *vlan-id*

View Port view

Parameter *group-address*: Multicast address of the multicast group that an interface will join.

vlan-id: Specifies the ID for the VLAN to which the port belongs.

Description Use the **igmp host-join vlan** command to configure simulated joining in port view.

Use the **undo igmp host-join vlan** command to restore the default.

By default, an Ethernet port does not join any multicast group.

Related command: **igmp group-policy**.

Example # Add Ethernet 2/0/1 in VLAN 10 to the multicast group at 225.0.0.1.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 10
[SW7750-Vlan-interface10] igmp enable
[SW7750-Vlan-interface10] quit
[SW7750] interface Ethernet 2/0/1
[SW7750-Ethernet2/0/1] port access vlan 10
[SW7750-Ethernet2/0/1] igmp host-join 225.0.0.1 vlan 10
```

igmp lastmember-queryinterval

Syntax **igmp lastmember-queryinterval** *seconds*

undo igmp lastmember-queryinterval

View VLAN interface view

Parameter *seconds*: Interval for the IGMP querier to send IGMP group-specific query packets when it receives IGMP leave packets from the host. It is in the range of 1 second to 5 seconds.

Description Use the **igmp lastmember-queryinterval** command to set the Interval for the IGMP querier to send IGMP group-specific query packets when it receives IGMP leave packets from the host.

Use the **undo igmp lastmember-queryinterval** command to restore the default value.

The interval for the IGMP querier to send IGMP group-specific query packets is one second by default.

In the shared network, that is, a same network segment including multiple hosts and multicast routers, the query router (also known as querier) is responsible for maintaining the IGMP group membership on the interface. When the IGMP v2 host leaves a group, it sends an IGMP Leave message.

When receiving the IGMP Leave message, the IGMP querier must send the IGMP group-specific query messages for specified times (by the *robust-value* argument in the **igmp robust-count** command, with default value as 2) in a specified time interval (by the *seconds* argument in the **igmp lastmember-queryinterval** command, with default value as 1 second). If other hosts which are interested in the specified group receive the IGMP query message from the IGMP query router, they will send back the IGMP Membership Report message within the specified maximum response time interval. If it receives the IGMP Membership Report message within the defined period (equal to *robust-value* × *seconds*), the IGMP query router continue to maintain the membership of this group. When receiving no IGMP Membership Report message from any hosts within the defined period, the IGMP query router considers it as timeout and stops membership maintenance for the group.

This command is only available on the IGMP query router running IGMP v2. For the host running IGMP v1, this command cannot take effect because the host does not send the IGMP Leave message when it leaves a group.

Related command: **igmp robust-count** and **display igmp interface**.

Example # Set the query interval at the Vlan-interface10 as 3 seconds.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 10
```

[SW7750-Vlan-interface10] igmp lastmember-queryinterval 3

igmp max-response-time

Syntax **igmp max-response-time** *seconds*

undo igmp max-response-time

View VLAN 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 is 10 seconds by default.

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 packets to 8 seconds.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 10
[SW7750-Vlan-interface10] igmp max-response-time 8
```

igmp proxy

Syntax **igmp proxy Vlan-interface** *interface-number*

undo igmp proxy

View Interface view

Parameter *interface-number*: Proxy interface number.

Description Use the **igmp proxy** command to specify an interface of the Layer 3 endpoint switch as the IGMP proxy interface of another interface.

Use the **undo igmp proxy** command to disable this configuration.

The IGMP proxy feature is disabled by default.

You must enable the PIM protocol on the interface first before enabling the **igmp proxy** command on the interface. Only one IGMP proxy interface can be configured for an interface.

One interface cannot serve as the IGMP proxy interface of two or more interfaces.

If the IGMP proxy feature is configured on the same interface for multiple times, the latest configuration takes effect.

Related command: **pim neighbor-policy**.

CAUTION:

- *Both multicast routing and IGMP must be enabled on a proxy interface.*
- *Before configuring the **igmp proxy** command on an interface, make sure that PIM DM is enabled on this interface. Otherwise, the IGMP proxy feature does not take effect.*

- *Only one IGMP proxy interface can be configured for an interface.*

Example # Configure VLAN-interface 2 as the IGMP proxy interface of VLAN-interface 1 on the Layer 3 switch.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] multicast routing-enable
[SW7750] interface vlan-interface 1
[SW7750-Vlan-interface1] igmp enable
[SW7750- Vlan-interface1] igmp proxy vlan-interface 2
```

igmp report-aggregation

Syntax **igmp report-aggregation**

View System view

Parameter None

Description Use the **igmp report-aggregation** command to enable suppression on Layer 3 multicast IGMP report packets. On an IP-multicast-routing-enabled switch, the VLAN interface receives only the first IGMP report packet from a multicast group in a query interval.

Use the **undo igmp-snooping report-aggregation** command to disable suppression on Layer 3 multicast IGMP report packets.

By default, suppression on IGMP report packets is disabled.

- *You must enable IP multicast routing globally before configuring suppression on IGMP report packets.*
- *If IP multicast routing is disabled globally, suppression on IGMP report packets is disabled simultaneously.*

Example # Enable suppression on Layer 3 multicast IGMP report packets on the switch.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] multicast routing-enable
[SW7750] igmp report-aggregation
```

igmp robust-count

Syntax **igmp robust-count** *robust-value*

undo igmp robust-count

View VLAN interface view

Parameter *robust-value*: IGMP robust value, number of sending the IGMP group-specific query packets after the IGMP querier receives the IGMP Leave packet from the host. It is in the range of 2 times to 5 times.

Description Use the **igmp robust-count** command to set the number of sending the IGMP group query message after the IGMP query router receives the IGMP Leave message from the host.

Use the **undo igmp robust-count** command to restore the default value.

By default, an IGMP querier sends IGMP group-specific query packets twice.

In the shared network, that is, a same network segment including multiple hosts and multicast routers, the query router is responsible for maintaining the IGMP group membership on the interface. When the IGMP v2 host leaves a group, it sends an IGMP Leave message. When receiving the IGMP Leave message, IGMP query router must send the IGMP group-specific query message for specified times (by the *robust-value* parameter in the **igmp robust-count** command, with default value as 2) in a specified time interval (by the *seconds* parameter in the **igmp lastmember-queryinterval** command, with default value as 1 second). If other hosts which are interested in the specific group receive the IGMP group-specific query packets from the IGMP query router, they will send back the IGMP Membership Report packets within the specified maximum response time interval. If it receives the IGMP Membership Report packets within the defined period (equal to *robust-value* × *seconds*), the IGMP query router continue to maintain the membership of this group. When receiving no IGMP Membership Report packet from any hosts within the defined period, the IGMP query router considers it as timeout and stops membership maintenance for the group.

This command is only available on the IGMP query router running IGMP v2. For the host running IGMP v1, this command cannot take effect because the host does not send IGMP Leave packets when it leaves a group.

Related command: **igmp lastmember-queryinterval** and **display igmp interface**.

Example # Set the robust value of the Vlan-interface 10 to 3.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 10
[SW7750-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 VLAN interface view

Parameter *seconds*: Presence time of the IGMP querier, in the range of 1 to 131,070 in seconds.

Description Use the **igmp timer other-querier-present** command to configure the presence time of the IGMP querier.

Use the **undo igmp timer other-querier-present** command to restore the default value.

By default, the presence time of the IGMP querier is twice the value of IGMP query message interval, that is, 120 seconds.

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 querier to be invalid and the router itself becomes a querier.

In IGMP version 1, the selection of a querier is determined by the multicast routing protocol. In IGMP version 2, the router with the lowest IP address on the shared network segment acts as the querier.

Related command: **igmp timer query**, and **display igmp interface**.

Example # Set the querier to expire after 300 seconds.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 10
[SW7750-Vlan-interface10] igmp timer other-querier-present 300
```

igmp timer query

Syntax **igmp timer query** *seconds*

undo igmp timer query

View VLAN interface view

Parameter *seconds*: Interval at which a router transmits IGMP query messages, in the range of 1 to 65,535 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.

By default, a router interface transmits IGMP query messages at the interval of 60 seconds.

A multicast router periodically sends out IGMP query messages to attached segments to find hosts that belong to different multicast groups. 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.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 2
[SW7750-Vlan-interface2] igmp timer query 150
```

igmp version

Syntax **igmp version** { **1** | **2** }

undo igmp version

View VLAN interface view

Parameter **1**: IGMP Version 1.

2: 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 default IGMP version is IGMP version 2.

All routers on a subnet must support the same version of IGMP. After detecting the presence of IGMP Version 1 system, a router cannot automatically switch to Version 1.

Example # Run IGMP Version 1 on VLAN-interface10.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 10
[SW7750-Vlan-interface10] igmp version 1
```

reset igmp group

Syntax **reset igmp group** { **all** | **interface** *interface-type interface-number* { **all** | *group-address* [*group-mask*] } }

View User view

Parameter

all: All IGMP groups.

interface-type interface-number: VLAN interface type and VLAN interface number.

group-address: IGMP group address.

group-mask: Mask of IGMP group address.

Description

Use the **reset igmp group** command to delete an existing IGMP group from the VLAN interface. The deleted group can be added to the VLAN interface again.

Example

# Delete all IGMP groups on all the VLAN interfaces.

```
<SW7750> reset igmp group all
```

# Delete all IGMP groups on Vlan-interface10.

```
<SW7750> reset igmp group interface Vlan-interface10 all
```

# Delete the group 225.0.0.1 from Vlan-interface10.

```
<SW7750> 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 Vlan-interface10.

```
<SW7750> reset igmp group interface Vlan-interface10 225.1.1.0 255.2
55.255.0
```

41 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 2,000 to 2,999.

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 malicious BSR proofing 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**, **rule (Basic ACL)**, **rule (Advanced ACL)**, **rule (Layer 2 ACL)**, and **rule (user-defined ACL)**.

Example # Configure BSR filtering policy on routers, only 101.1.1.1/32 can be BSR.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] multicast routing-enable
[SW7750] pim
[SW7750-pim] bsr-policy 2000
[SW7750-pim] quit
[SW7750] acl number 2000
[SW7750-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*: Specifies the VLAN interface. The candidate BSR is configured on the VLAN interface. PIM-SM must be enabled on the VLAN 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 switch as a BSR with priority 2 (and the C-BSR address is designated as the IP address of VLAN-interface10).

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
```

```
[SW7750] multicast routing-enable
[SW7750] pim
[SW7750-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*: Specifies the VLAN 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. The greatest value corresponds to the lowest priority level

all: Remove 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, and the value of RP priority is 0.

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 the BSR that the switch itself is the C-RP in the PIM. 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.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] multicast routing-enable
[SW7750] acl number 2000
[SW7750-acl-basic-2000] rule permit source 225.0.0.0 0.255.255.255
[SW7750] pim
[SW7750-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, 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 unicast 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**, **rule (Basic ACL)**, **rule (Advanced ACL)**, **rule (Layer 2 ACL)**, and **rule (user-defined ACL)**.

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.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] multicast routing-enable
[SW7750] pim
[SW7750-pim] crp-policy 3000
[SW7750-pim] quit
[SW7750] acl number 3000
[SW7750-acl-adv-3000] rule 0 permit source 1.1.1.1 0 destination 225.1.0.0 0.0.255.255
```

display pim bsr-info

Syntax **display pim bsr-info**

View Any view

Parameter None

Description Use the **display pim bsr-info** command to view the BSR information.

Related command: **c-bsr**, and **c-rp**.

Example # Display the BSR information.

```
<SW7750> display pim bsr-info
  Current BSR Address: 20.20.20.30
             Priority: 0
          Mask Length: 30
              Expires: 00:01:55
  Local host is BSR
```

Table 89 Field descriptions of the **display pim bsr-info** command

Field	Description
BSR	Bootstrap router
Priority	Priority of BSR
Mask Length: 30	Length of mask
Expires: 00:01:55	Value of the timer

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 VLAN interface.

Description Use the **display pim interface** command to view the PIM configuration information of the interface.

If neither the VLAN interface type nor the VLAN interface number is specified, the PIM configuration information of all VLAN interfaces is displayed; if both the VLAN interface type and the VLAN interface number are specified, the PIM configuration information about the specified VLAN interface is displayed.

Example # Display the PIM configuration information about the VLAN interface.

```
<SW7750> display pim interface
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 limit is 128
  PIM neighbor policy is none
  Total 1 PIM neighbor on interface
  PIM DR(designated router) is 10.10.1.20
```

Table 90 Field descriptions of the **display pim interface** command

Field	Description
PIM version	Version of PIM
PIM mode	PIM mode enabled on the VLAN interface (DM or SM)
PIM query interval	Hello packet interval
PIM neighbor limit	Limit of the PIM neighbors on the VLAN 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-type interface-number*: Interface type and interface number, used to specify the VLAN interface.

Description Use the **display pim neighbor** command to view the PIM neighbor information discovered by the VLAN interface of the switch. If the VLAN interface parameter is specified, only the PIM neighbor information about the specified VLAN interface is displayed.

Example # Display the PIM neighbor information discovered by the VLAN interface of the neighbor.

```
<SW7750> display pim neighbor
Neighbor’s Address      Interface Name       Uptime    Expires
8.8.8.6               VLAN-interface10     01:29:18  00:01:34
```

Table 91 Field descriptions of the **display pim neighbor** command

Field	Description
Neighbor’s Address	Neighbor address
Interface name	VLAN 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-type interface-number* | **null** } | { **dense-mode** | **sparse-mode** }] *

View Any view

Parameter

****rp**: (*, *, RP) route entry.

***g**: (*, G) route entry.

group-address: Address of the multicast group.

source-address: IP address of the multicast source.

incoming-interface *interface-type interface-number*: View the route entry whose incoming VLAN interface is the specified VLAN interface.

null: Specifies the VLAN 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 information about the PIM multicast routing table.

The displayed information about the PIM multicast routing table includes the SPT information and RPF information.

Example

Display the information about the PIM multicast routing table.

```
<SW7750> 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 92 Field descriptions of the **display routing-table** command

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*: Specifies the 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 the multicast group.

In addition, this command can also display the BSR and static RP information.

Example # View the RP information of the multicast group

```
<SW7750> display pim rp-info
PIM-SM RP-SET information:
    BSR is: 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
```

Table 93 Field descriptions of the **display pim rp-info** command

Field	Description
PIM-SM RP-SET information:	Combination of RP information sets
BSR is: 4.4.4.6	BSR is the VLAN interface of 4.4.4.6 in the network
Group/MaskLen: 224.0.0.0/4	The RP whose group address is 224.0.0.0 and mask length is 4 is the virtual interface of the IP address 4.4.4.6.
RP 4.4.4.6	
Version: 2	The priority of the version 2 RP is 0. It is up for 39 minutes and 50 seconds and expires in one minutes and forty seconds
Priority: 0	
Uptime: 00:39:50	
Expires: 00:01:40	

pim

Syntax **pim**

undo pim

View System view

Parameter None

Description

Use the **pim** command to enter PIM view to configure the global PIM parameters. You cannot use the **pim** command to enable the PIM protocol.

Use the **undo pim** command to exit PIM view to system view and clear the global PIM configuration parameters.

Example

Enter PIM view.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] multicast routing-enable
[SW7750] pim
[SW7750-pim]
```

pim bsr-boundary

Syntax

pim bsr-boundary

undo pim bsr-boundary

View

VLAN interface view

Parameter

None

Description

Use the **pim bsr-boundary** command to configure a VLAN interface of the switch as the PIM domain boundary.

Use the **undo pim bsr-boundary** command to remove the configured PIM domain boundary.

The switch does not set any PIM domain boundary by default.

After you use this command to set a PIM area boundary on a VLAN interface, all Bootstrap messages cannot cross this domain boundary. However, the other PIM packets can pass this domain boundary. In this way, you can divide the PIM-SM-running network into multiple domains, each of which uses a different Bootstrap router.

Note that you cannot use this command to set up a multicast boundary. Instead, what you use this command to set up is just a PIM Bootstrap packet boundary.

Related command:

c-bsr.

Example

Configure domain boundary on VLAN-interface10.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] multicast routing-enable
[SW7750] pim
[SW7750] interface Vlan-interface 10
[SW7750-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.

Once enabled PIM-DM on an interface, PIM-SM cannot be enabled on the same interface and vice versa.

Example # Enable the PIM-DM protocol on VLAN-interface10 of the Ethernet switch.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] multicast routing-enable
[SW7750] interface Vlan-interface 10
[SW7750-Vlan-interface10] pim dm
```

pim neighbor-limit

Syntax **pim neighbor-limit** *limit*

undo pim neighbor-limit

View VLAN interface view

Parameter *limit*: Upper limit of PIM neighbors on the VLAN interface, in the range of 0~128.

Description Use the **pim neighbor-limit** command to limit the number PIM neighbors on a router interface. No neighbor can be added to the router any more when the limit is reached.

Use the **undo pim neighbor-limit** command to restore the default setting.

By default, the number of PIM neighbors on a VLAN interface is limited within 128.

If the number of existing PIM neighbors exceeds the configured limit, they will not be deleted.

Example # Limit the number of PIM neighbors on Vlan-interface10 within 50.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] multicast routing-enable
[SW7750] interface Vlan-interface 10
[SW7750-Vlan-interface10] pim neighbor-limit 50
```

pim neighbor-policy

Syntax **pim neighbor-policy** *acl-number*

undo pim neighbor-policy

View VLAN interface view

Parameter *acl-number*: Basic ACL number, in the range of 2000 to 2999.

Description Use the **pim neighbor-policy** command to configure the router to filter the PIM neighbors on the current VLAN interface.

Use the **undo pim neighbor-policy** command to disable the filtering.

Only the routers that match the filtering rule in the ACL can serve as a PIM neighbor of the current VLAN 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.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] multicast routing-enable
[SW7750] interface Vlan-interface 10
[SW7750-Vlan-interface10] pim neighbor-policy 2000
[SW7750-Vlan-interface10] quit
[SW7750] acl number 2000
[SW7750-acl-basic-2000] rule permit source 10.10.1.2 0
[SW7750-acl-basic-2000] rule deny source 10.10.1.1 0
```

pim sm

Syntax **pim sm**

undo pim sm

View VLAN interface view

Parameter None

Description Use the **pim sm** command to enable the PIM-SM protocol.

Use the **undo pim sm** command to disable the PIM-SM protocol.

By default, the switch disables the PIM-SM protocol.

You must enable the PIM-SM protocol on each VLAN interface respectively. Generally, the PIM-SM protocol is enabled on each VLAN interface.

Related command: **multicast routing-enable**.

Example # Enable the PIM-SM protocol on VLAN-interface10.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] multicast routing-enable
[SW7750] interface Vlan-interface 10
[SW7750-Vlan-interface10] pim sm
```

pim timer hello

Syntax **pim timer hello** *seconds*

undo pim timer hello

View VLAN interface view

Parameter *seconds*: Interval at which a VLAN interface sends Hello packets, in the range of 1 second to 18,000 seconds.

Description Use the **pim timer hello** command to set the interval at which a VLAN interface sends Hello packets.

Use the **undo pim timer hello** command to restore the default value of the interval.

By default, a VLAN interface sends Hello packets at the interval of 30 seconds.

When the PIM-SM protocol is enabled on a VLAN interface, the switch will periodically send Hello packets to the network devices supporting PIM. If the VLAN interface receives Hello packets, it means that the VLAN interface has neighboring network devices supporting PIM, and the VLAN interface will add the neighbors into its own neighbor list. If the VLAN interface does not receive any Hello packet from a neighbor in its neighbor list within the specified time, the neighbor is considered to have left the multicast group.

Example # Configure to VLAN-interface 10 of the switch to send Hello packet at the interval of 40 seconds.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] multicast routing-enable
```

```
[SW7750] interface Vlan-interface 10
[SW7750-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 packets sent by the DR in the PIM-SM network and to accept the specified packets only.

Use the **undo register-policy** command to remove the configured packet 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.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] acl number 3010
[SW7750-acl-adv-3010] rule permit ip source 10.10.0.0 0.0.255.255 destination 225.1.0.0 0.0.25
5.255
[SW7750-acl-adv-3010] quit
[SW7750] multicast routing-enable
[SW7750] pim
[SW7750-pim] register-policy 3010
```

spt-switch-threshold

Syntax

spt-switch-threshold { *traffic-rate* | **infinity** } [**group-policy** *acl-number* [**order** *order-value*]]

undo spt-switch-threshold { *traffic-rate* | **infinity** } [**group-policy** *acl-number*]

View

PIM view

Parameter

traffic-rate: Rate of sending multicast packets, in kbps ranging from 0 to 65,535.

infinity: Specifies that RPT-to-SPT switchover never takes place.

acl-number: Basic ACL number, in the range of 2000 to 2999. It defines a group range in which the rate of sending multicast packets is suppressed.

Description

Use the **spt-switch-threshold** command to configure the threshold for performing RPT-to-SPT switchover.

Use the **undo spt-switch-threshold** command to restore the threshold for performing RPT-to-SPT switchover to the default value.

By default, the threshold for performing RPT-to-SPT switchover is 0.

In PIM-SM, Ethernet switches forward multicast packets through the RPT initially. If the rate of sending multicast packets exceeds the specified threshold, the last-hop switch of the multicast packets will perform RPT-to-SPT switchover.

*Only the threshold 0 and the **infinity** keyword are supported currently.*

- If the threshold is set to 0, the last-hop switch performs RPT-to-SPT switchover upon receiving the first multicast packet.
- The **infinity** keyword specifies that RPT-to-SPT switchover never takes place.

Example # Set the threshold for perform RPT-to-SPT switchover to 0, that is, specify the last-hop switch to perform RPT-to-SPT switchover upon receiving the first multicast packet.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] pim
[SW7750-pim] spt-switch-threshold 0
```

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: Specifies neighbor address.

interface *interface-type interface-number*: Specifies VLAN interface.

Description Use the **reset pim neighbor** command to clear all PIM neighbors or PIM neighbors on the specified VLAN interface.

Related command: **display pim neighbor**.

Example # Clear the PIM neighbor 25.5.4.3.

```
<SW7750> 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* } } * }

View User view

Parameter **all**: All PIM neighbors

group-address: Specifies group address.

mask *group-mask*: Specifies group mask.

group-mask-length: Specifies mask length of the group address.

source-address: Specifies source address.

mask *source-mask*: Specifies source mask.

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: Specifies the VLAN interface.

Description Use the **reset pim routing-table** command to clear all PIM route entries or the specified 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 224.0.0.0/4 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.

```
<SW7750> 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 configure the router to filter the received multicast data packets according to the source address or group address.

Use the **undo source-policy** 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.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] multicast routing-enable
[SW7750] pim
[SW7750-pim] source-policy 2000
[SW7750-pim] quit
[SW7750] acl number 2000
[SW7750-acl-basic-2000] rule permit source 10.10.1.2 0
[SW7750-acl-basic-2000] rule deny source 10.10.1.1 0
```

static-rp

Syntax **static-rp** *rp-address* [*acl-number*] [**preferred**]

undo static-rp *rp-address*

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.

preferred: If both a dynamic RP and a static RP exist simultaneously, and if you have configured the keyword **preferred**, the static RP is preferred.

Description

Use the **static-rp** command to configure static RP.

Use the **undo static-rp** command to remove the configuration.

If both C-RPs and static RPs exist simultaneously, an RP is selected from them as follows:

First, an RP is dynamically elected from the C-RPs based on the BSR mechanism and the first eligible static RP is selected from the static RPs.

Then, a comparison takes places between the dynamic RP and the static RP. If the **preferred** keyword is configured for the static RP, the static RP is preferred; otherwise, the dynamic RP is preferred.

The new configuration overwrites the old one if you execute the command for a second time.

Related command:

display pim rp-info.

Example

Configure 10.110.0.6 as a static RP.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] multicast routing-enable
[SW7750] pim
[SW7750-pim] static-rp 10.110.0.6
```

42 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 SA message cache mechanism.

Use the **undo cache-sa-enable** command to disable the cache mechanism.

By default, the SA message cache mechanism is enabled by default.

If the router is in the cache state, it sends no SA request message to the specified MSDP peer when it receives a Join message.

Example # Enable the SA message cache mechanism.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] msdp
[SW7750-msdp] cache-sa-enable
```

display msdp brief

Syntax **display msdp brief**

View Any view

Parameter None

Description Use the **display msdp brief** command to display the brief information of the MSDP peer state.

Example # Display the brief information of the MSDP peer state.

```
<SW7750> 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
```

Table 94 Field descriptions of the **display msdp brief** command

Field	Description
Peer's Address	Address of the MSDP peer
State	State
Up/Down time	Up/down time
AS	AS number
SA Count	SA count
Reset Count	Times of peer connection resets

display msdp peer-status

Syntax **display msdp peer-status** [*peer-address*]

View Any view

Parameter *peer-address*: IP address of an MSDP peer. This argument is expressed in dotted decimal notation.

Description Use the **display msdp peer-status** command to display the detailed information of the MSDP peer state.

Related command: **peer description**.

Example # Display the detailed information of MSDP peer 10.110.11.11.

```
<SW7750> 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 the (S, G) entry.

source-address: Source address of the (S, G) entry. If you do not specify a source address, the system displays all source information of the specified group. If you specify neither a group address nor a source address, the system displays all SA caches.

autonomous-system-number: Number of the AS from which the (S,G) entry comes. The value ranges from 1 to 65535.

Description Use the **display msdp sa-cache** command to display (S, G) state learned from an MSDP peer.

You must configure the **cache-sa-enable** command before the system can display the cache state information.

Example # Display SA messages learned from the MSDP peer.

```
<SW7750> display msdp sa-cache
MSDP Total Source-Active Cache - 5 entries

(Source, Group)                  Origin RP       Pro   AS   Uptime   Expires
(10.10.1.2, 225.1.1.1)             10.10.10.10     BGP  100   00:00:10 00:05:50
(10.10.1.3, 225.1.1.1)             10.10.10.10     BGP  100   00:00:11 00:05:49
(10.10.1.2, 225.1.1.2)             10.10.10.10     BGP  100   00:00:11 00:05:49
(10.10.2.1, 225.1.1.2)             10.10.10.10     BGP  100   00:00:11 00:05:49
(10.10.1.2, 225.1.2.2)             10.10.10.10     BGP  100   00:00:11 00:05:49

 MSDP matched 5 entries
```

Table 95 Field descriptions of the **display msdp sa-cache** command

Field	Description
(Source, Group)	(S, G) entry
Origin RP	Source RP address
Pro	Inter-domain unicast routing protocol
AS	AS number
Uptime	Up time
Expires	Expiry of a (S, G) entry

display msdp sa-count

Syntax **display msdp sa-count** [*autonomous-system-number*]

View Any view

Parameter *autonomous-system-number*: AS from which a source and group come The value ranges from 1 to 65535.

Description Use the **display msdp sa-count** command to display the number of sources and groups in MSDP cache.

The debugging output of this command is available only after the **cache-sa-enable** command is configured.

Example # Display the number of sources and groups in MSDP cache.

```
<SW7750> 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
  100    3                    3

  Total Source-Active entries: 5
```

Table 96 Field descriptions of the **display msdp sa-count** command

Field	Description
Peer’s Address	Address of an MSDP peer
Number of SA	Number of SA messages
AS	AS number
Number of source	Number of sources
Number of group	Number of groups

import-source

Syntax **import-source** [**acl** *acl-number*]

undo import-source

View MSDP view

Parameter *acl-number*: Basic or advanced IP ACL number, ranging from 2000 to 3999. An ACL controls SA message advertisement by filtering sources (with a basic ACL) and filtering sources or groups (with an advanced ACL). If you do not specify this argument, no multicast source is advertised.

Description Use the **import-source** command to specify the (S, G) entries in this domain that need to be advertised when an MSDP peer creates an SA message.

Use the **undo import-source** command to cancel the configuration.

By default, an SA message advertise all the (S, G) entries in the domain.

In addition, you can use the **peer sa-policy import** command or the **peer sa-policy export** command to filter forwarded SA messages.

Example # Configure the specific (S, G) entry in the multicast routing table to be advertised when an MSDP peer creates an SA message. For the specific (S, G) entry, the multicast source is on the 10.10.0.0/16 segment, and the multicast group address is 225.1.0.0/16.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] acl number 3101
[SW7750-acl-adv-3101] rule permit ip source 10.10.0.0 0.0.255.255 destination 225.1.0.0 0.0.25
5.255
[SW7750-acl-adv-3101] quit
[SW7750] msdp
[SW7750-msdp] import-source acl 3101
```

msdp

Syntax **msdp**

undo msdp

View System view

Parameter None

Description Use the **msdp** command to enable MSDP and enter MSDP view.

Use the **undo msdp** command to clear all configurations in MSDP view, release resources occupied by MSDP, and restore the initial state.

Related command: **peer description**.

Example # Enable MSDP and enter MSDP view.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] msdp
[SW7750-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 an RP

max-hops: Maximum number of hops to be traced, ranging from 1 to 255. The default value is 16.

next-hop-info: Collects the next hop information.

sa-info: Collects the SA entity information.

peer-info: Collects the MSDP peer information.

skip-hops: Number of hops to be skipped before the detailed information is collected, in the range of 0 to 255. This argument is 0 by default.

Description Use the **msdp-tracert** command to trace the path along which an SA message travels, so as to locate message loss and minimize configuration errors. After determining the path of the SA message, you can prevent SA flooding through correct configuration.

Example # Trace path information of 10.10.1.1, 225.2.2.2, and 20.20.20.20.

```
<SW7750> msdp-tracert 10.10.1.1 225.2.2.2 20.20.20.20
```

# Specify the maximum number of hops to be traced and collect the detailed SA and MSDP peer information.

```
<SW7750> 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 trace route 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 97 Field descriptions of the **msdp-tracert** command

Field	Description
Router Address	The address used by the local router to establish a peering session with the Peer-RPF neighbor
Peer Uptime	The time of the peering session between the local router and a Peer-RPF neighbor, in minutes. The maximum value is 255.

Table 97 Field descriptions of the **msdp-tracert** command

Field	Description
Cache Entry Uptime	Up time of the (S, G, RP) entry in SA cache of the local router, in minutes. The maximum value is 255.
D-bit: 1	An (S, G, RP) entry exists in the 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 may be another RP than the source RP in the (S, G, RP) entry.
NC-bit: 0	SA cache is enabled on the local router.
C-bit: 1	A (S, G, RP) entry exists in SA cache of the local router.
Return Code: Reached-max-hops	Maximum number of hops is reached. Another possible value is: Hit-src-RP: The router of this hop is the source RP in the (S, G, RP) entry.
Next-Hop Router Address: 0.0.0.0	If you use the **next-hop-info** keyword, the address of Peer-RPF neighbor is displayed.
Count of SA messages received for this (S,G,RP)	The number of SA messages received to trace the (S, G, RP) entry.
Count of encapsulated data packets received for this (S,G,RP)	The number of packets received to trace the (S, G, RP) entry.
SA cache entry uptime	The up time of an SA cache entry
SA cache entry expiry time	The expiry time of an SA cache entry
Peering Uptime: 10 minutes	The time of the peering session between the local router and a Peer-RPF neighbor
Count of Peering Resets	Count of 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 MSDP peer to use the specified interface IP address as the RP address in the SA message when the MSDP peer creates SA messages.

Use the **undo originating-rp** command to cancel configuration.

By default, the RP address in an SA message is the RP address configured by PIM.

Example # Configure the IP address of Vlan-interface100 as the RP address of the created SA message.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] msdp
[SW7750-msdp] originating-rp Vlan-interface 100
```

peer connect-interface

Syntax **peer** *peer-address* **connect-interface** *interface-type interface-number*

undo peer *peer-address*

View MSDP view

Parameter *peer-address*: IP address of the MSDP peer. This argument is expressed in dotted decimal notation.

interface-type interface-number: Interface type and interface number. The local router uses the primary address of this interface as the source IP to establish a TCP connection with the remote MSDP peer.

Description Use the **peer connect-interface** command to configure an MSDP peer.

Use the **undo peer connect-interface** command to disable the configured MSDP peer.

If the MSDP peer of the local router is also a BGP peer, the MSDP peer and the BGP peer must use the same IP addresses.

Related command: **static-rpf-peer**.

Example # Configure the router whose IP address is 125.10 .7.6 as the MSDP peer of the local router.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] msdp
[SW7750-msdp] peer 125.10.7.6 connect-interface Vlan-interface 100
```

peer description

Syntax **peer** *peer-address* **description** *text*

undo peer *peer-address* **description**

View MSDP view

Parameter *peer-address*: IP address of the MSDP peer. This argument is expressed in dotted decimal notation.

text: Description text, case-sensitive. The maximum length is 80 characters.

Description Use the **peer description** command to configure the description text for an MSDP peer. Use the **undo peer description** command to delete the configured description text.

By default, an MSDP peer has no description text.

An administrator can distinguish MSDP peers by means of the description texts.

Related command: **display msdp peer-status**.

Example # Add the description text "router CstmrA" for the router with the IP address 125.10.7.6 to specify that the router is customer A.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] msdp
[SW7750-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 *peer-address*: IP address of an MSDP peer in a mesh group. This argument is expressed in dotted decimal notation.

name: Name of a mesh group, case-sensitive and containing 1 to 32 characters.

Description Use the **peer mesh-group** command to add an MSDP peer to a mesh group.

Use the **undo peer mesh-group** command to cancel the configuration.

By default, an MSDP peer does not belong to any mesh group.

Example # Configure the MSDP peer whose address is 125.10.7.6 as a member of the mesh group Grp1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] msdp
[SW7750-msdp] peer 125.10.7.6 mesh-group Grp1
```

peer minimum-ttl

Syntax **peer** *peer-address* **minimum-ttl** *ttl-value*

undo peer *peer-address* **minimum-ttl**

View MSDP view

Parameter *peer-address*: IP address of the MSDP peer to which the TTL threshold applies. This argument is expressed in dotted decimal notation.

ttl-value: TTL threshold, ranging from 0 to 255.

Description Use the **peer minimum-ttl** command to configure the minimum TTL value of the multicast data packets encapsulated in SA messages and to be sent to the specified MSDP peer.

Use the **undo peerminimum-ttl** command to restore the default TTL threshold.

By default, the value of TTL threshold is 0.

Related command: **peer description**.

Example # Set the TTL threshold to 10 so that 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.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] msdp
[SW7750-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*: IP address of the MSDP peer. This argument is expressed in dotted decimal notation.

Description Use the **peer request-sa-enable** command to enable the router to send an SA request message to the specified MSDP peer upon receipt of a Join message.

Use the **undo peer request-sa-enable** command to remove the configuration.

By default, upon receipt of a Join message, the router sends no SA request message to the MSDP peer but waits for the next SA message.

Related command: **cache-sa-enable**.

Example # Configure to send an SA request message to the MSDP peer 125.10.7.6.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
```

```
[SW7750] msdp
[SW7750-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*: IP address of the MSDP peer. This argument is expressed in dotted decimal notation.

sa-limit: Maximum number of SA messages cached, ranging from 1 to 2,048.

Description Use the **peer sa-cache-maximum** command to set the maximum number of SA messages cached on the router.

Use the **undo peer sa-cache-maximum** command to restore the default configuration.

By default, the maximum number of SA messages cached on a router is 2,048.

You are recommended to perform this configuration on all MSDP peers on a network that is vulnerable to DoS attacks.

Related command: **display msdp sa-count**, **display msdp peer-status**, **display msdp brief**.

Example # Configure the SA cache of the router so that it caches a maximum of 100 SA messages received from the MSDP peer 125.10.7.6.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] msdp
[SW7750-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 the SA messages from the specified MSDP peer.

export: Forwards the SA messages from the specified MSDP peer.

peer-address: IP address of the MSDP peer whose SA messages need to be filtered.

acl *acl-number*: Specifies an advanced IP ACL number ranging from 3000 to 3999. If no ACL is specified, all (S, G) entries are filtered out.

Description Use the **peer sa-policy** command to configure the filtering list for receiving or forwarding the SA messages from the specified MSDP peer.

Use the **undo peer sa-policy** command to remove the configuration.

By default, no filtering is imposed on SA messages to be received or forwarded; namely, all SA messages from MSDP peers are received or forwarded.

Related command: **peer sa-request-policy**.

Example # Configure a filtering list so that only those SA messages permitted by the advanced IP ACL 3100 are forwarded.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] acl number 3100
[SW7750-acl-adv-3100] rule permit ip source 170.15.0.0 0.0.255.255 destination 225.1.0.0 0.0.255.255
[SW7750-acl-adv-3100] quit
[SW7750] msdp
[SW7750-msdp] peer 125.10.7.6 connect-interface Vlan-interface 100
[SW7750-msdp] peer 125.10.7.6 sa-policy export acl 3100
```

peer sa-request-policy

Syntax **peer** *peer-address* **sa-request-policy** [**acl** *acl-number*]

undo peer *peer-address* **sa-request-policy**

View MSDP view

Parameter *peer-address*: IP address of an MSDP peer, the SA request messages sent from which will be filtered

acl-number: Basic IP ACL number, describing a multicast group address and in the range of 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 the SA request messages that the router receives from an MSDP peer.

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 an ACL is specified, only those SA request messages from the groups that match the ACL rule will be processed and others are ignored.

Related command: **peer sa-policy**.

Example # Configure an ACL so that SA request messages from the group address range of 225.1.1.0/24 and from the MSDP peer 175.58.6.5 are received and other SA messages are ignored.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] acl number 2001
[SW7750-acl-basic-2001] rule permit source 225.1.1.0 0.0.0.255
[SW7750-acl-basic-2001] quit
[SW7750] msdp
[SW7750-msdp] peer 175.58.6.5 sa-request-policy acl 2001
```

reset msdp peer

Syntax **reset msdp peer** *peer-address*

View User view

Parameter *peer-address*: IP address of the MSDP peer. This argument is expressed in dotted decimal.

Description Use the **reset msdp peer** command to reset the TCP connection with the specified MSDP peer and clear all statistics information of that MSDP peer.

Related command: **peer description**.

Example # Reset the TCP connection with the MSDP peer 125.10.7.6 and the statistics of the MSDP peer.

```
<SW7750> reset msdp peer 125.10.7.6
```

reset msdp sa-cache

Syntax **reset msdp sa-cache** [*group-address*]

View User view

Parameter *group-address*: Group address; the cached (S, G) entries matching this address are to be deleted from the SA cache. If no multicast group address is specified, all cached SA entries will be cleared.

Description Use the **reset msdp sa-cache** command to clear cached SA entries of the MSDP peer.

Related command: **cache-sa-enable**, **display msdp sa-cache**.

Example # Clear the cached entries whose group address is 225.5.4.3 from the SA cache.

```
<SW7750> 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, reset information and input/output information will be cleared. If no MSDP peer address is specified, the statistics information of all MSDP peers will be cleared.

Description Use the **reset msdp statistics** command to clear the statistics information of one or more MSDP peers without resetting the MSDP peer(s).

Example # Clear the statistics information of the MSDP peer 125.10.7.6.

```
<SW7750> 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 an MSDP peer.

Description Use the **shutdown** command to shut down the specified MSDP peer.

Use the **undo shutdown** command to remove the configuration.

By default, no MSDP peer is shut down.

Related command: **peer description**.

Example # Shut down the MSDP peer 125.10.7.6.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] msdp
[SW7750-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 receiving SA messages.

rp-policy *ip-prefix-name*: Specifies a filtering policy based on RP addresses to filter RPs in SA messages. *ip-prefix-name* is the IP address prefix list containing 1 to 19 characters.

Description Use the **static-rpf-peer** command to configure a static RPF peer.

Use the **undo static-rpf-peer** command to remove a static RPF peer.

By default, no static RPF peer is configured.

If only one MSDP peer is configured with the **peer** command, the MSDP peer will be regarded as a static RPF peer. When configuring multiple static RPF peers for the same router, make sure you follow the following two configuration methods::

- In the case that all the peers use the **rp-policy** keyword: Multiple static RPF peers take effect at the same time. RPs in SA messages are filtered according to the prefix list configured; only SA messages whose RP addresses pass the filtering are received. If multiple static RPF peers using the same **rp-policy** keyword are configured, when any of the peers receives an SA message, it will forward the SA message to the other peers.
- In the case that none of the peers use the **rp-policy** keyword: According to the configuration sequence, only the first static RPF peer whose connection state is UP is active. All the SA messages from this peer will be received and those from other static RPF peers will be discarded. Once the active static RPF peer fails (because the configuration is removed or the connection is terminated), based on the configuration sequence, the subsequent first static RPF peer whose connection is in the UP state will be selected as the active static RPF peer.

Related command: **peer description**, **ip ip-prefix**.

Example # Configure a static RPF peer.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ip ip-prefix list1 permit 130.10.0.0 16 greater-equal 16 less-equal 32
[SW7750] msdp
[SW7750-msdp] peer 130.10.7.6 connect-interface Vlan-interface 100
[SW7750-msdp] static-rpf-peer 130.10.7.6 rp-policy list1
```

timer retry

Syntax **timer retry** *seconds*

undo timer retry

View MSDP view

Parameter *seconds*: Connection request retry interval in seconds, ranging from 1 to 60.

Description

Use the **timer retry** command to configure a connection request retry interval.

Use the **undo timer retry** command to restore the default value.

By default, the connection request retry interval is 30 seconds.

Related command: **peer description**.

Example

Set the connection request retry interval to 60 seconds.

```
<SW7750> system-view
[SW7750] msdp
[SW7750-msdp] timer retry 60
```

43 802.1x Configuration Commands

display dot1x

Syntax **display dot1x** [**sessions** | **statistics**] [**interface** *interface-list*]

View Any view

Parameter **sessions**: Displays the formation about 802.1x sessions.

statistics: Displays the statistics information about 802.1x.

interface: Display the 802.1x-related information about a specified port.

interface-list: Ethernet port list. You can specify multiple Ethernet ports by providing this argument in the form of *interface-list* = { *interface-name* [**to** *interface- name*] & < 1-10 >. The *interface-name* argument is the port index of an Ethernet port and can be specified in this form: *interface-name* = { *interface-type interface-num* }, where *interface-type* specifies the type of an Ethernet port and *interface-num* identifies the number of the port. "&<1-10>" means that up to 10 port indexes/port index lists can be provided.

Description Use the **display dot1x** command to display 802.1x-related information, such as configuration information, operation information (session information), and statistics.

By default, this command displays all 802.1x-related information of each port.

When the *interface-list* argument is not provided, this command displays 802.1x-related information on all ports. The output information can be used to verify 802.1 x-related configurations and to troubleshoot.

Related commands: **reset dot1x statistics**, **dot1x**, **dot1x retry**, **dot1x max-user**, **dot1x port-control**, **dot1x port-method**, and **dot1x timer**.

Example # Display 802.1x-related configuration information.

```
<SW7750> 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
Guest Vlan is disabled

 Configuration: Transmit Period     30 s,  Handshake Period       15 s
```

```
               ReAuth Period   003600 s
               Quiet Period        60 s,  Quiet Period Timer is disabled
               Supp Timeout        30 s,  Server Timeout         100 s
               Interval between version requests is 30s
               maximal request times for version information is 3
               The maximal retransmitting times          2

 Total maximum 802.1x user resource number is 4096
 Total current used 802.1x resource number is 0

 GigabitEthernet2/0/1  is link-up
   802.1X protocol is disabled
   Proxy trap checker is disabled
   Proxy logoff checker is disabled
   Guest Vlan is disabled
   Version-Check is disabled
   The port is a(n) authenticator
   Authenticate Mode is auto
   Port Control Type is Mac-based
   ReAuthenticate is disabled
   Max on-line user number is 1024
......
(Display omitted here)
```

Table 98 Field descriptions of the **display dot1x** command

Field	Description
Equipment 802.1x protocol is enabled	802.1x protocol (802.1x for short) is enabled on the switch.
CHAP authentication is enabled	CHAP authentication is enabled.
DHCP-launch is disabled	With DHCP enabled, manually configuring a static IP address triggers 802.1x authentication on the switch.
Proxy trap checker is disabled	Whether to check a supplicant system that logs in through a proxy: ■ Disable means the switch does not send Trap packets when it detects that a supplicant system logs in through a proxy. ■ Enable means the switch sends Trap packets when it detects that a supplicant system logs in through a proxy.
Proxy logoff checker is disabled	Whether to check a supplicant system that logs in through a proxy: ■ Disable means the switch does not disconnect a supplicant system when it detects that the latter logs in through a proxy. ■ Enable means the switch disconnects a supplicant system when it detects that the latter logs in through a proxy.
Guest Vlan is disabled	The Guest VLAN function is disabled.
Transmit Period	Setting of the Transmission period timer (the tx-period)
Handshake Period	Setting of the handshake period timer (the handshake-period)
ReAuth Period	802.1x re-authentication
Quiet Period	Setting of the quiet period timer (the quiet-period)
Quiet Period Timer is disabled	The quiet period timer is disabled.
Supp Timeout	Setting of the supplicant timeout timer (supp-timeout)
Server Timeout	Setting of the server-timeout timer (server-timeout)

Table 98 Field descriptions of the **display dot1x** command

Field	Description
Interval between version requests	Client version request timer
maximal request times for version information	The maximum number of times that the switch can send version request packets to an access user
The maximal retransmitting times	The maximum number of times that the switch can send authentication request packets to a supplicant system
Total maximum 802.1x user resource number	The maximum number of 802.1x users that a switch can accommodate
Total current used 802.1x resource number	The number of online supplicant systems
GigabitEthernet2/0/1 is link-up	The GigabitEthernet 2/0/1 port is in up state.
802.1x protocol is disabled	802.1x is disabled on the port
Proxy trap checker is disabled	Whether to check a supplicant system that logs in through a proxy: ■ Disable means the switch does not detect supplicant login through a proxy ■ Enable means the switch sends Trap packets when it detects that a supplicant system logs in through a proxy.
Proxy logoff checker is disabled	Whether to check a supplicant system that logs in through a proxy: ■ Disable means the switch does not detect supplicant login through a proxy ■ Enable means the switch disconnects a supplicant system when it detects that the latter logs in through a proxy.
Guest Vlan is disabled	The Guest VLAN function is disabled.
Version-Check is disabled	The client version check function is disabled.
The port is a(n) authenticator	The port acts as an authenticator.
Authenticate Mode is auto	The port access control mode is **auto**.
Port Control Type is Mac-based	The port access control method is MAC-based. That is, supplicant systems are authenticated based on their MAC addresses.
Max on-line user number	The maximum number of online users that the port can accommodate
…	Information omitted here

dot1x

Syntax **dot1x** [**interface** *interface-list*]

undo dot1x [**interface** *interface-list*]

View System view, Ethernet port view

Parameter *interface-list*: Ethernet port list. You can specify multiple Ethernet ports by providing this argument in the form of *interface-list* = { *interface-name* [**to** *interface- name*] & < 1-10 >. The *interface-name* argument is the port index of an

Ethernet port and can be specified in this form: *interface-name* = { *interface-type interface-num* }, where *interface-type* specifies the type of a port and *interface-num* identifies the port number. "&<1-10>" means that up to 10 port indexes/port index lists can be provided,

Description Use the **dot1x** command to enable 802.1x globally or for specified Ethernet ports.

Use the **undo dot1x** command to disable 802.1x globally or for specified Ethernet ports.

By default, 802.1x is disabled globally and also on all ports

When being executed in system view, the **dot1x** command enables 802.1x globally if you do not provide the *interface-list* argument. And if you specify the *interface-list* argument, the command enables 802.1x for the specified Ethernet ports. When being executed in Ethernet port view, this command enables 802.1x for the current Ethernet port only. In this case, the *interface-list* argument is not needed.

You can perform 802.1x-related configurations (globally or on specified ports) either before or after 802.1x is enabled. If you do not previously perform other 802.1x-related configurations when enabling 802.1x globally, the switch adopts the default 802.1x settings.

802.1x-related configurations take effect on a port only after 802.1x is enabled both globally and on the port.

Configurations of 8021.x and the maximum number of MAX addresses that can be learnt are mutually exclusive. This means that when 802.1x is enabled for a port, it cannot also have the maximum number of MAX addresses to be learned configured at the same time. And if you configure the maximum number of MAX addresses that can be learnt for a port, 802.1x is unavailable to it.

Related command: **display dot1x**.

Example # Enable 802.1x for Ethernet 2/0/1 port.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] dot1x interface Ethernet 2/0/1
```

# Enable 802.1x globally.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] dot1x
```

dot1x authentication-method

Syntax **dot1x authentication-method** { **chap** | **pap** | **eap** }

undo dot1x authentication-method

View System view

Parameter **chap**: Authenticates with the help of challenge handshake authentication protocol (CHAP).

pap: Authenticates with the help of password authentication protocol (PAP).

eap: Authenticates with the help of extensible authentication protocol (EAP).

Description Use the **dot1x authentication-method** command to set the 802.1x authentication method.

Use the **undo dot1x authentication-method** command to revert to the default 802.1x authentication method.

The default 802.1x authentication method is CHAP.

PAP applies a two-way handshaking procedure. In this method, passwords are transmitted in plain text.

CHAP applies a three-way handshaking procedure. In this method, user names are transmitted rather than passwords. Therefore this method is safer.

In an EAP authentication method, a switch sends 802.1x authentication information directly to the RADIUS server in EAP packets, instead of having to convert them into RADIUS packets before forwarding to the RADIUS server. EAP authentication can be realized in one of the three sub-methods: PEAP, EAP-TLS, and EAP-MD5.

Note that the RADIUS server must support PAP, CHAP, or EAP authentication before the corresponding authentication can be implemented.

Related command: **display dot1x**.

Example # Specify the authentication method for 802.1x users to be PAP.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] 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 specify an 802.1x-enqbled switch to launch the process to authenticate a supplicant system when the supplicant system applies for a dynamic IP address through DHCP.

Use the **undo dot1x dhcp-launch** command to disable an 802.1x-enqbled switch from authenticating a supplicant system when the supplicant system applies for a dynamic IP address through DHCP.

By default, an 802.1x-enabled switch does not authenticate a supplicant system when the latter applies for a dynamic IP address through DHCP.

Related command: **display dot1x**.

Example # Configure to authenticate a supplicant system when it applies for a dynamic IP address through DHCP.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] 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 port view

Parameter *vlan-id*: VLAN ID of a Guest VLAN, in the range from 1 to 4,094.

interface-list: List of Ethernet ports, expressed as *interface-list* = { *interface-name* [**to** *interface-name*] } & < 1-10 >. The *interface-name* argument is the port index of a port and can be specified in this form: *interface-name* = { *interface-type interface-num* }, where *interface-type* specifies the type of a port and *interface-num* identifies the port number. "&<1-10>" means that up to 10 port indexes/port index lists can be provided.

Description Use the **dot1x guest-vlan** command to enable the Guest VLAN function for specified ports.

Use the **undo dot1x guest-vlan** command to disable the Guest VLAN function for specified ports.

When being executed in system view:

- If you do not provide the *interface-list* argument, these two commands apply to all ports of the switch.
- If you specify the *interface-list* argument, these two commands apply to the specified Ethernet ports.

When being executed in Ethernet port view, these two commands apply to the current Ethernet port only. In this case, the *interface-list* argument is not needed.

CAUTION:

- *The Guest VLAN function is available only when the switch operates in a port-based authentication mode.*
- *Only one Guest VLAN can be configured for each switch.*
- *The Guest VLAN function is unavailable when the **dot1x dhcp-launch** command is configured on the switch, because the switch does not send authentication request packets.*

Related commands: **name**, **vlan-assignment-mode**.

Example # Specify the authentication method to be port-based authentication.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] dot1x port-method portbased
```

# Enable the Guest VLAN function for all ports.

```
[SW7750] 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*: Maximum number of users a port can accommodate, ranging from 1 to 1024. The default number is 1024.

interface-list: List of Ethernet ports, expressed as *interface-list* = { *interface-name* [**to** *interface-name*] } & < 1-10 >. The *interface-name* argument specifies the port index of an Ethernet port and can be specified in this form: *interface-name* = { *interface-type interface-num* }, where *interface-type* specifies the type of a port and *interface-num* identifies the port number. "&<1-10>" means that up to 10 port indexes/port index lists can be provided.

Description Use the **dot1x max-user** command to set the maximum number of supplicant systems an Ethernet port can accommodate.

Use the **undo dot1x max-user** command to revert to the default maximum supplicant system number.

When being executed in system view, these two commands apply to all Ethernet ports of the switch if you do not provide the *interface-list* argument. And if you specify the *interface-list* argument, these commands apply to the specified Ethernet ports.

When being executed in Ethernet port view, these two commands apply to the current Ethernet port only. In this case, the *interface-list* argument is not needed.

Related command: **display dot1x**.

Example # Configure the maximum number of users that Ethernet 3/01 can accommodate to be 32.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] dot1x max-user 32 interface Ethernet 2/0/1
```

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 port view

Parameter **auto**: Specifies to operate in **auto** access control mode. In this mode, a port is initialized to take all users as unauthorized: it only allows EAPoL packets to pass through and grants users no permission to network resources. Only after the users have passed the authentication will the port classify them as authorized and allow them access to the network resources, which is often the case.

authorized-force: Specifies to operate in **authorized-force** access control mode. **unauthorized-force**: Specifies to operate in **unauthorized-force** access control mode. Ports in this mode are constantly in unauthorized state. Supplicant systems connected to them cannot access the network.

interface-list: Ethernet port list. You can specify multiple Ethernet ports by providing this argument in the form of *interface-list* = { *interface-name* [**to** *interface- name*] & < 1-10 >. The *interface-name* argument is the port index of an Ethernet port and can be specified in this form: *interface-name* = { *interface-type interface-num* }, where *interface-type* specifies the type of a port and *interface-num* identifies the port number. "&<1-10>" means that up to 10 port indexes/port index lists can be provided.

Description Use the **dot1x port-control** command to specify the access control method for specified Ethernet ports.

Use the **undo dot1x port-control** command to revert to the default access control method.

The default access control method is **auto**.

Use the **dot1x port-control** command to configure the access control method for specified 802.1x-enabled ports.

When being executed in system view, these two commands apply to all Ethernet ports of the switch if you do not provide the *interface-list* argument. And if you specify the *interface-list* argument, these commands apply to the specified Ethernet ports.

When being executed in Ethernet port view, these two commands apply to the current Ethernet port only. In this case, the *interface-list* argument is not needed.

Related command: **display dot1x**.

Example # Specify Ethernet 2/0/1 port to operate in **unauthorized-force** access control mode.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] dot1x port-control unauthorized-force interface Ethernet 2/0/1
```

dot1x port-method

Syntax **dot1x port-method** { **macbased** | **portbased** } [**interface** *interface-list*]

undo dot1x port-method [**interface** *interface-list*]

View System view, Ethernet port view

Parameter **macbased**: Authenticates supplicant systems by MAC addresses.

portbased: Authenticates supplicant system by port numbers.

interface-list: Ethernet port list. You can specify multiple Ethernet ports by providing this argument in the form of *interface-list* = { *interface-name* [**to** *interface- name*] & < 1-10 >. The *interface-name* argument is the port index of an Ethernet port and can be specified in this form: *interface-name* = { *interface-type interface-num* }, where *interface-type* specifies the type of a port and *interface-num* identifies the port number. "&<1-10>" means that up to 10 port indexes/port index lists can be provided.

The default access control method is MAC address-based. That is, the **macbased** keyword is specified by default.

Description Use the **dot1x port-method** command to specify the access control method for specified Ethernet ports.

Use the **undo dot1x port-method** command to revert to the default access control method.

- If you specify to authenticate supplicant systems by MAC addresses (that is, the **macbased** keyword is specified), all supplicant systems connected to the specified Ethernet ports are authenticated separately. And if an online user logs off, others are not affected.

- If you specify to authenticate supplicant systems by port numbers (that is, the **portbased** keyword is specified), all supplicant systems connected to a specified Ethernet port are able to access the network without being authenticated if a supplicant system among them passes the authentication. And when the supplicant system logs off, the network is inaccessible to all other supplicant systems either.
- Changing the access control method on a port by the **dot1x port-method** command will forcibly log out the online 802.1x users on the port.

When being executed in system view, these two commands apply to all Ethernet ports of the switch if you do not provide the *interface-list* argument. And if you specify the *interface-list* argument, these commands apply to the specified Ethernet ports. When being executed in Ethernet port view, these two commands apply to the current Ethernet port only. In this case, the *interface-list* argument is not needed.

Related command: **display dot1x**.

Example # Specify to authenticate supplicant systems connected to Ethernet 2/0/1 port by port numbers.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] dot1x port-method portbased interface Ethernet 2/0/1
```

dot1x quiet-period

Syntax **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 the quiet-period timer.

When a supplicant system fails to pass the authentication, the authenticator system (such as a 3Com Ethernet switch) will stay quiet for a period (determined by the quiet-period timer) before it performs another authentication. During the quiet period, the authenticator system performs no 802.1x authentication.

By default, the quiet-period timer is disabled.

Related commands: **display dot1x**, **dot1x timer**.

Example # Enable the quiet-period timer.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] dot1x quiet-period
```

dot1x re-authenticate

Syntax **dot1x re-authenticate** [**interface** *interface-list*]

undo dot1x re-authenticate [**interface** *interface-list*]

View System view, Ethernet port view

Parameter *interface-list:* List of Ethernet ports, expressed as *interface-list* = { *interface-name* [**to** *interface-name*] } & < 1-10 >. The *interface-name* argument specifies the port index of an Ethernet port and can be specified in this form: *interface-name* = { *interface-type interface-num* }, where *interface-type* specifies the type of a port and *interface-num* identifies the port number. "&<1-10>" means that up to 10 port indexes/port index lists can be provided.

Description Use the **dot1x re-authenticate** command to enable 802.1x re-authentication on the specified port or on all Authenticator ports of the switch.

Use the **undo dot1x re-authenticate** command to disable 802.1x re-authentication on the specified port or on all Authenticator ports of the switch.

By default, 802.1x re-authentication is disabled on all ports.

When you use this command in system view, if you do not specify a port, this command will enable 802.1x re-authentication on all ports; if you provide a value for the *interface-list* argument, this command will enable 802.1x on the specified port.

When you use this command is Ethernet port view, the *interface-list* argument is not available and 8021.x re-authentication is enabled on the current port only.

- *802.1x must be enabled globally and on the current port before 802.1x re-authentication can be configured on the port.*
- *After re-authentication is enabled on a port, you cannot change the dynamic VLAN delivery attribute value for the port; if you do so, the re-authentication will cause users to be offline.*

Example # Enable 802.1x re-authentication on the port Ethernet 2/0/1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet 2/0/1
[SW7750-Ethernet2/0/1] dot1x re-authenticate
```

dot1x retry

Syntax **dot1x retry** *max-retry-value*

undo dot1x retry

View System view

Parameter *max-retry-value*: Maximum number of times that a switch sends authentication request packets to online supplicant systems. This argument ranges from 1 to 10 and defaults to 2.

Description Use the **dot1x retry** command to specify the maximum number of times that a switch will send authentication request packets to supplicant systems.

Use the **undo dot1x retry** command to revert to the default value.

Having sent authentication request packets to a supplicant system, a switch will resend the packets if within a preset period it still has not received any response from the supplicant system. The **dot1x retry** command is used to set the maximum number of times that a switch will resend the request packets. When set to 1, it means that the switch will send request packets only once, and when set to 2, it means that the switch will resend the packets once if no response comes back, and so on. This command applies to all ports.

Related command: **display dot1x**.

Example # Specify the maximum number of times that the switch will resend authentication request packets to be 9.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] dot1x retry 9
```

dot1x retry-version-max

Syntax **dot1x retry-version-max** *max-retry-version-value*

undo dot1x retry-version-max

View System view

Parameter *max-retry-version-value*: Maximum number of times that a switch will resend version request packets to a supplicant system. This argument ranges from 1 to 10.

Description Use the **dot1x retry-version-max** command to set the maximum number of times that a switch will resend version request packets to a connected supplicant system.

Use the **undo dot1x retry-version-max** command to revert to the default value.

By default, the switch can send version request packets to an access user for up to three times repeatedly.

Having sent a version request packet to the supplicant system, the switch will resend the packet if within a preset period (as determined by the client version timer) it still has not received any response from the supplicant system. When the number set by this command has reached and there is still no response from the supplicant system, the switch will continue its following authentication without sending further version requests. This command applies to all ports.

Related commands: **display dot1x**, **dot1x timer**.

Example # Configure the maximum number of times that the switch will resend version request packets to be 6.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] dot1x retry-version-max 6
```

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 port view

Parameter **logoff**: Disconnects a supplicant system if it logs in through a proxy or through multiple network modules.

trap: Sends Trap packets if a supplicant system logs in through a proxy or through multiple network modules.

interface-list: Ethernet port list. You can specify multiple Ethernet ports by providing this argument in the form of *interface-list* = { *interface-name* [**to** *interface- name*] & < 1-10 >. The *interface-name* argument is the port index of an Ethernet port and can be specified in this form: *interface-name* = { *interface-type interface-num* }, where *interface-type* specifies the type of a port and *interface-num* identifies the port number. "&<1-10>" means that up to 10 port indexes/port index lists can be provided.

Description Use the **dot1x supp-proxy-check** command to enable the checking and access control of the users who log in through a proxy.

Use the **undo dot1x supp-proxy-check** command to cancel the setting.

By default, supplicant proxy checking is disabled.

In system view, execution of the **dot1x supp-proxy-check** command enables the supplicant system proxy checking function for specified ports if the *interface-list* argument is provided; in Ethernet port view, the *interface-list* argument is not needed, only the current port can have the function.

In system view, after enabling global supplicant proxy checking, you also need to enable this function on specific ports for the function to take effect on these ports.

802.1x proxy checking checks for:

- Supplicant systems logging in through proxies
- Supplicant systems logging in through IE proxies
- Whether or not a supplicant system logs in through multiple network modules (that is, when supplicant system attempts to log in, it contains more than one active network modules)

A switch may take the following actions in response to any of the above three cases:

- Disconnects the supplicant system and sends Trap packets (using the **dot1x supp-proxy-check logoff** command.)
- Sends Trap packets without disconnecting the supplicant system (using the **dot1x supp-proxy-check trap** command.)

This function needs the support of 802.1x clients and CAMS:

- The 802.1x supplicant system must be able to detect whether the client uses multiple network modules, a proxy, or IE proxy;
- CAMS has disabled the use of multiple network modules, a proxy server, and an IE proxy server.

By default, an 802.1x supplicant system enables the use of multiple network modules, proxies, or IE proxies. If CAMS has these features disabled, it would notify the 802.1 supplicant system to have the corresponding features disabled as well after the latter has successfully passed the authentication.

- *The supplicant system proxy checking function needs the support of 3Com's 802.1x client program (V1.29 or later version).*
- *The supplicant system proxy checking function takes effect only after it has been enabled on CAMS and the client version checking function is enabled on the switch (using the* ***dot1x version-check*** *command).*

Related command: **display dot1x**.

Example # Configure to disconnect any supplicant system connected to Ethernet2/0/1 through Ethernet2/0/8 ports if it has been detected logging in through a proxy.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] dot1x supp-proxy-check logoff
[SW7750] dot1x supp-proxy-check logoff interface Ethernet 2/0/1 to Ethernet 2/0/8
```

# Configure the switch to send Trap packets if a supplicant system connected to Ethernet 2/0/9 port is detected logging in through a proxy.

```
[SW7750] dot1x supp-proxy-check trap
[SW7750] dot1x supp-proxy-check trap interface Ethernet 2/0/9
```

Or

```
[SW7750] dot1x supp-proxy-check trap
[SW7750] interface Ethernet 2/0/9
[SW7750-Ethernet2/0/9] dot1x supp-proxy-check trap
```

dot1x timer

Syntax **dot1x timer** { **handshake-period** *handshake-period-value* | **reauth-period** *reauth-period-value* | **quiet-period** *quiet-period-value* | **tx-period** *tx-period-value* | **supp-timeout** *supp-timeout-value* | **server-timeout** *server-timeout-value* | **ver-period** *ver-period-value* }

undo dot1x timer { **handshake-period** | **reauth-period** | **quiet-period** | **tx-period** | **supp-timeout** | **server-timeout** | **ver-period** }

View System view

Parameter **handshake-period**: Handshake period timer, triggered when the user has successfully passed the authentication. It sets the time interval for the switch to resend handshake request packets to check whether the user is still online. If, after N times (as specified by the **dot1x retry** command) of retries, the switch still has not received any response packet from the supplicant system, it will assume that the user is offline.

handshake-period-value: Value of the handshake timer, in seconds. This value can range from 1 to 1024 and defaults to 15.

reauth-period: Re-authentication period timer. Within this timer period, a supplicant system initializes 802.1x re-authentication.

reauth-period-value: Value (in seconds) of the re-authentication period timer. This value ranges from 1 to 86400 and defaults to 3600.

quiet-period: Quiet-period timer, triggered after the user has failed the authentication. After the time (as specified by the quiet-period timer) has elapsed, the user can resend the authentication request. During the period, the switch will perform no authentication.

quiet-period-value: Value of the quiet-period timer, in seconds. This value can range from 10 to 120 and defaults to 60.

tx-period: This timer sets the tx-period and is triggered by the switch in one of the following two cases: The first case is when the client requests for authentication. The switch sends a unicast request/identity packet to a supplicant system and then enables the transmission timer. The switch sends another request/identity packet to the supplicant system if the supplicant system fails to send a reply packet to the switch when this timer times out. The second case is when the switch authenticates the 802.1x client who does not request for authentication actively. The switch sends multicast request/identity packets continuously through the port enabled with 802.1x function, with the interval of tx-period.

tx-period-value: Value of the tx-period, in seconds. This value ranges from 10 to 120 and defaults to 30.

supp-timeout: Supplicant timeout timer, triggered when the switch sends a request/challenge packet (for MD5 ciphered text) to the supplicant system. If within the period, no response has been sent back from the supplicant system, the switch will resend the request/challenge packet.

supp-timeout-value: Time interval of the authentication timer, in seconds. This value can range from 10 to 120 with a default value of 30.

server-timeout: Server-timeout timer, if within the period, no response has been sent back from the Authentication server, the switch will resend the request/Identity packet.

server-timeout-value: Value of the server timeout timer, in seconds. This value can range from 100 to 300 with a default value of 100.

ver-period: Client-version-checking period timer, if within the period, no response packet has been sent back from the supplicant system, the switch will resend the client version checking request packet.

ver-period-value: Value of the client-version-checking period timer, in seconds. This value can range from 1 to 30 with a default value of 30.

Description

Use the **dot1x timer** command to set a specified 802.1x timer.

Use the **undo dot1x timer** command to resume the default value of a specified 802.1x timer.

During an 802.1x authentication process, multiple timers are triggered to ensure that the supplicant systems, the authenticator systems, and the Authentication servers interact with each other in an arranged way. To make authentications being processed in a desired way, you can use the **dot1x timer** command to set values for these timers as needed. This may be necessary in certain situations or for some tough network environments. Normally, the defaults are recommended. (Note that some timers cannot be adjusted.)

Related command: **display dot1x**.

Example

Set the server-timeout to 150 seconds.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] dot1x timer server-timeout 150
```

dot1x version-check

Syntax **dot1x version-check** [**interface** *interface-list*]

undo dot1x version-check [**interface** *interface-list*]

View System view, Ethernet port view

Parameter *interface-list*: Ethernet port list. You can specify multiple Ethernet ports by providing this argument in the form of *interface-list* = { *interface-name* [**to** *interface- name*] & < 1-10 >. The *interface-name* argument is the port index of an Ethernet port and can be specified in this form: *interface-name* = { *interface-type interface-num* }, where *interface-type* specifies the type of a port and *interface-num* identifies the port number. "&<1-10>" means that up to 10 port indexes/port index lists can be provided.

Description Use the **dot1x version-check** command to enable 802.1x client version checking for specified Ethernet ports.

Use the **undo dot1x version-check** command to disable 802.1x client version checking for specified Ethernet ports.

By default, 802.1x client version checking is disabled on all Ethernet ports.

In system view, execution of the **dot1x version-check** command enables the client version checking function for specified ports if the *interface-list* argument is specified, otherwise it enables the function globally. In Ethernet port view, only the current port can have their client version checking function enabled by executing this command and the *interface-list* argument is not needed.

Example # Configure Ethernet 2/0/1 port to check the version of the 802.1x client upon receiving authentication packets.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet 2/0/1
[SW7750-Ethernet2/0/1] dot1x version-check
```

reset dot1x statistics

Syntax **reset dot1x statistics** [**interface** *interface-list*]

View User view

Parameter *interface-list*: Ethernet port list. You can specify multiple Ethernet ports by providing this argument in the form of *interface-list* = { *interface-name* [**to** *interface- name*] & < 1-10 >. The *interface-name* argument is the port index of an Ethernet port and can be specified in this form: *interface-name* = { *interface-type interface-num* }, where *interface-type* specifies the type of a port and *interface-num* identifies the port number. "&<1-10>" means that up to 10 port indexes/port index lists can be provided.

Description Use the **reset dot1x statistics** command to clear 802.1x-related statistics.

Use this command to reset 802.1x-related statistics.

In this command:

If the *interface-list* argument is not specified, this command clears statistics globally and the 802.1x statistics on all ports. If the *interface-list* argument is specified, this command clears statistics on the ports specified by the argument.

Related command: **display dot1x**.

Example # Clear 802.1x-related statistics on Ethernet 2/0/1 port.

```
<SW7750> reset dot1x statistics interface Ethernet 2/0/1
```

44 HABP CONFIGURATION COMMANDS

display habp

Syntax **display habp**

View Any view

Parameter None

Description Use the **display habp** command to display HABP configuration and status information.

Example # Display HABP configuration and status information.

```
<SW7750> display habp
Global HABP information:
        HABP Mode: Server
        Sending HABP request packets every 20 seconds
        Bypass VLAN: 2
```

Table 99 Field descriptions of the **display habp** command

Field	Description
HABP Mode	Indicates the HABP mode of the switch. A switch can operate as an HABP server (displayed as Server) or an HABP client (displayed as Client).
Sending HABP request packets every 20 seconds	HABP request packets are sent once in every 20 seconds.
Bypass VLAN	Indicates the ID(s) of the VLAN(s) to which HABP request packets are sent

display habp table

Syntax **display habp table**

View Any view

Parameter None

Description Use the **display habp table** command to display the MAC address table maintained by HABP.

Example # Display the MAC address table maintained by HABP.

```
<SW7750> display habp table
MAC             Holdtime  Receive Port
001f-3c00-0030  53        Ethernet2/0/1
```

Table 100 Field descriptions of the **display habp table** command

Field	Description
MAC	MAC addresses listed in the HABP MAC address table.
Holdtime	Hold time of the entries in the HABP MAC address table. An address will be removed from the table if it has not been updated during the hold time.
Receive Port	The port from which a MAC address is learned

display habp traffic

Syntax **display habp traffic**

View Any view

Parameter None

Description Use the **display habp traffic** command to display statistics on HABP packets.

Example # Display statistics on HABP packets.

```
<SW7750> display habp traffic
HABP counters :
        Packets output: 0, Input: 0
        ID error: 0, Type error: 0, Version error: 0
        Sent failed: 0
```

Table 101 Field descriptions of the **display habp traffic** command

Field	Description
Packets output	Number of the HABP packets sent
Input	Number of the HABP packets received
ID error	Number of HABP packets with ID errors
Type error	Number of HABP packets with type errors
Version error	Number of HABP packets with version errors
Sent failed	Number of HABP packets that failed to be sent

habp enable

Syntax **habp enable**

undo habp enable

View System view

Parameter None

Description Use the **habp enable** command to enable HABP for a switch.

Use the **undo habp enable** command to disable HABP for a switch.

By default, HABP is enabled on a switch.

If an 802.1x-enabled switch does not have HABP enabled, it cannot manage the switches attached to it.

Example # Enable HABP.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] habp enable
```

habp server vlan

Syntax **habp server vlan** *vlan-id*

undo habp server

View System view

Parameter *vlan-id*: VLAN ID, ranging from 1 to 4,094.

Description Use the **habp server vlan** command to configure a switch to operate as an HABP server and HABP packets to be broadcast in specified VLAN.

Use the **undo habp server vlan** command to revert to the default HABP mode.

By default, a switch operates as an HABP client.

To specify a switch to operate as an HABP server, you need to enable HABP (using the **habp enable** command) for the switch first. Even if HABP is not enabled, the client can still configure the switch to work as an HABP client, although this has no effect.

Example # Specify the switch to operate as an HABP server and the HABP packets to be broadcast in VLAN 2.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] habp server vlan 2
```

habp timer

Syntax **habp timer** *interval*

undo habp timer

View System view

Parameter *interval*: Interval (in seconds) to send HABP request packets. This argument ranges from 5 to 600.

Description Use the **habp timer** command to set the interval for a switch to send HABP request packets.

Use the **undo habp timer** command to revert to the default interval.

The default interval for a switch to send HABP request packets is 20 seconds.

Use these two commands on switches operating as HABP servers only.

Example # Configure the switch to send HABP request packets once in every 50 seconds

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] habp timer 50
```

45 AAA CONFIGURATION COMMANDS

access-limit

Syntax

access-limit { **disable** | **enable** *max-user-number* }

undo access-limit

View

ISP domain view

Parameter

disable: Specifies not to limit the number of access users that can be contained in current ISP domain.

enable *max-user-number*: Specifies the maximum number of access users that can be contained in current ISP domain. The value of *max-user-number* ranges from 1 to 4120.

Description

Use the **access-limit** command to set the maximum number of access users that can be contained in current ISP domain.

Use the **undo access-limit** command to restore the default maximum number.

By default, the number of access users that can be contained in current ISP domain is unlimited.

Because resource contention may occur between access users, there is a need to properly limit the number of access users in an ISP domain to provide reliable performance to the users in the ISP domain.

Example

Allow ISP domain aabbcc.net to contain up to 500 access users.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] domain aabbcc.net
New Domain added.
[SW7750-isp-aabbcc.net] access-limit enable 500
```

attribute

Syntax

attribute { **ip** *ip-address* | **mac** *mac-address* | **idle-cut** *second* | **access-limit** *max-user-number* | **vlan** *vlan-id* | **location** { **nas-ip** *ip-address* **port** *port-number* | **port** *port-number* } }*

undo attribute { **ip** | **mac** | **idle-cut** | **access-limit** | **vlan** | **location** }*

View Local user view

Parameter **ip**: Sets the IP address to which the user is bound.

mac: Sets the MAC address to which the user is bound. *mac-address* is in dash-delimited hexadecimal notation, that is, in the *H-H-H* format.

idle-cut *second*: Allows/disallows the enabling of the idle-cut function by the local user (The data for idle-cut operation depends on the configuration in the ISP domain). The *second* argument is the idle time (in seconds) before cutting down. It ranges from 60 to 7200.

access-limit *max-user-number*: Sets the maximum number of users who can access the switch with current user name. The value of *max-user-number* ranges from 1 to 4096.

vlan *vlan-id*: Sets the VLAN to which the user is bound; that is, sets which VLAN the user belongs to. *vlan-id* is an integer ranging from 1 to 4094.

location: Sets the port binding attribute of the user.

nas-ip *ip-address*: Sets the permitted IP address of the network access server (RADIUS client) when the local device serves as the RADIUS sever. *ip-address* is in dotted decimal notation and is 127.0.0.1 (representing this device) by default.

port *port-number*: Sets the access limit on the specified port of the network access server when the local device serves as the RADIUS server. If this parameter is specified, the RADIUS sever accepts the authentication requests only from the specified port and drops those from other ports. *port-number* is in the format of "slot number subslot number port number". If the port has no subslot number, just input 0 for this item.

Description Use the **attribute** command to set the attributes of a local user.

Use the **undo attribute** command to cancel attribute settings of the local user.

Note that if the user is bound to a remote port, you must specify the **nas-ip** keyword. If the user is bound to a local port, you need not specify the nas-ip keyword.

If the accounting optional switch is turned on (with the ***accounting optional*** *command) in the ISP domain to which the local user belongs or the RADIUS scheme referenced by the ISP, you cannot limit the number of accesses by the local user. That is, the* ***attribute access-limit*** *command does not take effect.*

Related command: **display local-user**.

Example # Set the IP address of user1 to 10.110.50.1.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] local-user user1
[SW7750-luser-user1] attribute ip 10.110.50.1
```

accounting

Syntax

accounting { **none** | **radius-scheme** *radius-scheme-name* | **hwtacacs-scheme** *hwtacacs-scheme-name* }

undo accounting

View

ISP domain view

Parameter

none: Specifies not to perform user accounting.

radius-scheme *radius-scheme-name*: Name of a RADIUS scheme, a character string of up to 32 characters.

hwtacacs-scheme *hwtacacs-scheme-name*: Name of a HWTACACS scheme, a string of up to 32 characters.

Description

Use the **accounting** command to configure the accounting scheme that will be used by current ISP domain.

Use the **undo accounting** command to remove the accounting scheme used by current ISP domain.

By default, no accounting scheme is configured for the ISP domain.

When you use the **accounting** command to reference a RADIUS scheme or HWTACACS scheme for current ISP domain, the RADIUS scheme or HWTACACS scheme must have already been configured.

If the **accounting** command is used in ISP domain view, the system uses the scheme referenced in this command to charge the users. Or else, the system uses the scheme referenced in the **scheme** command to charge the users.

Related command:

scheme, **radius scheme**, **hwtacacs scheme**

Example

Specify "radius" as the RADIUS accounting scheme that will be referenced by current ISP domain.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] domain aabbcc.net
New Domain added.
[SW7750-isp-aabbcc.net] accounting radius-scheme radius
```

accounting optional

Syntax

accounting optional

undo accounting optional

View ISP domain view

Parameter None

Description Use the **accounting optional** command to open the accounting-optional switch.

Use the **undo accounting optional** command to close the accounting-optional switch.

By default, the accounting-optional switch is closed.

Note the following:

When the system charges an online user but it does not find any available RADIUS accounting server or fails to communicate with any RADIUS accounting server, the user can continue the access to network resources if the **accounting optional** command has been used; otherwise, the user is disconnected from the system. The **accounting optional** command is often used in the cases where only authentication is needed and no accounting is needed.

Example # Turn on the accounting-optional switch for the ISP domain named aabbcc.net.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] domain aabbcc.net
New Domain added.
[SW7750-isp-aabbcc.net] accounting optional
```

authentication

Syntax **authentication** { **radius-scheme** *radius-scheme-name* [**local**] | **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** | **none** }

undo authentication

View ISP domain view

Parameter **radius-scheme** *radius-scheme-name*: Specifies to use a RADIUS authentication scheme.

hwtacacs-scheme *hwtacacs-scheme-name*: Name of a HWTACACS scheme, a string of up to 32 characters.

local: Specifies to use local authentication scheme.

none: Specifies not to perform authentication.

Description Use the **authentication** command to configure an authentication scheme for current ISP domain.

Use the **undo authentication** command to restore the default authentication scheme of current domain.

By default, no separate authentication scheme is configured.

Before you use the **authentication** command to specify a RADIUS scheme to be referenced by current ISP domain, the RADIUS scheme must has already been configured.

If you execute the **authentication radius-scheme** *radius-scheme-name* **local** command, the **local** scheme is used as the secondary authentication scheme in case the RADIUS server does not respond normally. That is, if the communication between the switch and the RADIUS server is normal, no local authentication is performed; otherwise, local authentication is performed.

If you execute the **authentication hwtacacs-scheme** *hwtacacs-scheme-name* **local** command, the **local** scheme is used as the secondary authentication scheme in case the TACACS server does not respond normally. That is, if the communication between the switch and the TACACS server is normal, no local authentication is performed; otherwise, local authentication is performed.

If you execute the **authentication local** command, the local scheme is used as the primary scheme. In this case, only local authentication is performed. If you execute the **authentication none** command, no authentication is performed.

With the **authentication** command configured in an ISP domain view, the system adopts the authentication scheme referenced in the command to authenticate the users in the domain, or else it adopts the scheme referenced in the **scheme** command.

Related command: **scheme** and **radius scheme**, **hwtacacs scheme**.

Example # Specify "radius" as the RADIUS authentication scheme to be referenced by the ISP domain aabbcc.net.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] domain aabbcc.net
New Domain added.
[SW7750-isp-aabbcc.net] authentication radius-scheme radius
```

# Specify "rd" as the RADIUS authentication scheme to be referenced by the ISP domain aabbcc, and the local scheme as the secondary authentication scheme.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] domain aabbcc
New Domain added.
[SW7750-isp-aabbcc] authentication radius-scheme rd local
```

authorization

Syntax **authorization** { **none** | **hwtacacs-scheme** *hwtacacs-scheme-name* }

undo authorization

View ISP domain view

Parameter **none**: Specifies that no authentication scheme is to be adopted.

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies the name of a HWTACACS scheme, a string of up to 32 characters.

Description Use the **authorization** command to configure the authorization scheme of the current ISP domain.

Use the **undo authorization** command to restore the default authorization scheme of the ISP domain.

By default, no separate authorization scheme is configured.

Related command: **scheme** and **radius scheme**, **hwtacacs scheme**.

Example # Allow users in current ISP domain to access the network services without being authorized.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] domain aabbcc.net
New Domain added.
[SW7750-isp-aabbcc.net] authorization none
```

cut connection

Syntax **cut connection** { **all** | **access-type dot1x** | **domain** *domain-name* | **interface** *interface-type interface-number* | **ip** *ip-address* | **mac** *mac-address* | **radius-scheme** *radius-scheme-name* | **vlan** *vlan-id* | **ucibindex** *ucib-index* | **user-name** *user-name* }

View System view

Parameter **all**: Cuts down all user connections

access-type dot1x: Cuts down all 802.1x user connections.

domain *isp-name*: Cuts down all user connections in the specified ISP domain. *isp-name* is the name of an ISP domain. It is a character string of up to 24 characters. You can only specify an existing ISP domain.

interface *interface-type interface-number*: Cuts down all user connections to the specified port.

ip *ip-address*: Cuts down the connection of the user with the specified IP address.

mac *mac-address*: Cuts down the user connection with the specified MAC address. *mac-address* is in dash-delimited hexadecimal notation, that is, in the *H-H-H* format.

radius-scheme *radius-scheme-name*: Cuts down all user connections using the specified RADIUS scheme. *radius-scheme-name* is a character string of up to 32 characters.

vlan *vlan-id*: Cuts down all user connections of the specified VLAN. *vlan-id* ranges from 1 to 4094.

ucibindex *ucib-index*: Cuts down the user connection with the specified connection index. The value of *ucib-index* ranges from 0 to 4119.

user-name *user-name*: Cuts down the user connection of the specified user. *user-name* is a character string of up to 80 characters. The string cannot contain the following characters: /:*?<>. It can contain no more than one @ character. The pure user name (user ID, that is, the part before @) can contain no more than 55 characters.

Description Use the **cut connection** command to cut down one user connection or one type of user connections forcibly.

This command cuts down the connections of 802.1x users only.

Related command: **display connection**.

Example # Cut down all 802.1x user connections in the ISP domain named aabbcc.net.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] cut connection domain aabbcc.net
```

display connection

Syntax **display connection** [**access-type dot1x** | **domain** *domain-name* | **interface** *interface-type interface-number* | **ip** *ip-address* | **mac** *mac-address* | **radius-scheme** *radius-scheme-name* | **vlan** *vlan-id* | **ucibindex** *ucib-index* | **user-name** *user-name*]

View Any view

Parameter **access-type dot1x**: Displays all 802.1x user connections.

domain *isp-name*: Displays all user connections in the specified ISP domain. *isp-name* is the name of an ISP domain, a character string of up to 24 characters. You can only specify an existing ISP domain.

interface *interface-type interface-number*: Displays all user connections on the specified port.

ip *ip-address*: Displays all user connections with the specified IP address.

mac *mac-address*: Displays the connection of the user with the specified MAC address. *mac-address* is in dash-delimited hexadecimal notation (in the form of *H-H-H*).

radius-scheme *radius-scheme-name*: Displays all user connections using the specified RADIUS scheme. *radius-scheme-name* is a character string of up to 32 characters.

vlan *vlan-id*: Displays all user connections of the specified VLAN. The value of *vlan-id* ranges from 1 to 4094.

ucibindex *ucib-index*: Displays the user connection with the specified connection index.

user-name *user-name*: Displays the user connection with the specified user name. *user-name* is a character string of up to 32 characters. The string cannot contain the following characters: /:*?<>. It can contain no more than one @ character. The pure user name (user ID, that is, the part before @) can contain no more than 24 characters.

Description

Use the **display connection** command to display information about the specified user connection or all user connections, so as to troubleshoot user connections.

If you execute this command without specifying any argument, all user connections will be displayed.

This command displays information about the connections of 802.1x users only.

Related command:

cut connection.

Example

Display information about all 802.1x user connections.

```
<SW7750> display connection
Total 0 connections matched ,0 listed.
```

display domain

Syntax

display domain [*isp-name*]

View

Any view

Parameter

isp-name: Name of an ISP domain, a character string of up to 24 characters. This must be the name of an existing ISP domain.

Description

Use the **display domain** command to display the configuration information about one specific or all ISP domains.

If you execute this command without specifying any argument, the configuration of all ISP domains will be displayed.

The output information helps ISP domain diagnosis and troubleshooting

Related command: **access-limit**, **domain**, **radius-scheme**, user-template, **state**, **display domain**.

Example # Display the configuration information about all ISP domains.

```
<SW7750> display domain
0  Domain = system
   State = Active
   Scheme = LOCAL
   Access-limit = Disable
   Vlan-assignment-mode = Integer
   accounting-mode = time
   Domain User Template:
   Idle-cut = Disable
   Self-service = Disable
   Messenger Time = Disable

Default Domain Name: system
Total 1 domain(s).1 listed.
```

Table 102 Field descriptions of the **display domain** command

Field	Description
0 Domain	ISP domain index...Domain name
State	State
Scheme	AAA scheme: LOCAL (local authentication), NONE (no authentication), or RADIUS scheme name
Access-Limit	Limit on the number of access users
Vlan-assignment-mode	Dynamic VLAN assignment mode: integer or string
accounting-mode	Accounting mode: time (time-based accounting) and traffic (traffic-based accounting)
Domain User Template	Domain user template
Idle-cut	Sets the idle-cut function. Disable means the idle-cut function is disabled; enable means the function is enabled.
Self-service	URL of the self-service server. Disable means the self-service server location function is disabled. After the self-service server location function is enabled, the URL of the configured self-service server.
Messenger Time	State of the messenger time service. Disable means the messenger time service is disabled. After the messenger time service is configured, the time and interval of the prompt messages.

display local-user

Syntax **display local-user** [**domain** *isp-name* | **idle-cut** { **enable** | **disable** } | **service-type** { **telnet** | **ftp** | **ssh** | **terminal** | **lan-access** } | **state** { **active** | **block** } | **user-name** *user-name* | **vlan** *vlan-id*]

View Any view

Parameter

domain *isp-name*: Displays all local users belonging to the specified ISP domain. *isp-name* is the name of an ISP domain, a character string of up to 24 characters. You can only specify an existing ISP domain.

idle-cut: Displays the local users who are inhibited from enabling the idle-cut function, or the local users who are allowed to enable the idle-cut function. **disable** specifies the inhibited local users and **enable** specifies the allowed local users. This argument only applies to the users configured with lan-access service. For users configured with any other type of service, the **display local-user idle-cut enable** and **display local-user idle-cut disable** commands do not output any user information.

service-type: Displays the local users of the specified type. You can specify one of the following user types: **telnet**, **ftp**, **lan-access** (generally, this type of users are Ethernet access users, for example, 802.1x users), **ssh**, **terminal** (this type of users are terminal users who log into the switch through the Console port).

state { **active** | **block** }: Displays the local users in the specified state. **active** represents the users allowed to request network services, and **block** represents the users inhibited to request network services.

user-name *user-name*: Displays the local user who has the specified user name. *user-name* is a character string of up to 80 characters. The string cannot contain the following characters: /:*?<>. It can contain no more than one @ character. The pure user name (user ID, that is, the part before @) can contain no more than 55 characters.

vlan *vlan-id*: Displays the local users belonging to the specified VLAN. The value of *vlan-id* ranges from 1 to 4094.

Description

Use the **display local-user** command to display information about a specific or all local users, so as to troubleshoot local user configuration.

By default, this command displays the information about all local users.

Related command:

local-user, **service-type**.

Example

Display information about all local users.

```
<SW7750> display local-user
The contents of local user user1:
State:          Active            ServiceType Mask: T
 Idle-cut:       Disable
 Access-limit:   Disable           Current AccessNum: 0
 Bind location:  Disable
 Vlan ID:        Disable
 IP address:     Disable
 MAC address:    Disable
 User Privilege: 0

Total 1 local user(s) Matched, 1 listed.
```

Table 103 Field descriptions of the **display local-user** command

Field	Description
State	State of the local user
ServiceType Mask	Service type mark of local user: T: Telnet S: SSH C: Terminal service LM: lan-access F: FTP None: No service type is set.
Idle Cut	State of the idle-cut function
Access-Limit	Limit on the number of access users
Bind location	Whether or not bound to a port
VLAN ID	VLAN of the user
IP address	IP address of the user
MAC address	MAC address of the user
User Privilege	User privilege

domain

Syntax **domain** { *isp-name* | **default** { **disable** | **enable** *isp-name* } }

undo domain *isp-name*

View System view

Parameter *isp-name*: Name of a ISP domain, a character string of up to than 24 characters. This string cannot contain the following characters: /:*?<>.

default enable *isp-name*: Specifies the default ISP domain.

disable: Restores the default ISP domain to "system".

Description Use the **domain** command to create an ISP domain or enter the view of an existing ISP domain.

Use the **undo domain** command to delete a specified ISP domain.

The default ISP domain is "system".

An ISP domain is an ISP user group comprising the users of the same ISP. Normally, in a username (such as gw20010608@aabbcc.net) in the userid@isp-name format, isp-name (such as aabbcc.net in the above example) after "@" is the name of the ISP domain. When implementing access control, for ISP users with the name format userid@isp-name, a 3Com series Ethernet switch uses the userid as the username for authentication and uses "isp-name" for domain name.

ISP domains are intended to support a multi-ISP application environment where an access device may be accessed by users of different ISPs. The user attributes, such as username/password formation and service type/privilege, of ISP users may vary. Therefore, it is necessary to distinguish between them by setting ISP domains. You can configure a complete set of independent ISP domain attributes, including AAA schemes (such as the RADIUS scheme used), for each ISP domain in ISP domain view.

For the switch, each access user belongs to an ISP domain.

You can configure up to 16 ISP domains in the system. If the specified ISP domain does not exist when you issue this command, the system creates a new ISP domain. An ISP domain is active immediately after being created.

Related command: **access-limit**, **scheme**, **state**, **display domain**

Example # Create an ISP domain named aabbcc.net and enter its view.

```
[SW7750] domain aabbcc.net
New Domain added.
[SW7750-isp-aabbcc.net]
```

idle-cut

Syntax **dle-cut** { **disable** | **enable** *minute flow* }

View ISP domain view

Parameter **disable**: Inhibits users from enabling the idle-cut function.

enable: Allows users to enable the idle-cut function.

minute: Maximum idle time, ranging from 1 minute to 120 minutes.

flow: Minimum data flow, ranging from 1 byte to 10,240,000 bytes (10 M).

Description Use the **idle-cut** command to set the user idle-cut function in current ISP domain.

By default, this function is disabled.

A user template is a set of default user attributes. If a user requesting for a network service does not possess a required attribute, the attribute in a user template is used as the user's default attribute. If neither the user nor the RADIUS server specifies whether its idle-cut function is enabled, the idle-cut function state of the user template is specified as that of the user.

A user template applies to only one ISP domain. Therefore, you need to configure different user template attributes for users in different ISP domains.

Related command: **domain**.

Example

Allow users in ISP domain aabbcc.net to enable the idle-cut attribute in user template (that is, allow the user to use the idle-cut function), with the maximum idle time of 50 minutes and the minimum data flow of 500 bytes.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] domain aabbcc.net
New Domain added.
[SW7750-isp-aabbcc.net] idle-cut enable 50 500
```

level

Syntax

level *level*

undo level

View

Local user view

Parameter

level: Priority level of the user. It is an integer ranging from 0 to 3 and defaulting to 0.

Description

Use the **level** command to set the priority level of the user.

Use the **undo level** command to restore the default priority level of the user.

The commands that a user can access after login is determined by the priority level of the user and the level set on the user interface. If the two levels are different

- *The command level that a user passing AAA/RADIUS authentication can access is determined by the priority level of the user. For example, if the priority level of a user is 3 and the command level set on the VTY 0 user interface is 1, the user can access the commands under level 3 after logging in to the system from VTY 0.*
- *The command level that a user passing RSA authentication can access is determined by the level set on the user interface.*

Example

Set the level of user1 to 3.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] local-user user1
[SW7750-luser-user1] level 3
```

local-user

Syntax

local-user *user-name*

undo local-user { *user-name* | **all** [**service-type** { **telnet** | **ftp** | **lan-access** | **ssh** | **terminal** }] }

View

System view

Parameter *user-name*: Name of the local user, a character string of up to 80 characters. This string cannot contain the following characters: /:*?<>. It can contain no more than one @ character. The pure user name (user ID, that is, the part before @) cannot be longer than 55 characters. The local user name is case insensitive.

service-type: Specifies the local users of the specified type. You can specify one of the following user types: **telnet**, **ftp**, and **lan-access** (generally, this type of users are Ethernet access users, for example, 802.1x users), **ssh**, and **terminal** (this type of users are terminal users who log into the switch through the Console port).

all: Specifies all local users.

Description Use the **local-user** command to add a local user and enter local user view.

Use the **undo local-user** command to delete one or more specified local users.

By default, there is no local user in the system.

Related command: **display local-user** and **service-type**.

Example # Add a local user named user1.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] local-user user1
[SW7750-luser-user1]
```

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**: Adopts the forcible cipher mode so that the passwords of all local users must be displayed in cipher text.

auto: Adopts the automatic mode so that the passwords of local users are displayed in the modes set with the **password** command.

Description Use the **local-user password-display-mode** command to set the password display mode of all local users

Use the **undo local-user password-display-mode** command to restore the default password display mode of all local users.

When the **cipher-force** mode is adopted, all passwords will be displayed in cipher text even through some users have specified to display their passwords in plain text by using the **password** command with the **simple** keyword.

By default, the password display mode of all access users is **auto**.

Related command: **display local-user** and **password**.

Example # Specify to display all local user passwords in cipher text forcibly.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] local-user password-display-mode cipher-force
```

messenger

Syntax **messenger time** { **enable** *limit interval* | **disable** }

undo messenger time

View ISP domain view

Parameter *limit*: Time limit in minutes, ranging from 1 to 60. The switch will send prompt messages at regular intervals to users whose remaining online time is less than this limit.

interval: Interval to send prompt messages (in minutes). This argument ranges from 5 to 60 and must be a multiple of 5.

Description Use the **messenger time enable** command to enable the messenger function and set the related parameters.

Use the **messenger time disable** command to disable the messenger function.

Use the **undo messenger time** command to restore the messenger function to its default state.

By default, the messenger function is disabled on the switch.

The purpose of this function is to remind online users of their remaining online time through clients in the form of message dialog.

You can use **messenger time enable** command to set a remaining online time limit and the interval to send prompt messages. After that, the switch regularly sends prompt messages at the set interval to the clients of the users whose remaining online time is less than the set limit, and the clients inform the users of their remaining online time in the form of message dialog.

Example # Enable the switch to send prompt messages at intervals of 5 minutes to users after their remaining online time is less than 30 minutes.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] domain system
New Domain added.
[SW7750-isp-system] messenger time enable 30 5
```

name

Syntax **name** *string*

undo name

View VLAN view

Parameter *string*: VLAN Name for VLAN assignment, a character string of up to 32 characters.

Description Use the **name** command to set a VLAN name, which will be used for VLAN assignment.

Use the **undo name** command to cancel the VLAN name.

By default, an VLAN uses its VLAN ID (like VLAN 0001) as its name.

This command is used for the dynamic VLAN assignment function. For details about this function, refer to the **vlan-assignment-mode** command.

Related command: **dot1x guest-vlan** and **vlan-assignment-mode**.

Example # Set the name of VLAN 100 to test.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] vlan 100
[SW7750-vlan100] name test
```

password

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

undo password

View Local user view

Parameter **simple**: Specifies to display the password in plain text.

cipher: Specifies to display the password in cipher text.

password: Password you want to set, a character string.

- For **simple** mode, the password must be in plain text.
- For **cipher** mode, the password can be either in cipher text or in plain text, depending on your input.

A password in plain text can be a string with of up to 16 consecutive characters, for example, user918. A password in cipher text can be 24 characters in length, for example, _(TT8F]Y5SQ=^Q'MAF4<1!!.

Description Use the **password** command to set a password for the local user.

Use the **undo password** command to cancel the password configured.

Note that, after the **local-user password-display-mode cipher-force** command is executed, the password will be displayed in cipher text even though you use the **password** command to set the password to be displayed in plain text, that is, in the **simple** mode.

Related command: **display local-user**.

Example # Set the password of a user named user1 to 20030422 and specify to display the password in plain text.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] local-user user1
[SW7750-luser-user1] password simple 20030422
```

radius-scheme

Syntax **radius-scheme** *radius-scheme-name*

View ISP domain view

Parameter *radius-scheme-name*: Name of a RADIUS scheme, a character string of up to 32 characters.

Description Use the **radius-scheme** command to specify the RADIUS scheme to be used by current ISP domain.

Once an ISP domain is created, it uses the local AAA scheme instead of any RADIUS scheme by default.

The RADIUS scheme you specified in the **radius-scheme** command must be an existing scheme. This command is equivalent to the **scheme radius-scheme** command.

Related command: **radius scheme**, **display radius**.

Example # Specify the scheme "radius1" as the RADIUS scheme to be used by current ISP domain "aabbcc.net".

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] domain aabbcc.net
```

```
New Domain added.
[SW7750-isp-aabbcc.net] radius-scheme radius1
```

scheme

Syntax **scheme** { **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] | **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] }

undo scheme { **none** | **radius-scheme** | **hwtacacs-scheme** }

View ISP domain view

Parameter *radius-scheme-name*: RADIUS scheme name, a string of up to 32 characters.

hwtacacs-scheme-name: HWTACACS scheme name, a string of up to 32 characters.

local: Specifies to use local authentication.

none: Specifies not to perform authentication.

Description Use the **scheme** command to specify the AAA scheme used by current ISP domain.

Use the **undo scheme** command to restore the default AAA scheme used by the ISP domain.

By default, the ISP domain uses the **local** AAA scheme.

Note the following:

- *The* ***scheme*** *command is used to specify a RADIUS scheme to be used by the current ISP domain. Make sure you specify an existing RADIUS scheme.*
- *If you execute the* ***scheme radius-scheme*** radius-scheme-name ***local*** *command, the local scheme becomes the secondary scheme in case the RADIUS server does not response normally. That is, if the communication between the switch and the RADIUS server is normal, no local authentication is performed; otherwise, local authentication is performed.*
- *If you execute the* ***scheme hwtacacs-scheme*** hwtacacs-scheme-name ***local*** *command, the local scheme becomes the secondary scheme in case the TACACS server does not response normally. That is, if the communication between the switch and the TACACS server is normal, no local authentication is performed; otherwise, local authentication is performed.*
- *If the primary scheme is specified as* ***local*** *or* ***none****, the system uses local authentication only or performs no authentication; no RADIUS scheme can be used at the same time.*

Related command: **radius scheme** and **display radius**

Example # Specify the RADIUS scheme "radius1" as the AAA scheme referenced by the ISP domain "aabbcc.net".

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] domain aabbcc.net
New Domain added.
[SW7750-isp-aabbcc.net] scheme radius-scheme radius1
```

self-service-url

Syntax **self-service-url enable** *url-string*

self-service-url disable

View ISP domain view

Parameter *url-string*: URL of the web page used to modify user password on the self-service server. It is a character string with 1 character to 64 characters. This string cannot contain a question mark "?". If the actual URL of the self-service server contains any question mark, you should change it to an elect bar "|".

Description Use the **self-service-url enable** command to enable the self-service server location function

Use the **self-service-url disable** command to disable the self-service server location function

By default, this function is disabled.

This command must be used with the cooperation of a self-service-supported RADIUS server (such as CAMS). Through self-service, users can manage and control their accounts or module numbers by themselves. A server installed with the self-service software is called a self-service server.

After this command is executed on the switch, users can locate the self-service server through the following operation:

- Choose [change user password] on the 802.1x client.
- The client opens the default browser (for example, IE or Netscape) and locates the specified URL page used to change user password on the self-service server.
- Then, the user can change the password.

A user can choose the [change user password] option on the client only after passing the authentication. If the user fails the authentication, this option is in grey and is unavailable.

Example # Under the default ISP domain "system", set the URL of the web page used to modify user password on the self-service server to http://10.153.89.94/selfservice/modPasswd1x.jsp|userName.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
```

```
[SW7750] domain system
[SW7750-isp-system] self-service-url enable http://10.153.89.94/selfservice/modPasswd1x.jsp|us
erName
```

service-type

Syntax **service-type** { **ftp** [**ftp-directory** *directory*] | **lan-access** | { **ssh** | **telnet** | **terminal** }* [**level** *level*] }

undo service-type { **ftp** [**ftp-directory**] | **lan-access** | { **ssh** | **telnet** | **terminal** }* }

View Local user view

Parameter **ftp**: Specifies that this is a ftp user.

ftp-directory *directory*: Specifies the path for FTP users. *directory* is a string of up to 64 characters.

lan-access: Specifies that this is a LAN access user (who is generally an Ethernet access user, for example, 802.1x user).

ssh: Specifies that this is an ssh user.

telnet: Specifies that this is a Telnet user.

terminal: Authorizes the user to access the terminal service (that is, allows the user to log into the switch through the Console port).

level *level*: Specifies the level of the Telnet, terminal or SSH user. Where, *level* is an integer ranging from 0 to 3 and defaulting to 0.

Description Use the **service-type** command to authorize the user to access the specified type(s) of service(s).

Use the **undo service-type** command to inhibit the user from accessing the specified type(s) of service(s).

By default, the user is inhibited from accessing any type of service.

Example # Authorize user1 to access the lan-access service.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] local-user user1
[SW7750-luser-user1] service-type lan-access
```

state

Syntax **state** { **active** | **block** }

View ISP domain view or local user view

Parameter **active**: Activates the current ISP domain (in ISP domain view) or current user (in local user view), to allow users in current ISP domain or current user to access the network.

block: Hangs up the current ISP domain (in ISP domain view) or current user (in local user view), to inhibit users in current ISP domain or current user from accessing the network.

Description Use the **state** command to set the status of current ISP domain or the status of the local user.

By default, an ISP domain is in the **active** state once it is created (in ISP domain view), and a local user is in the **active** state once the user is created (in local user view).

In ISP domain view, each ISP domain can be in one of two states: **active** and **block**. Users in an **active** ISP domain are allowed to access the network. After an ISP domain is set to the **block** state, except the online users, the users under this domain are not allowed to access the network.

Related command: **domain**.

Example # Set the ISP domain aabbcc.net to the block state, so that all its offline users cannot access the network.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] domain aabbcc.net
New Domain added.
[SW7750-isp-aabbcc.net] state block
```

# Set user1 to the block state.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] local-user user1
[SW7750-luser-user1] state block
```

vlan-assignment-mode

Syntax **vlan-assignment-mode** { **integer** | **string** }

View ISP domain name

Parameter **integer**: Sets the VLAN assignment mode to integer.

string: Sets the VLAN assignment mode to string.

Description Use the **vlan-assignment-mode** command to set the VLAN assignment mode (integer or string) on the switch.

By default, the VLAN assignment mode is integer, that is, the switch supports its RADIUS authentication server to assign integer VLAN IDs.

The dynamic VLAN assignment feature enables a switch to dynamically add the ports of the successfully authenticated users to different VLANs according to the attributes assigned by the RADIUS server, so as to control the network resources that different users can access. In actual applications, to use this feature together with Guest VLAN, you should better set port control to port-based mode.

Currently, the switch supports the RADIUS authentication server to assign the following two types of VLAN IDs: integer and string.

- Integer: If the RADIUS server assigns integer type of VLAN IDs, you can set the VLAN assignment mode to integer on the switch (this is also the default mode on the switch). Then, upon receiving an integer ID assigned by the RADIUS authentication server, the switch adds the port to the VLAN whose VLAN ID is equal to the assigned integer ID. If no such a VLAN exists, the switch first creates a VLAN with the assigned ID, and then adds the port to the newly created VLAN.
- String: If the RADIUS server assigns string type of VLAN IDs, you can set the VLAN assignment mode to string on the switch. Then, upon receiving a string ID assigned by the RADIUS authentication server, the switch compares the ID with existing VLAN names on the switch. If it finds a match, it adds the port to the corresponding VLAN. Otherwise, the VLAN assignment fails and the user cannot pass the authentication.

The two dynamic VLAN assignment modes, integer and string, supported by the switch are set according to the authentication server. Different authentication servers adopt different dynamic VLAN assignment modes, you are recommended to configure the device according to the dynamic VLAN assignment mode in use.

Table 104 lists some common dynamic VLAN assignment modes.

Table 104 Common dynamic VLAN assignment modes

Server type	Dynamic VLAN assignment mode
CAMS	Integer (the latest version is determined by the attribute)
ACS	String
FreeRADIUS	Determined by the attribute (100 is integer; "100" is string)
Shiva Access Manager	String
Steel-Belted Radius Administrator	String

CAUTION:

- *You are recommended to configure the VLAN assignment mode for the switch the same as that of the assignment attribute value of the RADIUS authentication server. Configure the correct assignment mode with the* ***vlan-assignment-mode*** *command so that the switch correctly identifies the dynamic VLAN assigned by the server. If the assignment modes are different, the expected configuration may not take effect.*

- *In string mode, the VLAN to be assigned must exist on the switch and must have been configured with a VLAN name. This is not required in integer mode.*
- *In string mode, if the VLAN ID assigned by the RADIUS server is a character string containing only digits (for example, 1024), the switch first regards it as an integer VLAN ID: the switch transforms the string to an integer value and judges if the value is in the valid VLAN ID range; if it is, the switch adds the authenticated port to the VLAN with the value as the VLAN ID (VLAN 1024, for example).*

Related command: **name**, **dot1x guest-vlan**

Example # Set the VLAN assignment mode to string.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] domain aabbcc.net
New Domain added.
[SW7750-isp-aabbcc.net] vlan-assignment-mode string
```

46 RADIUS CONFIGURATION COMMANDS

accounting-on enable

Syntax

accounting-on enable [**send** *times* | **interval** *interval*]

undo accounting-on { **enable** | **send** | **interval** }

View

RADIUS scheme view

Parameter

times: Maximum number of attempts to send Accounting-On packets, ranging from 1 to 256 and defaulting to 40.

interval: Interval to send Accounting-On packets, ranging from 1 to 30 and defaulting to 3 seconds.

Description

Use the **accounting-on enable** command to enable the user re-authentication upon device restart function.

Use the **undo accounting-on enable** command to disable the user re-authentication upon device restart function and restore the default interval and maximum number of attempts to transmit Accounting-On packets.

Use the **undo accounting-on send** command to restore the default maximum number of attempts to transmit Accounting-On packets.

Use the **undo accounting-on interval** command to restore the default interval to transmit Accounting-On packets.

By default, this function is disabled.

The purpose of this function is to resolve this problem: users cannot re-log into the switch after the switch restarts because they are already online. After this function is enabled, every time the switch restarts:

- The switch generates an Accounting-On packet, which mainly contains the following information: NAS-ID, NAS-IP address (source IP address), and session ID.
- The switch sends the Accounting-On packet to CAMS at regular intervals.
- Once the CAMS receives the Accounting-On packet, it sends a response to the switch. At the same time it finds and deletes the original online information of the users who accessed the network through the switch before the restart according to the information contained in this packet (NAS-ID, NAS-IP address

and session ID), and ends the accounting of the users based on the last accounting update packet.

- Once the switch receives the response from the CAMS, it stops sending other Accounting-On packets.
- If the switch does not receives any response from the CAMS after the times it transmit Accounting-On packet reaches the configured maximum times, it does not send any more Accounting-On packets.

The switch can automatically generate the main attributes (NAS-ID, NAS-IP address and session ID) in the Accounting-On packets. However, you can also manually configure the NAS-IP address with the ***nas-ip*** *command. If you choose to manually configure this attribute, be sure to configure an appropriate and legal IP address. If this attribute is not configured, the switch will automatically use the IP address of the VLAN interface as the NAS-IP address.*

Related command: **nas-ip**.

Example # Enable the user re-authentication upon device restart function for the RADIUS scheme named CAMS.

```
<SW7750> system-view
[SW7750] radius scheme CAMS
[SW7750-radius-CAMS] accounting-on enable
```

accounting optional

Syntax **accounting optional**

undo accounting optional

View RADIUS scheme view/ISP domain view

Parameter None

Description Use the **accounting optional** command to open the accounting-optional switch.

Use the **undo accounting optional** command to close the accounting-optional switch so that users are charged forcibly.

By default, once an ISP domain is created, the accounting-optional switch is closed.

Note that:

- *When the system charges an online user but it does not find any available RADIUS accounting server or fails to communicate with any RADIUS accounting server, the user can continue the access to network resources if the* ***accounting optional*** *command has been used.*

- *After the **accounting optional** command is used for a RADIUS scheme, the system will no longer send real-time accounting update packets and stop-accounting packets for any user who adopts the RADIUS scheme.*
- *This configuration takes effect only on the accounting using this RADIUS scheme.*

Example # Execute the accounting-optional command for the RADIUS scheme CAMS.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] radius scheme CAMS
[SW7750-radius-cams] accounting optional
```

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

View RADIUS scheme view

Parameter **data**: Sets the unit of measure for data.

byte: Specifies to measure data in bytes.

giga-byte: Specifies to measure data in gigabytes.

kilo-byte: Specifies to measure data in kilobytes.

mega-byte: Specifies to measure data in megabytes.

packet: Sets the unit of measure for packets.

giga-packet: Specifies to measure packets in giga-packets.

kilo-packet: Specifies to measure packets in kilo-packets.

mega-packet: Specifies to measure packets in mega-packets.

one-packet: Specifies to measure packets in packets.

Description Use the **data-flow-format** command to set the units of measure for data flows sent to RADIUS servers.

Use the **undo data-flow-format** command to restore the default units of measure.

By default, the unit of measure for data is byte and that for packets is one-packet.

Related command: **display radius**.

Example # Specify to measure data and packets in data flows sent to RADIUS server in kilobytes and kilo-packets respectively.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] radius scheme radius1
[SW7750-radius-radius1] data-flow-format data kilo-byte packet kilo-packet
```

display local-server statistics

Syntax **display local-server statistics**

View Any view

Parameter None

Description Use the **display local-server statistics** command to display the statistics about all local RADIUS authentication servers.

Related command: **local-server**.

Example # Display the statistics about local RADIUS authentication server.

```
<SW7750> display local-server statistics
The localserver packet statistics:
Receive:                     30         Send:                       30
Discard:                     0          Receive Packet Error:       0
Auth Receive:                10        Auth Send:                   10
Acct Receive:                20        Acct Send:                   20
```

display radius

Syntax **display radius** [*radius-scheme-name*]

View Any view

Parameter *radius-scheme-name*: Name of a RADIUS scheme, a character string of up to 32 characters. If this argument is not specified, this command displays the configuration information about all RADIUS schemes.

Description Use the **display radius** command to display the configuration information about one specific or all RADIUS schemes.

By default, this command displays the configuration information about all RADIUS schemes.

Related command: **radius scheme**.

Example # Display the configuration information about all RADIUS schemes.

```
<SW7750> display radius
------------------------------------------------------------------
SchemeName  =system                             Index=0    Type=extended
Primary Auth IP  =127.0.0.1        Port=1645   State=active
Primary Acct IP  =127.0.0.1        Port=1646   State=active
Second  Auth IP  =0.0.0.0          Port=1812   State=block
Second  Acct IP  =0.0.0.0          Port=1813   State=block
Auth Server Encryption Key= Not configured
Acct Server Encryption Key= Not configured
Accounting method = required
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
Source-IP-address                               =0.0.0.0
Quiet-interval(min)                             =5
Username format                                 =without-domain
Data flow unit                                  =Byte
Packet unit                                     =1

------------------------------------------------------------------
Total 1 RADIUS scheme(s). 1 listed
```

Table 105 Field descriptions of the **display radius** command

Field	Description
SchemeName	Name of the RADIUS scheme
Index	Index number of the RADIUS scheme
Type	Type of the RADIUS servers
Primary Auth IP/ Port/ State	IP address/access port number/state of the primary authentication server
Primary Acct IP/ Port/ State	IP address/access port number/state of the primary accounting server
Second Auth IP/ Port/ State	IP address/access port number/state of the secondary authentication server
Second Acct IP/ Port/ State	IP address/access port number/state of the secondary accounting server
Auth Server Encryption Key	Login password for the authentication servers
Acct Server Encryption Key	Login password for the accounting servers
TimeOutValue (seconds)	RADIUS server response timeout time
RetryTimes	Maximum number of transmission attempts
Permitted send realtime PKT failed counts	Maximum allowed number of continuous no-response real-time accounting requests
Retry sending times of non-response acct-stop-PKT	Maximum number of transmission attempts of the buffered stop-accounting requests
Username format	User name format
Data flow unit	Unit of measure for data in data flows
Packet unit	Unit of measure for packets

display radius statistics

Syntax

display radius statistics

View

Any view

Parameter None

Description Use the **display radius statistics** command to display the statistics about RADIUS packets, so as to troubleshoot RADIUS configuration.

Related command: **radius scheme**.

Example # Display the statistics about RADIUS packets.

```
<SW7750> 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

Received and Sent packets statistic:
Sent PKT total  :0        Received PKT total:0
RADIUS received packets statistic:
Code= 2,Num=0       ,Err=0
Code= 3,Num=0       ,Err=0
Code= 5,Num=0       ,Err=0
Code=11,Num=0       ,Err=0

Running statistic:
RADIUS received messages statistic:
Normal auth request             , Num=0       , Err=0       , Succ=0
EAP auth request                , Num=0       , Err=0       , Succ=0
Account request                 , Num=0       , Err=0       , Succ=0
Account off request             , Num=0       , Err=0       , Succ=0
PKT auth timeout                , Num=0       , Err=0       , Succ=0
PKT acct_timeout                , Num=0       , Err=0       , Succ=0
(The following display is omitted.)
```

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-scheme-name*: Displays the buffered stop-accounting requests of the specified RADIUS scheme. Where, *radius-scheme-name* is a character string of up to 32 characters.

session-id *session-id*: Displays the buffered stop-accounting requests of the specified session ID. Where, *session-id* is a character string of up to 50 characters.

time-range *start-time stop-time*: Displays the buffered stop-accounting requests in the specified request time range. Where, *start-time* is the start time of the request time range, *stop-time* is the end time of the request time range, and both are in the format hh:mm:ss-mm/dd/yyyy or hh:mm:ss-yyyy/mm/dd. With this argument specified, this command displays the buffered stop-accounting requests from the start time to the end time.

user-name *user-name*: Displays the buffered stop-accounting requests of the specified user. Where, *user-name* is a character string of up to 32 characters.

Description Use the **display stop-accounting-buffer** command to display the no-response stop-accounting request packets buffered in the switch.

- You can choose to display the buffered stop-accounting packets of a specified RADIUS scheme, session ID, or user name. You can also specify a time range to display those which are sent within the specified time range. The displayed packet information helps you to diagnose and resolve problems relevant to RADIUS.
- When the switch sends out a stop-accounting packet but gets no response from the RADIUS server, it first buffers the packet and then retransmits it until the maximum number of retransmission attempts (set by the **retry stop-accounting** command) is reached.

Related command: **reset stop-accounting-buffer**, **stop-accounting-buffer enable** and **retry stop-accounting**.

Example # Display the buffered stop-accounting requests from 0:0:0 08/31/2003 to 23:59:59 08/31/2003.

```
<SW7750> display stop-accounting-buffer time-range 0:0:0-2003/08/31 23:59:59-2003/08/31
Total find    0 record
```

key

Syntax **key** { **accounting** | **authentication** } *string*

undo key { **accounting** | **authentication** }

View RADIUS scheme view

Parameter **accounting**: Sets a shared key for the RADIUS accounting packets.

authentication: Sets a shared key for the RADIUS authentication/authorization packets.

string: Shared key, a string of up to 16 characters.

Description Use the **key** command to set a shared key for the RADIUS authentication/authorization packets or accounting packets.

Use the **undo key** command to restore the corresponding default shared key.

By default, no shared key is configured.

The RADIUS client (that is, the switch) and server adopt MD5 algorithm to encrypt the RADIUS packets exchanged with each other. The two parties verify the validity of the exchanged packets by using the encrypted keys that have been set on them, and can accept and respond to the packets sent from each other only if both of them have the same encrypted keys. If the authentication/authorization server and the accounting server are two separate devices and the two servers have different encrypted keys, you must set the encrypted keys for authentication/authorization packets and accounting packets respectively on the switch.

Related command: **primary accounting**, **primary authentication**, and **radius scheme**.

Example # Set the encrypted key for the RADIUS authentication/authorization packets in RADIUS scheme radius1 to hello.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] radius scheme radius1
[SW7750-radius-radius1] key authentication hello
```

# Set the encrypted key for the RADIUS accounting packets in RADIUS scheme radius1 to ok.

```
[SW7750-radius-radius1] key accounting ok
```

local-server

Syntax **local-server nas-ip** *ip-address* [**key** *password*]

undo local-server nas-ip *ip-address*

View System view

Parameter **nas-ip** *ip-address*: Specifies the NAS-IP address of the local RADIUS server. Where, *ip-address* is in dotted decimal notation.

key *password*: Specifies the shared key of the authentication server and access server. Where, *password* is a character string of up to 16 characters.

Description Use the **local-server** command to create a local RADIUS authentication server (that is, set the related parameters of the server).

Use the **undo local-server** command to delete the specified local RADIUS authentication server.

By default, a local RADIUS authentication server is used, whose default NAS-IP is 127.0.0.1. That is, the local device serves as a RADIUS authentication server and a network access server, and all authentications are performed locally.

Note that:

- *The switch not only supports the traditional RADIUS client service to accomplish user AAA management through foreign authentication/authorization server and accounting server, but also provides a* *simple local RADIUS server function for authentication and authorization. This function is called local RADIUS authentication server function.*

- *When you use the local RADIUS authentication server function, the UDP port number for the authentication/authorization service must be 1645, the UDP port number for the accounting service is 1646.*
- *The packet encryption key set by the* ***local-server*** *command with the* ***key*** *password parameter must be identical with the authentication/authorization packet encryption key set by the* ***key authentication*** *command in RADIUS scheme view.*
- *The switch supports at most 16 IP addresses and shared keys of the network access server (including the default local RADIUS authentication server); that is, when the switch serves as a RADIUS authentication server, it can support at most 16 network access servers simultaneously to provide authentication.*
- *As a local RADIUS authentication server, the switch does not support EAP authentication.*

Related command: **radius scheme** and **state**.

Example # Create a network access server granted by the RADIUS authentication server with an IP address of 10.110.1.2 and a shared key of aabbcc.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] local-server nas-ip 10.110.1.2 key aabbcc
```

nas-ip

Syntax **nas-ip** *ip-address*

undo nas-ip

View RADIUS scheme view

Parameter *ip-address*: Source IP address for RADIUS packets, an IP address of this device. This address can neither be the all zero address nor be a Class-D address.

Description Use the **nas-ip** command to set the source IP address used by the switch to send RADIUS packets.

Use the **undo nas-ip** command to remove the source IP address setting.

The ***nas-ip*** *command in RADIUS scheme view has the same function as the* ***radius nas-ip*** *command in system view; and the priority of configuration in RADIUS scheme view is higher than in system view.*

You can specify the source address used to send RADIUS packets to prevent the unreachability of the packets returned from the server due to physical interface trouble. It is recommended to use the loopback interface address as the source IP address.

By default, the IP address of the outbound interface is used as the source IP address of the packet.

Related command: **display radius** and **radius nas-ip**.

Example # Set the source IP address used by the switch to send the RADIUS packets to 10.1.1.1.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] radius scheme test1
[SW7750-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 notation.

port-number: UDP port number, ranging from 1 to 65535.

Description Use the **primary accounting** command to set the IP address and port number of the primary RADIUS accounting server.

Use the **undo primary accounting** command to restore the default IP address and port number of the primary RADIUS accounting server.

The IP address and UDP port number of the primary accounting server used by the default RADIUS scheme "system" are 127.0.0.1 and 1646. The IP address and the UDP port number of the primary accounting server used by a newly created RADIUS scheme are 0.0.0.0 and 1813.

After creating a new RADIUS scheme, you should configure the IP address and UDP port number of each RADIUS server you want to use in this scheme. These RADIUS servers fall into two types: authentication/authorization, and accounting. And for each kind of server, you can configure two servers in a RADIUS scheme: primary and secondary servers.

In an actual network environment, you can configure the above parameters as required. But you should configure at least one authentication/authorization server and one accounting server. At the same time, you should keep the RADIUS service port settings on the switch consistent with those on the RADIUS servers.

Related command: **key**, **radius scheme** and **state**.

Example # Set the IP address and UDP port number of the primary accounting server of the RADIUS scheme radius1 to 10.110.1.2 and 1813.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] radius scheme radius1
[SW7750-radius-radius1] 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 notation.

port-number: UDP port number, ranging from 1 to 65535.

Description Use the **primary authentication** command to set the IP address and port number of the primary RADIUS authentication/authorization server.

Use the **undo primary authentication** command to restore the default IP address and port number of the primary RADIUS authentication/authorization server.

The IP address and UDP port number of the primary authentication server used by the default RADIUS scheme "system" are 127.0.0.1 and 1645. The IP address and UDP port number of the secondary authentication server is 0.0.0.0 and 1812. The IP address and the UDP port number of the primary/secondary authentication server used by a newly created RADIUS scheme are 0.0.0.0 and 1812.

After creating a new RADIUS scheme, you should configure the IP address and UDP port number of each RADIUS server you want to use in this scheme. These RADIUS servers fall into two types: authentication/authorization, and accounting. And for each kind of server, you can configure two servers in a RADIUS scheme: primary and secondary servers.

In an actual network environment, you can configure the above parameters as required. But you should configure at least one authentication/authorization server and one accounting server. At the same time, you should keep the RADIUS service port settings on the switch consistent with those on the RADIUS servers.

Related command: **key**, **radius scheme** and **state**.

Example # Set the IP address and UDP port number of the primary authentication/authorization server used by the RADIUS scheme radius1 to 10.110.1.1 and 1812.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] radius scheme radius1
[SW7750-radius-radius1] primary authentication 10.110.1.1 1812
```

radius nas-ip

Syntax **radius nas-ip** *ip-address*

undo radius nas-ip

View System view

Parameter *ip-address*: Source IP address, in dotted decimal notation.

Description Use the **radius nas-ip** command to set the source address used by the NAS to send RADIUS packets.

Use the **undo radius nas-ip** command to restore the default setting.

By default, no source address is specified, and the address of the outbound interface is used as the source address of the packet.

*The **nas-ip** command in RADIUS scheme view has the same function as the **radius nas-ip** command in system view; and the priority of configuration in RADIUS scheme view is higher than in system view.*

Note that:

- *You can specify the source IP address used to send RADIUS packet to prevent the unreachability of the packets returned from the server due to physical interface trouble. It is recommended to use the loopback interface address as the source IP address.*
- *You can specify only one source IP address by using this command. When you use this command again, the newly specified source IP address will overwrite the old one.*

Related command: **nas-ip**.

Example # Set the source address used by the switch to send the RADIUS packets to 129.10.10.1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] radius nas-ip 129.10.10.1
```

radius scheme

Syntax **radius scheme** *radius-scheme-name*

undo radius scheme *radius-scheme-name*

View System view

Parameter *radius-scheme-name*: Name of the RADIUS scheme, a character string of up to 32 characters.

Description Use the **radius scheme** command to create a RADIUS scheme and enter its view.

Use the **undo radius scheme** command to delete the specified RADIUS scheme.

By default, a RADIUS scheme named "system" has already been created in the system. All attributes of the scheme take the default values.

The RADIUS protocol configuration is performed on a RADIUS scheme basis. For each RADIUS scheme, you should specify at least the IP addresses and UDP port numbers of the RADIUS authentication/authorization and accounting servers, and the parameters required for the RADIUS client (that is, the switch) to interact with the RADIUS servers. Therefore, you should first create a RADIUS scheme and enter its view before performing other RADIUS protocol configurations.

A RADIUS scheme can be referenced by multiple ISP domains simultaneously. You can configure up to 16 RADIUS schemes, including the default scheme "system".

The **undo radius scheme** command cannot be used to delete the default RADIUS scheme. Note that you cannot delete a RADIUS scheme which is being used by an online user.

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**, and **display radius statistics**.

Example # Create a RADIUS scheme named radius1 and enter its view.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] radius scheme radius1
[SW7750-radius-radius1]
```

reset radius statistics

Syntax **reset radius statistics**

View User view

Parameter None

Description Use the **reset radius statistics** command to clear the statistics about the RADIUS protocol.

Related command: **display radius**.

Example # Clear the statistics about the RADIUS protocol.

```
<SW7750> 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-scheme-name*: Deletes the buffered stop-accounting requests depending on the specified RADIUS scheme. *radius-scheme-name* is the name of a RADIUS scheme. This name is a character string of up to 32 characters.

session-id *session-id*: Deletes the buffered stop-accounting requests depending on the specified session ID. Where, *session-id* is a character string of up to 50 characters.

time-range *start-time stop-time*: Deletes the buffered stop-accounting requests depending on the time of the stop-accounting request. Where, *start-time* is the start time of the request period, the *stop-time* is the end time of the request period, and both are in the format hh:mm:ss-mm/dd/yyyy or hh:mm:ss-yyyy/mm/dd. With this argument specified, this command displays the buffered stop-accounting requests from the start time to the end time.

user-name *user-name*: Deletes the buffered stop-accounting request packets depending on the specified user name. *user-name* is a character string of up to 32 characters.

Description Use the **reset stop-accounting-buffer** command to delete the buffered no-response stop-accounting request packets.

When the switch sends out a stop-accounting packet but gets no response from the RADIUS server, it first buffers the packet and then retransmits it until the maximum number of retransmission attempts (set by the **retry stop-accounting** command) is reached.

The **reset stop-accounting-buffer** command is used to delete the stop-accounting request packets buffered in the switch. You can choose to delete the buffered stop-accounting packets of a specified RADIUS scheme, session ID, or user name. You can also specify a time range to delete the stop-accounting packets sent within the specified time range.

Related command: **stop-accounting-buffer enable**, **retry stop-accounting** and **display stop-accounting-buffer**.

Example # Delete the stop-accounting request packets buffered in the system for the user user0001@aabbcc.net.

```
<SW7750> reset stop-accounting-buffer user-name user0001@aabbcc.net
```

# Delete the stop-accounting request packets buffered from 0:0:0 08/31/2002 to 23:59:59 08/31/2002 in the system.

```
<SW7750> 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*: Maximum number of transmission attempts, ranging from 1 to 20 and defaulting to 3.

Description Use the **retry** command to set the maximum number of transmission attempts of RADIUS requests.

Use the **undo retry** command to restore the default maximum number of transmission attempts.

Note that:

- *The communication in RADIUS is unreliable because this protocol adopts UDP packets to carry data. Therefore, it is necessary for the switch to retransmit a RADIUS request if it gets no response from the RADIUS server after the response timeout timer expires. If the maximum number of transmission attempts is reached but the switch still receives no response, the switch considers that the request fails.*
- *Appropriately set this maximum number of transmission attempts according to the network situation can improve the reacting speed of the system.*

Related command: **radius scheme**.

Example # Set the maximum transmission times of RADIUS requests in the RADIUS scheme radius1 to five.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] radius scheme radius1
[SW7750-radius-radius1] retry 5
```

retry realtime-accounting

Syntax **retry realtime-accounting** *retry-times*

undo retry realtime-accounting

View RADIUS scheme view

Parameter *retry-times*: Maximum number of real-time accounting request attempts, ranging from 1 to 255.

Description

Use the **retry realtime-accounting** command to set the maximum number of real-time accounting request attempts.

Use the **undo retry realtime-accounting** command to restore the default maximum number of real-time accounting request attempts.

By default, the system can allow five real-time accounting request attempts at most.

Note that:

- *Generally, the RADIUS server uses the connection timeout timer to determine whether a user is online or not. If the RADIUS server receives no real-time accounting packet for a specified period of time, it will consider that the line or the switch is in trouble and stop the accounting of the user. To make the switch cooperate with this feature on the RADIUS server, it is necessary to cut down the user connection on the switch as soon as possible after the RADIUS server terminates the charging and connection of the user in the case of unforeseen trouble. For this purpose, you can limit the number of continuous real-time no-response accounting requests, and the switch will cut down the user connection if it sends out the maximum number of real-time accounting requests but does not receive any response.*
- *A real-time account request may be sent multiple times (set by the **retry** command in RADIUS scheme view) for an accounting attempt. If no response is received even after the number of transmission attempts reaches the maximum, the accounting attempt fails. Suppose that the response timeout time of the RADIUS server is three seconds (set by the **timer response-timeout** command), that the maximum number of transmission attempts (set by the **retry** command) is 3, and that the real-time accounting interval is 12 minutes (set by the **timer realtime-accounting** command), the maximum number of real-time accounting request attempts is 5 (set by the **retry realtime-accounting** command). In this case, the switch sends an accounting request every 12 minutes; if the switch does not receive a response within 3 seconds after it sends out an accounting request, it resends the request; if the switch continuously sends the accounting request for three times but does not receive any response; it considers this real-time accounting a failure. Then, the switch sends the accounting request every 12 minutes; if the number of accounting failures exceeds five, the user connection is cut down.*

Related command: **radius scheme** and **timer realtime-accounting**.

Example

Allow the switch to continuously send at most 10 real-time accounting requests for the RADIUS scheme radius1.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] radius scheme radius1
[SW7750-radius-radius1] retry realtime-accounting 10
```

retry stop-accounting

Syntax **retry stop-accounting** *retry-times*

undo retry stop-accounting

View RADIUS scheme view

Parameter *retry-times*: Maximum number of transmission attempts of the buffered stop-accounting requests, ranging from 10 to 65535 and defaulting to 500.

Description Use the **retry stop-accounting** command to set the maximum number of transmission attempts of the stop-accounting requests buffered due to no response.

Use the **undo retry stop-accounting** command to restore the default maximum number of transmission attempts of the buffered stop-accounting requests.

Stop-accounting requests are critical to billing and will eventually affect the charges of the users; they are important for both the users and the ISP. Therefore, the NAS should do its best to transmit them to the RADIUS accounting server. If the RADIUS server does not respond to such a request, the switch should first buffer the request on itself, and then retransmit the request to the RADIUS accounting server until it gets a response, or the maximum number of transmission attempts is reached (in this case, it discards the request).

Related command: **reset stop-accounting-buffer**, **radius scheme** and **display stop-accounting-buffer**.

Example # In RADIUS scheme radius1, specify that the switch can transmit a buffered stop-accounting request at most 1,000 times

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] radius scheme radius1
[SW7750-radius-radius1] 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 notation. By default, the IP address of the secondary accounting server is 0.0.0.0.

port-number: UDP port number, ranging from 1 to 65535. By default, the UDP port number of the secondary accounting service is 1813.

Description Use the **secondary accounting** command to set the IP address and port number of the secondary RADIUS accounting server.

Use the **undo secondary accounting** command to restore the default IP address and port number of the secondary RADIUS accounting server.

See the description of **primary accounting** on page 628 for details.

Related command: **key**, **radius scheme** and **state**.

Example # Set the IP address and UDP port number of the secondary accounting server of the RADIUS scheme radius1 to 10.110.1.1 and 1813.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] radius scheme radius1
[SW7750-radius-radius1] 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 notation. By default, the IP address of the secondary authentication/authorization server is 0.0.0.0.

port-number: UDP port number, ranging from 1 to 65535. By default, the UDP port number of the secondary authentication/authorization service is 1812.

Description Use the **secondary authentication** command to set the IP address and port number of the secondary RADIUS authentication/authorization server.

Use the **undo secondary authentication** command to restore the default IP address and port number of the secondary RADIUS authentication/authorization server.

See the description of **primary authentication** on page 629 for details.

Related command: **key**, **radius scheme** and **state**.

Example # Set the IP address and UDP port number of the secondary authentication/authorization server used by the RADIUS scheme radius1 to 10.110.1.2 and 1812.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] radius scheme radius1
[SW7750-radius-radius1] secondary authentication 10.110.1.2 1812
```

server-type

Syntax **server-type** { **extended** | **standard** }

undo server-type

View RADIUS scheme view

Parameter **extended**: Specifies that the switch supports 3Com's RADIUS server. That is, it is required that the RADIUS client (on the switch) and the RADIUS server (generally the CAMS) interact with each other. by using 3Com's proprietary RADIUS protocol (such as the procedure and packet format)

standard: Specifies to use the standard RADIUS protocol. That is, it is required that the RADIUS client (on the switch) and the RADIUS server interact with each other following the procedure and packet format of the standard RADIUS protocol (RFC2865/2866 or above).

Description Use the **server-type** command to specify the RADIUS server type supported by the switch.

Use the **undo server-type** command to restore the default RADIUS server type supported by the switch.

By default, the RADIUS server type of a new RADIUS scheme is **standard**. The type of RADIUS server in the default RADIUS scheme "system" is **extended**.

Related command: **radius scheme**.

Example # Set the RADIUS server type in RADIUS scheme radius1 to extended.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] radius scheme radius1
[SW7750-radius-radius1] server-type extended
```

state

Syntax **state** { **primary** | **secondary** } { **accounting** | **authentication** } { **block** | **active** }

View RADIUS scheme view

Parameter **primary**: Specifies the server to be set is a primary RADIUS server.

secondary: Specifies the server to be set is a secondary RADIUS server.

accounting: Specifies the server to be set is a RADIUS accounting server.

authentication: Specifies the server to be set is a RADIUS authentication/authorization server.

block: Sets the status of the specified RADIUS server to **block** (that is, the down state).

active: Sets the status of the specified RADIUS server to **active** (that is, the normal working state).

Description Use the **state** command to set the status of a RADIUS server.

By default, all the RADIUS servers in a user-defined RADIUS scheme are in the **block** state.

For the primary and secondary servers (authentication/authorization servers, or accounting servers) in a RADIUS scheme, note that:

- When the NAS fails to communicate with the primary server due to some server trouble, the NAS will actively exchange packets with the secondary server.
- After the primary server recovers, the NAS does not immediately restore the communication with the primary server, but keeps communicating with the secondary server unit the secondary server also fails. In order for the NAS to quickly restore the communication with the recovered primary server, you need to manually set the state of the primary server to **active** by using the **state** command.
- When both the primary and secondary servers are in the active state, the NAS sends packets to the primary server only.

Related command: **radius scheme**, **primary authentication**, **secondary authentication**, **primary accounting**, and **secondary accounting**.

Example # Set the status of the secondary authentication server in RADIUS scheme radius1 to active.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] radius scheme radius1
[SW7750-radius-radius1] 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 enable the switch to buffer the stop-accounting requests that bring no response.

Use the **undo stop-accounting-buffer enable** command to disable the switch from buffering the stop-accounting requests that bring no response.

By default, the switch is enabled to buffer the stop-accounting requests that bring no response.

Stop-accounting requests are critical to billing and will eventually affect the charges; they are important for both the users and the ISP. Therefore, the NAS should do its best to transmit them to the RADIUS accounting server. If the RADIUS accounting server does not respond to such a request, the switch should first buffer the request on itself, and then retransmit the request to the RADIUS accounting server until it gets a response, or the maximum number of transmission attempts is reached (in this case, it discards the request).

Related command: **reset stop-accounting-buffer**, **radius scheme** and **display stop-accounting-buffer**.

Example # Enable the switch to buffer the stop-accounting requests that bring no response from the servers in RADIUS scheme radius1.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] radius scheme radius1
[SW7750-radius-radius1] stop-accounting-buffer enable
```

timer

Syntax **timer** *seconds*

undo timer

View RADIUS scheme view

Parameter *seconds*: Response timeout time of RADIUS server, ranging from 1 second to 10 seconds. By default, the response timeout time of the RADIUS server is three seconds.

Description Use the **timer** command to set the response timeout time of RADIUS server (that is, the timeout time of the response timeout timer of RADIUS server).

Use the **undo timer** command to restore the default response timeout timer of RADIUS server.

Note that:

- *If the switch gets no response from the RADIUS server after sending out a RADIUS request (authentication/authorization request or accounting request) and waiting for a time, it should retransmit the packet to ensure that the user can obtain the RADIUS service. This wait time is called response timeout time* *of RADIUS server; and the timer in the switch system that is used to control this time is called the response timeout timer of RADIUS server. You can use the* ***timer*** *command to set the timeout time of this timer.*

- *Appropriately setting the timeout time of this timer according to the network situation can improve the performance of the system.*
- *The* ***timer*** *command has the same effect with the* ***timer response-timeout*** *command.*

Related command: **radius scheme** and **retry**.

Example # Set the timeout time of the response timeout timer for the RADIUS scheme radius1 to 5 seconds.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] radius scheme radius1
[SW7750-radius-radius1] timer 5
```

timer quiet

Syntax **timer quiet** *minutes*

undo timer quiet

View RADIUS scheme view

Parameter *minutes*: Wait time, ranging from 1 minute to 255 minutes. By default, it is 5 minutes.

Description Use the **timer quiet** command to set the wait time for the primary server to restore the active state.

Use the **undo timer quiet** command to restore the default wait time.

Wait time works as follows:

The switch sends a RADIUS packet to the primary RADIUS server.

After confirming that no response will be received from the primary server, the switch starts to send RADIUS packets to the secondary RADIUS server.

At the interval of wait time, the switch sets the state of the primary server to **active** and sends RADIUS packets to the primary server.

Example # Set the wait time for the RADIUS scheme "radius1" to three minutes.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] radius scheme radius1
[SW7750-radius-radius1] timer quiet 3
```

timer realtime-accounting

Syntax **timer realtime-accounting** *minutes*

undo timer realtime-accounting

View RADIUS scheme view

Parameter *minutes*: Real-time accounting interval. It ranges from 3 minutes to 60 minutes and must be a multiple of 3. By default, this interval 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 real-time accounting interval.

Note that:

- *To charge the users in real time, you should set the interval of real-time accounting. After the setting, the NAS sends the accounting information of online users to the RADIUS server at regular intervals.*
- *The setting of the real-time accounting interval depends to some degree on the performance of the NAS and the RADIUS server. The higher the performance of the NAS and the RADIUS server is, the shorter the interval can be. You are recommended to set the interval as long as possible when the number of users is relatively great (¬¶1000). Table 106 lists the numbers of users and the corresponding recommended intervals.*

Table 106 Numbers of users and corresponding recommended intervals

Number of users	Real-time accounting interval
1 to 99	3
100 to 499	6
500 to 999	12
¬¶1000	¬¶15

Related command: **retry realtime-accounting** and **radius scheme**.

Example # Set the real-time accounting interval of the RADIUS scheme radius1 to 51 minutes.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] radius scheme radius1
[SW7750-radius-radius1] timer realtime-accounting 51
```

timer response-timeout

Syntax **timer response-timeout** *seconds*

undo timer response-timeout

View RADIUS scheme view

Parameter *seconds*: Response timeout time of RADIUS servers, ranging from 1 second to 10 seconds. By default, the response timeout time of the RADIUS server is three seconds.

Description Use the **timer response-timeout** command to set the response timeout time of RADIUS servers.

Use the **undo timer response-timeout** command to restore the default response timeout timer of RADIUS servers.

Note that:

- *If the switch gets no response from the RADIUS server after sending out a RADIUS request (authentication/authorization request or accounting request) and waiting for a time, it should retransmit the packet to ensure that the user can obtain the RADIUS service. This wait time is called response timeout time of RADIUS servers; and the timer in the switch system that is used to control this time is called the response timeout timer of RADIUS servers. You can use the* ***timer response-timeout*** *command to set the timeout time of this timer.*
- *Appropriately setting the timeout time of this timer according to the network situation can improve the performance of the system.*
- *This command has the same effect with the* ***timer*** *command.*

Related command: **radius scheme** and **retry**.

Example # Set the response timeout time in the RADIUS scheme radius1 to five seconds.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] radius scheme radius1
[SW7750-radius-radius1] timer response-timeout 5
```

user-name-format

Syntax **user-name-format** { **with-domain** | **without-domain** }

View RADIUS scheme view

Parameter **with-domain**: Specifies to include ISP domain names in the user names to be sent to RADIUS servers.

without-domain: Specifies to exclude ISP domain names from the user names to be sent to RADIUS servers.

Description Use the **user-name-format** command to set the format of the user names to be sent to RADIUS server

By default, except for the default RADIUS scheme "system", the user names sent to RADIUS servers in any RADIUS scheme carry ISP domain names.

Generally, an access user is named in the *userid@isp-name* format. *isp-name* behind the @ character represents the ISP domain name, by which the device determines which ISP domain it should ascribe the user to. However, some old RADIUS servers cannot accept the user names that carry ISP domain names. In this case, it is necessary to remove the domain names carried in the user names before sending the user names to the RADIUS server. For this reason, the **user-name-format** command is available for you to specify whether or not ISP domain names are carried in the user names sent to the RADIUS server.

For a RADIUS scheme, if you have specified that no ISP domain names are carried in the user names, you should not use this RADIUS scheme in more than one ISP domain. Otherwise, such errors may occur: the RADIUS server regards two different users having the same name but belonging to different ISP domains as the same user (because the user names sent to it are the same).

Related command: **radius scheme**.

Example # Specify that the user names sent to a RADIUS server in RADIUS scheme radius1 does not carry ISP domain names.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] radius scheme radius1
[SW7750-radius-radius1] user-name-format without-domain
```

47 HWTACACS CONFIGURATION COMMANDS

data-flow-format

Syntax

data-flow-format data { **byte | giga-byte | kilo-byte | mega-byte** }

data-flow-format 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. This means each giga-packet contains 1 G packets.

kilo-packet: Sets ’kilo-packet’ as the unit of packet flow. This means each kilo-packet contains 1 K packets.

mega-packet: Sets ’mega-packet’ as the unit of packet flow. This means each mega-packet contains 1 M packets.

one-packet: Sets ’one-packet’ as the unit of packet flow. This means each one-packet contains one packet.

Description

Use the **data-flow-format** command to configure the unit of data flows sent to the TACACS server.

Use the **undo data-flow-format** command to restore the default.

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 destined for the HWTACACS server to kilo-byte and the data packet unit to kilo-packet.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] hwtacacs scheme test1
[SW7750- hwtacacs-test1] data-flow-format data kilo-byte
[SW7750- hwtacacs-test1] data-flow-format packet kilo-packet
```

display hwtacacs

Syntax **display hwtacacs** [*hwtacacs-scheme-name* [**statistics**]]

View Any view

Parameter *hwtacacs-scheme-name*: HWTACACS scheme name, a string of 1 to 32 case-insensitive characters. If no HWTACACS scheme is specified, the system displays the configuration of all HWTACACS schemes.

statistics: Displays complete statistics about the HWTACACS scheme.

Description Use the **display hwtacacs** command to displays the configuration or statistics of the specified or all HWTACACS schemes.

By default, this command displays the configuration of all HWTACACS schemes.

Related command: **hwtacacs scheme**.

Example # View configuration information of HWTACACS scheme gy.

```
<SW7750> 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
-------------------------------------------------------------
Total 1,1 printed
```

display stop-accounting-buffer

Syntax **display stop-accounting-buffer** { **hwtacacs-scheme** *hwtacacs-scheme-name* | **session-id** *session-id* | **time-range** *start-time stop-time* | **user-name** *user-name* }

View Any view

Parameter **hwtacacs-scheme** *hwtacacs-scheme-name*: Displays information on buffered stop-accounting requests according to the HWTACACS scheme specified by *hwtacacs-scheme-name*, the name of HWTACACS scheme, a character string of up to 32 characters.

session-id *session-id*: Displays information on buffered stop-accounting requests according to the session ID specified by *session-id*, a character string of up to 50 characters.

time-range *start-time stop-time*: Displays information on buffered stop-accounting requests according to the request time, where, *start-time* is the start time of the stop-accounting request; *stop-time* is the end time of stop-accounting request. This argument is in the format hh:mm:ss - mm/dd/yyyy or *hh:mm:ss-yyyy/mm/dd* and is used to display the buffered stop-accounting requests from the start time to the end time.

user-name *user-name*: Displays information on buffered stop-accounting requests according to the user name specified by *user-name*, a character string of up to 32 characters.

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**, and **retry stop-accounting**.

Example # Display the stop-accounting requests buffered in the HWTACACS scheme "ht".

```
<SW7750> display stop-accounting-buffer hwtacacs-scheme ht
```

hwtacacs nas-ip

Syntax **hwtacacs nas-ip** *ip-address*

undo hwtacacs nas-ip

View System view

Parameter *ip-address*: Specifies a source IP address for the switch, which cannot be an all-zero address, class D address, class A, B, and C broadcast address, or 127 network segment address.

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.

Note that:

- *By specifying the source address of the hwtacacs packet, you can avoid destination unreachable packets as returned from the server upon interface failure. The source address is normally recommended to be a loopback interface address.*
- *When you configure the source address for the NAS to send HWTACACS packets, the priority of HWTACACS scheme view is higher than that of 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.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] hwtacacs nas-ip 129.10.10.1
```

hwtacacs scheme

Syntax **hwtacacs scheme** *hwtacacs-scheme-name*

undo hwtacacs scheme *hwtacacs-scheme-name*

undo hwtacacs scheme *hwtacacs-scheme-name*

View System view

Parameter *hwtacacs-scheme-name*: Specifies an HWTACACS server scheme, with a character string of up to characters.

Description Use the **hwtacacs scheme** command to enter HWTACACS scheme view and create the specified HWTACACS scheme if it does not exist.

Use the **undo hwtacacs scheme** command to delete an HWTACACS scheme.

Example # Create an HWTACACS scheme named "test1" and enter the relevant HWTACACS view.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] hwtacacs scheme test1
Create a new HWTACACS-server scheme
[SW7750-hwtacacs-test1]
```

key

Syntax

key { **accounting** | **authentication** | **authorization** } *string*

undo key { **accounting** | **authentication** | **authorization** } *string*

View

HWTACACS scheme view

Parameter

accounting: Specifies a shared key for the accounting server.

authentication: Specifies a shared key for the authentication server.

authorization: Specifies a shared key for the authorization server.

string: Shared key, a string of up to 16 characters.

Description

Use the **key** command to configure a shared key for HWTACACS authentication, authorization or accounting server.

Use the **undo key** command to delete the configuration.

By default, no shared key is set.

The TACACS client (on the switch) and the TACACS server use the MD5 algorithm to encrypt the HWTACACS packets communicated between them. They authenticate packets by using shared keys. Either of them receives and responds to the packet sent from the other party only when their shared keys are the same. Therefore, the shared key set on the switch and that on the TACACS server must be the same.

If the authentication/authorization server and the accounting server are different and the shared key for the two servers are different, a shared key must be set for authentication/authorization packets and accounting packets.

Related command:

display hwtacacs.

Example

Use hello as the shared key for TACACS accounting server.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] hwtacacs scheme test1
[SW7750-hwtacacs-test1] key accounting hello
```

nas-ip

Syntax

nas-ip *ip-address*

undo nas-ip

View

HWTACACS scheme view

Parameter *ip-address*: Specified source IP address, in dotted decimal notation.

Description Use the **nas-ip** command to specify the source address for sending HWTACACS packets so that all packets sent to the TACACS server carry the same source IP address.

Use the **undo nas-ip** command to remove the configuration.

By specifying the source address of the hwtacacs packet, you can avoid destination unreachable packets as returned from the server upon interface failure. The source address is normally recommended to be a loopback interface address.

By default, the source IP address of the packets is the IP address of the sending interface.

Related command: **display hwtacacs** and **hwtacacs nas-ip**.

Example # Set the source IP address of the HWTACACS packets sent by the NAS (switch) to 10.1.1.1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] hwtacacs scheme test1
[SW7750-hwtacacs-test1] nas-ip 10.1.1.1
```

primary accounting

Syntax **primary accounting** *ip-address* [*port*]

undo primary accounting

View HWTACACS scheme view

Parameter *ip-address*: IP address of the server, a valid unicast address in dotted decimal format. *port*: 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 TACACS accounting server is 0.0.0.0.

Note that:

- *You are not allowed to assign the same IP address to both primary and secondary accounting servers; otherwise, unsuccessful operation is prompted.*

- *If you repeatedly use this command, the latest configuration overwrites the previous one.*
- *You can remove an accounting server only when it is not being used by any active TCP connections, and the removal impacts only packets forwarded afterwards.*

Example # Configure a primary accounting server.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] hwtacacs scheme test1
[SW7750-hwtacacs-test1] primary accounting 10.163.155.12 49
```

primary authentication

Syntax **primary authentication** *ip-address* [*port*]

undo primary authentication

View HWTACACS scheme view

Parameter *ip-address*: IP address of the server, a valid unicast address in dotted decimal format. *port*: 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 TACACS authentication server.

Use the **undo primary authentication** command to delete the configured authentication server.

By default, the IP address of TACACS authentication server is 0.0.0.0.

Note that:

- *You are not allowed to assign the same IP address to both primary and secondary authentication servers; otherwise, unsuccessful operation is prompted.*
- *If you repeatedly use this command, the latest configuration overwrites the previous one.*
- *You can remove an authentication server only when it is not being used by any active TCP connections, and the removal impacts only packets forwarded afterwards.*

Related command: **display hwtacacs**.

Example # Configure a primary authentication server.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
```

```
[SW7750] hwtacacs scheme test1
[SW7750-hwtacacs-test1] primary authentication 10.163.155.13 49
```

primary authorization

Syntax **primary authorization** *ip-address* [*port*]

undo primary authorization

View HWTACACS scheme view

Parameter *ip-address*: IP address of the server, a valid unicast address in dotted decimal format. *port*: 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 TACACS authorization server is 0.0.0.0.

Note that:

- *You are not allowed to assign the same IP address to both primary and secondary authorization servers; otherwise, unsuccessful operation is prompted.*
- *If you repeatedly use this command, the latest configuration overwrites the previous one.*
- *You can remove an authorization server only when it is not being used by any active TCP connections, and the removal impacts only packets forwarded afterwards.*

Related command: **display hwtacacs**.

Example # Configure a primary authorization server.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] hwtacacs scheme test1
[SW7750-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.

```
<SW7750> reset hwtacacs statistics all
```

reset stop-accounting-buffer

Syntax **reset stop-accounting-buffer** { **hwtacacs-scheme** *hwtacacs-scheme-name* | **session-id** *session-id* | **time-range** *start-time stop-time* | **user-name** *user-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 of up to 32 characters, excluding question marks (?).

session-id *session-id*: Displays information on buffered stop-accounting requests according to the session ID specified by *session-id*, a character string of up to 50 characters.

time-range *start-time stop-time*: Displays information on buffered stop-accounting requests according to the request time, where, *start-time* is the start time of the stop-accounting request; *stop-time* is the end time of stop-accounting request. This argument is in the format hh:mm:ss - mm/dd/yyyy or *hh:mm:ss-yyyy/mm/dd* and is used to display the buffered stop-accounting requests from the start time to the end time. With this argument specified, this command displays the buffered stop-accounting requests from the start time to the end time.

user-name *user-name*: Displays information on buffered stop-accounting requests according to the user name specified by *user-name*, a character string of up to 32 characters.

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 according to the HWTACACS scheme "ht".

```
<SW7750> reset stop-accounting-buffer hwtacacs-scheme ht
```

retry stop-accounting

Syntax **retry stop-accounting** *retry-times*

undo retry stop-accounting

View HWTACACS scheme view

Parameter *retry-times*: Maximum number of real-time 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 has 100 attempts for each request.

Related command: **reset stop-accounting-buffer**, **hwtacacs scheme**, and **display stop-accounting-buffer**.

Example # Enable stop-accounting packet transmission and allow up to 50 attempts for each request.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] hwtacacs scheme test1
[SW7750-hwtacacs-test1] retry stop-accounting 50
```

secondary accounting

Syntax **secondary accounting** *ip-address* [*port*]

undo secondary accounting

View HWTACACS scheme view

Parameter *ip-address*: IP address of the server, a valid unicast address in dotted decimal notation. *port*: Port number of the server, which is in the range of 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, the IP address of TACACS accounting server is 0.0.0.0.

Note that:

- *You are not allowed to assign the same IP address to both primary and secondary accounting servers; otherwise, unsuccessful operation is prompted.*
- *If you repeatedly use this command, the latest configuration overwrites the previous one.*
- *You can remove an accounting server only when it is not being used by any active TCP connections.*

Example # Configure a secondary accounting server.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] hwtacacs scheme test1
[SW7750-hwtacacs-test1] secondary accounting 10.163.155.12 49
```

secondary authentication

Syntax **secondary authentication** *ip-address* [*port*]

undo secondary authentication

View HWTACACS scheme view

Parameter *ip-address*: IP address of the server, a valid unicast address in dotted decimal format. *port*: Port number of the server, which is in the range of 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 server.

By default, the IP address of TACACS authentication server is 0.0.0.0.

Note that:

- *You are not allowed to assign the same IP address to both primary and secondary authentication servers; otherwise, unsuccessful operation is prompted.*
- *If you repeatedly use this command, the latest configuration overwrites the previous one.*

- *You can remove an authentication server only when it is not being used by any active TCP connections.*

Related command: **display hwtacacs**.

Example # Configure a secondary server.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] hwtacacs scheme test1
[SW7750-hwtacacs-test1] secondary authentication 10.163.155.13 49
```

secondary authorization

Syntax **secondary authorization** *ip-address* [*port*]

undo secondary authorization

View HWTACACS scheme view

Parameter *ip-address*: IP address of the server, a valid unicast address in dotted decimal format. *port*: Port number of the server, in the range of 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, the IP address of TACACS authorization server is 0.0.0.0.

Note that:

- *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 an authorization server only when it is not being used by any active TCP connections.*

Related command: **display hwtacacs**.

Example # Configure the secondary authorization server.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] hwtacacs scheme test1
[SW7750-hwtacacs-test1] secondary authorization 10.163.155.13 49
```

stop-accounting-buffer enable

Syntax **stop-accounting-buffer enable**

undo stop-accounting-buffer enable

View HWTACACS scheme view

Parameter None

Description Use the **stop-accounting-buffer enable** command to enable the switch to buffer the stop-accounting requests that bring no response.

Use the **undo stop-accounting-buffer enable** command to disable the switch from buffering the stop-accounting requests that bring no response.

By default, the switch is enabled to buffer the stop-accounting requests that bring no response.

Stop-accounting requests are critical to billing and will eventually affect the charges; they are important for both the users and the ISP. Therefore, the switch should do its best to transmit them to the HWTACACS accounting server. If the HWTACACS accounting server does not respond to such a request, the switch should first buffer the request on itself, and then retransmit the request to the HWTACACS accounting server until it gets a response, or the maximum number of transmission attempts is reached (in this case, it discards the request).

Related command: **reset stop-accounting-buffer**, **hwtacacs scheme**, and **display stop-accounting-buffer**.

Example # Enable the switch to buffer the stop-accounting requests that bring no response from the servers in HWTACACS scheme test1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] hwtacacs scheme test1
[SW7750-hwtacacs-test1] stop-accounting-buffer enable
```

timer quiet

Syntax **timer quiet** *minutes*

undo timer quiet

View HWTACACS scheme view

Parameter *minutes*: Length of the timer in minutes, in the range of 1 to 255. By default, the primary server must wait five minutes before it resumes the active state.

Description

Use the **timer quiet** command to set the duration that a primary server must wait before it can resume the active state.

Use the **undo timer quiet** command to restore the default (five minutes).

With the **timer quiet** command configured, the switch stops processing the request packets from users when the communication between the switch and the server is interrupted. The switch does not send user request packets to the server until the wait time of the switch is equal to or greater than the time configured with the **timer quiet** command.

Related command: **display hwtacacs**.

Example

Set the quiet timer for the primary server to ten minutes.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] hwtacacs scheme test1
[SW7750-hwtacacs-test1] timer quiet 10
```

timer realtime-accounting

Syntax

timer realtime-accounting *minutes*

undo timer realtime-accounting

View

HWTACACS scheme view

Parameter

minutes: Real-time accounting interval, which is a multiple of 3 in the range 3 to 60 minutes. By default, the real-time accounting interval is 12 minutes.

Description

Use the **timer realtime-accounting** command to configure a real-time accounting interval.

Use the **undo timer realtime-accounting** command to restore the default interval.

Note that:

- *Real-time accounting interval is necessary for real-time accounting. After an interval value is set, the switch transmits the accounting information of online users to the TACACS accounting server at intervals of this value.*
- *The setting of real-time accounting interval depends somewhat on the performance of the switch 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). Table 107 recommends the real-time accounting intervals for different numbers of users.*

Table 107 Recommended intervals for different numbers of users

Number of users	Real-time accounting interval (minute)
1 to 99	3
100 to 499	6
500 to 999	12
¬¶1000	¬¶15

Example # Set the real-time accounting interval in the HWTACACS scheme "test1" to 51 minutes.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] hwtacacs scheme test1
[SW7750-hwtacacs-test11] timer realtime-accounting 51
```

timer response-timeout

Syntax **timer response-timeout** *seconds*

undo timer response-timeout

View HWTACACS scheme view

Parameter *seconds*: Length of the response timer in seconds. It ranges from 1 to 300 and defaults to 5.

Description Use the **timer response-timeout** command to set the response timeout timer of the TACACS server.

Use the **undo timer response-timeout** command to restore the default (five seconds).

As the HWTACACS is based on TCP, either the server response timeout and/or the TCP timeout may cause disconnection to the TACACS server.

Related command: **display hwtacacs**.

Example # Set the response timeout time of the TACACS server to 30 seconds.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] hwtacacs scheme test1
[SW7750-hwtacacs-test1] timer response-timeout 30
```

user-name-format

Syntax **user-name-format** { **with-domain** | **without-domain** }

View HWTACACS scheme view

Parameter **with-domain**: Specifies to send the username with a domain name to the TACACS server.

without-domain: Specifies to send the username without any domain name to the TACACS server.

Description Use the **user-name-format** command to configure the username format sent to the TACACS server.

By default, an HWTACACS scheme acknowledges that the username sent to it includes an ISP domain name.

Note that:

- *The supplicants are generally named in userid@isp-name format. The part following the @ sign is the ISP domain name, according to which the switch assigns a user to the corresponding ISP domain. However, some earlier TACACS servers reject the user name including an ISP domain name. In this case, the user name is sent to the TACACS server after its domain name is removed. Accordingly, the switch provides this command to decide whether the username sent to the TACACS server carries an ISP domain name or not.*
- *If a HWTACACS scheme is configured to reject usernames including ISP domain names, the TACACS scheme shall not be simultaneously used in more than one ISP domains. Otherwise, the TACACS 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: **hwtacacs scheme**.

Example # Specify to send the username without any domain name to the HWTACACS scheme "test1".

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] hwtacacs scheme test1
[SW7750-hwtacacs-test1] user-name-format without-domain
```

48 EAD CONFIGURATION COMMANDS

security-policy-server

Syntax **security-policy-server** *ip-address*

undo security-policy-server { *ip-address* | **all** }

View RADIUS scheme view

Parameter *ip-address*: IP address of the security policy server.

all: All IP addresses of security policy servers.

Description Use the **security-policy-server** command to specify an IP address for a security policy server.

Use the **undo security-policy-server** command to delete the specified IP address.

You may specify up to eight security policy servers in a RADIUS scheme.

Each RADIUS scheme supports at most eight IP addresses of security policy servers. The switch only responds to the session control packets coming from the authentication server and security policy server.

Example # Set the IP address of the security policy server to 192.168.0.1.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] radius scheme 3Com
[SW7750-radius-3Com] security-policy-server 192.168.0.1
[SW7750-radius-3Com] display current-configuration
...
radius scheme 3Com
primary authentication 1.1.11.29 1812
secondary authentication 127.0.0.1 1645
security-policy-server 192.168.0.1
user-name-format without-domain
...
```

49 TRAFFIC ACCOUNTING CONFIGURATION COMMANDS

accounting enable

Syntax

accounting enable

undo accounting enable

View

Traffic accounting view

Parameter

None

Description

Use the **accounting enable** command to enable the traffic accounting function on the traffic accounting module.

Use the **undo accounting enable** command to disable the traffic accounting function on the traffic accounting module.

The traffic accounting module starts traffic accounting immediately after the traffic accounting function is enabled.

By default, the traffic accounting function is disabled on the traffic accounting module.

Example

Enable the traffic accounting function.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] traffic-accounting accounting-slot 3
[SW7750-accounting-slot-3] accounting enable
```

# Disable the traffic accounting function.

```
[SW7750-accounting-slot-3] undo accounting enable
```

accounting-mode traffic

Syntax

accounting-mode traffic

View

ISP domain view

Parameter

None

Description Use the **accounting-mode traffic** command to set the accounting mode to traffic accounting.

Use the **undo accounting-mode traffic** command to restore the default accounting mode.

By default, the system adopts the time accounting mode.

Example # Set the accounting mode to traffic accounting.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] domain cams
[SW7750-isp-cams] accounting-mode traffic
```

# Restore the default accounting mode.

```
[SW7750-isp-cams] undo accounting-mode traffic
```

display traffic-accounting accounting-slot

Syntax **display traffic-accounting accounting-slot** [*slot-num*]

View Any view

Parameter *slot-num*: Traffic accounting slot.

Description Use the **display traffic-accounting-slot** command to display the configuration information of the traffic accounting slots.

If you specify the *slot-num* argument, the command displays the configuration information of the specified traffic accounting slot. Otherwise, the command displays the configuration information of all traffic accounting slots.

At present, the system supports only one traffic accounting slot. Therefore the same configuration information is displayed regardless whether or not you specify the traffic accounting slot.

Example # Display the configuration information of the traffic accounting slot 2.

```
<SW7750> display traffic-accounting accounting-slot 2
Accounting slot number : 2
 traffic-slot 3
 traffic accounting is enabled
```

display traffic-accounting statistics

Syntax **display traffic-accounting statistics** [*ip-address*]

View Any view

Parameter *ip-address*: IP address.

Description Use the **display traffic-accounting statistics** command to display the traffic accounting statistics of one or all online users.

If you specify the *ip-address* argument, the command displays the traffic accounting statistics of the specified online IP address. Otherwise, this command displays the traffic accounting statistics of all the online IP addresses.

Example # Display the traffic accounting statistics of all online users.

```
<SW7750> display traffic-accounting statistics
User IP: 10.0.0.1
  group name :somegroup
    output octets low-32: 1920           output octets high-32: 0
    input octets low-32 : 480           input octets high-32 : 0
```

display traffic-accounting traffic-group

Syntax **display traffic-accounting traffic-group** [*group-name*]

View Any view

Parameter *group-name*: Name of a traffic group.

Description Use the **display traffic-accounting traffic-group** command to display the configuration information of one or all traffic groups.

If you specify the *group-name* argument, this command displays the configuration information of the specified traffic group. Otherwise, it displays the configuration information of all traffic groups.

Example # Display the configuration information of the traffic group named somegroup.

```
<SW7750> display traffic-accounting traffic-group somegroup
Traffic group : somegroup
      1.1.1.0/255.255.255.0
      not referenced
```

# Display the configuration information of all traffic groups.

```
<SW7750> display traffic-accounting traffic-group
Traffic group : default-group
      0.0.0.0/0.0.0.0
      not referenced
Traffic group : somegroup
      1.1.1.0/255.255.255.0
      referenced
```

network

Syntax **network** *ip-address* { *mask* | *mask-len* }

undo network *ip-address* { *mask* | *mask-len* }

View Traffic group view

Parameter i*p-address*: IP address.

mask: Subnet mask.

Mask-len: Mask length.

Description Use the **network** command to configure a network address for the traffic group, so as to add a destination network segment to the traffic group.

Use the **undo network** command to remove a network address from the traffic group, so as to remove a destination network segment from the traffic group.

The address range of the network segment to be set for a traffic group can neither overlaps the existing address range of this traffic group nor be identical with the address range of any other traffic group.

Example # Add a network segment to the traffic group named somegroup.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] traffic-accounting traffic-group somegroup
[SW7750-traffic-group-somegroup] network 10.0.0.0 16
```

# Remove the network segment from the traffic group.

```
[SW7750-traffic-group-somegroup] undo network 10.0.0.0 16
```

traffic-accounting accounting-slot

Syntax **traffic-accounting accounting-slot** *slot-num*

undo traffic-accounting accounting-slot *slot-num*

View System view

Parameter *slot-num*: Slot number.

Description Use the **traffic-accounting accounting-slot** command to specify a traffic accounting slot.

Use the **undo traffic-accounting accounting-slot** command to remove the specified traffic accounting slot.

By default, no slot is specified as traffic accounting slot.

Related command: **display traffic-accounting accounting-slot**.

Example # Specify slot 2 as the traffic accounting slot.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] traffic-accounting accounting-slot 2
```

# Remove the specified traffic accounting slot 2.

```
[SW7750] undo traffic-accounting accounting-slot 2
```

traffic-accounting traffic-group

Syntax **traffic-accounting traffic-group** *group-name*

undo traffic-accounting traffic-group *group-name*

View System view

Parameter *group-name*: Name of a traffic group, a string of up to 32 characters.

Description Use the **traffic-accounting traffic-group** command to create a traffic group or enter the view of an existing traffic group.

Use the **undo traffic-accounting traffic-group** command to delete an existing traffic group.

The system allows you to configure up to 15 traffic groups. In addition, there is a default traffic group which you are not allowed to configure.

By default, there is a default traffic group.

Related command: **display traffic-accounting traffic-group**.

Example # Create a traffic group test-group.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] traffic-accounting traffic-group test-group
```

# Delete the created traffic group test-group.

```
[SW7750] undo traffic-accounting traffic-group test-group
```

traffic-group

Syntax **traffic-group** *group-name* **rate** *id-num*

View Domain view

Parameter *group-name*: Name of a traffic group, up to 32 characters long.

id-num: Charging rate ID, in the range of 1 to 255, used to identify different charging rates. This argument is not really implemented in the current command, it is left for future use..

Description Use the **traffic-group** command to configure the domain to use a traffic group.

Use the **undo traffic-group** command to cancel the configuration.

If a domain is configured to use a traffic group, when a user who belongs to the domain accesses an address in the traffic group, the generated traffic is accounted for and the user is charged based on the traffic.

By default, no traffic group is used by a domain.

Related command: **display traffic-accounting traffic-group**.

Example # Configure the domain "CAMS" to use the traffic group "test-group", with the rate of 1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] domain cams
[SW7750-isp-cams] traffic-group test-group rate 1
```

traffic-slot

Syntax **traffic-slot** *slot-num*

undo traffic-slot *slot-num*

View Traffic accounting view

Parameter *slot-num*: Slot number.

Description Use the **traffic-slot** command to specify a traffic collection module.

Use the **undo traffic-slot** command to cancel the specified traffic collection module.

By default, no traffic collection module is specified.

Related command: **traffic-accounting accounting-slot**.

Example # Specify the slot 2 as the traffic accounting slot and the slot 3 as the traffic collection slot.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] traffic-accounting accounting-slot 2
[SW7750-accounting-slot-2] traffic-slot 3
```

50 VRRP CONFIGURATION COMMANDS

display vrrp

Syntax **display vrrp** [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]

View Any view

Parameter *interface-type interface-number*: Displays the VRRP status information of the specified interface.

virtual-router-id: Displays the status information of the specified VRRP backup group. The virtual router ID ranges from 1 to 255.

Description Use the **display vrrp** command to display the VRRP status information.

- If the interface and backup group ID are not specified, the status information about all the backup groups on the switch is displayed.
- If only the interface is specified, the status information about all the backup groups on the interface is displayed.
- If both the interface and backup group ID are specified, the status information about the specified backup group on the interface is displayed.

Example # Display the status information about all the backup groups on the switch.

```
<SW7750> display vrrp
Run Method       : VIRTUAL-MAC
 Virtual Ip Ping : Disable
 The total number of the vitual routers:  1
  Interface        VRID  State     Run   Adver.  Auth     Virtual
                                   Pri   Time    Type     IP
----------------------------------------------------------------
Vlan1           1      Master   100   1       NONE     192.168.0.133
```

# Display the status information of VLAN-interface 1. The VRRP backup group 1 has been created on the device.

```
<SW7750> system-view
[SW7750] interface Vlan-interface 1
[SW7750-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            : Master
```

```
Config Pri      : 100                  Run Pri         : 100
Preempt Mode    : YES                  Delay Time      : 0
Auth Type       : NONE
Virtual IP      : 192.168.0.133
Virtual MAC     : 0000-5e00-0101
Master IP       : 192.168.0.68
```

Table 108 Field descriptions of the **display vrrp** command

Field	Description
Run Method	Current VRRP running mode, which could be Real MAC or virtual MAC
Virtual Ip Ping	Whether the ping operation is applicable to the virtual IP address
Interface	Interface where the backup group resides
VRID	Virtual backup group ID
Adver. Timer	Interval at which the VRRP advertisement is sent
Admin Status	Administrative status, which could be UP or DOWN.
State	Status of the current router in the backup group, which could be Master, Backup, or Initialize.
Config Pri	Configuration priority
Run Pri	Running priority
Preempt Mode	Preemption mode
Delay Time	Preemption delay
Auth Type	Authentication type
Virtual IP	Virtual IP address of the backup group
Virtual MAC	Virtual MAC address corresponding to the virtual IP address of the backup group. This item is displayed only when the router is in Master status.
Master IP	Master IP address of the interface corresponding to the router in Master status.

display vrrp statistics

Syntax **display vrrp statistics** [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]

View Any view

Parameter *interface-type interface-number*: Displays the VRRP statistics information of the specified interface.

virtual-router-id: Displays the statistics information of the specified VRRP backup group. The virtual router ID ranges from 1 to 255.

Description Use the **display vrrp statistics** command to display the VRRP statistics information.

- If the interface and backup group ID are not specified, the statistics information about all the backup groups on the switch is displayed.
- If only the interface is specified, the statistics information about all the backup groups on the interface is displayed.

- If both the interface and backup group ID are specified, the statistics information about the specified backup group on the interface is displayed.

Example # Display the statistics information about all the backup groups on the switch.

```
<SW7750> display vrrp statistics
Interface              : Vlan-interface1
 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         : 1         Priority Zero Pkts Rcvd       : 0
 Advertise Rcvd        : 0         Priority Zero Pkts Sent       : 0
 Invalid Type Pkts Rcvd : 0
Global statistics
 CheckSum Errors       : 0
 Version Errors        : 0
 VRID Errors           : 0
```

Table 109 Field descriptions of the **display vrrp statistics** command

Field	Description
Interface	Interface where the backup group resides
VRID	Backup group ID
CheckSum Errors	Number of checksum errors
Version Errors	Number of version errors
VRID Errors	Number of backup group ID errors
Advertisement Interval Errors	Number of advertisement interval errors
IP TTL Errors	Number of TTL errors
Auth Failures	Number of authentication errors
Invalid Auth Type	Number of invalid authentication types
Auth Type Mismatch	Number of mismatched authentication types
Packet Length Errors	Number of VRRP packet length errors
Address List Errors	Number of the virtual IP address list errors
Become Master	Number of the occasions that the switch operates as the master router
Priority Zero Pkts Rcvd	Number of the received advertisements with the priority of 0
Advertise Rcvd	Number of the received advertisements
Priority Zero Pkts Sent	Number of the sent advertisements with the priority of 0
Invalid Type Pkts Rcvd	Number of packet type errors
Global statistics	Global statistics

display vrrp verbose

Syntax **display vrrp verbose** [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]

View Any view

Parameter None

Description Use the **display vrrp verbose** command to display the detailed VRRP information.

- If the interface and backup group ID are not specified,detailed VRRP information about all the backup groups on the switch is displayed.
- If only the interface is specified, the detailed VRRP information about all the backup groups on the interface is displayed.
- If both the interface and backup group ID are specified, the detailed VRRP information about the specified backup group on the interface is displayed.

Example # Display the detailed VRRP information.

```
<SW7750> display vrrp verbose
 Run Method      : VIRTUAL-MAC
 Virtual Ip Ping : Disable
 Interface       : Vlan-interface1
 VRID            : 1                     Adver. Timer    : 1
 Admin Status    : UP                    State           : Master
 Config Pri      : 100                   Run Pri         : 100
 Preempt Mode    : YES                   Delay Time      : 0
 Auth Type       : NONE
 Virtual IP      : 192.168.0.133
 Virtual MAC     : 0000-5e00-0101
 Master IP       : 192.168.0.68
```

Table 110 Field descriptions of the **display vrrp verbose** command

Field	Description
Run Method	Current VRRP running mode, which could be Real MAC or virtual MAC
Virtual Ip Ping	Whether the ping operation is applicable to the virtual IP address
Interface	Interface where the backup group resides
VRID	Virtual backup group ID
Adver. Timer	Interval at which the VRRP advertisement is sent
Admin Status	Administrative status, which could be UP or DOWN.
State	Status of the current router in the backup group, which could be Master, Backup, or Initialize.
Config Pri	Configuration priority
Run Pri	Running priority
Preempt Mode	Preemption mode
Delay Time	Preemption delay
Auth Type	Authentication type
Virtual IP	Virtual IP address of the backup group
Virtual MAC	Virtual MAC address corresponding to the virtual IP address of the backup group. This item is displayed only when the router is in Master status.
Master IP	Master IP address of the interface corresponding to the router in Master status.

reset vrrp statistics

Syntax **reset vrrp statistics** [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]

View User view

Parameter *interface-type interface-number*: Interface type and interface number

virtual-router-id: VRRP backup group ID, in the range of 1 to 255.

Description Use the **reset vrrp** command to clear the statistics information about VRRP.

When you execute this command,

- If the interface and backup group ID are not specified, the statistics information about all the backup groups on the switch is cleared.
- If only the interface is specified, the statistics information about all the backup groups on the interface is cleared.
- If both the interface and backup group ID are specified, the statistics information about the specified backup group on the interface is cleared.

Example # Clear the VRRP statistics information of all backup groups on all the interfaces.

```
<SW7750> reset vrrp statistics
```

undo vrrp vrid

Syntax **undo vrrp vrid** *virtual-router-id*

View VLAN interface view

Parameters *virtual-router-id*: VRRP backup group ID, ranging from 1 to 255.

Description Use the **undo vrrp vrid** command to remove all the configurations of the specified backup group on the VLAN interface.

Examples # Remove the configurations of VRRP backup group 1 on VLAN-interface 2.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 2
[SW7750-Vlan-interface2] undo vrrp vrid 1
```

vrrp method

Syntax **vrrp method** { **real-mac** | **virtual-mac** }

undo vrrp method

View System view

Parameter **real-mac**: Maps the real MAC address of a Layer 3 switch routing interface to virtual router IP addresses.

virtual-mac: Maps the virtual MAC address to virtual router IP addresses of backup groups.

Description Use the **vrrp method** command to map the MAC address of a backup group to the virtual router IP addresses. You can map the actual or virtual MAC address of a Layer 3 switch routing interface to virtual router IP addresses.

Use the **undo vrrp method** command to restore the default map settings.

By default, the virtual MAC address of a backup group is mapped to the IP address of the virtual router.

Note that as the mapping relationship between the MAC addresses of a backup group and a virtual router IP address cannot be configured after the backup group is created, configure the mapping relationship before you create a backup group.

Due to the chips installed, when you map the virtual IP addresses to the virtual MAC addresses, the type of chips decides the number of backup groups that can be configured on a VLAN interface. Refer to device specification for detail.

Example # Map the real MAC address of a routing interface to a virtual router IP address.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] vrrp method real-mac
```

vrrp ping-enable

Syntax **vrrp ping-enable**

undo vrrp ping-enable

View System view

Parameter None

Description Use the **vrrp ping-enable** command to enable a backup group to respond to ping operations destined for its virtual router IP address.

Use the **undo vrrp ping-enable** command to revert to the default.

By default, a backup group does not respond to ping operations destined for its virtual router IP address.

Example # Enable a backup group to respond to ping operations destined for its virtual router IP address.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] 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 TTL check of VRRP packet.

Use the **undo vrrp un-check ttl** command to enable the TTL check of VRRP packet.

By default, the TTL field in the VRRP packet is checked.

Example # Disable the TTL check of VRRP packet on VLAN-interface 1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 1
[SW7750-Vlan-interface1] vrrp un-check ttl
```

vrrp vrid authentication-mode

Syntax **vrrp vrid** *virtual-router-id* **authentication-mode** *authentication-type authentication-key*

undo vrrp vrid *virtual-router-id* **authentication-mode**

View VLAN interface view

Parameter *virtual-router-id*: VRRP backup group ID, in the range of 1 to 255.

authentication-type: Authentication type, which can be:

- **simple**: Indicates to perform simple character authentication.
- **md5**: Indicates to perform the authentication with MD5 algorithm.

authentication-key: Authentication key. When you specify *authentication-type* to be **simple**, the authentication key can contain up to eight characters. When you specify *authentication-type* to be **md5**, the authentication key can be a string comprising up to eight characters in plain text or a 24-character encrypted string.

Description

Use the **vrrp vrid authentication-mode** command to specify the authentication type and the authentication key for a VRRP backup group.

Use the **undo vrid vrrp authentication-mode** command to clear the configured authentication type and authentication key.

By default, authentication is disabled for the VRRP backup group.

If the **simple** or **md5** authentication is configured, the authentication key is required.

This command sets the authentication type and authentication key for all the VRRP backup groups on one or multi interface. As defined in the protocol, all the backup groups on an interface share the same authentication type and authentication key. And all the members joining the same backup group share the same authentication type and authentication key too.

Note that the authentication key is case-sensitive.

Example

Specify the authentication type as **simple**, and authentication key as aabbcc for the VRRP backup group 1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 2
[SW7750-Vlan-interface2] vrrp vrid 1 authentication-mode simple aabb
cc
```

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 backup group ID ranging from 1 to 255.

delay-value: Delay period (in seconds) ranging from 0 to 255.

Description

Use the **vrrp vrid preempt-mode** command to configure a switch to operate in the preemptive mode and set the delay period.

Use the **undo vrrp vrid preempt-mode** command to cancel the configuration.

By default, switches in a backup group operate in the preemptive mode, with the delay period set to 0 seconds.

If you want backup switches to preempt the master switch, configure them to operate in the preemptive mode. You can also set the delay period for preemption as needed.

As long as a switch in the backup group becomes the master switch, other switches, even if they are configured with a higher priority later, do not preempt the master switch unless they operate in preemptive mode. The switch operating in preemptive mode will become the master switch when it finds its priority is higher than that of the current master switch, and the former master switch becomes a backup switch accordingly.

You can configure a Switch 7750 to operate in preemptive mode. You can also set the delay period. A backup switch waits for a period of time (the delay period) before becoming a master switch. Setting a delay period aims at:

In an unstable network, backup switches in a backup group possibly cannot receive packets from the master in time due to network congestions even if the master operates properly. This causes the master of the backup group being determined frequently. With the configuration of delay period, the backup switch will wait for a while if it does not receive packets from the master switch in time. A new master is determined only after the backup switches do not receive packets from the master switch after the specified delay time.

*You can use the **undo vrrp vrid preempt-mode** command to set switches in a backup group to operate in non-preemptive mode.*

Example # Configure the switches to operate in the preemptive mode.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 2
[SW7750-Vlan-interface2] vrrp vrid 1 preempt-mode
```

# Set the delay period.

```
[SW7750-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5
```

# Configure the switches to operate in non-preemptive mode.

```
[SW7750-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 backup group ID ranging from 1 to 255.

priority: Switch priority to be set. This argument ranges from 1 to 254.

Description

Use the **vrrp vrid priority** command to set the priority of a switch in a backup group.

Use the **undo vrrp vrid priority** command to revert to the default priority.

By default, the priority of a switch in a backup group is 100.

Switch priority determines the possibility for the switch to become a master switch. A switch with larger priority is more likely to become a master switch. Note that the priority of 0 is reserved for special use, and the priority of 255 is for IP address owners. That is, the priority of a switch that owns a virtual router IP address is fixed to 255 and cannot be modified.

Example

Set the priority to 120 for a switch in the backup group.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 2
[SW7750-Vlan-interface2] vrrp vrid 1 priority 120
```

vrrp vrid timer advertise

Syntax

vrrp vrid *virtual-router-id* **timer advertise** *adver-interval*

undo vrrp vrid *virtual-router-id* **timer advertise**

View

VLAN interface view

Parameter

virtual-router-id: VRRP backup group ID ranging from 1 to 255.

adver-interval: Interval (in seconds) for the master switch of a backup group to send VRRP packets. This argument ranges from 1 to 255.

Description

Use the **vrrp vrid timer advertise** command to set the interval for the master switch of a backup group to send VRRP packets.

Use the **undo vrrp vrid timer advertise** command to revert to the default interval.

Note that configuration error occurs if switches of the same backup group are configured with different *adver-interval* values.

By default, the interval for the master switch in a backup group to send VRRP packets is 1 second.

Example

Set the interval for the master switch to send VRRP packets to 15 seconds.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 2
[SW7750-Vlan-interface2] vrrp vrid 1 timer advertise 15
```

vrrp vrid track

Syntax

vrrp vrid *virtual-router-id* **track** *interface-type interface-number* [**reduced** *value-reduced*]

undo vrrp vrid *virtual-router-id* **track** [*interface-type interface-number*]

View

VLAN interface view

Parameter

virtual-router-id: VRRP backup group ID ranging form 1 to 255.

Interface-type interface-number: VLAN interface or port to be tracked.

value-reduced: Value by which the priority is to decrease. This argument ranges from 1 to 255.

Description

Use the **vrrp vrid track** command to set a VLAN interface/Ethernet port to be tracked.

Use the **undo vrrp vrid track** command to disable a VLAN interface/Ethernet port from being tracked.

By default, the value by which the priority of the VLAN interface decreases is 10.

The VLAN interface/Ethernet port tracking function extends the use of the backup function. With this function enabled, the backup function is provided not only when the interface where the backup group resides fails, but also when other interfaces/Ethernet ports are unavailable. By executing the related command you can track an interface/Ethernet port.

When a tracked VLAN interface/Ethernet port goes down, the priority of the switch owning the interface/port will reduce automatically by a specified value (the *value-reduced* argument). If the switches with their priorities higher than that of the current master switch exist in the backup group, a new master switch will be then determined.

- *The Ethernet port tracked can be in or out of the VLAN in whose interface the backup group resides.*
- *If a switch is the IP address owner, the VLAN interface/Ethernet port tracking function can not be enabled for the switch.*
- *If a tracked VLAN interface/Ethernet port goes down, when it is up again, the priority of the corresponding switch is automatically restored.*
- *Each backup group can track up to eight VLAN interfaces/Ethernet ports.*

Example

Configure VLAN 2 interface to track VLAN 1 interface and specify the priority of the master switch of backup group 1 (on VLAN 2 interface) decreases by 50 when VLAN 1 interface goes down.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 2
```

```
[SW7750-Vlan-interface2] vrrp vrid 1 track vlan-interface 1 reduced
50
```

vrrp vrid virtual-ip

Syntax **vrrp vrid** *virtual-router-id* **virtual-ip** *virtual-address*

undo vrrp vrid *virtual-router-id* [**virtual-ip** *virtual-address*]

View VLAN interface view

Parameter *virtual-router-id*: VRRP backup group ID ranging from 1 to 255.

virtual-address: Virtual router IP address to be configured.

Description Use the **vrrp vrid virtual-ip** command to add a virtual router IP address to an existing backup group.

Use the **undo vrrp vrid virtual-ip** command to remove a virtual router IP address from an existing backup group.

The **vrrp vrid virtual-ip** command can also be used to create a backup group. You can add up to 16 virtual router IP addresses to a backup group. The **undo vrrp vrid virtual-ip** command can also be used to remove an existing backup group. A backup group is removed if all the virtual router IP addresses configured for it are removed.

Note that the virtual router IP address and the IP addresses used by the member switches in a backup group must belong to the same network segment. If not, the backup group will be in the initial state (the state before you configure the VRRP for the switches). In this case, VRRP does not take effect.

Example # Create a backup group.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 2
[SW7750-Vlan-interface2] vrrp vrid 1 virtual-ip 10.10.10.10
```

# Add a virtual router IP address to an existing backup group.

```
[SW7750-Vlan-interface2] vrrp vrid 1 virtual-ip 10.10.10.11
```

# Remove a virtual router IP address from a backup group.

```
[SW7750-Vlan-interface2] undo vrrp vrid 1 virtual-ip 10.10.10.10
```

# Remove a backup group.

```
[SW7750-Vlan-interface2] undo vrrp vrid 1
```

51 HA CONFIGURATION COMMANDS

display switchover state

Syntax **display switchover state** [*slot-id*]

View Any view

Parameter *slot-id*: Slot number of master/slave module.

Description Use the **display switchover state** command to display the backup status of master/slave module.

This command displays the backup state of master/slave module according to the specified slot number. If the *slot-id* is not specified, the status of master module will be displayed.

Example # Display the status of master module.

```
<SW7750> display switchover state
HA FSM State(master): Slave is absent.
```

slave auto-update config

Syntax **slave auto-update config**

undo slave auto-update config

View System view

Parameter None

Description Use **slave auto-update config** command to enable the automatic synchronization of configuration files between the master/slave systems.

Use the **undo slave auto-update config** command to disable the automatic synchronization.

By default, the automatic synchronization of configuration files between the master and slave system is enabled.

Related command: **slave update configuration**.

Example # Enable automatic synchronization between master/slave systems.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] slave auto-update config
```

slave restart

Syntax **slave restart**

View User view

Parameter None

Description Use the **slave restart** command to restart the slave module.

When the application of the backup system operates unmorally and requires for reloading the applications, you can use this command to restart the slave module.

Example # Restart the slave module.

```
<SW7750> 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 perform master/slave switchover manually.

When the slave module operates normally and the master module is in the real-time backup state, if you want the slave module to operate in place of the master module, you can use this command to implement master/slave switchover. After that, the slave module becomes the new master module and controls the system, and the original master module restarts automatically.

Example # Perform master/slave switchover manually.

```
<SW7750> 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 synchronise the configurations files on master/slave module.

You can use this command to manually synchronize the configuration files on the master module to the slave module.

Example # Synchronize the configuration files on the master module to the slave module.

```
<SW7750> slave update configuration
Now saving the current configuration to the slave board.
Please wait...
The configuration has been saved to the slave board successfully.
```

52 ARP CONFIGURATION COMMANDS

arp check enable

Syntax **arp check enable**

undo arp check enable

View System view

Parameter None

Description Use the **arp check enable** command to enable the ARP entry checking function.

Use the **undo arp check enable** command to disable the ARP entry checking function.

With the ARP entry checking function enabled, the switch cannot learn any ARP entry with a multicast MAC address. Configuring such a static ARP entry is not allowed either; otherwise, the system prompts error information.

After the ARP entry checking function is disabled, the switch can learn the ARP entry with a multicast MAC address, and you can also configure such a static ARP entry on the switch.

By default, the ARP entry checking function is enabled.

Example # Disable the ARP entry checking function.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] undo arp check enable
```

arp gratuitous-updating enable

Syntax **arp gratuitous-updating enable**

undo arp gratuitous-updating enable

View System view

Parameter None

Description Use the **arp gratuitous-updating enable** command to enable gratuitous ARP packets to be sent periodically.

Use the **undo arp gratuitous-updating enable** command to disable gratuitous ARP packets from being sent periodically. With this function enabled, the switch periodically broadcasts gratuitous ARP packets from the current interface IP address within the VLAN whose interfaces are configured with an IP address.

By default, the switch is disabled from sending gratuitous ARP packets periodically.

With VRRP enabled on a VLAN interface of a switch:

- If the switch is the master switch, it sends gratuitous ARP messages with the IP address of the VRRP virtual router.
- If it is not the master switch, it sends gratuitous ARP messages with the primary and all the secondary IP addresses of the VLAN interface.

Example # Enable the switch to send gratuitous ARP packets periodically.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] arp gratuitous-updating enable
```

arp mac-arp-map limit

Syntax **arp mac-arp-map limit** *number*

undo arp mac-arp-map limit

View System view

Parameter *number*: Maximum number of IP addresses to be bound to a MAC address of a VLAN, in the range 1 to 8192.

Description Use the **arp mac-arp-map limit** command to set the maximum number of IP addresses to be bound to a MAC address of a VLAN.

Use the **undo arp mac-arp-map limit** command to restore the default value.

By default, a maximum of 8192 IP addresses can be bound to a MAC address of a VLAN.

Note that:

If secondary IP addresses are configured for a VLAN interface, the specified maximum number of IP addresses to be bound to a MAC address should be bigger than the total number of the primary and secondary IP addresses of the VLAN interface.

Example # Set the maximum number of IP addresses to be bound to a MAC address of a VLAN to 5.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] arp mac-arp-map limit 5
```

arp max-entry

Syntax **arp max-entry** *number*

undo arp max-entry

View System view

Parameter *number:* Total maximum number of ARP entries, in the range of 4,096 to 8,192.

Description Use the **arp max-entry** command to set the total maximum number of ARP entries.

Use the **undo arp max-entry** command to restore the default setting.

By default, the total maximum number of ARP entries is 8,192.

Example # Set the total maximum number of ARP entries to 4,096.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] arp max-entry 4096
```

arp max-dynamic-entry

Syntax **arp max-dynamic-entry** *number*

undo arp max-dynamic-entry

View Port view

Parameter *number:* Maximum number of dynamic ARP entries that can be learnt by the port, ranging from 0 to 8,192.

Description Use the **arp max-dynamic-entry** command to set the maximum number of dynamic ARP entries that can be learnt by a port.

Use the **undo arp max-dynamic-entry** command to restore the default setting.

By default, the maximum number of dynamic ARP entries that can be learnt by a port is 2,048.

Example # Set maximum number of dynamic ARP entries that can be learnt by Ethernet3/0/1 to 6,000.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet 3/0/1
[SW7750-Ethernet3/0/1] arp max-dynamic-entry 6000
```

arp protective-down recover interval

Syntax **arp protective-down recover interval** *time*

undo protective-down recover interval

View System view

Parameter *time*: Recovery time (in the range 1 to 3600 seconds) of a port that has been disabled from receiving any packet temporarily because its ARP packet receive rate exceeded the upper limit.

Description Use the **arp protective-down recover interval** command to specify a recovery interval. A port is brought up after the interval (since it was disabled).

Use the **undo arp protective-down recover interval** command to restore the default.

By default, the recovery interval is 300 seconds.

Example # Set the auto-recovery interval to 500 seconds.

<SW7750> system

```
System View: return to User View with Ctrl+Z.
[SW7750] arp protective-down recover interval 500
```

arp rate-limit enable

Syntax **arp rate-limit enable**

undo arp rate-limit enable

View System view

Parameter None

Description Use the **arp rate-limit enable** command to enable the ARP packet rate limit function.

Use the **undo arp rate-limit enable** command to disable the ARP packet rate limit function.

With the ARP packet rate limit function enabled, the maximum ARP packet receive rate on each port is 15 pps by default.

By default, the ARP packet rate limit function is disabled.

Example # Enable the ARP packet rate limit function.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] arp rate-limit enable
```

arp rate-limit

Syntax **arp rate-limit** *rate*

undo arp rate-limit

View System view

Parameter *rate*: Maximum ARP packet receive rate, in the range of 1 to 1,024 pps.

Description Use the **arp rate-limit** command to specify the maximum ARP packet receive rate on ports.

Use the **undo arp rate-limit** command to restore the default.

By default, the maximum ARP packet receive rate on a port (except the trusted port) is 15 pps.

Example # Set the maximum ARP packet receive rate to 20 pps.

<SW7750> system

```
System View: return to User View with Ctrl+Z.
[SW7750] arp rate-limit 20
```

arp rate-limit trust

Syntax **arp rate-limit trust**

undo arp rate-limit trust

View Ethernet port view

Parameter None

Description Use the **arp rate-limit trust** command to configure the port as a trusted port for ARP packet rate limit.

Use the **undo arp rate-limit trust** command to configure the port as an untrusted port for ARP packet rate limit.

By default, the port is an untrusted port for ARP packet rate limit.

Example # Configure Ethernet 2/0/1 as a trusted port for ARP packet rate limit.

```
<SW7750> system
System View: return to User View with Ctrl+Z.
[SW7750] int Ethernet2/0/1
[SW7750-Ethernet2/0/1] arp rate-limit trust
```

arp relay enable

Syntax **arp relay enable**

undo arp relay

View System view

Parameter None

Description Use the **arp relay enable** command to enable ARP forwarding in the protocol-based VLAN(s).

Use the **undo arp relay** command to disable ARP forwarding in the protocol-based VLAN(s).

This feature is enabled by default.

Example # Disable ARP forwarding in the protocol-based VLAN(s).

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] undo arp relay
```

arp source-suppression limit

Syntax **arp source-suppression limit** { **total** | **local** | **through** } *limit-value*

undo arp source-suppression limit { **total** | **local** | **through** }

View System view

Parameter **total**: Sets the maximum number of total arbitrary ARP packets that can be sent to the CPU in a unit of time. (There is no limit on source and destination IP addresses in ARP packets.)

local: Sets the maximum number of locally-terminated ARP packets (packets having the same source IP address and using the IP address of the current switch as their destination IP address) that can be sent to the CPU in a unit of time.

through: Sets the maximum number of pass-through ARP packets (packets having the same source IP address and not using the IP address of the current switch as their destination IP addresses) that can be sent to the CPU in a unit of time.

limit-value: Maximum number of a type of ARP packets that can be sent to the CPU in a unit of time. When **local** or **total** is adopted, this argument ranges from 1 to 4294967295; when **through** is adopted, the value ranges from 0 to 4294967295.

Description

Use the **arp source-suppression limit** command to set the maximum number of a type of ARP packets that can be sent to the CPU in a unit of time.

Use the **undo arp source-suppression limit** command to restore the default setting.

The default setting varies with the type of ARP packets.

- When **total** is adopted in the command, the default setting is 100.
- When **local** is adopted in the command, the default setting is 3.
- When **through** is adopted in the command, the default setting is 3.

Make sure your setting for **total** is greater than the settings for **local** and **through**.

Related commands:

display arp source-suppression.

Example

Configure to allow a maximum of 200 ARP packets to be sent to the CPU totally.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] arp source-suppression limit total 200
```

arp static

Syntax

arp static *ip-address mac-address* [*vlan-id interface-type interface-number*]

undo arp *ip-address*

View

System view

Parameter

ip-address: IP address for the ARP entry to be created/removed.

mac-address: MAC address for the ARP entry to be created, in the format of H-H-H.

vlan-id: ID of the VLAN to which the static ARP entry belongs, in the range of 1 to 4094.

interface-type: Type of the port to which the static ARP entry belongs.

interface-number: Number of the port to which the static ARP entry belongs.

Description Use the **arp static** command to create a static ARP entry in the ARP table.

Use the **undo arp** command to remove an ARP entry.

By default, there is no static ARP entry in the ARP table, and ARP entries are dynamically created by ARP.

Note that:

- *A static ARP entry keeps valid as long as the Ethernet switch operates normally, but removing the VLAN of the entry removes the ARP entry.*
- *The VLAN specified by the vlan-id argument in the* ***arp static*** *command must be an existing VLAN configured with the corresponding VLAN interface and its IP address, and the port specified by the interface-type and interface-number arguments must belong to the VLAN.*

Related commands: **reset arp**, **display arp**.

Example # Create a static ARP entry belonging to Ethernet 2/0/1 in VLAN 1, with IP address 202.38.10.2 and MAC address 000f-e201-0000.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] arp static 202.38.10.2 000f-e201-0000 1 Ethernet 2/0/1
```

arp timer aging

Syntax **arp timer aging** *aging-time*

undo arp timer aging

View System view

Parameter *aging-time*: Aging time for dynamic ARP entries. This argument ranges from 1 to 1,440 in minutes.

Description Use the **arp timer aging** command to configure the aging time for dynamic ARP entries.

Use the **undo arp timer aging** command to restore the default aging time.

By default, the aging time for dynamic ARP entries is 20 minutes.

Related commands: **display arp timer aging**.

Example # Set the aging time for dynamic ARP entries to 10 minutes.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] arp timer aging 10
```

arp timer gratuitous-updating

Syntax **arp timer gratuitous-updating** *updating-interval*

undo arp timer gratuitous-updating

View System view

Parameter *updating-interval*: Interval, in minutes, at which gratuitous ARP packets are sent. The value range is 1 to 10.

Description Use the **arp timer gratuitous-updating** command to set a gratuitous ARP update interval.

Use the **undo arp timer gratuitous-updating** command to restore the default gratuitous ARP update interval.

The gratuitous ARP update interval defaults to five minutes after this function is enabled on the switch.

Related commands: **arp gratuitous-updating enable**.

Example # Set the gratuitous ARP update interval to 10 minutes on the switch.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] arp timer gratuitous-updating 10
```

display arp

Syntax **display arp** [**dynamic** | **static** | *ip-address*]

View Any view

Parameter **dynamic**: Displays dynamic ARP entries.

static: Displays static ARP entries.

ip-address: IP address. The ARP entry containing this IP address will be displayed.

Description Use the **display arp** command to display ARP entries.

Executing this command without any parameter will display all ARP entries.

Related commands: **arp static**, **reset arp**.

Example # Display all ARP entries.

```
<SW7750> display arp
            Type: S-Static   D-Dynamic
IP Address       MAC Address     VLAN ID  Port Name              Aging Type
10.2.72.162      000a-000a-0aaa  N/A      N/A                    N/A   S
192.168.0.77     0000-e8f5-6a4a  1        Ethernet2/0/2          13    D
192.168.0.2      000d-88f8-4e88  1        Ethernet2/0/2          14    D
192.168.0.200    0014-222c-9d6a  1        Ethernet2/0/2          14    D
192.168.0.45     000d-88f6-44c1  1        Ethernet2/0/2          15    D
192.168.0.110    0011-4301-991e  1        Ethernet2/0/2          15    D
192.168.0.32     0000-e8f5-73ee  1        Ethernet2/0/2          16    D
192.168.0.3      0014-222c-aa69  1        Ethernet2/0/2          16    D
192.168.0.17     000d-88f6-379c  1        Ethernet2/0/2          17    D
192.168.0.115    000d-88f7-9f7d  1        Ethernet2/0/2          18    D
192.168.0.43     000c-760a-172d  1        Ethernet2/0/2          18    D
192.168.0.33     000d-88f6-44ba  1        Ethernet2/0/2          20    D
192.168.0.35     000f-e202-2181  1        Ethernet2/0/2          20    D
192.168.0.5      000f-3d80-2b38  1        Ethernet2/0/2          20    D

---   14 entries found   ---
```

Table 111 Field descriptions of the **display arp** command

Field	Description
IP Address	IP address contained in an ARP entry
MAC Address	MAC address contained in the ARP entry
VLAN ID	ID of the VLAN to which the ARP entry belongs
Port Name	Index of the port to which the ARP entry belongs
Aging	Aging time of the dynamic ARP entry, in minutes
Type	Type of the ARP entry

display arp |

Syntax **display arp** | { **begin** | **exclude** | **include** } *text*

View Any view

Parameter **begin**: Displays the ARP entries from the first ARP entry that contains the string specified by the *text* argument.

exclude: Displays the ARP entries that do not contain the string specified by the *text* argument.

include: Displays the ARP entries that contain the string specified by the *text* argument.

text: String used to filter ARP entries.

Description Use the **display arp |** command to display the ARP entries matching a specified rule.

Related commands: **arp static**, **reset arp**.

Example # Display the ARP entries that contain the string "77".

```
<SW7750> display arp | include 77
            Type: S-Static   D-Dynamic
IP Address       MAC Address     VLAN ID  Port Name             Aging Type
192.168.0.77     0000-e8f5-6a4a  1        Ethernet2/0/2          12    D

---   1 entry found   ---
```

# Display the ARP entries that do not contain the string "68".

```
<SW7750> display arp | exclude 68
            Type: S-Static   D-Dynamic
IP Address       MAC Address     VLAN ID  Port Name            Aging Type
10.2.72.162      000a-000a-0aaa  N/A      N/A                    N/A   S

---   1 entry found   ---
```

See Table 111 for the description of the output fields.

display arp attack-list

Syntax **display arp attack-list**

View Any view

Parameter None

Description Use the **display arp attack-list** command to display the ARP attack information, including the attacking MAC address, IP address and the attack time.

Example # Display the ARP attack information.

```
<SW7750> display arp attack-list
MAC ADDR       VLAN IP ADDR         PORT NAME             LAST-ATTACK   COUNT
000d-88f7-b090 1    192.168.0.2   GigabitEthernet2/0/11 11:19:58 08/08 9
```

Table 112 Field descriptions of the **display arp attack-list** command

Field	Description
MAC ADDR	MAC address of the ARP attack packet
VLAN	VLAN of the ARP attack packet
IP ADDR	IP address of the ARP attack packet
PORT NAME	Port that received the ARP attack packet
LAST-ATTACK	Time of the last ARP attack
COUNT	Number of the ARP attack packets

display arp entry-limit

Syntax **display arp entry-limit** [*interface-type interface-number*]

View Any view

Parameter *interface-type*: Port type.

interface-number: Port number.

Description Use the **display arp entry-limit** command to display the number limits of ARP entries.

If you specify a port, the command will display the total maximum number of ARP entries and the maximum number of dynamic ARP entries on the port.

If you do not specify a port, the command will display the total maximum number of ARP entries and the maximum number of dynamic ARP entries on each port.

Example # Display the current number limits of ARP entries.

```
<SW7750> display arp entry-limit
 The maximum ARP entry number is 8192
 The maximum dynamic ARP entry number of the port GigabitEthernet0/0/1 is 2048
 The maximum dynamic ARP entry number of the port GigabitEthernet0/0/2 is 2048
 The maximum dynamic ARP entry number of the port GigabitEthernet0/0/3 is 2048
 The maximum dynamic ARP entry number of the port GigabitEthernet0/0/4 is 2048
 The maximum dynamic ARP entry number of the port GigabitEthernet3/0/1 is 6000
......
```

display arp interface

Syntax **display arp interface** *interface-type interface-number*

View Any view

Parameter *interface-type*: Port type.

Interface-number: Port number.

Description Use the **display arp interface** command to display the ARP entries of a specified port.

Example # Display the ARP entries of Ethernet 3/0/1.

```
<SW7750> display arp interface ethernet 3/0/1
              Type: S-Static   D-Dynamic
IP Address     MAC Address    VLAN ID Port Name         Aging Type
10.1.1.2       000f-e201-0102 1       Ethernet3/0/1     N/A   S
```

display arp rate-limit

Syntax **display arp rate-limit**

View System view

Parameter None

Description Use the **display arp rate-limit** command to display ARP packet rate limit configuration information.

Example # Display ARP packet rate limit configuration information.

<SW7750> display arp rate-limit

```
ARP rate limit is on!
 Arp rate limit is 15 packets persecond.
 Blocked ports will be recovered in 300 seconds.

 Blocked Ports:
 ---------------------------------

 GigabitEthernet2/0/11 is blocked and will be recovered in 200 seconds
```

display arp slot

Syntax **display arp slot** *slot-id*

View Any view

Parameter *slot-id*: ID of a slot.

Description Use the **display arp slot** command to display the ARP entries of all ports on the specified slot.

Example # Display the ARP entries on the third slot.

```
<SW7750> display arp slot 3
            Type: S-Static   D-Dynamic
IP Address     MAC Address    VLAN ID Port Name        Aging Type
10.1.1.2       000f-e201-0102 1       Ethernet3/0/1    N/A   S
```

display arp source-suppression

Syntax **display arp source-suppression**

View Any view

Parameter None

Description Use the **display arp source-suppression** command to display the ARP source suppression configuration on the current switch.

Example # Display the ARP source suppression configuration on the current switch.

```
<SW7750> display arp source-suppression
 ARP suppression limit total: 100
 ARP suppression limit local: 3
 ARP suppression limit through: 3
```

display arp timer aging

Syntax **display arp timer aging**

View Any view

Parameter None

Description Use the **display arp timer aging** command to display the setting for ARP aging timer.

Related commands: **arp timer aging**.

Example # Display the setting for ARP aging timer.

```
<SW7750> display arp timer aging
 Current ARP aging time is 20 minute(s)(default)
```

The above information shows that the time for ARP aging timer is 20 minutes.

display arp vlan

Syntax **display arp vlan** *vlan-id*

View Any view

Parameter *vlan-id*: VLAN ID.

Description Use the **display arp vlan** command to display the ARP entries of all ports in a specified VLAN.

Example # Display the ARP entries of VLAN 1.

```
<SW7750> display arp vlan 1
            Type: S-Static   D-Dynamic
IP Address     MAC Address    VLAN ID Port Name        Aging Type
10.1.1.2       000f-e201-0102 1       Ethernet3/0/1    N/A   S
```

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 gratuitous ARP learning.

Use the **undo gratuitous-arp-learning enable** command to disable gratuitous ARP learning.

By default, gratuitous ARP learning is disabled.

With gratuitous ARP learning enabled, a switch operates as follows when receiving a gratuitous ARP packet:

If an ARP entry in the cache matches the packet, the switch updates the ARP entry using the sender hardware address carried in the gratuitous ARP packet.

If no ARP entry in the cache matches the packet, an ARP entry corresponding to the packet is added to the cache.

Example # Enable gratuitous ARP learning on the switch.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] gratuitous-arp-learning enable
```

reset arp

Syntax **reset arp** [**dynamic** | **static** | **interface** *interface-type interface-number*]

View User view

Parameter **dynamic**: Clears dynamic ARP entries.

static: Clears static ARP entries.

interface: Clears ARP entries of a specified port. *interface-type* identifies the port type, and *interface-number* identifies the port number.

Description Use the **reset arp** command to clear ARP entries.

Related commands: **arp static**, **display arp**.

Example # Clear static ARP entries.

```
<SW7750> reset arp static
```

reset arp attack-list

Syntax **reset arp attack-list**

View User view

Parameter None

Description Use the **reset arp attack-list** command to clear the ARP attack information.

Related commands: **arp mac-arp-map limit**, **display arp attack-list**.

Example # Clear the ARP attack information.

```
<SW7750> reset arp attack-list
```

53 PROXY ARP CONFIGURATION COMMANDS

arp proxy enable

Syntax **arp proxy enable**

undo arp proxy enable

View VLAN interface view

Parameter None

Description Use the **arp proxy enable** command to enable proxy ARP.

Use the **undo arp proxy enable** command to disable proxy ARP.

By default, proxy ARP is disabled.

Related commands: **display arp proxy**.

Example # Enable proxy ARP on VLAN-interface 2.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 2
[SW7750-Vlan-interface2] arp proxy enable
```

arp proxy source-vlan enable

Syntax **arp proxy source-vlan enable**

undo arp proxy source-vlan enable

View VLAN interface view

Parameter None

Description Use the **arp proxy source-vlan enable** command to enable intra-VLAN proxy ARP, so that proxy ARP is able to process intra-VLAN ARP requests to provide Layer 3 connectivity between Layer 2 isolated ports in the same VLAN.

Use the **undo arp proxy source-vlan enable** command to disable intra-VLAN proxy ARP, so that proxy ARP only processes inter-VLAN ARP requests instead of intra-VLAN ARP request.

By default, intra-VLAN proxy ARP is disabled, and proxy ARP only processes inter-VLAN ARP requests after it is enabled.

Note that intra-VLAN proxy ARP can be enabled only after proxy ARP is enabled.

Related commands: **arp proxy enable**, **display arp proxy**.

Example # With proxy ARP enabled, enable intra-VLAN proxy ARP for VLAN 2.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 2
[SW7750-Vlan-interface2] arp proxy source-vlan enable
```

display arp proxy

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

View Any view

Parameter **interface** *interface-type interface-number*: Specifies an interface by its type and number.

Description Use the **display arp proxy** command to display the status of proxy ARP (enabled/disabled).

Related commands: **arp proxy enable**.

Example # Display the status of proxy ARP on VLAN-interface 2.

```
<SW7750> display arp proxy interface Vlan-interface 2
Interface Vlan-interface2
 Proxy ARP status: disabled
```

54 DHCP SERVER CONFIGURATION COMMANDS

dhcp enable

Syntax **dhcp enable**

undo dhcp enable

View System view

Parameter None

Description Use the **dhcp enable** command to enable DHCP.

Use the **undo dhcp enable** command to disable DHCP.

By default, DHCP is enabled.

You must first enable DHCP before performing other DHCP-related configurations. This configuration is necessary for both DHCP servers and DHCP relay agents.

Example # Enable DHCP.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] dhcp enable
```

dhcp select global

Syntax VLAN interface view:

dhcp select global

undo dhcp select

System view:

dhcp select global { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }

undo dhcp select { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }

View System view, VLAN interface view

Parameter **interface** *interface-type interface-number* [**to** *interface-type interface-number*]: Specifies the interface(s) to operate in global address pool mode. The *interface-type* and *interface-number* arguments are the type and number of an interface. The **to** keyword separates the start and the end of an interface range.

all: Specifies all ports to operate in global address pool mode.

Description Use the **dhcp select global** command to configure the specified interface(s) or all interfaces to operate in global DHCP address pool mode. Upon receiving a DHCP packet from a DHCP client through an interface operating in global DHCP address pool mode, the DHCP server chooses an IP address from a global DHCP address pool of the local DHCP server and assigns the address to the DHCP client.

Use the **undo dhcp select** command to restore the default DHCP packet processing mode.

By default, an interface operates in local DHCP server global address pool mode.

Example # Configure all interfaces to operate in global DHCP address pool mode, so that when a DHCP packet is received from a DHCP client through any interface, the DHCP server assigns an IP address in local global DHCP address pools to the DHCP client.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] dhcp select global all
```

dhcp select interface

Syntax VLAN interface view:

dhcp select interface

undo dhcp select

System view:

dhcp select interface { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }

undo dhcp select { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }

View System view, VLAN interface view

Parameter **interface** *interface-type interface-number* [**to** *interface-type interface-number*]: Specifies the interface(s) to operate in interface address pool mode.

all: Specifies all interfaces to operate in interface address pool mode.

Description Use the **dhcp select interface** command to configure the specified interface(s) to operate in DHCP interface address pool mode. Upon receiving a DHCP packet from a DHCP client through an interface operating in interface address pool mode, the DHCP server chooses an IP address from the interface address pool of the local DHCP server and assigns the address to the DHCP client.

Use the **undo dhcp select** command to restore the default DHCP packet processing mode.

By default, an interface operates in local DHCP server global address pool mode.

Example # Configure all interfaces to operate in interface address pool mode, so that when a DHCP packet is received from a DHCP client through any interface, the DHCP server assigns an IP address in the local interface address pool to the DHCP client.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] dhcp select interface all
```

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 the unauthorized DHCP server detecting function.

Use the **undo dhcp server detect** command to disable the unauthorized DHCP server detecting function.

By default, the unauthorized DHCP server detecting function is disabled.

With the unauthorized DHCP server detecting function enabled, a DHCP server tracks the information (such as the IP addresses and interfaces) of DHCP servers to enable the administrator to detect unauthorized DHCP servers in time and take proper measures.

Example # Enable the unauthorized DHCP server detecting function.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] dhcp server detect
```

dhcp server dns-list

Syntax VLAN interface view:

dhcp server dns-list *ip-address*&<1-8>

undo dhcp server dns-list { *ip-address* | **all** }

System view:

dhcp server dns-list *ip-address*&<1-8> { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }

undo dhcp server dns-list { *ip-address* | **all** } { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }

View System view, VLAN interface view

Parameter *ip-address*&<1-8>: IP address of a DNS server. &<1-8> means you can provide up to eight DNS server IP addresses. When inputting more than one DNS server IP address, separate two neighboring IP addresses with a space.

interface *interface-type interface-number* [**to** *interface-type interface-number*]: Specifies the interface(s), through which you can specify the corresponding interface address pools.

all: (In comparison with the *ip-address* argument) Specifies all DNS server IP addresses.

all: (In comparison with the **interface** keyword) Specifies all interface address pools.

Description Use the **dhcp server dns-list** command to configure DNS server IP address(es) for the DHCP address pool(s) of specified interface(s).

Use the **undo dhcp server dns-list** command to remove the DNS server IP address(es) configured for the DHCP address pool(s) of the specified interface(s).

By default, no DNS server IP address is configured for a DHCP interface address pool.

If you execute the **dhcp server dns-list** command repeatedly, the new configuration overwrites the previous one.

Related commands: **dns-list**.

Example # Configure the DNS server IP address 1.1.1.254 for the DHCP address pool of the VLAN-interface 1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 1
[SW7750-Vlan-interface1] dhcp server dns-list 1.1.1.254
```

dhcp server domain-name

Syntax VLAN interface view:

dhcp server domain-name *domain-name*

undo dhcp server domain-name

System view:

dhcp server domain-name *domain-name* { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }

undo dhcp server domain-name { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }

View System view, VLAN interface view

Parameter *domain-name*: Domain name of the DHCP clients whose IP addresses are from the specified interface address pool(s). This argument is a string of 3 to 50 characters.

interface *interface-type interface-number* [**to** *interface-type interface-number*]: Specifies the interface(s), through which you can specify the corresponding interface address pool(s).

all: Specifies all interface address pools.

Description Use the **dhcp server domain-name** command to configure a domain name for the DHCP clients whose IP addresses are from the specified interface address pool(s).

Use the **undo dhcp server domain-name** command to remove the configured domain name.

By default, no domain name is configured for the DHCP clients.

Related commands: **domain-name**.

Example # Set aabbcc.com as the domain name of the DHCP client whose IP address is obtained from the DHCP address pool of the current VLAN-interface 1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 1
[SW7750-Vlan-interface1] dhcp server domain-name aabbcc.com
```

dhcp server expired

Syntax VLAN interface view:

dhcp server expired { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** }

undo dhcp server expired

System view:

dhcp server expired { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** } { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }

undo dhcp server expired { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }

View System view, VLAN interface 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 that the lease time is unlimited. (But actually, the system limits the maximum lease time to about 25 years.)

interface *interface-type interface-number* [**to** *interface-type interface-number*]: Specifies the interface(s), through which you can specify the corresponding interface address pool(s).

all: Specifies all interface address pools.

Description Use the **dhcp server expired** command to configure the lease time of the IP addresses in the specified interface address pool(s).

Use the **undo dhcp server expired** command to restore the default lease time.

The default lease time is one day.

Related commands: **expired**.

Example # Set the lease time of the IP addresses in all interface address pools to be 1 day, 2 hours and 3 minutes.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] dhcp server expired day 1 hour 2 minute 3 all
```

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: IP address that is not available for being assigned to DHCP clients automatically (An IP address of this kind is known as a forbidden IP address). This argument also marks the lower end of the range of the forbidden IP addresses.

high-ip-address: IP address that is not available for being assigned to DHCP clients. This argument also marks the higher end of the range of the forbidden IP addresses. Note that this argument cannot be less than the *low-ip-address* argument. If you do not provide this argument, only the IP address specified by the *low-ip-address* argument is forbidden.

Description

Use the **dhcp server forbidden-ip** command to forbid the specified IP addresses in a DHCP address pool to be automatically assigned.

Use the **undo dhcp server forbidden-ip** command to cancel this configuration.

By default, all IP addresses in an address pool are allowed to be automatically assigned.

Note that the specified address range cannot contain statically-bound addresses when you use the **undo dhcp server forbidden-ip** command.

Related commands:

dhcp server ip-pool, **network**, **static-bind ip-address**, **dhcp server static-bind**.

Example

Forbid the IP addresses in the range 10.110.1.1 to 10.110.1.63 to be automatically assigned.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] 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 a DHCP address pool, which uniquely identifies the address pool. This argument is a string of 1 to 35 characters.

Description

Use the **dhcp server ip-pool** command to create a global DHCP address pool and enter DHCP address pool view. If the address pool identified by the *pool-name* argument already exists, this command leads you to DHCP address pool view.

Use the **undo dhcp server ip-pool** command to remove a specified DHCP address pool.

By default, no global DHCP address pool is created.

Related commands: **dhcp enable**.

Example # Create DHCP address pool 0.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] dhcp server ip-pool 0
[SW7750-dhcp-pool-0]
```

dhcp server nbns-list

Syntax VLAN interface view:

dhcp server nbns-list *ip-address*&<1-8>

undo dhcp server nbns-list { *ip-address* | **all** }

System view:

dhcp server nbns-list *ip-address*&<1-8> { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }

undo dhcp server nbns-list { *ip-address* | **all** } { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }

View System view, VLAN interface view

Parameter *ip-address*&<1-8>: IP address of a WINS server. &<1-8> means you can provide up to eight WINS server IP addresses. When inputting more than one WINS server IP address, separate two neighboring IP addresses with a space.

interface *interface-type interface-number* [**to** *interface-type interface-number*]: Specifies the interface(s), through which you can specify the corresponding interface address pool(s).

all: (In comparison with the *ip-address* argument) Specifies all WINS server IP addresses.

all: (In comparison with the **interface** keyword) Specifies all interface address pools.

Description Use the **dhcp server nbns-list** command to configure WINS server IP address(es) for the specified DHCP interface address pool(s).

Use the **undo dhcp server nbns-list** command to remove the WINS server IP address(es) configured for the specified DHCP interface address pool(s).

By default, no WINS server IP address is configured for a DHCP interface address pool.

If you execute the **dhcp server nbns-list** command repeatedly, the new configuration overwrites the previous one.

Related commands: **nbns-list**, **dhcp server netbios-type**.

Example

Configure the WINS server IP address 10.12.1.99 for all the DHCP interface address pools.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] dhcp server nbns-list 10.12.1.99 all
```

dhcp server netbios-type

Syntax

VLAN interface view:

dhcp server netbios-type { **b-node** | **h-node** | **m-node** | **p-node** }

undo dhcp server netbios-type

System view:

dhcp server netbios-type { **b-node** | **h-node** | **m-node** | **p-node** } { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }

undo dhcp server netbios-type { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }

View

System view, VLAN interface view

Parameter

b-node: Specifies the broadcast type. Nodes of this type acquire host name-to-IP address mapping by broadcasting.

p-node: Specifies the peer-to-peer type. Nodes of this type acquire host name-to-IP address mapping by communicating with the WINS server.

m-node: Specifies the m-typed mixed type. Nodes of this type are p-nodes with some broadcasting features. (The character m here stands for mixed.)

h-node: Specifies the hybrid type. Nodes of this type are b-nodes with peer-to-peer communicating features.

interface *interface-type interface-number* [**to** *interface-type interface-number*]: Specifies the interface(s), through which you can specify the corresponding interface address pools.

all: Specifies all interface address pools.

Description

Use the **dhcp server netbios-type** command to configure the NetBIOS node type of the DHCP clients whose IP addresses are from the specified interface address pool(s).

Use the **undo dhcp server netbios-type** command to restore the default NetBIOS node type.

By default, no NetBIOS node type is specified and the default NetBIOS node type is h-node.

Related commands: **netbios-type**, **dhcp server nbns-list**.

Example # Specify p-node as the NetBIOS node type of the DHCP clients whose IP addresses are from the DHCP address pool of VLAN-interface 1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface vlan-interface 1
[SW7750-Vlan-interface1] dhcp server netbios-type p-node
```

dhcp server option

Syntax VLAN interface view:

dhcp server option *code* { **ascii** *ascii-string* | **hex** *hex-string*&<1-10> | **ip-address** *ip-address*&<1-8> }

undo dhcp server option *code*

System view:

dhcp server option *code* { **ascii** *ascii-string* | **hex** *hex-string*&<1-10> | **ip-address** *ip-address*&<1-8> } { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }

undo dhcp server option *code* { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }

View System view, VLAN interface view

Parameter *code*: Customized option number, ranging from 2 to 254. Note that this argument cannot be 3, 6, 15, 44, 46, 50 through 55, 57 through 59.

ascii *ascii-string*: Specifies a string that is of 1 to 63 characters. Note that each character of the string must be an ASCII character.

hex *hex-string*&<1-10>: Specifies strings, a hexadecimal number of 1 to 8 digits. &<1-10> means you can provide up to 10 such strings. When inputting more than one string, separate two neighboring strings with a space.

ip-address *ip-address*&<1-8>: Specifies IP addresses. &<1-8> means you can provide up to eight IP addresses. When inputting more than one IP address, separate two neighboring IP addresses with a space.

interface *interface-type interface-number* [**to** *interface-type interface-number*]: Specifies the interface(s), through which you can specify the corresponding interface address pools.

all: Specifies all interface address pools.

Description Use the **dhcp server option** command to customize DHCP options for the specified DHCP interface address pool(s).

Use the **undo dhcp server option** command to remove the customized DHCP options.

If you execute the **dhcp server option** command repeatedly, the new configuration overwrites the previous one.

Related commands: **option**.

Example # Configure option 100 to be 0x11 and 0x22 for all DHCP interface address pools.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] dhcp server option 100 hex 11 22 all
```

dhcp server ping

Syntax **dhcp server ping** { **packets** *number* | **timeout** *milliseconds* }

undo dhcp server ping { **packets** | **timeout** }

View System view

Parameter **packets** *number*: Specifies the number of the packets to be sent in a ping test. The *number* argument ranges from 0 to 10 and defaults to 2. Value 0 means no packet will be sent.

timeout *milliseconds*: Specifies the timeout time (in milliseconds) of each packet. The *milliseconds* argument ranges from 0 to 10,000 and defaults to 500.

Description Use the **dhcp server ping** command to set the maximum number of the ICMP packets a DHCP server sends in a ping test and the maximum response timeout time of each ICMP packet.

Use the **undo dhcp server ping** command to restore the default settings.

Example # Set the maximum number of the packets the DHCP server sends in a ping test to 10, and the timeout time of each packet to 300 milliseconds.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] dhcp server ping packets 10
[SW7750] dhcp server ping timeout 300
```

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 statically bound. Note that the specified IP address must belong to the same network segment as that of the VLAN interface.

mac-address: MAC address to which the IP address is statically bound.

Description Use the **dhcp server static-bind** command to statically bind an IP address of the current address pool to a MAC address.

Use the **undo dhcp server static-bind** command to cancel an IP-MAC address binding.

By default, no IP address in an address pool is statically bound.

It should be noted that:

- An IP address can be statically bound to only one MAC address. A MAC address can be bound with only one IP address statically.
- The IP address to be statically bound cannot be an interface IP address of the device; otherwise the static binding does not take effect. The device of the bound MAC address can also obtain another IP address.

Example # Statically bind the IP address 10.1.1.1 to the MAC address 0000-e03f-0305. (Assume that the interface address pool of VLAN-interface 1 already exists and the IP address belongs to the address pool.)

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface vlan-interface 1
[SW7750-Vlan-interface1] dhcp server static-bind ip-address 10.1.1.1
 mac-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-address: Specifies an IP address.

Description

Use the **display dhcp server conflict** command to display the statistics of IP address conflicts on the DHCP server.

Related commands:

reset dhcp server conflict.

Example

Display the statistics of IP address conflicts.

```
<SW7750> display dhcp server conflict all
Address             Discover Time
10.110.1.2         Jan 11 2003 11:57:07 PM
```

Table 113 Field descriptions of the **display dhcp server conflict** command

Field	Description
Address	Conflicting IP address
Discover Time	Time when the conflict is detected

display dhcp server expired

Syntax

display dhcp server expired { **ip** *ip-address* | **pool** [*pool-name*] | **interface** [*interface-type interface-number*] | **all** }

View

Any view

Parameter

ip *ip-address*: Specifies an IP address.

pool [*pool-name*]: Specifies a global address pool. The *pool-name* argument, a string of 1 to 35 characters, is the name of an address pool. If you do not provide this argument, this command applies to all global address pools.

interface [*interface-type interface-number*]: Specifies a VLAN interface. If you do not specify a VLAN interface, this command applies to all VLAN interfaces.

all: Specifies all DHCP address pools.

Description

Use the **display dhcp server expired** command to display the lease expiration information about an IP address, or the lease expiration information about all IP addresses in one or all DHCP address pools. When all the IP addresses in an address pool are assigned, the DHCP server assigns the IP addresses that are expired to DHCP clients.

Example

Display the lease expiration information about the IP addresses in all DHCP address pools.

```
<SW7750> display dhcp server expired all
Global pool:
IP address    Hardware address    Lease expiration          Type

Interface pool:
 IP address    Hardware address    Lease expiration          Type

--- total 0 entry ---
```

Table 114 Field descriptions of the **display dhcp server expired** command

Field	Description
Global pool	The information about the expired IP addresses of global address pools
Interface pool	The information about the expired IP addresses of interface address pools
IP address	Bound IP addresses
Hardware address	MAC addresses to which IP addresses are bound
Lease expiration	The time when a lease time expires
Type	Address 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 free (that is, unassigned) IP addresses.

Example # Display the free IP addresses.

```
<SW7750> 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** [*interface-type interface-number*] | **all** }

View Any view

Parameter **ip** *ip-address*: Specifies an IP address.

pool [*pool-name*]: Specifies a global address pool. The *pool-name* argument, a string of 1 to 35 characters, is the name of an address pool. If you do not provide this argument, this command applies to all global address pools.

interface [*interface-type interface-number*]: Specifies a VLAN interface. If you do not specify a VLAN interface, this command applies to all VLAN interfaces.

all: Specifies all address pools.

Description Use the **display dhcp server ip-in-use** command to display the address binding information of an IP address, the specified DHCP address pool(s) or all DHCP address pools.

Related commands: **reset dhcp server ip-in-use**.

Example # Display the address binding information of all DHCP address pools.

```
<SW7750> display dhcp server ip-in-use all
Global pool:
IP address    Hardware address   Lease expiration           Type
2.2.2.2        4444-4444-4444     NOT Used                  Manual

Interface pool:
 IP address    Hardware address   Lease expiration          Type
5.5.5.1        0050-ba28-930a      NOT Used                 Manual

--- total 2 entry ---
```

Table 115 Field descriptions of the **display dhcp server ip-in-use** command

Field	Description
Global pool	Address binding information of global DHCP address pools
Interface pool	Address binding information of interface DHCP address pools
IP address	Bound IP address
Hardware address	MAC address to which the IP address is bound
Lease expiration	Time when the lease expires
Type	Address 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 the statistics on a DHCP server.

Related commands: **reset dhcp server statistics**.

Example # Display the statistics on a DHCP server.

```
<SW7750> 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 116 Field descriptions of the **display dhcp server statistics** command

Field	Description
Global Pool	Statistics about global address pools
Interface Pool	Statistics about interface address pools
Pool Number	Number of address pools
Auto	Number of the automatically bound IP addresses
Manual	Number of the manually bound IP addresses
Expire	Number of the expired IP addresses
Boot Request: 6	Statistics about the DHCP packets received from DHCP clients
Dhcp Discover: 1	
Dhcp Request: 4	
Dhcp Decline: 0	
Dhcp Release: 1	
Dhcp Inform: 0	
Boot Reply: 4	Statistics about the DHCP packets sent to DHCP clients
Dhcp Offer: 1	
Dhcp Ack: 3	
Dhcp Nak: 0	
Bad Messages	Number of the error DHCP packets

display dhcp server tree

Syntax **display dhcp server tree** { **pool** [*pool-name*] | **interface** [*interface-type interface-number*] | **all** }

View Any view

Parameter **pool** [*pool-name*]: Specifies a global address pool. The *pool-name* argument, a string of 1 to 35 characters, is the name of an address pool. If you do not provide this argument, this command applies to all global address pools.

interface [*interface-type interface-number*]: Specifies a VLAN interface. If you do not specify a VLAN interface, this command applies to all VLAN interfaces.

all: Specifies all address pools.

Description

Use the **display dhcp server tree** command to display information about address pool tree.

Example

Display the information about address pool tree.

```
<SW7750> 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 10 ip-address 255.0.0.0
  expired 1 0 0

Pool name: 6
  static-bind ip-address 10.10.1.2 mask 255.0.0.0
  static-bind mac-address 000f-e2fc-0001
Parent node:5
  option 10 ip-address 255.255.0.0
  expired 1 0 0

Pool name: 7
network 10.10.1.64 mask 255.255.255.192
PrevSibling node:5
  option 10 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
```

Table 117 Field descriptions of the **display dhcp server tree** command

Field	Description
Global pool	Information about global address pools
Interface pool	Information about interface address pools
Pool name	Address pool name
network	Assignable IP address range
static-bind ip-address 10.10.1.2 mask 255.0.0.0	Statically bound IP and MAC addresses
static-bind mac-address 000f-e2fc-0001	

Table 117 Field descriptions of the **display dhcp server tree** command

Field	Description
Child node:6	The address pool 6 is the child node of this node. This field can display the information about the following types of node: Child node: Displays the information about an address pool that is a child of the current address pool. Parent node: Displays the information about the address pool that is the parent of the current address pool. Sibling node: Displays the information about the next sibling address pool of the current address pool. (The order of sibling address pools are determined by the time when they are configured.) PrevSibling node: Displays the information about the previous sibling address pool of the current address pool.
option	Customized DHCP options
expired	The address lease time (in terms of number of days, hours, and minutes)
gateway-list	List of the gateways configured for the DHCP clients
dns-list	List of the DNS servers configured for the DHCP clients
domain-name	The domain name configured for the DHCP clients
nbns-list	List of the WINS servers configured for the DHCP clients

dns-list

Syntax **dns-list** *ip-address*&<1-8>

undo dns-list { *ip-address* | **all** }

View DHCP address pool view

Parameter *ip-address*&<1-8>: IP address of a DNS server. &<1-8> string means you can provide up to eight DNS server IP addresses. When inputting more than one IP address, separate two neighboring IP addresses with a space.

all: Specifies all configured DNS server IP addresses.

Description Use the **dns-list** command to configure one or multiple 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 the DHCP address pool.

By default, no DNS server IP address is configured.

If you execute the **dns-list** command repeatedly, the new configuration overwrites the previous one.

Related commands: **dhcp server dns-list**, **dhcp server ip-pool**.

Example # Configure the DNS server IP address 1.1.1.254 for global DHCP address pool 0.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] dhcp server ip-pool 0
[SW7750-dhcp-pool-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 for the DHCP clients of a global DHCP address pool, a string of 3 to 50 characters.

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.

By default, no domain name is configured for the DHCP clients of a global DHCP address pool.

Related commands: **dhcp server ip-pool**, **dhcp server domain-name**.

Example # Configure the domain name "mydomain.com" for the DHCP clients of the global DHCP address pool 0.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] dhcp server ip-pool 0
[SW7750-dhcp-pool-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 that the lease time is unlimited. (But actually, the system limits the maximum lease time to about 25 years.)

Description

Use the **expired** command to configure the lease time of the IP addresses in a global DHCP address pool.

Use the **undo expired** command to restore the default lease time.

The default lease time is one day.

Related commands: **dhcp server ip-pool**, **dhcp server expired**.

Example

Set the lease time of the IP addresses in the global DHCP address pool 0 to 1 day, 2 hours and 3 minutes.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] dhcp server ip-pool 0
[SW7750-dhcp-pool-0] expired day 1 hour 2 minute 3
```

gateway-list

Syntax

gateway-list *ip-address*&<1-8>

undo gateway-list { *ip-address* | **all** }

View

DHCP address pool view

Parameter

ip-address&<1-8>: IP address of a gateway. &<1-8> means you can provide up to eight gateway IP addresses. When inputting more than one IP address, separate two neighboring IP addresses with a space.

all: Specifies all configured gateway IP addresses.

Description

Use the **gateway-list** command to configure one or multiple gateway IP addresses for the DHCP clients of a DHCP address pool.

Use the **undo gateway-list** command to remove one or all the configured gateway IP addresses configured for the DHCP address pool.

By default, no gateway IP address is configured.

If you execute the **gateway-list** command repeatedly, the new configuration overwrites the previous one.

Example # Configure the gateway IP address 10.110.1.99 for the global DHCP address pool 0.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] dhcp server ip-pool 0
[SW7750-dhcp-pool-0] gateway-list 10.110.1.99
```

nbns-list

Syntax **nbns-list** *ip-address*&<1-8>

undo nbns-list { *ip-address* | **all** }

View DHCP address pool view

Parameter *ip-address*&<1-8>: IP address of a WINS server. &<1-8> means you can provide up to eight WINS server IP addresses. When inputting more than one IP address, separate two neighboring IP addresses with a space.

all: Specifies all configured WINS server IP addresses.

Description Use the **nbns-list** command to configure one or multiple WINS server IP addresses for the DHCP clients of a global DHCP address pool.

Use the **undo nbns-list** command to remove one or all WINS server IP addresses configured for the DHCP clients.

By default, no WINS server IP address is configured.

If you execute the **nbns-list** command repeatedly, the new configuration overwrites the previous one.

Related commands: **dhcp server ip-pool**, **dhcp server nbns-list**, **netbios-type**.

Example # Configure the WINS server IP address 10.12.1.99 for the global DHCP address pool 0.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] dhcp server ip-pool 0
[SW7750-dhcp-pool-0] nbns-list 10.12.1.99
```

netbios-type

Syntax **netbios-type** { **b-node** | **h-node** | **m-node** | **p-node** }

undo netbios-type

View DHCP address pool view

Parameter

b-node: Specifies the broadcast type. Nodes of this type acquire host name-to-IP address mapping by broadcasting.

p-node: Specifies the peer-to-peer type. Nodes of this type acquire host name-to-IP address mapping by communicating with the WINS server.

m-node: Specifies the mixed type. Nodes of this type are p-nodes with some broadcasting features.

h-node: Specifies the hybrid type. Nodes of this type are b-nodes with peer-to-peer communicating features.

Description

Use the **netbios-type** command to configure the DHCP clients of a global address pool to be of specified NetBIOS node type.

Use the **undo netbios-type** command to restore the default NetBIOS node type.

By default, no NetBIOS node type is specified. In this case, the client uses h-node.

Related commands: **dhcp server ip-pool**, **dhcp server netbios-type**, **nbns-list**.

Example

Configure the DHCP clients of the global DHCP address pool 0 to be of b-node type.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] dhcp server ip-pool 0
[SW7750-dhcp-pool-0] netbios-type b-node
```

network

Syntax

network *ip-address* [**mask** *mask*]

undo network

View

DHCP address pool view

Parameter

ip-address: IP address of a network segment, used to specify an IP address range.

mask *mask*: Specifies a subnet mask in dotted decimal notation. If you do not specify the *mask* argument, the default subnet mask is used.

Description

Use the **network** command to configure a dynamically assigned IP address range (where IP addresses will be dynamically assigned to DHCP clients).

Use the **undo network** command to remove a dynamically assigned IP address range.

By default, no such IP address range is configured for a DHCP address pool.

Note that you can configure only one such IP address range for a DHCP address pool. If you execute the **network** command repeatedly, the new configuration overwrites the previous one.

Related commands: **dhcp server ip-pool**, **dhcp server forbidden-ip**.

Example # Configure the dynamically assigned IP address range 192.168.8.0/24 for the global DHCP address pool 0.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] dhcp server ip-pool 0
[SW7750-dhcp-pool-0] network 192.168.8.0 mask 255.255.255.0
```

option

Syntax **option** *code* { **ascii** *ascii-string* | **hex** *hex-string*&<1-10> | **ip-address** *ip-address*&<1-8> }

undo option *code*

View DHCP address pool view

Parameter *code*: Customized option number ranging from 2 to 254. Note that this argument cannot be 3, 6, 15, 44, 46, 50 through 55, 57 through 59.

ascii *ascii-string*: Specifies a string that is of 1 to 63 ASCII characters.

hex *hex-string*&<1-10>: Specifies strings, a hexadecimal number of 1 to 8 digits. &<1-10> means that you can provide up to 10 such strings. When entering more than one strings, separate two neighboring strings with a space.

ip-address *ip-address*&<1-8>: Specifies IP addresses. &<1-8> means that you can provide up to eight IP addresses. When entering more than one IP address, separate two neighboring IP addresses with a space.

Description Use the **option** command to customize DHCP options for a global DHCP address pool.

Use the **undo option** command to remove the customized DHCP options.

If you execute the **option** command repeatedly, the new configuration overwrites the previous one.

Related commands: **dhcp server ip-pool**, **dhcp server option**.

Example # Configure option 100 to be 0x11 and 0x22 for the global DHCP address pools.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] dhcp server ip-pool 0
[SW7750-dhcp-pool-0] option 100 hex 11 22
```

reset dhcp server conflict

Syntax **reset dhcp server conflict** { **all** | **ip** *ip-address* }

View User view

Parameter **ip** *ip-address*: Specifies an IP address, whose conflict statistics will be cleared.

all: Clears all address conflict statistics.

Description Use the **reset dhcp server conflict** command to clear address conflict statistics.

Related commands: **display dhcp server conflict**.

Example # Clear all address conflict statistics.

```
<SW7750> reset dhcp server conflict all
```

reset dhcp server ip-in-use

Syntax **reset dhcp server ip-in-use** { **all** | **interface** [*interface-type interface-number*] | **ip** *ip-address* | **pool** [*pool-name*] }

View User view

Parameter **all**: Clears the dynamic address binding information about all IP addresses.

interface [*interface-type interface-number*]: Clears the dynamic address binding information about a specified interface address pool. If you do not specify the *interface-number* argument, this command clears the dynamic address binding information about all interface address pools.

ip *ip-address*: Clears the dynamic address binding information about a specified IP address.

pool [*pool-name*]: Clears the dynamic address binding information about a specified address pool. The *pool-name* argument, a string of 1 to 35 characters, is the name of an address pool. If you do not provide this argument, this command clears the dynamic address binding information about all global address pools.

Description Use the **reset dhcp server ip-in-use** command to clear the specified or all dynamic address binding information.

Related commands: **display dhcp server ip-in-use**.

Example # Clear the dynamic address binding information about the IP address 10.110.1.1.

```
<SW7750> 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 the statistics on a DHCP server, such as the number of DHCP unrecognized packets/request packets/response packets.

Related commands: **display dhcp server statistics**.

Example # Clear the statistics on a DHCP server.

```
<SW7750> reset dhcp server statistics
```

static-bind ip-address

Syntax **static-bind ip-address** *ip-address* [**mask** *mask*]

undo static-bind ip-address

View DHCP address pool view

Parameter *ip-address*: IP address to be bound.

mask *mask*: Subnet mask of the specified IP address. If you do not specify the *mask* argument, the default subnet mask is used.

Description Use the **static-bind ip-address** command to specify an IP address to be statically bound to a MAC address.

Use the **undo static-bind ip-address** command to remove a statically bound IP address.

By default, no IP address is statically bound.

Note that:

- *The **static-bind ip-address** command must be used together with the **static-bind mac-address** command, to specify a statically bound IP address or MAC address.*
- *If you execute the **static-bind ip-address** command repeatedly, the new configuration overwrites the previous one.*

Related commands: **dhcp server ip-pool**, **static-bind mac-address**.

Example # Bind the IP address 10.1.1.1 (with the subnet mask 255.255.255.0) to the MAC address 0000-e03f-0305.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] dhcp server ip-pool 0
[SW7750-dhcp-pool-0] static-bind ip-address 10.1.1.1 mask 255.255.255.0
[SW7750-dhcp-pool-0] static-bind mac-address 0000-e03f-0305
```

static-bind mac-address

Syntax **static-bind mac-address** *mac-address*

undo static-bind mac-address

View DHCP address pool view

Parameter *mac-address*: MAC address of the host to which the IP address is to be bound. You need to provide this argument in the form of H-H-H.

Description Use the **static-bind mac-address** command to specify a MAC address to which an IP address will be bound statically.

Use the **undo static-bind mac-address** command to remove such a MAC address.

By default, no such MAC address is specified.

Note that:

- *The **static-bind ip-address** command must be used together with the **static-bind mac-address** command, to respectively specify a statically bound IP address and MAC address.*
- *If you execute the **static-bind mac-address** command repeatedly, the new configuration overwrites the previous one.*

Related commands: **dhcp server ip-pool**, **static-bind ip-address**.

Example # Bind the IP address 10.1.1.1 (with the subnet mask 255.255.255.0) to the MAC address 0000-e03f-0305.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] dhcp server ip-pool 0
[SW7750-dhcp-pool-0] static-bind ip-address 10.1.1.1 mask 255.255.255.0
[SW7750-dhcp-pool-0] static-bind mac-address 0000-e03f-0305
```

55 DHCP RELAY AGENT CONFIGURATION COMMANDS

address-check

Syntax **address-check enable**

address-check disable

View VLAN interface view

Parameter None

Description Use the **address-check enable** command to enable the address checking function of the DHCP relay agent.

Use the **address-check disable** command to disable the address checking function of the DHCP relay agent.

By default, the address checking function of the DHCP relay agent is disabled on a VLAN interface.

Example # Enable the address checking function of the DHCP relay agent on VLAN-interface 1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface vlan-interface 1
[SW7750-Vlan-interface1] address-check enable
Address check turns on!
```

address-check dhcp-relay

Syntax **address-check dhcp-relay enable**

address-check dhcp-relay disable

View VLAN interface view

Parameter None

Description Use the **address-check dhcp-relay enable** command to validate the dynamic entries generated by the DHCP relay agent.

Use the **address-check dhcp-relay disable** command to invalidate the dynamic entries generated by the DHCP relay agent.

By default, the dynamic entries generated by the DHCP relay agent are valid.

This configuration will take effect only after the address checking function of the DHCP relay agent on the VLAN interface is enabled.

Example # Invalidate the dynamic entries generated by the DHCP relay agent.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 1
[SW7750-Vlan-interface1] address-check enable
[SW7750-Vlan-interface1] address-check dhcp-relay disable
```

address-check field enable

Syntax **address-check field** { **mac** | **vlan** | **port** } **enable**

address-check field { **mac** | **vlan** | **port** } **disable**

View VLAN interface view

Parameter **mac**: Enables or disables checking the MAC address.

vlan: Enables or disables checking the VLAN ID.

port: Enables or disables checking the port number.

Description Use the **address-check field enable** command to enable checking of the specified field.

Use the **address-check field disable** command to disable checking of the specified field.

By default, after enabled with the address checking function, the DHCP relay agent checks the IP address, MAC address, VLAN ID, and port number of a DHCP client respectively.

Example # Disable the checking of the VLAN ID and port number on VLAN-interface 1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 1
[SW7750-Vlan-interface1] address-check field vlan disable
[SW7750-Vlan-interface1] address-check field port disable
```

address-check no-matched

Syntax **address-check no-matched enable**

address-check no-matched disable

View VLAN interface view

Parameter None

Description Use the **address-check no-matched enable** command to forbid freely-connected clients to pass DHCP security check.

Use the **address-check no-matched disable** command to allow freely-connected clients to pass DHCP security check.

By default, freely-connected clients are not allowed to pass DHCP security check.

Freely-connected clients refer to the clients whose IP addresses and MAC addresses are not in the DHCP security table.

This configuration will take effect only after the address checking function of the DHCP relay agent on the VLAN interface is enabled.

Example # Configure to not allow freely-connected clients to pass DHCP security check on VLAN-interface 1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 1
[SW7750-Vlan-interface1] address-check enable
[SW7750-Vlan-interface1] address-check no-matched enable
```

dhcp-relay gateway interface

Syntax **dhcp-relay gateway** *ip-address* **interface** *interface-type interface-number* [**to** *interface-type interface-number*]

undo dhcp-relay gateway [*ip-address* | **interface** *interface-type interface-number* [**to** *interface-type interface-number*]]

View VLAN interface view

Parameter *ip-address*: IP address (primary or secondary) of the VLAN interface.

interface *interface-type interface-number* [**to** *interface-type interface-number*]: Specifies a port or multiple ports in the VLAN.

Description Use the **dhcp-relay gateway interface** command to specify a gateway address by binding one or multiple ports in the VLAN to one of the VLAN interface's IP addresses.

Use the **undo dhcp-relay gateway interface** command to remove the specified binding entry.

By default, no such a binding is created.

Example # Specify a gateway address by binding Ethernet 2/0/3 in VLAN 10 to IP address 10.1.1.1 of VLAN-interface 10.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 10
[SW7750-Vlan-interface10] dhcp-relay gateway 10.1.1.1 interface ethe
rnet2/0/3
```

dhcp-relay gateway vlan

Syntax **dhcp-relay gateway** *ip-address* **vlan** *vlan-id*

undo dhcp-relay gateway [**vlan** *vlan-id*]

View Ethernet port view

Parameter *ip-address*: IP address (primary or secondary) of the VLAN interface.

vlan *vlan-id*: ID of the VLAN to which the port belongs.

Description Use the **dhcp-relay gateway vlan** command to specify a gateway address by binding the Ethernet port in a VLAN to one of the VLAN interface's IP addresses.

Use the **undo dhcp-relay gateway** command to remove the specified binding entry.

Note that:

If the Ethernet port belongs to a sub-VLAN, you need to specify the ip address argument as the primary or secondary IP address of the corresponding super VLAN interface, and specify the vlan-id argument as the VLAN ID of the super VLAN; otherwise, the system prompts error information due to VLAN mismatch.

Example # Specify a gateway address by binding Ethernet 2/0/4 in VLAN 2 to the secondary IP address 10.1.1.2 of VLAN-interface 2.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet2/0/4
[SW7750-Ethernet2/0/4] dhcp-relay gateway 10.1.1.2 vlan 2
```

dhcp relay information enable

Syntax **dhcp relay information enable**

undo dhcp relay information enable

View System view

Parameter None

Description Use the **dhcp relay information enable** command to enable option 82 supporting on a DHCP relay agent, through which you can enable the DHCP relay agent to insert option 82 into DHCP request packets sent to a DHCP server.

Use the **undo dhcp relay information enable** command to disable option 82 supporting on a DHCP relay agent, through which you can disable the DHCP relay agent from inserting option 82 into DHCP request packets sent to a DHCP server.

By default, this function is disabled.

Related commands: **dhcp relay information strategy**.

Example # Enable option 82 supporting on a DHCP relay agent.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] dhcp relay information enable
```

dhcp relay information strategy

Syntax **dhcp relay information strategy** { **drop** | **keep** | **replace** }

undo dhcp relay information strategy

View System view

Parameter **drop**: Specifies to discard the DHCP request packets that carry option 82.

keep: Specifies to remain the DHCP request packets that carry option 82 unchanged.

replace: Specifies to replace option 82 carried by a DHCP request packet with that of the DHCP relay agent.

Description Use the **dhcp relay information strategy** command to instruct a DHCP relay agent to perform specified operations to DHCP request packets that carry option 82.

Use the **undo dhcp relay information strategy** command to instruct a DHCP relay agent to perform the default operations to DHCP request packets that carry option 82.

By default, the DHCP relay agent replaces the option 82 carried by a DHCP request packet with its own option 82.

Related commands: **dhcp relay information enable**

Example # Instruct the DHCP relay agent to drop the DHCP request packets that carry option 82.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] dhcp relay information strategy drop
```

dhcp relay reply broadcast

Syntax **dhcp relay reply broadcast**

undo dhcp relay reply broadcast

View System view

Parameter None

Description Use the **dhcp relay reply broadcast** command to force the DHCP relay agent to broadcast the responses (including DHCP-OFFER, DHCP-ACK, or DHCP-ACK) to the clients.

Use the **undo dhcp relay reply broadcast** command to restore the default settings.

Generally, the DHCP relay agent determines to broadcast or unicast responses to the clients according to the flag field in the DHCP-DISCOVER packet sent by the client.

Example # Force the DHCP relay agent to broadcast responses to clients.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] dhcp relay reply broadcast
```

dhcp relay source-ip source-interface

Syntax **dhcp relay source-ip source-interface**

undo dhcp relay source-ip source-interface

View System view

Parameter None

Description Use the **dhcp relay source-ip source-interface** command to specify the source IP address of uplink packets to the DHCP server as the IP address of the relay agent’s interface that connects to the clients.

Use the **undo dhcp relay source-ip source-interface** command to disable this function.

By default, this function is disabled. That is, the source IP address of packets forwarded to the DHCP server is the IP address of the relay agent's interface that connects to the DHCP server.

Example # Specify the source IP address of uplink packets as that of the receiving interface.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] dhcp relay source-ip source-interface
```

dhcp-security static

Syntax **dhcp-security static** *ip-address* **mac** *mac-address* [**vlan** *vlan-id* | **port** *interface-type interface-number*]*

undo dhcp-security { *ip-address* | **all** | **dynamic** | **static** }

View System view

Parameter *ip-address*: User IP address.

mac-address: User MAC address.

vlan *vlan-id*: Specifies a VLAN ID.

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

all: Removes all user address entries.

dynamic: Removes dynamic user address entries.

static: Removes static user address entries.

Description Use the **dhcp-security static** command to configure a static client address entry on the DHCP relay agent, in which an IP address can be bound to one or more objects among MAC address, VLAN, and port.

Use the **undo dhcp-security** command to remove one or all client address entries from the DHCP relay agent.

Related commands: **display dhcp-security**.

Example # Configure a static client address entry on the DHCP relay agent.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z
[SW7750] dhcp-security static 1.1.1.1 mac 0005-5D02-F2B3 vlan 1 port
 Ethernet2/0/2
```

dhcp-server

Syntax **dhcp-server** *groupNo*

undo dhcp-server

View VLAN interface view

Parameter *groupNo*: DHCP server group number. This argument ranges from 0 to 19.

Description Use the **dhcp-server** command to map the current VLAN interface to a DHCP server group.

Use the **undo dhcp-server** command to cancel the mapping.

Related commands: **dhcp-server ip**, **display dhcp-server**, **display dhcp-server interface**.

Example # Specify that VLAN-interface 1 corresponds to DHCP server group 1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface vlan-interface 1
[SW7750-Vlan-interface1] dhcp-server 1
```

dhcp-server ip

Syntax **dhcp-server** *groupNo* **ip** *ip-address*&<1-8>

undo dhcp-server *groupNo*

View System view

Parameter *groupNo*: DHCP server group number, ranging from 0 to 19.

ip-address&<1-8>: IP address of the DNS server. &<1-8> indicates that up to eight IP addresses can be input, with any two IP addresses separated by a space.

Description Use the **dhcp-server ip** command to configure the DHCP server IP address(es) in a specified DHCP server group.

Use the **undo dhcp-server** command to remove all DHCP server IP addresses in a DHCP server group.

Related commands: **dhcp-server**, **display dhcp-server**.

Example # Configure three DHCP server IP addresses 1.1.1.1, 2.2.2.2, and 3.3.3.3 for DHCP server group 1, so that this group contains three DHCP servers (server 1, server 2 and server 3).

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] dhcp-server 1 ip 1.1.1.1 2.2.2.2 3.3.3.3
```

display dhcp-security

Syntax **display dhcp-security** [*ip-address* | **dynamic** | **static**]

View Any view

Parameter *ip-address*: IP address. This argument is used to display the user address entry with the specified IP address.

dynamic: Displays the dynamic user address entries.

static: Displays the static user address entries.

Description Use the **display dhcp-security** command to display one or all user address entries, or a specified type of user address entries in the valid user address table of a DHCP server group.

Example # Display all user address entries contained in the valid user address table of the DHCP server group.

```
<SW7750> display dhcp-security
IP Address      MAC Address     Vlan ID      Port                        Type
 192.168.4.1    00e0-fc00-000b  100          GigabitEthernet2/0/13    Dynamic
 192.168.0.3    000d-88f8-4e71  ---          ---                         Static
 192.168.0.45   00d0-eee3-ff11  ---          ---                         Static
---   3 dhcp-security item(s) found   ---
```

Table 118 Field descriptions of the **display dhcp-security** command

Field	Description
IP Address	IP address of the DHCP client
MAC Address	MAC address of the DHCP client
VLAN ID	ID of the VLAN to which the DHCP client belongs
Port	Type and number of the relay agent’s port connecting to the DHCP client
Type	Type of the user address entry (static or dynamic)

display dhcp-server

Syntax **display dhcp-server** *groupNo*

View Any view

Parameter *groupNo*: DHCP server group number, ranging from 0 to 19.

Description Use the **display dhcp-server** command to display information about a specified DHCP server group.

Related commands: **dhcp-server ip**, **dhcp-server**, **display dhcp-server interface**.

Example # Display information about DHCP server group 0.

```
<SW7750> display dhcp-server 0
IP address of DHCP server group 0:         1.1.1.1
IP address of DHCP server group 0:         2.2.2.2
IP address of DHCP server group 0:         3.3.3.3
IP address of DHCP server group 0:         4.4.4.4
IP address of DHCP server group 0:         5.5.5.5
IP address of DHCP server group 0:         6.6.6.6
IP address of DHCP server group 0:         7.7.7.7
IP address of DHCP server group 0:         8.8.8.8
Messages from this server group: 0
Messages to this server group: 0
Messages from clients to this server group: 0
Messages from this server group to clients: 0
DHCP_OFFER messages: 0
DHCP_ACK messages: 0
DHCP_NAK messages: 0
DHCP_DECLINE messages: 0
DHCP_DISCOVER messages: 0
DHCP_REQUEST messages: 0
DHCP_INFORM messages: 0
DHCP_RELEASE messages: 0
BOOTP_REQUEST messages: 0
BOOTP_REPLY messages: 0
```

Table 119 Field descriptions of the **display dhcp-server** command

Field	Description
IP address of DHCP server group 0:	DHCP server IP addresses of DHCP server group 0
Messages from this server group	Number of packets received from the DHCP server group
Messages to this server group	Number of packets sent to the DHCP server group
Messages from clients to this server group	Number of packets received from the DHCP clients
Messages from this server group to clients	Number of packets sent to the DHCP clients
DHCP_OFFER messages	Number of received DHCP-OFFER packets
DHCP_ACK messages	Number of received DHCP-ACK packets
DHCP_NAK messages	Number of received DHCP-NAK packets
DHCP_DECLINE messages	Number of received DHCP-DECLINE packets
DHCP_DISCOVER messages	Number of received DHCP-DISCOVER packets
DHCP_REQUEST messages	Number of received DHCP-REQUEST packets
DHCP_INFORM messages	Number of received DHCP-INFORM packets
DHCP_RELEASE messages	Number of received DHCP-RELEASE packets
BOOTP_REQUEST messages	Number of BOOTP request packets
BOOTP_REPLY messages	Number of BOOTP response packets

display dhcp-server interface

Syntax **display dhcp-server interface Vlan-interface** *vlan-id*

View Any view

Parameter *vlan-id*: VLAN ID.

Description Use the **display dhcp-server interface** command to display information about the DHCP server group to which a VLAN interface is mapped.

Related commands: **dhcp-server**, **display dhcp-server**.

Example # Display information about the DHCP server group to which VLAN 2 interface is mapped.

```
<SW7750> display dhcp-server interface vlan-interface 2
 The DHCP server group of this interface is 0
```

The above display information indicates the VLAN 2 interface is mapped to DHCP server group 0.

reset dhcp-server

Syntax **reset dhcp-server** *groupNo*

View User view

Parameter *groupNo*: DHCP server group number, ranging from 0 to 19.

Description Use the **reset dhcp-server** command to clear the statistics information of the specified DHCP server group.

Related commands: **dhcp-server**, **display dhcp-server**.

Example # Clear the statistics information of DHCP server group 2.

```
<SW7750> reset dhcp-server 2
```

undo dhcp-relay gateway all

Syntax **undo dhcp-relay gateway all**

View System view

Parameter None

Description Use the **undo dhcp-relay gateway all** command to delete all the gateways configured on the DHCP relay agent, that is, to remove the bindings between the VLAN interfaces’ IP addresses (primary or secondary) and the ports in the VLANs.

Example # Delete all the gateways configured on the DHCP relay agent.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] undo dhcp-relay gateway all
```

56 DHCP SNOOPING CONFIGURATION COMMANDS

dhcp-snooping

Syntax **dhcp-snooping**

undo dhcp-snooping

View System view

Parameter None

Description Use the **dhcp-snooping** command to enable the DHCP snooping function, so as to allow the switch to listen to the DHCP broadcast packets.

Use the **undo dhcp-snooping** command to disable the DHCP snooping function.

By default, the DHCP snooping function is disabled.

Related commands: **display dhcp-snooping**.

Example # Enable the DHCP snooping function.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] dhcp-snooping
```

dhcp-snooping information enable

Syntax **dhcp-snooping information enable**

undo dhcp-snooping information enable

View System view

Parameter None

Description Use the **dhcp-snooping information enable** command to enable DHCP snooping Option 82.

Use the **undo dhcp-snooping information enable** command to disable DHCP snooping Option 82.

DHCP snooping Option 82 is disabled by default.

Example # Enable DHCP snooping Option 82.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] dhcp-snooping information enable
 DHCP snooping option 82 is enabled globally.
```

dhcp-snooping information format

Syntax **dhcp-snooping information format** { **hex** | **ascii** }

View System view

Parameter **hex**: Specifies the storage format of Option 82 as HEX (namely, hexadecimal string).

ascii: Specifies the storage format of Option 82 as ASCII.

Description Use the **dhcp-snooping information format** command to configure the storage format of Option 82 as HEX or ASCII.

By default, the Option 82 is in HEX format.

*The **dhcp-snooping information format** command applies only to the default content of the Option 82 field. If you have configured the circuit ID or remote ID sub-option, the storage format of the sub-option is ASCII, instead of the one specified with the **dhcp-snooping information format** command.*

Example # Configure the storage format of Option 82 as ASCII.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] dhcp-snooping information format ascii
```

dhcp-snooping information packet-format

Syntax **dhcp-snooping information packet-format** { **extended** | **standard** }

View System view

Parameter **extended**: Specifies the padding format for Option 82 as the extended format.

standard: Specifies the padding format for Option 82 as the standard format.

Description Use the **dhcp-snooping information packet-format** command to configure the padding format for Option 82 as the extended or standard one.

By default, the padding format for Option 82 is the extended one.

Example # Configure the padding format for Option 82 as the standard one.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] dhcp-snooping information packet-format standard
```

dhcp-snooping information remote-id

Syntax **dhcp-snooping information remote-id** { **sysname** | **string** *string* }

undo dhcp-snooping information remote-id

View System view

Parameter **sysname**: Uses the system name of the DHCP snooping device to pad the remote ID sub-option in Option 82.

string: Customized content of the remote ID sub-option, a string of 1 to 63 ASCII characters.

Description Use the **dhcp-snooping information circuit-id** command to configure the remote ID sub-option in Option 82.

Use the **undo dhcp-snooping information circuit-id** command to restore the default value of the remote ID sub-option in Option 82.

By default, the remote ID sub-option in Option 82 is the MAC address of the DHCP Snooping device that received the DHCP client's request.

Example # Configure the remote ID sub-option of Option 82 as the system name of the DHCP snooping device.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] dhcp-snooping information remote-id sysname
```

dhcp-snooping information strategy

Syntax **dhcp-snooping information strategy** { **drop** | **keep** | **replace** }

undo dhcp-snooping information strategy

View System view, Ethernet port view

Parameter **drop**: If a packet contains Option 82, DHCP snooping drops this packet.

keep: If a packet contains Option 82, DHCP snooping keeps and forwards this packet.

replace: If a packet contains Option 82, DHCP snooping replaces the original Option 82 field with the Option 82 field having the specified padding content and forwards the packet.

Description Use the **dhcp-snooping information strategy** command in system view to configure a handling policy for DHCP requests that contain Option 82 sent by the DHCP client.

Use the **undo dhcp-snooping information strategy** command to restore the default handling policy.

Use the **dhcp-snooping information strategy** command in Ethernet port view to configure a handling policy for requests that contain Option 82 received on the current port.

Use the **undo dhcp-snooping information strategy** command to restore the default handling policy.

By default, DHCP snooping replaces the Option 82 field in the requests sent by the DHCP clients.

CAUTION:

- *Enable DHCP-snooping and DHCP-snooping Option 82 before performing this configuration.*
- *If a handling policy is configured on a port, this configuration overrides the globally configured handling policy for requests received on this port, while the globally configured handling policy applies on those ports where a handling policy is not natively configured.*

Example # Configure the **keep** handling policy for DHCP requests that contain Option 82 on the DHCP snooping device.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] dhcp-snooping information strategy keep
```

dhcp-snooping information vlan circuit-id

Syntax **dhcp-snooping information** [**vlan** *vlan-id*] **circuit-id string** *string*

undo dhcp-snooping information { [**vlan** *vlan-id*] **circuit-id** | **circuit-id all** }

View Ethernet port view

Parameter **vlan** *vlan-id*: Specifies a VLAN. DHCP packets from the VLAN are padded with the circuit ID sub-option.

string: Content of the circuit ID sub-option, a string of 1 to 63 ASCII characters.

Description Use the **dhcp-snooping information vlan circuit-id** command to configure the content of the circuit ID field in Option 82.

Use the **undo dhcp-snooping information circuit-id** command to restore the default.

With **vlan** *vlan-id* specified, the customized circuit ID sub-option applies only to the DHCP packets from the specified VLAN. With no **vlan** *vlan-id* specified, the customized circuit ID sub-option applies to all DHCP packets that pass through the current port.

Use the **undo dhcp-snooping information vlan** *vlan-id* **circuit-id** command to restore the default circuit ID in DHCP packets from the specified VLAN.

Use the **undo dhcp-snooping information circuit-id** command to restore the default circuit ID for all DHCP packets except those from the specified VLAN.

Use the **undo dhcp-snooping information circuit-id all** command to restore the default circuit ID for all DHCP packets.

By default, the circuit ID field in Option 82 contains the VLAN ID and index of the port that received the client's request.

If you have configured a circuit ID with the **vlan** *vlan-id* argument specified, and the other one without the argument in Ethernet port view, the former circuit ID applies to the DHCP messages from the specified VLAN, while the latter one applies to DHCP messages from other VLANs.

Example # Set the circuit ID field in Option 82 to **abc**

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet2/0/1
[SW7750-Ethernet2/0/1] dhcp-snooping information circuit-id string abc
```

dhcp-snooping information vlan remote-id

Syntax **dhcp-snooping information** [**vlan** *vlan-id*] **remote-id string** *string*

undo dhcp-snooping information { [**vlan** *vlan-id*] **remote-id** | **remote-id all** }

View Ethernet port view

Parameter **vlan** *vlan-id*: Specifies the VLAN ID of the remote ID to be customized.

string: Customized content of the remote ID sub-option, a string of 1 to 63 ASCII characters.

Description Use the **dhcp-snooping information vlan remote-id** command to configure the content of the remote ID in Option 82

Use the **undo dhcp-snooping information remote-id** command to restore the default remote ID in Option 82.

With **vlan** *vlan-id* specified*,* the customized remote ID sub-option applies only to the DHCP packets from the specified VLAN. Without **vlan** *vlan-id* specified, the customized remote ID sub-option applies to all DHCP packets that pass through the current port.

Use the **undo dhcp-snooping information vlan** *vlan-id* **remote-id** command to restore the default remote ID in DHCP packets from the specified VLAN.

Use the **undo dhcp-snooping information remote-id** command to restore the default remote ID in all DHCP packets except those from the specified VLAN.

Use the **undo dhcp-snooping information remote-id all** command to restore the default remote ID in all DHCP packets.

By default, the remote ID sub-option in Option 82 is the MAC address of the DHCP Snooping device that received the DHCP client's request.

If you have configured a remote ID with the **vlan** *vlan-id* argument specified, and the other one without the argument in Ethernet port view, the former remote ID applies to the DHCP messages from the specified VLAN, while the latter one applies to DHCP messages from other VLANs.

Example # Configure the remote ID of Option 82 in DHCP packets to **abc** on the port Ethernet 2/0/1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet2/0/1
[SW7750-Ethernet2/0/1] dhcp-snooping information remote-id string abc
```

dhcp-snooping trust

Syntax **dhcp-snooping trust**

undo dhcp-snooping trust

View Ethernet port view

Parameter None

Description Use the **dhcp-snooping trust** command to specify an Ethernet port as a trusted port.

Use the **undo dhcp-snooping trust** command to restore an Ethernet port to an untrusted port.

DHCP snooping security allow you to specify a port as a trusted port or an untrusted port, so that DHCP clients can obtain IP addresses from valid DHCP servers.

- Trusted ports can be used to connect DHCP servers or ports of other switches. Untrusted ports can be used to connect DHCP clients or networks.

- Trusted ports forward any received DHCP packets to ensure that DHCP clients can obtain IP addresses from valid DHCP servers. Untrusted ports discard the DHCP-ACK and DHCP-OFFER responses received from DHCP servers.

By default, all the ports of a switch are untrusted ports.

Related commands: **display dhcp-snooping trust**.

Example # Specify the Ethernet 2/0/1 port as a trusted port.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet 2/0/1
[SW7750-Ethernet2/0/1] dhcp-snooping trust
```

display dhcp-snooping

Syntax **display dhcp-snooping**

View Any view

Parameter None

Description Use the **display dhcp-snooping** command to display the IP-MAC mapping relations recorded by the DHCP snooping-enabled switch.

Related commands: **dhcp-snooping**.

Example # Display the IP-MAC mapping relations recorded by the DHCP snooping-enabled switch.

```
<SW7750> display dhcp-snooping
DHCP snooping is enabled globally.
 Type : D--Dynamic , S--Static
 Type IP Address      MAC Address     Lease      VLAN Interface
 ==== =============== =============== ========= ==== =================
---   0 DHCP snooping item(s) found   ---
```

display dhcp-snooping count

Syntax **display dhcp-snooping count**

View Any view

Parameter None

Description Use the **display dhcp-snooping count** command to display the total number of DHCP-Snooping entries.

Example # Display the total number of DHCP-Snooping entries.

```
<SW7750> display dhcp-snooping count
  1 dhcp-snooping item(s) found
```

display dhcp-snooping trust

Syntax **display dhcp-snooping trust**

View Any view

Parameter None

Description Use the **display dhcp-snooping trust** command to display the (enabled/disabled) state of the DHCP snooping function and the trusted ports.

Related commands: **dhcp-snooping trust**.

Example # Display the state of the DHCP snooping function and the trusted ports.

```
<SW7750> display dhcp-snooping trust
Interface       Trusted
 =================================
Ethernet3/0/3     Trusted
```

The above information indicates that the Ethernet 3/0/3 port is a trusted port.

display dhcp-snooping vlan

Syntax **display dhcp-snooping vlan** { *vlan-list* | **all** }

View Any view

Parameter *vlan-list*: Displays the VLAN lists in the specified VLAN range, in the format of *vlan-list* = { *vlan-id* [**to** *vlan-id*] }&<1-10>. where, *vlan-id* is in the range of 1 to 4094, and &<1-10> means that you can specify up to 10 VLANs or VLAN ranges for this argument.

all: Displays all the IP-MAC mapping relations recorded by the DHCP-Snooping-enabled switch.

Description Use the **display dhcp-snooping vlan** command to display the IP-MAC mapping relations recorded by the DHCP-Snooping-enabled switch in the specified VLAN.

Example # Display the IP-MAC mapping relations recorded by the DHCP-Snooping-enabled switch in VLAN 2.

```
<SW7750> display dhcp-snooping vlan 2
DHCP snooping is enabled globally.
 The client binding table for untrusted ports on the VLANs assigned.
 Type : D--Dynamic , S--Static
 Type IP Address        MAC Address     Lease     VLAN Interface
 ==== =============== ============== ========= ==== =================
 D    3.3.3.2           0012-3f83-6eef   20        2    Ethernet3/0/1
---   1 dhcp snooping item(s) found   ---
```

display ip source static binding

Syntax **display ip source static binding** [**vlan** *vlan-id* | **interface** *interface-type interface-number*]

View Any view

Parameter *vlan-id*: ID of the VLAN whose IP static binding entries are to be displayed.

interface-type interface-number: Type and number of the port whose IP static binding entries are to be displayed.

Description Use the **display ip source static binding** command to display the IP static binding entries configured. If you specify a VLAN, all the IP static binding entries for the specified VLAN will be displayed. If you specify a port, all the IP static binding entries for the specified port will be displayed.

Example # Display all IP static binding entries configured.

```
<SW7750> display ip source static binding
 Type IP Address      MAC Address     Lease      VLAN Interface
 ==== =============== ==============  =========  ==== =================
 S    192.168.0.25    0015-e20f-0101  infinit     1    Ethernet2/0/2
 S    192.168.0.58    0001-e201-4f01  infinit     1    Ethernet2/0/3
 S    192.168.0.101   000f-0101-0204  infinit     1    Ethernet2/0/2
 S    192.168.0.122   000f-e20f-21a3  infinit     1    Ethernet2/0/3
 S    192.168.0.144   0015-e943-712f  infinit     1    Ethernet2/0/2
---   5 static binding item(s) found   ---
```

ip check source ip-address

Syntax **ip check source ip-address** [**mac-address**]

undo ip check source ip-address [**mac-address**]

View Ethernet port view

Parameter **mac-address**: Enables IP filtering based on the source MAC address of the packets.

Description Use the **ip check source ip-address** command to enable the filtering of the IP packets received through the current port based on the source IP address of the packets.

Use the **undo ip check source ip-address** command to disable the filtering of the IP packets received through the current port based on the source IP address of the packets.

Use the **ip check source ip-address mac-address** command to enable the filtering of the IP packets received through the current port based on the source IP address and source MAC address of the packets.

Use the **undo ip check source ip-address mac-address** command to disable the filtering of the IP packets received through the current port based on the source IP address and source MAC address of the packets.

By default, the filtering of the IP packets received on a port based on the source IP address and/or source MAC address of the packets is disabled.

Example # Enable the filtering of the IP packets received through port Ethernet 2/0/11 based on the source IP address of the packets.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet 2/0/11
[SW7750-Ethernet2/0/11] ip check source ip-address
```

ip source static binding

Syntax **ip source static binding ip-address** *ip-address* [**mac-address** *mac-address*]

undo ip source static binding ip-address *ip-address*

View Ethernet port view

Parameter **ip-address** *ip-address*: Specifies the IP address to be statically bound.

mac-address *mac-address*: Specifies the MAC address to be statically bound.

Description Use the **ip source static binding ip-address** command to configure the static binding among source IP address, source MAC address, and the port number so as to generate static binding entries.

Use the **undo ip source static binding ip-address** command to remove the static binding among source IP address, source MAC address, and the port.

By default, no binding among source IP address, source MAC address, and the port number is configured.

Example # Configure static binding among source IP address, source MAC address, and Ethernet 2/0/3.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet 2/0/3
[SW7750-Ethernet2/0/3] ip source static binding ip-address 1.1.1.1 mac-address 0015-e20f-0101
```

reset dhcp-snooping

Syntax **reset dhcp-snooping** [*ip-address*]

View User view

Parameter *ip-address*: Clears the IP-MAC mapping relations recorded by the DHCP-Snooping-enabled switch.

Description Use the **reset dhcp-snooping** command to clear the specified IP-MAC mapping relation or all the IP-MAC mapping relations recorded by the DHCP-Snooping-enabled switch.

Related commands: **dhcp-server**, **display dhcp-server**.

Example # Clear the 10.1.1.1-MAC mapping relation recorded by the DHCP-Snooping-enabled switch.

```
<SW7750> reset dhcp-snooping 10.1.1.1
```

57 ACL COMMANDS

Type A I/O Modules include 3C16860, 3C16861, LS81FS24A, 3C16858, 3C16859, 3C16860, 3C16861, LS81FS24, 3C16858, and 3C16859.

acl

Syntax **acl** { **number** *acl-number* | **name** *acl-name* [**advanced** | **basic** | **link** | **user**] } [**match-order** { **config** | **auto** }]

undo acl { **number** *acl-number* | **name** *acl-name* | **all** }

View System view

Parameter **number** *acl-number*: Specifies the number of an access control list (ACL) in the range of:

- 2,000 to 2,999: identifies basic ACLs.
- 3,000 to 3,999: identifies advanced ACLs (ACL 3998 and ACL 3999 are reserved for cluster management, and you cannot configure them.).
- 4,000 to 4,999: identifies layer 2 ACLs.
- 5,000 to 5,999: identifies user-defined ACLs.

acl-name: ACL name, a string of 1 to 32 characters, which must be started with an English letter (i.e., a-z or A-Z), and there should not be a space or quotation mark in it; case insensitive, and you cannot use the word **all** as the ACL name in case of confusion.

advanced: Advanced ACL.

basic: Basic ACL.

link: Layer 2 ACL.

user: User-defined ACL..

config: When matching ACL rules, the user’s configuration order is employed.

auto: When matching ACL rules, depth first order is employed.

all: Cancels all ACLs (including those identified by a number or a name).

Description Use the **acl** command to define an ACL and enter the corresponding ACL view.

Use the **undo acl** command to delete all entries of an ACL identified by a number or a name, or the entire ACL.

By default, ACL rules are matched according to the configured order (**config**).

After entering the corresponding ACL view, you can use the **rule** command to add entries to the ACL (use the **quit** command to quit ACL view).

User-defined ACL can only be activated on the I/O Modules other than Type A.

You can use the **match-order** keyword to specify whether to use the configured order or "depth-first" order (rules with smaller ranges are matched first) to match rules. If neither match orders are specified, the configured match order will be adopted.

You cannot modify the match order for an ACL once you have specified it, unless you delete all the entries of the ACL, and specify the match order over again.

The ACL match order feature is effective only when the ACL is referenced by software for data filtering and traffic classification.

Related command: **rule (Basic ACL)**, **rule (Advanced ACL)**, **rule (Layer 2 ACL)**, **rule (user-defined ACL)**, and **acl mode**.

Example # Define rules for ACL 2000, and specify "depth-first" order as the rule match order.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] acl number 2000 match-order auto
```

acl mode

Syntax **acl mode** { **ip-based** | **link-based** }

View System view

Parameter **ip-based**: Performs traffic classification based on Layer 3 information.

link-based: Performs traffic classification based on Layer 2 information.

Description Use the **acl mode** command to set the traffic classification mode for the device.

By default, traffic classification is performed based on Layer 3 information.

Related command: **acl**.

This configuration is only effective on Type A I/O Modules.

Example # Specify to perform traffic classification based on Layer 3 information.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] acl mode ip-based
```

acl order

Syntax **acl order** { **auto** | **first-config-first-match** | **last-config-first-match** }

View System view

Parameter **auto**: Specifies the ACL rules sent to hardware are match according to the depth-first order.

first-config-first-match: Specifies the ACL rules sent to hardware are matched according to the sending order: first sent, first matched.

last-config-first-match: Specifies the ACL rules sent to hardware are matched according to the sending order: last sent, first matched.

Description Use the **acl order** command to set the match order for the ACL rules sent to hardware.

By default, the configured ACL rules sent to hardware take effect in the depth-first order.

Use the **acl match-order** { **config** | **auto** } command to set the match order of ACL rules when they are configured (before they are sent to hardware). While use the **acl order** command is to set the match order of ACL rules after they are configured (after they are sent to hardware).

Example # Configure the match order of ACL rules sent to hardware as first-config-first-match order.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] acl order first-config-first-match
```

display acl config

Syntax **display acl config** { **all** | *acl-number* | *acl-name* }

View Any view

Parameter **all**: Displays all ACLs (including those identified by a number or a name).

acl-number: Sequence number of the ACL to be displayed. It can be a number chosen from 2000~5999.

acl-name: Name of the ACL to be displayed. It is a case insensitive character string started with an English letter (a-z or A-Z), and there should not be a space or quotation mark in it; and the word **all** is not allowed to use in the ACL name to avoid confusion.

Description Using the **display acl config** command, you can view the detailed configuration information of an ACL, including every subrule, sequence number and the times matched with this rule.

The matched times displayed by this command is software matched times, namely, the matched times of ACL to be processed by switch CPU. You can use the **traffic-statistic** command to calculate the matched times of hardware during packet-forwarding. You can use the **display qos-interface traffic-statistic** command to view the calculation result. See **traffic-statistic** on page 803 and **display qos-interface traffic-statistic** on page 783 for more information.

Example # Display all content of ACL.

```
<SW7750> display acl config all
Basic ACL  2000, 1 rule,
 rule 0 permit source 1.1.1.1 0 (0 times matched)
```

display acl config statistics

Syntax **display acl config statistics**

View Any view

Parameter None

Description Use the command **display acl config statistics** to display the statistics of the current configured ACL rules, including the basic, advanced, Layer 2 and user-defined ACL rules number, and the total number of ACL rules configured by the system.

Example # Display statistics information about the current configured ACL rules.

```
<SW7750> display acl config statistics
 The configured rule statistics:
 Basic rule(s): 5
 Advanced rule(s): 132
 Link rule(s): 4
 User rule(s): 2

 Total 143 rule(s) configured
```

display acl mode

Syntax **display acl mode**

View Any view

Parameter None

Description Use the **display acl mode** command to view the ACL running mode chosen by the switch for filtering the traffic.

Related command: **acl mode**.

Example # Display the ACL running mode chosen by the switch.

```
<SW7750> display acl mode
The current acl mode: ip-based.
```

display acl order

Syntax **display acl order**

View Any view

Parameter None

Description Use the **display acl order** command to display the match order of the ACL rules sent to a port.

Related command: **acl order**.

Example # Display the match order of ACL rules sent to a port

```
<SW7750> display acl order
the current order is auto
```

display acl remaining entry

Syntax **display acl remaining entry slot** *slot-number*

View Any view

Parameter *slot-number*: Number of a slot. The number 0 indicates the Fabric.

Description Use the **display acl remaining entry slot** command to display the remaining ACL entries on a specified slot. The displayed content includes the entry resource type, total entries resource number, reserved entries number for system ACL, number of configured ACL entries, number of remaining ACL entries, and the corresponding start port number and end port number of each type of entry.

Example # Display the remaining ACL resource on the module in slot 3.

```
<SW7750> display acl remaining entry slot 3
  Slot: 3
  Resource  Total   Reserved  Configured  Remaining   Start       End
```

```
    Type    Number   Number     Number      Number   Port Name  Port Name
--------------------------------------------------------------------------
    MASK      16        6          1           9       GE3/0/1    GE3/0/1
    RULE     128       17          1         110       GE3/0/1    GE3/0/1
   METER     128       11          1         116       GE3/0/1    GE3/0/1
 COUNTER     128       14          1         113       GE3/0/1    GE3/0/1
    MASK      16        6          1           9       GE3/0/2    GE3/0/2
    RULE     128       17          1         110       GE3/0/2    GE3/0/2
   METER     128       11          1         116       GE3/0/2    GE3/0/2
 COUNTER     128       14          1         113       GE3/0/2    GE3/0/2
```

Table 120 Field descriptions of the **display acl remaining entry slot** command

Field	Description
Resource Type	Entry resource type
Total Number	Total entries resource number
Reserved Number	Number of entries reserved for system ACL during initiation
Configured Number	Number of entries used by the ACL configured by users
Remaining Number	Number of remaining entries
Start Port Name	The corresponding start port number of each type of entry
End Port Name	The corresponding end port number of each type of entry

display acl running-packet-filter

Syntax **display acl running-packet-filter** { **all** | **interface** *interface-type interface-number* }

View Any view

Parameter **all**: Represents all the ACLs to be displayed (including those identified by a number or a name).

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

Description Use the **display acl running -packet-filter** command to view the information of the activated ACL. The displayed content includes the interface on which ACL is activated, the activation direction, ACL name, ACL rule number and activation status.

Example # Display the information of the activated ACL of all interfaces.

```
<SW7750> display acl running-packet-filter all
Ethernet3/0/1
 Inbound:
 Acl 2000 rule 0  running
```

display time-range

Syntax **display time-range** { **all** | *time-name* }

View Any view

Parameter

all: Specifies to display all time ranges.

time-name: Name of a time range, a case insensitive string that starts with an English letter a-z or A-Z and contains up to 32 characters. To avoid confusion, you are not allowed to use the word **all** in the time range name.

Description

Use the **display time-range** command to view the configuration and status of the current time range. For an active time range, this command displays "Active"; for an inactive time range, this command displays "Inactive".

Note that there is a delay (about 1 minute) when the system updates the ACL status. And the **display time-range** command will judge according to the current time. Therefore, sometimes you may find that a time range is active while the ACL referencing the time range is not activated by using the **display time-range** command. This is natural.

Related command:

time-range.

Example

Display all time ranges.

```
<SW7750> 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


Total Time-range : 2
```

Table 121 Field descriptions of the **display time-range** command

Field	Description
Current time is 14:36:36 4-3-2003 Thursday	System time
Time-range : hhy (Inactive) from 08:30 2-5-2005 to 18:00 2-19-2005	Time range hhy. "Inactive" indicates that this time range is currently in the inactive state (while "Active" indicates that the time range is in the active state), and the time range is from 8:30 February 5, 2005 to 18:00 February 19 2005.
Total Time-range	Number of time ranges defined in the system.

# Display the time range named "tm1".

```
<SW7750> 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 122 Description of the fields of the **display time-range** command

Field	Description
Current time is 14:36:36 4-3-2003 Thursday	The current time of the system.

Table 122 Description of the fields of the **display time-range** command

Field	Description
Time-range : tm1 (Inactive) from 08:30 2-5-2005 to 18:00 2/19/2005	Time range tm1. "Inactive" indicates that this time range is currently in the inactive state (while "Active" indicates that the time range is in the active state), and the time range is from 8:30 February 5, 2005 to 18:00 February 19 2005.

packet-filter

Syntax **The command line format for Type A I/O Modules:**

packet-filter { **inbound** | **outbound** } *acl-rule* [**system-index** *system-index*] [**not-care-for-interface**]

undo packet-filter { **inbound** | **outbound** } *acl-rule* [**not-care-for-interface**]

The command line format for the I/O Modules other than Type A:

packet-filter inbound *acl-rule* [**system-index** *system-index*]

undo packet-filter inbound *acl-rule*

Combined activating of IP ACL and Link ACL is supported by the I/O Modules other than Type A. But the total character number of the fields defined by IP ACL and Link ACL can not exceed 32 characters; otherwise the ACL can not be activated.

View QoS view

Parameter **inbound**: Specifies to filter packets received on the port.

outbound: Specifies to filter packets sent through the port.

acl-rule: Applied ACL rules, which can be the combination of different types of ACL rules. Table 123and Table 125 describe the ACL combinations on Type A I/O Modules and the corresponding parameter description. Table 124 and Table 125 describe the ACL combinations on I/O Modules other than Type A and the corresponding parameter description.

Table 123 Combined application of ACLs on Type A I/O Modules

Combination mode	Form of acl-rule
Apply all rules in an IP type ACL separately	**ip-group** { *acl-number* | *acl-name* }
Apply one rule in an IP type ACL separately	**ip-group** { *acl-number* | *acl-name* } **rule** *rule-id*
Apply all rules in a link type ACL separately	**link-group** { *acl-number* | *acl-name* }
Apply one rule in a link type separately	**link-group** { *acl-number* | *acl-name* } **rule** *rule-id*

Table 124 Combined application of ACLs on I/O Modules other than Type A.

Combination mode	Form of acl-rule
Apply all rules in an IP type ACL separately	**ip-group** { *acl-number* | *acl-name* }
Apply one rule in an IP type ACL separately	**ip-group** { *acl-number* | *acl-name* } **rule** *rule-id*
Apply all rules in a link type ACL separately	**link-group** { *acl-number* | *acl-name* }
Apply one rule in a link type separately	**link-group** { *acl-number* | *acl-name* } **rule** *rule-id*
Apply all rules in a user-defined ACL separately	**user-group** { *acl-number* | *acl-name* }
Apply one rule in a user-defined ACL separately	**user-group** { *acl-number* | *acl-name* } **rule** *rule-id*
Apply one rule in an IP type ACL and one rule in a Link type ACL simultaneously	**ip-group** { *acl-number* | *acl-name* } **rule** *rule-id* **link-group** { *acl-number* | *acl-name* } **rule** *rule-id*

Table 125 Parameters description of ACL combinations

Parameter	Description
ip-group { *acl-number* | *acl-name* }	Basic and advanced ACL. *acl-number*: ACL number, ranging from 2,000 to 3,999. *acl-name*: ACL name, case insensitive string, up to 32 characters long, beginning with an English letter (a to z or A to Z), without space or quotation mark.
link-group { *acl-number* | *acl-name* }	Layer 2 ACL *acl-number*: ACL number, ranging from 4,000 to 4,999. *acl-name*: ACL name, case insensitive string, up to 32 characters long, beginning with an English letter (a to z or A to Z), without space or quotation mark.
user-group { *acl-number* | *acl-name* }	User-defined ACL *acl-number*: ACL number, ranging from 5,000 to 5,999. *acl-name*: ACL name, case insensitive string, up to 32 characters long, beginning with an English letter (a to z or A to Z), without space or quotation mark.
rule-id	Number of the ACL rule, ranging from 0 to 127. If this argument is not specified, all rules in the specified ACL will be applied.

system-index: Specifies an interior index value which is used when an ACL rule is applied to the port. The index value ranges from 0 to 4294,967,295. This keyword is only available when the ACL rule number is specified in the command. After the specified ACL takes effect, there are three scenarios when you input the index value:

- If you do not input an index value or the index value you input is 0, the system will automatically assign an index whose value is greater than 0;

- If the input index value is not 0 and does not conflict with the interior index used by the system, the system will adopt the index value input by you;
- If the input index value is not 0 but conflicts with the interior index used by the system, the system will reassign an index value.

When the specified ACL rule is not effective, the system will adopt the index value input by you.

not-care-for-interface: As for non-48-port interface module, the packet-filtering function will take place on the interface module where the current port resides after the parameter is chosen. As for the 48-port interface, if the number of the current port belong to the range of 1 to 24, the packet filtering will take effect on port 1 to port 24 after the parameter is chosen; if the number of the current port belong to the range of 25 to 48, the packet filtering will take effect on port 25 to port 48 after the parameter is chosen.

Description

Use the **packet-filter** command to activate ACL on a port to filter packets.

Use the **undo packet-filter** command to cancel it.

Example

Apply ACL 2000 on Ethernet 2/0/1 to filter packets.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet 2/0/1
[SW7750-Ethernet2/0/1] qos
[SW7750-qosb-Ethernet2/0/1] packet-filter inbound ip-group 2000
```

reset acl counter

Syntax

reset acl counter { **all** | *acl-number* | *acl-name* }

View

User view

Parameter

all: All ACLs (including those identified by a number or a name).

acl-number: The sequence number of an ACL, ranging from 2000~3999.

acl-name: ACL name, a case insensitive string, 1 to 32 characters, which must start with an English letter (a-z or A-Z), and there should not be a space or quotation mark in it; key word **all** is not allowed to use in the ACL name to avoid confusion.

Description

Use the **reset acl counter** command to clear ACL statistics.

Table 126 The comparison between **reset** commands of statistics information

Command	Function
reset acl counter	Reset the statistics information of the ACL which is used to filter or classify the data treated by the software of a switch. The case includes: ACL cited by route policy function, ACL used for controlling logon user, etc.

Table 126 The comparison between **reset** commands of statistics information

Command	Function
reset traffic-statistic	Reset statistic information of traffic. This command is applicable to the ACL which is used to filter or classify the data transmitted by the hardware of a switch. Commonly, this command is used to reset the statistics information recorded by the **traffic-statistic** command.

Example # Clear the statistic information of ACL 2000.

```
<SW7750> reset acl counter 2000
```

rule (Basic ACL)

Syntax **rule** [*rule-id*] { **permit** | **deny** } [**source** { *source-addr wildcard* | **any** } | **fragment** | **time-range** *time-name*]*

undo rule *rule-id* [**source** | **fragment** | **time-range**]*

View Basic ACL view

Parameter *rule-id*: ACL rule ID, in the range of 0 to 127.

deny: Drops packets that satisfy the condition.

permit: Permits packets that satisfy the condition to pass.

fragment: Specifies that the rule takes effect on non-initial fragment packets.

source { *sour-addr sour-wildcard* | **any** }: Specifies the source address information in the rule. *sour-addr* is used to specify the source IP address of the packet, expressed in dotted decimal notation. *sour-wildcard* is the wildcard mask for the source subnet mask of the packet, expressed in dotted decimal notation. For example, you need to input 0.0.255.255 for the subnet mask 255.255.0.0. You can set *sour-wildcard* to 0 to represent the host IP address. **any** is used to represent any arbitrary IP address.

time-range *time-name*: Specifies a time range within which the rule is valid. *time-name* is the time range name, a case insensitive string of 1 to 32 characters, must start with an English letter a to A or A to Z. To avoid confusion, you are not allowed to use the word **all** in the time range name.

Description Use the **rule** command to define an ACL rule.

Use the **undo rule** command to delete an ACL rule or the attribute information of an ACL rule.

Before you can delete a rule, you need to specify the rule ID. If you do not know the rule ID, you can view it by the **display acl** command.

In the case that you specify the rule ID when defining a rule:

- If the rule corresponding to the specified rule ID already exists, you will edit the rule, and the modified part in the rule will replace the original content, while other parts remain unchanged.
- If the rule corresponding to the specified rule ID does not exists, you will create and define a new rule.
- The content of a newly created rule must not be identical with the content of any existing rule; otherwise the rule creation will fail, and the system will prompt that the rule already exists.

If you do not specify a rule ID, you will create and define a new rule, and the system will assign an ID for the rule automatically.

*Type A I/O Modules do not support to apply ACL rules configured with **fragment** to hardware..*

Example # Define a rule to deny the packets whose source IP addresses are 1.1.1.1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] acl number 2000
[SW7750-acl-basic-2000] rule deny source 1.1.1.1 0
```

rule (Advanced ACL)

Syntax **rule** [*rule-id*] { **permit** | **deny** } *rule-string*

undo rule *rule-id* [**source** | **destination** | **source-port** | **destination-port** | **icmp-type** | **precedence** | **tos** | **dscp** | **fragment** | **time-range**]*

View Advanced ACL view

Parameter *rule-id*: ACL rule ID, in the range of 0 to 127.

deny: Drops packets that satisfy the condition.

permit: Permits packets that satisfy the condition to pass.

rule-string: Rule information, which can be combination of the parameters described in Table 127. You need to configure the *protocol* argument in the rule information before you can configure other arguments.

Table 127 Rule information

Parameter	Type	Function	Description
protocol	Protocol type	Type of the protocols carried by IP	When expressed in numerals, the value range is 1 to 255. When expressed with a name, the value can be GRE, ICMP, IGMP, IP, IPinIP, OSPF, TCP, and UDP.

Table 127 Rule information

Parameter	**Type**	**Function**	**Description**
source { *sour-addr sour-wildcard* | **any** }	Source address information	Specifies the source address information in the rule	*sour-addr sour-wildcard* is used to specify the source address of the packet, expressed in dotted decimal notation. **any** represents any source address.
destination { *dest-addr dest-wildcard* | **any** }	Destination address information	Specifies the destination address information in the rule	*dest-addr dest-wildcard* is used to specify the destination address of the packet, expressed in dotted decimal notation. **any** represents any destination address.
precedence *precedence*	Packet precedence	IP priority	Value range: 0 to 7
tos *tos*	Packet precedence	ToS priority	Value range: 0 to 15
dscp *dscp*	Packet precedence	DSCP priority	Value range: 0 to 63
fragment	Fragment information	Specifies that the rule is effective for non-initial fragment packets	-
time-range *time-name*	Time range information	Specifies the time range in which the rule is active	*time-name* is the time range name, a case insensitive string of 1 to 32 characters, must start with an English letter a to A or A to Z. To avoid confusion, you are not allowed to use the word **all** in the time range name.

sour-wildcard/dest-wildcard is the wildcard mask of the source/destination subnet mask. For example, you need to input 0.0.255.255 to specify the subnet mask 255.255.0.0. The arguments can be set as 0 to represent the host IP address.

To define DSCP priority, you can directly input a value ranging from 0 to 63, or input a keyword listed in Table 128.

Table 128 Description of DSCP values

Keyword	**DSCP value in decimal**	**DSCP value in binary**
ef	46	101110
af11	10	001010
af12	12	001100
af13	14	001110
af21	18	010010
af22	20	010100

Table 128 Description of DSCP values

Keyword	DSCP value in decimal	DSCP value in binary
af23	22	010110
af31	26	011010
af32	28	011100
af33	30	011110
af41	34	100010
af42	36	100100
af43	38	100110
cs1	8	001000
cs2	16	010000
cs3	24	011000
cs4	32	100000
cs5	40	101000
cs6	48	110000
cs7	56	111000
be (default)	0	000000

To define the IP precedence, you can directly input a value ranging from 0 to 7, or input a keyword listed in the following table.

Table 129 Description of IP precedence value

Keyword	IP Precedence value in decimal	IP Precedence value in binary
routine	0	000
priority	1	001
immediate	2	010
flash	3	011
flash-override	4	100
critical	5	101
internet	6	110
network	7	111

To define the ToS value, you can directly input a value ranging from 0 to 15, or input a keyword listed in the following table.

Table 130 Description of ToS value

Keyword	ToS value in decimal	ToS value in binary
normal	0	0000
min-monetary-cost	1	0001
max-reliability	2	0010
max-throughput	4	0100
min-delay	8	1000

If the protocol type is TCP or UDP, you can also define the following information:

Table 131 TCP/UDP-specific rule information

Parameter	Type	Function	Description
source-port *operator port1* [*port2*]	Source port(s)	Defines the source port information of UDP/TCP packets	The value of *operator* can be lt (less than), gt (greater than), eq (equal to), neq (not equal to) or range (within the range of) Only the *range* requires two port numbers as the operands, and other operators require only one port number as the operand. *port1* and *port2*: TCP/UDP port number(s), expressed with name(s) or numerals; when expressed with numerals, the value range is 0 to 65,535.
destination-port *operator port1* [*port2*]	Destination port(s)	Defines the destination port information of UDP/TCP packets	
established	TCP connection established" flag	Indicates the rule is only valid to the first SYN packet (when TCP connection began)	TCP-specific argument

Only Type A I/O Modules support the "range" operation on the TCP/UDP port.

If the protocol type is ICMP, you can also define the following information:

Table 132 ICMP-specific rule information

Parameter	Type	Function	Description
icmp-type *icmp-type icmp-code*	Type and message code information of ICMP packets	Specifies the type and message code information of ICMP packets in the rule	*icmp-type*: ICMP message type, ranging 0 to 255 *icmp-code*: ICMP message code, ranging 0 to 255

If the protocol type is ICMP, you can also directly input the ICMP message name after the **icmp-type** argument. Table 133 describes some common ICMP messages.

Table 133 ICMP messages

Name	ICMP TYPE	ICMP CODE
echo	Type=8	Code=0
echo-reply	Type=0	Code=0
fragmentneed-DFset	Type=3	Code=4
host-redirect	Type=5	Code=1
host-tos-redirect	Type=5	Code=3
host-unreachable	Type=3	Code=1

Table 133 ICMP messages

Name	ICMP TYPE	ICMP CODE
information-reply	Type=16	Code=0
information-request	Type=15	Code=0
net-redirect	Type=5	Code=0
net-tos-redirect	Type=5	Code=2
net-unreachable	Type=3	Code=0
parameter-problem	Type=12	Code=0
port-unreachable	Type=3	Code=3
protocol-unreachable	Type=3	Code=2
reassembly-timeout	Type=11	Code=1
source-quench	Type=4	Code=0
source-route-failed	Type=3	Code=5
timestamp-reply	Type=14	Code=0
timestamp-request	Type=13	Code=0
ttl-exceeded	Type=11	Code=0

Description Use the **rule** command to define an ACL rule.

Use the **undo rule** command to delete an ACL rule or the attribute information of an ACL rule.

Before you can delete a rule, you need to specify the rule ID. If you do not know the rule ID, you can view it by the **display acl** command.

In the case that you specify the rule ID when defining a rule:

- If the rule corresponding to the specified rule ID already exists, you will edit the rule, and the modified part in the rule will replace the original content, while other parts remain unchanged.
- If the rule corresponding to the specified rule ID does not exists, you will create and define a new rule.
- The content of a newly created rule must not be identical with the content of any existing rule; otherwise the rule creation will fail, and the system will prompt that the rule already exists.

If you do not specify a rule ID, you will create and define a new rule, and the system will assign an ID for the rule automatically.

Type A I/O Modules do not support to apply ACL rules configured with ***tos*** *tos, or* ***fragment*** *to hardware.*

Example # Define a rule to permit TCP packets from hosts in the network segment of 129.9.0.0 to hosts in the network of 202.38.160.0 and with the port number of 80 to pass.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] acl number 3101
```

```
[SW7750-acl-adv-3101] rule permit tcp source 129.9.0.0 0.0.255.255 d
estination 202.38.160.0 0.0.0.255 destination-port eq 80
```

rule (Layer 2 ACL)

Syntax **rule** [*rule-id*] { **permit** | **deny** } [*rule-string*]

undo rule *rule-id*

View Layer 2 ACL view

Parameter *rule-id*: ACL rule ID, in the range of 0 to 127.

deny: Drops packets that satisfy the condition.

permit: Permits packets that satisfy the condition to pass.

rule-string: ACL rule information, which can be combination of the parameters described in Table 134.

Table 134 Rule information

Parameter	Type	Function	Description
protocol-type	Protocol type	Type of the protocols carried by IP	*protocol-type*: the value can be arp, rarp, ipx, nbx, pppoe-control, and pppoe-data.
format-type	Link layer encapsulation type	Defines the link layer encapsulation type in the rule	*format-type*: the value can be 802.3/802.2, 802.3, ether_ii, or snap.
ingress { { *source-vlan-id* | *source-mac-addr* [*source-mac-mask*] }* | **any** }	Source MAC address information	Specifies the source MAC address range in the rule	*source-mac-addr*: source MAC address, in the format of H-H-H *source-mac-mask*: source MAC address mask, in the format of H-H-H, defaults to ffff-ffff-ffff *source-vlan-id*: source VLAN ID, in the range of 1 to 4,094 **any** indicates all packets received from all ports.

Table 134 Rule information

Parameter	Type	Function	Description
egress { *dest-mac-addr* [*dest-mac-mask*] | **any** }	Destination MAC address information	Specifies the destination MAC address range in the rule	*dest-mac-addr*: destination MAC address, in the format of H-H-H *dest-mac-mask*: destination MAC address mask, in the format of H-H-H, defaults to ffff-ffff-ffff **any** indicates all packets forwarded by all ports.
cos *cos*	Priority	Defines the 802.1p priority of the rule	*cos*: ranges from 0 to 7
time-range *time-name*	Time range information	Specifies the time range in which the rule is active	*time-name*: name of the time range; a case insensitive string of 1 to 32 characters, must start with an English letter a to z or A to Z. To avoid confusion, you are not allowed to use the word **all** in the time range name.

To define the CoS value, you can directly input a value ranging from 0 to 7, or input a keyword listed in the following table.

Table 135 Description of CoS value

Keyword	CoS value in decimal	CoS value in binary
best-effort	0	000
background	1	001
spare	2	010
excellent-effort	3	011
controlled-load	4	100
video	5	101
voice	6	110
network-management	7	111

Description

Use the rule command to define an ACL rule.

Use the **undo rule** command to delete an ACL rule.

Before you can delete a rule, you must specify the rule ID. If you do not know the rule ID, you can view it by using the **display acl** command.

In the case that you specify the rule ID when defining a rule:

- If the rule corresponding to the specified rule ID already exists, you will edit the rule, and the modified part in the rule will replace the original content, while other parts remain unchanged.

- If the rule corresponding to the specified rule ID does not exists, you will create and define a new rule.
- The content of a newly created rule must not be identical with the content of any existing rule; otherwise the rule creation will fail, and the system will prompt that the rule already exists.

If you do not specify a rule ID, you will create and define a new rule, and the system will assign an ID for the rule automatically.

Example # Define an ACL to deny the packets with the source MAC address being 000d-88f5-97ed, the destination MAC address being 0011-4301-991e, and the 802.1p priority being 3, to pass.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] acl number 4000
[SW7750-acl-link-4000] rule deny cos 3 ingress 000d-88f5-97ed ffff-f
fff-ffff egress 0011-4301-991e ffff-ffff-ffff
```

rule (user-defined ACL)

Syntax **rule** [*rule-id*] { **permit** | **deny** } { *rule-string rule-mask offset* } &<1-8> [**time-range** *time-name*]

undo rule *rule-id*

View User-defined ACL view

Parameter *rule-id*: ACL rule ID, in the range of 0 to 127.

deny: Drops packets that satisfy the condition.

permit: Permits packets that satisfy the condition to pass.

rule-string: User-defined string of the rule. It must be an even number containing 2 to 160 hexadecimal characters.

rule-mask: User-defined mask of the rule. It is used to perform the logical AND operations with packets and must be an even number containing 2 to 160 hexadecimal characters. Note that its length must be the same with that of *rule-string*.

offset: Mask offset of the rule. It specifies a byte, through its offset from the packet header, in the packet as the starting point to perform logical AND operations. It ranges from 0 to 79 bytes, and the maximum value becomes one byte less when the value of *rule-string* (and *rule-mask*) has two more characters. For example, when *rule-string* and *rule-mask* contains two characters respectively, the maximum value of *offset* is 79 bytes; when the former contains four characters respectively, the maximum value of *offset* is 78 bytes, and so on.

&<1-8>: At most eight *rule-string rule-mask offset*s can be defined at one time.

time-name: Specifies a time range within which the rule is valid. *time-name*: Name of a time range, a case insensitive string that starts with an English letter (a-z or A-Z) and contains up to 32 characters. To avoid confusion, you are not allowed to use the word **all** in the time range name.

Description

Use the **rule** command to define an ACL rule.

Use the **undo rule** command to delete an ACL rule or the attribute information of an ACL rule.

Before you can delete a rule, you need to specify the rule ID. If you do not know the rule ID, you can view it by the **display acl** command.

In the case that you specify the rule ID when defining a rule:

- If the rule corresponding to the specified rule ID already exists, you will edit the rule, and the modified part in the rule will replace the original content, while other parts remain unchanged.
- If the rule corresponding to the specified rule ID does not exists, you will create and define a new rule.
- The content of a newly created rule must not be identical with the content of any existing rule; otherwise the rule modification or creation will fail, and the system will prompt that the rule already exists.

If you do not specify a rule ID, you will create and define a new rule, and the system will assign an ID for the rule automatically.

Only I/O Modules other than Type A support the user-defined ACL.

Example

Define a rule to forbid all TCP packets to pass through.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
```

[SW7750] time-range t1 18:00 to 23:00 sat

```
[SW7750] acl number 5001
[SW7750-acl-user-5001] rule 25 deny 06 ff 27 time-range t1
```

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 time range, a case insensitive string that starts with an English letter a-z or A-Z and contains up to 32 characters. To avoid confusion, you are not allowed to use the word **all** in the time range name.

start-time: Start time of a special time range, in the form of hh:mm. Optional argument.

end-time: End time of a special time range, in the form of hh:mm. Optional argument.

days-of-the-week: Day of the week when the special time range is effective. Optional argument. Available arguments and argument combinations are as follows:

- Numerals (0 to 6)
- Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday
- Working days (Monday through Friday)
- Off days (Saturday and Sunday)
- Daily, namely everyday of the week

from *start-time start-date*: Specifies the start date of a special time range, optional. In the form of hh:mm MM/DD/ YYYY, *start-time start-date* and *end-time end-date* jointly define a date in which the special time range takes effect.

to *end-time end-date*: Specifies the end date of a special time range, optional. In the form of hh:mm MM/DD/ YYYY, *start-time start-date* and *end-time end-date* jointly define a date on which the special time range takes effect.

all: Deletes all time ranges.

Description

Use the **time-range** command to define a time range.

Use the **undo time-range** command to delete a time range.

Use the **undo time-range all** command to delete all time ranges.

The time range defined by means of the **time-range** command can include absolute time sections and periodic time sections. *start-time* and *end-time days-of-the-week* jointly define a periodic time section, while *start-time start-date* and *end-time end-date* jointly define an absolute time section.

If only a periodic time section is defined in a time range, the time range is active only within the defined periodic time section.

If only an absolute time section is defined in a time, the time range is active only within the defined absolute time section.

If both a periodic time section and an absolute time section are defined in a time range, the time range is active only when the periodic time range and the absolute time range are both matched. Assume that a time range defines an absolute time section from 00:00 January 1, 2004 to 23:59 December 31, 2004, and a periodic time section from 12:00 to 14:00 every Wednesday. This time range is active only from 12:00 to 14:00 every Wednesday in 2004.

The time ranges supported by the switch are within 1970/1/1 to 2100/12/31 (January 1, 1970 to December 31, 2100).

Example

Defines an absolute time section "test" that is effective from 00:00 January 1, 2000.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] time-range test from 00:00 2000/1/1
```

58 QOS COMMANDS

- *Type-A I/O Modules include 3C16860, 3C16861, LS81FS24A, 3C16858, 3C16859, 3C16860, 3C16861, LS81FS24, 3C16858, and 3C16859.*
- *On type-A I/O Modules, the prompt for QoS view is **qoss**; on non-type-A I/O Modules, the prompt for QoS view is **qosb**.*

display priority-trust

Syntax **display priority-trust**

View Any view

Parameter None

Description Use the **display priority-trust** command to display the priority type according to which the switch puts a packet into an output queue on a port.

Related command: **priority-trust**.

Example # Display the queue scheduling mode and the related parameters.

```
<SW7750> display priority-trust

Priority trust mode: local-precedence
```

The information above shows that the switch put a packet into an output queue on a port according to the local precedence of the packet.

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-to-local-precedence" mapping table.

Example # Display the "COS-to-local-precedence" mapping table.

```
<SW7750> 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 type and number.

Description Use the **display qos-interface all** command to view all the QoS configuration of the ports. If you do not provide the *interface-type interface-number* argument, this command will display the QoS parameter configuration of all the ports of the switch; if you provide the *interface-type interface-number* argument, this command will display QoS parameter configuration of the specified port.

Example # Display the QoS parameter configuration of all ports.

```
<SW7750> display qos-interface all

GigabitEthernet0/0/1:
 Queue scheduling mode: strict-priority
 COS configuration:
  Config (max queues): 8
  Schedule mode: strict
  Egress port queue statistics(in bytes):
    Priority    CosQ        Threshold   Count       Used(%):
    0           2           18432       0           0
    1           3           2560        0           0
    2           4           2560        0           0
    3           1           2560        0           0
    4           7           2560        0           0
    5           0           2560        0           0
    6           5           2560        0           0
    7           6           2560        0           0
  common queue statistics(in bytes):
                            49152       0           0

GigabitEthernet0/0/2:
 Queue scheduling mode: strict-priority
 COS configuration:
  ---- More ----
```

display qos-interface line-rate

Syntax **display qos-interface** [*interface-type interface-number*] **line-rate**

View Any view

Parameter *interface-type interface-number*: Port type and number.

Description Use the **display qos-interface line-rate** command to view the rate limit configuration (including the outbound port and the limit rate) for the outbound direction of a port or all the ports of a switch. If you do not specify the *interface-type interface-number* argument, you will view the rate limit configuration for the outbound direction of all the ports of a switch; if you specify that argument, you will view the rate limit configuration for the outbound direction of the specified port.

Example # Display the rate limit configuration of all ports.

```
<SW7750> display qos-interface line-rate

 GigabitEthernet2/0/2: line-rate
   Line rate: 3072 kbps
 GigabitEthernet2/0/4: line-rate
   Line rate: 5120 kbps
```

Table 136 Field descriptions of the **display qos-interface line-rate** command

Field	Description
GigabitEthernet2/0/2: line-rate Line rate: 3072 kbps	Rate limit configuration on GigabitEthernet 2/0/2: The maximum sum of all the packet rates on GigabitEthernet 2/0/2 is 3,072 kbps.

display qos-interface queue-scheduler

Syntax **display qos-interface** [*interface-type interface-number*] **queue-scheduler**

View Any view

Parameter *interface-type interface-number*: Port type and number.

Description Use the **display qos-interface queue-scheduler** command to display the queue scheduling mode configuration of the specified port or all ports. If the *interface-type interface-number* argument is not specified, you will view the queue scheduling mode parameters of all the ports. If you specify the *interface-type interface-number* argument, you will view the queue scheduling mode parameter of the specified port.

Example # Display the queue scheduling mode parameter of GigabitEthernet 2/0/1.

```
<SW7750> display qos-interface gigabitethernet 2/0/1 queue-scheduler
GigabitEthernet2/0/1:
 Queue scheduling mode: weighted round robin
 weight of queue 1: 10
 weight of queue 2: 5
 weight of queue 3: 10
 weight of queue 4: 10
 weight of queue 5: 5
 weight of queue 6: 10
 weight of queue 7: 5
 weight of queue 8: 10
 COS configuration:
  Config (max queues): 8
  Schedule mode: weighted round-robin
  Weighting (in packets):
    COSQ 0 = 10 packets
    COSQ 1 = 5 packets
    COSQ 2 = 10 packets
    COSQ 3 = 10 packets
    COSQ 4 = 5 packets
    COSQ 5 = 10 packets
    COSQ 6 = 5 packets
    COSQ 7 = 10 packets
  Egress port queue statistics(in bytes):
    Priority    CosQ        Threshold   Count       Used(%):
    0           2           18432       0           0
    1           0           2560        0           0
    2           1           2560        0           0
    3           3           2560        0           0
    4           4           2560        0           0
    5           5           2560        0           0
    6           6           2560        0           0
    7           7           2560        0           0
  common queue statistics(in bytes):
                            49152       0           0
```

display qos-interface traffic-bandwidth

Syntax **display qos-interface** [*interface-type interface-number*] **traffic-bandwidth**

View Any view

Parameter *interface-type interface-number*: Port type and number.

Description Use the **display qos-interface traffic-bandwidth** command to view the configuration information about bandwidth guarantee.

Related command: **traffic-bandwidth**.

Example # Display the bandwidth guarantee parameters.

```
<SW7750> display qos-interface traffic-bandwidth
Ethernet2/0/1: traffic-bandwidth
 Outbound:
   Matches: Acl 2000 rule 0  running
     Minimum guaranteed bandwidth: 64 Kbps
     Maximum available bandwidth: 128 Kbps
     Bandwidth weight: 20
```

display qos-interface traffic-limit

Syntax **display qos-interface** [*interface-type interface-number*] **traffic-limit**

View Any view

Parameter *interface-type interface-number*: Port type and number.

Description Use the **display qos-interface traffic-limit** command to view the traffic limit configuration of a port or all the ports of a switch, including the applied ACLs for traffic limit, committed average rate (CAR), and the corresponding actions.

Related command: **traffic-limit**.

Example # Display the traffic limit configuration.

```
<SW7750> display qos-interface traffic-limit
GigabitEthernet2/0/1: traffic-limit
 Inbound:
   Matches: Acl 3000 rule 1  running
     Target rate: 20480 Kbps
     Exceed action: remark-dscp 4
```

display qos-interface traffic-priority

Syntax **display qos-interface** [*interface-type interface-number*] **traffic-priority**

View Any view

Parameter *interface-type interface-number*: Port type and number.

Description Use the **display qos-interface traffic-priority** command to view the traffic priority configuration. The information displayed includes the ACL corresponding to the traffic tagged with priority, priority type and value.

Related command: **traffic-priority**.

Example # Display the traffic priority configuration.

```
<SW7750> display qos-interface traffic-priority
Ethernet2/0/1: traffic-priority
 Outbound:
   Matches: Acl 2000 rule 0  running
     Priority action: dscp be
```

display qos-interface traffic-red

Syntax **display qos-interface** [*interface-type interface-number*] **traffic-red**

View Any view

Parameter *interface-type interface-number*: Port type and number.

Description Use the **display qos-interface traffic-red** command to view the RED configuration.

Related command: **traffic-red**.

Example # Display the RED configuration.

```
<SW7750> display qos-interface traffic-red
Ethernet2/0/1: traffic-red
 Outbound:
   Matches: Acl 2000 rule 0  running
     Queue length of start random discarding: 16 Kbyte
     Queue length of stop random discarding: 32 Kbyte
     Max probability of discarding: 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 type and number.

Description Use the **display qos-interface traffic-redirect** command to view the configuration of traffic redirect. The displayed content includes the corresponding ACLs of the traffics to be redirected, and the port to which the traffic is redirected.

Related command: **traffic-redirect**.

Example # Display the configuration of traffic redirect.

```
<SW7750> display qos-interface traffic-redirect
GigabitEthernet2/0/1: traffic-redirect
 Inbound:
   Matches: Acl 2002 rule 0  running
     Redirected to: interface GigabitEthernet2/0/8
```

display qos-interface traffic-remark

Syntax **display qos-interface** [*interface-type interface-number*] **traffic-remark**

View Any view

Parameter *interface-type interface-number*:: Port type and number.

Description Use the **display qos-interface traffic-remark** command to display the configuration of the traffic-based flexible QinQ function. The displayed information includes the ACL rules used for traffic identifying and the ID of the external VLAN tag.

Related command: **traffic-remark**.

Example # Display the configuration of traffic-based flexible QinQ.

```
<SW7750> display qos-interface traffic-remark

Ethernet2/0/1: traffic-remark
 Inbound:
   Matches: Acl 3000 rule 3  running
     RemarkVlanId action: remark-vlan 25 uplink Ethernet 2/0/2 untag
ged
```

display qos-interface traffic-statistic

Syntax **display qos-interface** [*interface-type interface-number*] **traffic-statistic**

View Any view

Parameter *interface-type interface-number*: Port type and number.

Description Use the **display qos-interface traffic-statistic** command to view the traffic statistics information. The information displayed includes the ACL corresponding to the traffic to be counted and the number of packets counted.

Related command: **traffic-statistic**.

Example # Display the traffic statistics information.

```
<SW7750> display qos-interface traffic-statistic
Ethernet2/0/1: traffic-statistic
 Inbound:
   Matches: Acl 2000 rule 0  running
     105 packets
```

inboundcar

Syntax **inboundcar** { **enable** | **disable** }

View System view

Parameters **enable**: Enables bidirectional CAR.

disable: Disables bidirectional CAR.

Description Use the **inboundcar enable** command to enable bidirectional CAR.

Use the **inboundcar disable** command to disable bidirectional CAR.

By default, bidirectional CAR is disabled.

This command applies to only type-A I/O Modules. To make the configuration take effect, reboot the switch.

With bidirectional CAR enabled, the switch considers an ACL rule applied to different ports as different rules. As a result, an applied rule can occupy multiple entries. If you enable CAR for traffic matching a certain rule on multiple ports, the switch provides the specified bandwidth for the traffic matching the CAR rule on a per-port basis.

With bidirectional CAR disabled, the switch considers an ACL rule applied to different ports as the same rule. As a result, an applied rule occupies only one entry. If you enable CAR for traffic matching a certain rule on multiple ports, the switch provides the specified bandwidth for all the traffic matching the CAR rule on these ports to share.

Suppose you want to allocate 2 Mbps of CAR bandwidth for the incoming traffic matching ACL rule 0 and enable CAR on two ports with the **traffic-limit** command.

- If bidirectional CAR is enabled, each port guarantees 2 Mbps of bandwidth for its incoming traffic matching ACL rule 0.
- If bidirectional CAR is disabled, the switch guarantees 2 Mbps of bandwidth for the traffic matching ACL rule 0 received on the two ports.

Examples # Enable bidirectional CAR.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] inboundcar enable
```

line-rate

Syntax **line-rate** [**kbps**] *target-rate*

undo line-rate

View QoS view

Parameter **kbps**: Specifies the rate unit as kbps when the rate limit function is configured.

target-rate: Total limit rate of all the packets sent by the port. If the **kbps** keyword is specified, the rate is measured in kbps, in the range of 64 to 1,024,000 with the granularity being 64. If the number you input is in the range of N*64 to (N+1)*64 (N is a natural number), the switch will set the value to (N+1)*64 kbps automatically. If the **kbps** keyword is not specified, the rate is in the range of 1 to 1,000 in mbps.

Description Use the **line-rate** command to limit the rate of the packets on the port.

Use the **undo line-rate** command to cancel the rate limit configuration on the port.

Only type-A I/O Modules support the rate limit configuration.

Example # Limit the rate of packets on GigabitEthernet 2/0/1 to 10 Mbps.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface GigabitEthernet2/0/1
[SW7750-GigabitEthernet2/0/1] qos
[SW7750-qosb-GigabitEthernet2/0/1] line-rate 10
```

priority

Syntax **priority** *priority-level*

undo priority

View Ethernet port view

Parameter *priority-level*: Priority value of the port, ranging from 0 to 7.

Description Use the **priority** command to configure the priority of the Ethernet port.

Use the **undo priority** command to restore the default priority of the Ethernet port.

By default, the priority of a port is 0.

If the switch receives a packet without VLAN tags, the switch will tag the packet with the default VLAN of the port receiving the packet. In this case the switch assigns the port priority of the port receiving the packet to the 802.1p priority of the VLAN tag in the packet.

The switch does not perform the operation above if it receives a packet with VLAN tags.

Example # Set the local precedence of Ethernet 2/0/1 to 6.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet2/0/1
[SW7750-Ethernet2/0/1] priority 6
```

priority-trust

Syntax **priority-trust** { **dscp** | **ip-precedence** | **cos** | **local-precedence** }

View

System view

Parameter

dscp: Puts a packet into the corresponding output queue on a port according to the DSCP precedence.

ip-precedence: Puts a packet into the corresponding output queue on a port according to the IP precedence.

cos: Puts a packet into the corresponding output queue on a port according to the COS precedence.

local-precedence: Puts a packet into the corresponding output queue on a port according to the local precedence.

Description

Use the **priority-trust** command to specify the priority according to which the switch puts a packet into the output queue on a port.

By default, the switch puts a packet into the output queue on a port according to the local precedence of the packet.

You can use the **priority-trust** command to choose a packet precedence, according to which the switch puts packets with different priorities into the corresponding output queues during queue scheduling.

The switch ports support eight output queues with different levels of precedence. The higher the precedence is, the earlier it will be delivered. The switch puts a packet into an output queue on a port according to the precedence of the packet.

1. **dscp** precedence: **dscp** precedence value ranges from 0 to 63 inclusive, the packets with precedence value from 0 to 7 are put into queue 0, and those with precedence value from 8 to 15 are put into queue 1, and so on.
2. **ip-precedence**: **ip-precedence** value ranges from 0 to 7, the packets with precedence value 0 are put into queue 0, and those with precedence value 1 are put into queue 1, and so on.
3. **cos** precedence: **cos** precedence value ranges from 0 to 7, the packet whose precedence value is 0 is put into queue 2, the packet whose precedence value is 1 is put into queue 0, the packet whose precedence value is 2 is put into queue 1. As for the left precedence values, the queue number is equal to the precedence value. For example, the packet whose precedence value is 3 is put into queue 3.
4. **local-precedence**: **local-precedence** value ranges from 0 to 7. The packet whose precedence value is 0 is put into queue 0, and so on.

You can choose the corresponding packet precedence as the basis for putting a packet into an output queue on a port as required.

Example

Specify the switch to put a packet into an output queue according to the DSCP precedence of the packet.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] priority-trust dscp
```

qos

Syntax **qos**

View Ethernet port view

Parameter None

Description Use the **qos** command to enter QoS view and perform the corresponding QoS configuration.

Different I/O Modules of Switch 7750s support different QoS functions. You can use "?" to query the supported QoS configurations after entering different QoS views.

Example # Enter QoS view of a non-type-A I/O Module and query the QoS configuration supported by the I/O Module.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface GigabitEthernet 2/0/1
[SW7750-GigabitEthernet2/0/1] qos
[SW7750-qosb-GigabitEthernet2/0/1] ?
Qosb view commands:
  display                Display current system information
  line-rate              Limit the rate of the outbound packets of t
he
                         interface
  mirrored-to            Mirror the packets
  msdp-tracert           MSDP traceroute to source RP
  packet-filter          Filter packets based on acl
  ping                   Send echo messages
  queue-scheduler        Specify queue scheduling mode and parameter
s
  quit                   Exit from current command view
  reset                  Reset operation
  return                 Exit to User View
  tracert                Trace route function
  traffic-limit          Limit the rate of the packets
  traffic-priority       Specify new priority of the packets
  traffic-redirect       Redirect the packets
  traffic-remark  Remark vlan ID of the packets
  traffic-statistic      Count the packets
  undo                   Cancel current setting
```

# Enter QoS view of a type-A I/O Module and query the QoS configuration supported by the I/O Module.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet 3/0/1
[SW7750-Ethernet3/0/1] qos
[SW7750-qoss-Ethernet3/0/1]?
Qoss view commands:
```

```
display               Display current system information
msdp-tracert          MSDP traceroute to source RP
packet-filter         Filter packets based on acl
ping                  Send echo messages
quit                  Exit from current command view
reset                 Reset operation
return                Exit to User View
tracert               Trace route function
traffic-bandwidth     Guarantee the bandwidth of the packets
traffic-limit         Limit the rate of the packets
traffic-priority      Specify new priority of the packets
traffic-red           Random early detect the packets
traffic-remark  Remark vlan ID of the packets
traffic-statistic     Count the packets
undo                  Cancel current setting
```

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*: Local precedence to which the CoS 0 is to be mapped, in the range of 0 to 7.

cos1-map-local-prec: Local precedence to which the CoS 1 is to be mapped, in the range of 0 to 7.

cos2-map-local-prec: Local precedence to which the CoS 2 is to be mapped, in the range of 0 to 7.

cos3-map-local-prec: Local precedence to which the CoS 3 is to be mapped, in the range of 0 to 7.

cos4-map-local-prec: Local precedence to which the CoS 4 is to be mapped, in the range of 0 to 7.

cos5-map-local-prec: Local precedence to which the CoS 5 is to be mapped, in the range of 0 to 7.

cos6-map-local-prec: Local precedence to which the CoS 6 is to be mapped, in the range of 0 to 7.

cos7-map-local-prec: Local precedence to which the CoS 7 is to be mapped, in the range of 0 to 7.

Description Use the **qos cos-local-precedence-map** command to configure the "CoS-to-local-precedence" mapping table.

Use the **undo qos cos-local-precedence-map** command to restore the default values.

The following is the default "CoS-to-local-precedence" mapping table.

Table 137 Default "CoS-to-local-precedence" mapping table

CoS value	Local precedence
0	2
1	0
2	1
3	3
4	4
5	5
6	6
7	7

Example # Configure the "CoS-to-local-precedence" mapping table.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] qos cos-local-precedence-map 0 1 2 3 4 5 6 7
```

The following is the configured "CoS-to-local-precedence" mapping table.

Table 138 "CoS-to-local-precedence" mapping table

CoS value	Local precedence
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

queue-scheduler

Syntax **queue-scheduler** { **rr** | **strict-priority** | **wrr** *queue1-weight queue2-weight queue3-weight queue4-weight queue5-weight queue6-weight queue7-weight queue8-weight* }

undo queue-scheduler

View QoS view

Parameter **rr**: Adopts round robin (RR) algorithm.

strict-priority: Adopts strict priority (SP) scheduling.

wrr *queue1-weight queue2-weight queue3-weight queue4-weight queue5-weight queue6-weight queue7-weight queue8-weight*: Adopts the weighted round robin (WRR) algorithm, with the weight in the range of 0 to 15.

Description Use the **queue-scheduler** command to configure the queue scheduling mode and related parameters.

Use the **undo queue-scheduler** command to restore the default queue scheduling mode.

By default, the SP algorithm is adopted.

Related command: **display qos-interface queue-scheduler**.

Only non-type-A I/O Modules support the configuration of queue scheduling mode.

Example # Adopt the WRR queue scheduling mode, and the weight value of each queue is 10, 5, 10, 10, 5, 10, 5, and 10.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface GigabitEthernet 2/0/1
[SW7750-GigabitEthernet2/0/1] qos
[SW7750-qosb-GigabitEthernet2/0/1] queue-scheduler wrr 10 5 10 10 5
10 5 10
```

reset traffic-statistic

Syntax **For type-A I/O Modules:**

reset traffic-statistic { **inbound** | **outbound** } *acl-rule*

For non-type-A I/O Modules:

reset traffic-statistic inbound *acl-rule*

I/O Modules, except type-A I/O Modules, support applying the combination of IP ACL rules and link ACL rules. However, the field defined by the IP ACL rules and link ACL rules cannot be of more than 32 characters. Otherwise, the combination cannot be applied successfully.

View QoS view

Parameter *acl-rule*: Applied ACL which can be the combination of various ACL rules. For the ways of type-A I/O Modules to combine ACLs and the description on related parameters, refer to Table 139 and Table 141. For the ways of non-type-A I/O Modules to combine ACLs and the description on related parameters, refer to Table 140 and Table 141.

Table 139 Type-A I/O Modules' ways of applying combined ACLs

ACL combination	Form of the acl-rule argument
Apply all the rules in an IP ACL separately	**ip-group** { *acl-number* | *acl-name* }
Apply a rule in an IP ACL separately	**ip-group** { *acl-number* | *acl-name* } **rule** *rule-id*
Apply all the rules in a Link ACL separately	**link-group** { *acl-number* | *acl-name* }
Apply a rule in a Link ACL separately	**link-group** { *acl-number* | *acl-name* } **rule** *rule-id*

Table 140 Non-type-A I/O Modules' ways of applying combined ACLs

ACL combination	Form of the acl-rule argument
Apply all the rules in an IP ACL separately	**ip-group** { *acl-number* | *acl-name* }
Apply a rule in an IP ACL separately	**ip-group** { *acl-number* | *acl-name* } **rule** *rule-id*
Apply all the rules in a Link ACL separately	**link-group** { *acl-number* | *acl-name* }
Apply a rule in a Link ACL separately	**link-group** { *acl-number* | *acl-name* } **rule** *rule-id*
Apply all the rules in an user-defined ACL separately	**user-group** { *acl-number* | *acl-name* }
Apply a rule in an user-defined ACL separately	**user-group** { *acl-number* | *acl-name* } **rule** *rule-id*
Apply a rule in an IP ACL and a rule in a Link ACL at the same time	**ip-group** { *acl-number* | *acl-name* } **rule** *rule-id* **link-group** { *acl-number* | *acl-name* } **rule** *rule-id*

Table 141 Description on the parameters in the ACL combination

Parameter	Description
ip-group { *acl-number* | *acl-name* }	Basic and advanced ACL *acl-number*: ACL number in the range of 2,000 to 3,999. *acl-name*: ACL name which contains up to 32 characters. It must start with English letters (a to z or A to Z) and cannot contain spaces or quotation marks. It is not sensitive to capitals.
link-group { *acl-number* | *acl-name* }	Layer 2 ACL *acl-number*: ACL number in the range of 4,000 to 4,999. *acl-name*: ACL name which contains up to 32 characters. It must start with English letters (a to z or A to Z) and cannot contain spaces or quotation marks. It is not sensitive to capitals.
user-group { *acl-number* | *acl-name* }	User-defined ACL *acl-number*: ACL number in the range of 5,000 to 5,999. *acl-name*: ACL name which contains up to 32 characters. It must start with English letters (a to z or A to Z) and cannot contain spaces or quotation marks. It is not sensitive to capitals.

Table 141 Description on the parameters in the ACL combination

Parameter	Description
rule-id	ID of an ACL rule, in the range of 0 to 127. If the *rule-id* argument is not specified, the **rule** keyword refers to all the rules in the ACL.

Description

Use the **reset traffic-statistic** command to clear the statistics of all or specified traffic.

Table 142 The reset acl counter command vs. the reset traffic-statistic command

Command	Function
reset acl counter	Clear the ACL statistics. This command is applicable to ACLs used for filtering and classifying the traffic processed by software. ACLs are referenced by software in the following cases: ■ Referenced by routing policies ■ Referenced when login users are controlled In these cases, the ACL number is in the range of 2,000 to 3,999. Refer to **reset acl counter** on page 764 for the introduction to this command.
reset traffic-statistic	Clear the traffic statistics. This command is applicable to ACLs applied to the hardware of the switch for filtering and classifying traffic during data forwarding. Generally, this command is used to clear the statistics information obtained through the **traffic-statistic** command.

Example

Clear the statistics about traffic matching ACL 2000.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet 2/0/1
[SW7750-Ethernet2/0/1] qos
[SW7750-qoss-Ethernet2/0/1] reset traffic-statistic inbound ip-group
 2000
```

traffic-bandwidth

Syntax

traffic-bandwidth outbound *acl-rule* [**system-index** *system-index*] *min-guaranteed-bandwidth max-guaranteed-bandwidth weight*

undo traffic-bandwidth outbound *acl-rule*

View

QoS view

Parameter

outbound: Guarantees the bandwidth for the outbound packets sent by the port.

acl-rule: Applied ACL rules which can be the combination of various ACL rules. For the ways of combining ACLs and the description on related parameters, refer to Table 139 and Table 141.

system-index: Specifies an interior index value which is used when an ACL rule is applied to the port. The index value ranges from 0 to 4294,967,295. This keyword is only available when the ACL rule number is specified in the command. After the specified ACL takes effect, there are three scenarios when you input the index value:

- If you do not input an index value or the index value you input is 0, the system will automatically assign an index whose value is greater than 0;
- If the input index value is not 0 and does not conflict with the interior index used by the system, the system will adopt the index value input by you;
- If the input index value is not 0 but conflicts with the interior index used by the system, the system will reassign an index value.

When the specified ACL rule is not effective, the system will adopt the index value input by you.

min-guaranteed-bandwidth: Minimum guaranteed bandwidth in kbps, in the range of 0 to 8,388,608. It must be the multiple(s) of 64.

max-guaranteed-bandwidth: Maximum guaranteed bandwidth in kbps, in the range of 0 to 8,388,608. It must be the multiple(s) of 64.

weight: Bandwidth weight in the range of 1 to 100, in percentage. It is used in the situations when there is several traffic bandwidth guarantees at the current port. For instance, there is 10 M of bandwidth supporting two flows on a port. The minimum guaranteed bandwidth for each flow is 2 M, the maximum guaranteed bandwidth is 8 M, and the bandwidth weights are 40% and 80% respectively. After the port guarantees the minimum bandwidth for both flows (that is, 4 M), the remaining bandwidth (6M) cannot support the maximum bandwidth of both flows (16M). If the bandwidth occupied by the two flows exceeds the minimum guaranteed bandwidth, then the remaining bandwidth (6 M) will be allocated to each flow according to the bandwidth weights (40% : 80%).

Assume there are N flows on a port, the bandwidth of the port is Bp, the minimum guaranteed bandwidth of the ith flow is Bimin, and the maximum guaranteed bandwidth of the ith flow is Bimax, and the weight is Wi. If the bandwidth occupied by all the flows is greater than their minimum guaranteed bandwidth, and the sum of maximum guaranteed bandwidth is greater than port bandwidth Bp, the bandwidth allocated to the ith flow is

$$\mathrm{Bi} = \mathrm{Bimin} + \left(\mathrm{Bp} - \sum_{N} B_{\mathrm{imin}}\right) \times \mathrm{Wi} \big/ \left(\sum_{N} \mathrm{Wi}\right) .$$

Description

Use the **traffic-bandwidth** command to activate the ACL for traffic identifying and provide bandwidth guarantee for the corresponding traffic. This command is applicable to only the **permit** rule).

Use the **undo traffic-bandwidth** command to remove this function.

This configuration provides the minimum guaranteed bandwidth and maximum available bandwidth for the specific traffic. Note that the maximum available bandwidth must be no smaller than the minimum guaranteed bandwidth.

Related command: **display qos-interface traffic-bandwidth**.

- *Only type-A I/O Modules support this command.*
- *Only the permit rule can be referenced in this command and applied to hardware.*

Example # Guarantee the bandwidth of the packets that match the **permit** rule in ACL 2000: The minimum guaranteed bandwidth is 64 k, the maximum available bandwidth is 128 k, and bandwidth weight is 50.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet 2/0/1
[SW7750-Ethernet2/0/1] qos
[SW7750-qoss-Ethernet2/0/1] traffic-bandwidth outbound ip-group 2000
 64 128 50
```

traffic-limit

Syntax **For type-A I/O Modules:**

traffic-limit { **inbound** | **outbound** } *acl-rule* [**system-index** *system-index*] *target-rate*

undo traffic-limit { **inbound** | **outbound** } *acl-rule*

For non-type-A I/O Modules:

traffic-limit inbound *acl-rule* [**system-index** *system-index*] [**kbps**] *target-rate* [**exceed** *action*]

undo traffic-limit inbound *acl-rule*

I/O Modules, except type-A I/O Modules, support applying the combination of IP ACL rules and link ACL rules. However, the field defined by the IP ACL rules and link ACL rules cannot be of more than 32 characters. Otherwise, the combination cannot be applied successfully.

View QoS view

Parameter **inbound**: Performs traffic policing on the packets received by the port.

outbound: Performs traffic policing on the packets sent by the port.

acl-rule: Applied ACL which can be the combination of various ACL rules. For the ways of type-A I/O Modules to combine ACLs and the description on related parameters, refer to Table 139 and Table 141. For the ways of non-type-A I/O

Modules to combine ACLs and the description on related parameters, refer to Table 140 and Table 141.

system-index: Specifies an interior index value which is used when an ACL rule is applied to the port. The index value ranges from 0 to 4294,967,295. This keyword is only available when the ACL rule number is specified in the command. After the specified ACL takes effect, there are three scenarios when you input the index value:

- If you do not input an index value or the index value you input is 0, the system will automatically assign an index whose value is greater than 0;
- If the input index value is not 0 and does not conflict with the interior index used by the system, the system will adopt the index value input by you;
- If the input index value is not 0 but conflicts with the interior index used by the system, the system will reassign an index value.

When the specified ACL rule is not effective, the system will adopt the index value input by you.

kbps: Specifies the limit rate to be measured in kbps. If the **kbps** keyword is specified, the rate is measured in kbps, in the range of 64 to 1,024,000 with the granularity being 64. If the number you input is in the range of N*64 to (N+1)*64 (N is a natural number), the switch will set the value to (N+1)*64 kbps automatically.

target-rate: Total rate to limit all the packets sent on a port. For type-A I/O Modules, the *target-rate* argument is in the range of 64 to 8,388,608 in kbps with the granularity being 64. If the **kbps** keyword is not provided, the *target-rate* argument is in mbps in the range of 1 to 1,000.

exceed *action*: Optional. The action is taken when the traffic exceeds the threshold. Only type-A I/O Modules support this keyword. The *action* argument can be:

- **drop**: Drops the packets.
- **remark-dscp** *value*: Sets new DSCP value.

Description

Use the **traffic-limit** command to activate ACL for traffic identifying and perform traffic policing.

Use the **undo traffic-limit** command to remove traffic policing.

The granularity of traffic limit is 64 kbps.

This command performs traffic limit on the packets matching the **permit** rule only.

*Only the **permit** rule can be referenced in this command and applied to hardware.*

Example

Perform traffic limit on the packets matching the **permit** rule in ACL 2000 on Ethernet 2/0/1 of a type-A I/O Module. The maximum rate is 128 kbps.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet 2/0/1
[SW7750-Ethernet2/0/1] qos
[SW7750-qoss-Ethernet2/0/1] traffic-limit inbound ip-group 2000 128
```

# Perform traffic limit on the packets matching the **permit** rule in ACL 2000 on GigabitEthernet 3/0/1 of a non-type-A I/O Module. The maximum rate is 128 kbps.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface GigabitEthernet 3/0/1
[SW7750-GigabitEthernet3/0/1] qos
[SW7750-qosb-GigabitEthernet3/0/1] traffic-limit inbound ip-group 2000 kbps 128
```

traffic-priority

Syntax **For type-A I/O Modules:**

traffic-priority { **inbound** | **outbound** } *acl-rule* [**system-index** *system-index*] { { **dscp** *dscp-value* | **ip-precedence** *pre-value* } | **local-precedence** *pre-value* }*

undo traffic-priority { **inbound** | **outbound** } *acl-rule*

For non-type-A I/O Modules:

traffic-priority inbound *acl-rule* [**system-index** *system-index*] { { **dscp** *dscp-value* | **ip-precedence** *pre-value* } | { **cos** *cos* | **local-precedence** *pre-value* } }*

undo traffic-priority inbound *acl-rule*

I/O Modules, except type-A I/O Modules, support applying the combination of IP ACL rules and link ACL rules. However, the field defined by the IP ACL rules and link ACL rules cannot be of more than 32 characters. Otherwise, the combination cannot be applied successfully.

View QoS view

Parameter **inbound**: Performs priority marking to the packets received by the port.

outbound: Performs priority marking to the packets sent by the port.

acl-rule: Applied ACL which can be the combination of various ACL rules. For the ways of type-A I/O Modules to combine ACLs and the description on related parameters, refer to Table 139 and Table 141. For the ways of non-type-A I/O Modules to combine ACLs and the description on related parameters, refer to Table 140 and Table 141.

system-index: Specifies an interior index value which is used when an ACL rule is applied to the port. The index value ranges from 0 to 4294,967,295. This keyword is only available when the ACL rule number is specified in the command. After the specified ACL takes effect, there are three scenarios when you input the index value:

- If you do not input an index value or the index value you input is 0, the system will automatically assign an index whose value is greater than 0;
- If the input index value is not 0 and does not conflict with the interior index used by the system, the system will adopt the index value input by you;
- If the input index value is not 0 but conflicts with the interior index used by the system, the system will reassign an index value.

When the specified ACL rule is not effective, the system will adopt the index value input by you.

dscp *dscp-value*: Sets DSCP precedence, ranging from 0 to 63. You can also enter the keywords in Table 143.

Table 143 Description on DSCP precedence values

Keyword	DSCP value (decimal)	DSCP value (binary)
ef	46	101110
af11	10	001010
af12	12	001100
af13	14	001110
af21	18	010010
af22	20	010100
af23	22	010110
af31	26	011010
af32	28	011100
af33	30	011110
af41	34	100010
af42	36	100100
af43	38	100110
cs1	8	001000
cs2	16	010000
cs3	24	011000
cs4	32	100000
cs5	40	101000
cs6	48	110000
cs7	56	111000
be (default)	0	000000

ip-precedence *pre-value*: Sets IP precedence. The *pre-value* argument ranges from 0 to 7. You can also enter the keywords in Table 144.

Table 144 Description on IP precedence values

Keyword	IP Precedence (decimal)	IP Precedence (binary)
routine	0	000
priority	1	001
immediate	2	010
flash	3	011

Table 144 Description on IP precedence values

Keyword	IP Precedence (decimal)	IP Precedence (binary)
flash-override	4	100
critical	5	101
internet	6	110
network	7	111

cos *cos*: Sets 802.1p priority. The *pre-value* argument ranges from 0 to 7. You can also enter the keywords in Table 145.

Table 145 Description on 802.1p priority values

Keyword	802.1p priority (decimal)	802.1p priority value (binary)
best-effort	0	000
background	1	001
spare	2	010
excellent-effort	3	011
controlled-load	4	100
video	5	101
voice	6	110
network-management	7	111

If you have redirected the packets to CPU, it is not recommended to set the 802.1p priority to 7, and vice versa.

local-precedence *pre-value*: Sets local precedence. The *pre-value* argument ranges from 0 to 7.

Description

Use the **traffic-priority** command to enable ACLs for remarking priority.

Use the **undo traffic-priority** command to remove the function of remarking priority .

Related command: **display qos-interface traffic-priority**.

Only the permit rule can be referenced in this command and applied to hardware.

Example

Remark the local precedence of the packets matching the **permit** rule in ACL 2000 as 0.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet2/0/1
[SW7750-Ethernet2/0/1] qos
[SW7750-qosb-Ethernet2/0/1] traffic-priority inbound ip-group 2000 l
ocal-precedence 0
```

traffic-red

Syntax

traffic-red outbound *acl-rule* [**system-index** *system-index*] *qstart qstop probability*

undo traffic-red outbound *acl-rule*

View

QoS view

Parameter

outbound: Performs RED operation on the sent packets.

acl-rule: Applied ACL rules which can be the combination of various ACL rules. For the ways of combining ACLs and the description on related parameters, refer to Table 139 and Table 141.

system-index: Specifies an interior index value which is used when an ACL rule is applied to the port. The index value ranges from 0 to 4294,967,295. This keyword is only available when the ACL rule number is specified in the command. After the specified ACL takes effect, there are three scenarios when you input the index value:

- If you do not input an index value or the index value you input is 0, the system will automatically assign an index whose value is greater than 0;
- If the input index value is not 0 and does not conflict with the interior index used by the system, the system will adopt the index value input by you;
- If the input index value is not 0 but conflicts with the interior index used by the system, the system will reassign an index value.

When the specified ACL rule is not effective, the system will adopt the index value input by you.

qstart: Queue length where the system starts to drop packets at random, in the range of 0 to 262,128 in KB. The packets in the queue whose length is less than the *qstart* argument will not be dropped. The value must be the multiples of 16 KB.

qstop: Queue length where the system stops dropping of packets at random, in the range of 0 to 262,128 in KB. All the packets in the queue whose length is greater than the *qstop* argument will be dropped. The value must be the multiples of 16 KB.

probability: Drop probability when the *qstop* argument is reached, in the range of 0% to 100%.

Description

Use the **traffic-red** command to enable the RED operation and set RED parameters.

Use the **undo traffic-red** command to remove the RED configuration.

Note that the *qstop* argument in this command must be no smaller than the *qstart* argument.

Related command: **display qos-interface traffic-red**.

- *Only type-A I/O Modules support this command.*
- *Only the permit rule can be referenced in this command and applied to hardware.*

Example # Perform the RED operation on the packets matching the **permit** rule in ACL 2000. RED parameters can be set as follows: the *qstart* argument is 64 KB, the *qstop* argument is 128 KB, and the *probability* argument is 20%.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet 2/0/1
[SW7750-Ethernet2/0/1] qos
[SW7750-qoss-Ethernet2/0/1] traffic-red outbound ip-group 2000 64 12
8 20
```

traffic-redirect

Syntax **traffic-redirect inbound** *acl-rule* [**system-index** *system-index*] { **cpu** | **interface** *interface-type interface-number* }

undo traffic-redirect inbound *acl-rule*

View QoS view

Parameter **inbound**: Performs traffic redirect on the packets received by the port.

outbound: Performs traffic redirect on the packets sent by the port.

acl-rule: Applied ACL rules which can be the combination of various ACL rules. For the ways of combining ACLs and the description on related parameters, refer to Table 139 and Table 141.

system-index: Specifies an interior index value which is used when an ACL rule is applied to the port. The index value ranges from 0 to 4294,967,295. This keyword is only available when the ACL rule number is specified in the command. After the specified ACL takes effect, there are three scenarios when you input the index value:

- If you do not input an index value or the index value you input is 0, the system will automatically assign an index whose value is greater than 0;
- If the input index value is not 0 and does not conflict with the interior index used by the system, the system will adopt the index value input by you;
- If the input index value is not 0 but conflicts with the interior index used by the system, the system will reassign an index value.

When the specified ACL rule is not effective, the system will adopt the index value input by you.

cpu: Redirects the traffic to the CPU.

interface-type interface-number: Redirects the packets to the specified Ethernet port. The *interface-type* argument refers to the port type, and the *interface-number* argument refers to the port number.

Description Use the **traffic-redirect** command to enable the ACL to identify and redirect the traffic. This command is applicable to the **permit** rules in an ACL only.

Use the **undo traffic-redirect** command to disable the traffic redirect function. .

Related command: **display qos-interface traffic-redirect**.

- *Only type-A I/O Modules support this command.*
- *Only the permit rule can be referenced in this command and applied to hardware.*

Example # Redirect the packets matching the **permit** rule in ACL 2000 to GigabitEthernet 2/0/1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface GigabitEthernet 2/0/1
[SW7750-GigabitEthernet2/0/1] qos
[SW7750-qosb-GigabitEthernet2/0/1] traffic-redirect inbound ip-group
 2000 interface gigabitethernet2/0/1
```

traffic-remark

Syntax **traffic-remark inbound** *acl-rule* [**system-index** *system-index*] **remark-vlan** *vlan-id* **uplink** *interface-type interface-number* [**untagged**]

undo traffic-remark inbound *acl-rule*

I/O Modules support applying the combination of IP ACL rules and link ACL rules. However, the field defined by the IP ACL rules and link ACL rules cannot be of more than 32 characters. Otherwise, the combination cannot be applied successfully.

View QoS view

Parameter **inbound**: Tags the packets received by the port with external VLAN tags.

acl-rule: Applied ACL rules which can be the combination of various ACL rules. For the ways of combining ACLs and the description on related parameters, refer to Table 140 and Table 141.

vlan-id: ID of the external VLAN tag which is tagged to the packet, in the range of 1 to 4,094.

system-index: Specifies an interior index which is used when an ACL rule is applied to the port. The index value ranges from 0 to 4294,967,295. This keyword is only available when the ACL rule number is specified in the command. After the specified ACL takes effect,

- If you do not enter an index value or the index value is 0, the system will automatically assign an index value greater than 0.
- If you enter a non-zero index and this index does not conflict with the interior index used by the system, the system will adopt this index value.
- If you enter a non-zero index but this index conflicts with the interior index used by the system, the system will reassign an index value.

When the specified ACL rule is not effective, the system will adopt the index value entered by you.

interface-type interface-number: Specifies the uplink port of the packet, whose outer-layer VLAN Tag must be encapsulated.

untagged: Specifies whether it is required to reserve the VLAN Tag when the VLAN encapsulated with the VLAN ID is sent through the uplink port.

Description

Use the **traffic-remark** command to enable the ACL for traffic identifying and tag the packet matching the ACL with the external VLAN tag to implement the traffic-based flexible QinQ function.

Use the **undo traffic-remark-vlanid** command to disable the configuration.

This command is applicable to only the **permit** rules in the ACL.

Refer to "QinQ Configuration Commands" on page 187 for the detailed information about flexible QinQ.

CAUTION:

- *Execute the **vlan-vpn enable** command in the corresponding port view before executing the **traffic-remark** command.*
- *The traffic-based flexible QinQ function is generally configured on the hybrid port of the edge device connecting the user device to the carrier's network.*
- *QinQ is mutually exclusive with Voice VLAN. That is, you cannot configure both features on the same port.*
- *Type-A, 3C16863, and 3C16862 I/O Modules do not support the traffic-based flexible QinQ function.*
- *The port on which the traffic-based flexible QinQ function is configured and the specified uplink port cannot be in the same aggregation group.*

Example

Tag the packets matching the **permit** rule in ACL 2000 with the external VLAN tag on GigabitEthernet 2/0/1, thus implementing the traffic-based flexible QinQ function.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] vlan 25
[SW7750-vlan25] quit
[SW7750] acl number 2000
[SW7750-acl-basic-2000] rule permit source 10.1.1.1 0.0.0.255
[SW7750-acl-basic-2000] quit
[SW7750] interface GigabitEthernet 2/0/1
[SW7750-GigabitEthernet2/0/1] port link-type hybrid
```

```
[SW7750-GigabitEthernet2/0/1] port hybrid vlan 25 untagged
[SW7750-GigabitEthernet2/0/1] vlan-vpn enable
[SW7750-GigabitEthernet2/0/1] qos
[SW7750-qosb-GigabitEthernet2/0/1] traffic-remark inbound ip-group 2000 remark-vlan 25 uplink Gigabit
Ethernet 2/0/2
```

traffic-statistic

Syntax

For type-A I/O Modules:

traffic-statistic { **inbound** | **outbound** } *acl-rule* [**system-index** *system-index*]

undo traffic-statistic { **inbound** | **outbound** } *acl-rule*

For non-type-A I/O Modules:

traffic-statistic inbound *acl-rule* [**system-index** *system-index*]

undo traffic-statistic inbound *acl-rule*

I/O Modules, except type-A I/O Modules, support applying the combination of IP ACL rules and link ACL rules. However, the field defined by the IP ACL rules and link ACL rules cannot be of more than 32 characters. Otherwise, the combination cannot be applied successfully.

View QoS view

Parameter

inbound: Performs traffic statistic on the packets received by the port.

outbound: Performs traffic statistic on the packets sent by the port.

acl-rule: Applied ACL rules which can be the combination of various ACL rules. For the ways of combining ACLs and the description on related parameters, refer to Table 139 and Table 141.

system-index: Specifies an interior index value which is used when an ACL rule is applied to the port. The index value ranges from 0 to 4294,967,295. This keyword is only available when the ACL rule number is specified in the command. After the specified ACL takes effect, there are three scenarios when you input the index value:

- If you do not input an index value or the index value you input is 0, the system will automatically assign an index whose value is greater than 0;
- If the input index value is not 0 and does not conflict with the interior index used by the system, the system will adopt the index value input by you;
- If the input index value is not 0 but conflicts with the interior index used by the system, the system will reassign an index value.

When the specified ACL rule is not effective, the system will adopt the index value input by you.

Description

Use the **traffic-statistic** command to activate the ACL for traffic identifying and count the traffic. This command is applicable to only the **permit** rules in the ACL.

Use the **undo traffic-statistic** command to cancel the traffic statistics.

The statistics information of **traffic-statistic** command includes the times of ACL matches on the hardware. You can use **display qos-interface traffic-statistic** command to display the statistics information.

Related command: **display qos-interface traffic-statistic**.

Example # Perform traffic statistics on the packets matching the permit rule in ACL 2000.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet 2/0/1
[SW7750-Ethernet2/0/1] qos
[SW7750-qosb-Ethernet2/0/1] traffic-statistic inbound ip-group 2000
```

59 MIRRORING COMMANDS

display mirroring-group

Syntax **display mirroring-group** { *group-id* | **all** | **local** | **remote-destination** | **remote-source** }

View Any view

Parameter *group-id*: Group number of a mirroring group, in the range of 1 to 20.

local: Specifies the mirroring group to be a local mirroring group.

remote-destination: The specified mirroring group is the destination group for remote mirroring.

remote-source: The specified mirroring group is the source group for remote mirroring.

all: All mirroring groups

Description Use the **display mirroring-group** command to display the parameter settings of a mirroring group.

Local mirroring group information includes:

- Group number
- Group type: **local**
- Group status
- Information about the source port of mirroring
- Information about the destination port of mirroring

Information displayed on the destination mirroring group for remote mirroring includes:

- Group number
- Group type: **remote-destination**
- Group status
- Information of the destination port
- Remote-probe VLAN information

Information displayed on the source mirroring group for remote mirroring includes:

- Group number
- Group type: **remote-source**
- Group status
- Information of the source port
- Information of the reflector port
- Remote-probe VLAN information

Example # Display the parameter settings of the mirroring group.

```
<SW7750> display mirroring-group all
mirroring-group 2:    type: local    status: active
mirroring port:        GigabitEthernet2/0/1  both
monitor port: GigabitEthernet2/0/4
```

display qos-interface mirrored-to

Syntax **display qos-interface** [*interface-type interface-number*] **mirrored-to**

View Any view

Parameter *interface-type interface-number*: Port type and port number. If you enter this argument, the switch will display the parameter settings of the specified port. If not, the switch will display the parameters settings of all ports.

Description Use the **display qos-interface mirrored-to** command to display the parameter settings of traffic mirroring.

Information displayed includes:

- Port name and action name of traffic mirroring
- Direction of traffic mirroring
- ACL for identifying traffics
- Mirroring group

Related command: **mirrored-to**

Example # Display the parameter settings of traffic mirroring on GigabitEthernet 2/0/1.

```
<SW7750> display qos-interface GigabitEthernet 2/0/1 mirrored-to

GigabitEthernet2/0/1: mirrored-to
 Inbound:
   Matches: Acl 2000 rule 0  running
     Mirrored to: mirroring-group 3
```

mirrored-to

Syntax **mirrored-to inbound** *acl-rule* [**system-index** *system-index*] { **interface** *interface-type interface-number* [**reflector**] | **mirroring-group** *group-id* }

undo mirrored-to inbound *acl-rule*

View QoS view

Parameter **inbound**: Mirrors packets received on the port.

acl-rule: Applied ACL rules. Table 146 and Table 147 describe the ACL combinations on I/O Modules other than Type A and the corresponding parameter description.

Table 146 Combined application of ACLs on I/O Modules other than Type A.

Combination mode	Form of acl-rule
Apply all rules in an IP type ACL separately	**ip-group** { *acl-number* | *acl-name* }
Apply one rule in an IP type ACL separately	**ip-group** { *acl-number* | *acl-name* } **rule** *rule-id*
Apply all rules in a link type ACL separately	**link-group** { *acl-number* | *acl-name* }
Apply one rule in a link type separately	**link-group** { *acl-number* | *acl-name* } **rule** *rule-id*
Apply all rules in a user-defined ACL separately	**user-group** { *acl-number* | *acl-name* }
Apply one rule in a user-defined ACL separately	**user-group** { *acl-number* | *acl-name* } **rule** *rule-id*
Apply one rule in an IP type ACL and one rule in a link type ACL simultaneously	**ip-group** { *acl-number* | *acl-name* } **rule** *rule-id* **link-group** { *acl-number* | *acl-name* } **rule** *rule-id*

Table 147 Parameters description of ACL combinations

Parameter	Description
ip-group { *acl-number* | *acl-name* }	Basic and advanced ACL. *acl-number*: ACL number, ranging from 2,000 to 3,999. *acl-name*: ACL name, up to 32 characters long, beginning with an English letter (a to z or A to Z) without space and quotation mark, case insensitive.
link-group { *acl-number* | *acl-name* }	Layer 2 ACL *acl-number*: ACL number, ranging from 4,000 to 4,999. *acl-name*: ACL name, up to 32 characters long, beginning with an English letter (a to z or A to Z) without space and quotation mark, case insensitive.

Table 147 Parameters description of ACL combinations

Parameter	Description
user-group { *acl-number* | *acl-name* }	User-defined ACL *acl-number*: ACL number, ranging from 5,000 to 5,999. *acl-name*: ACL name, up to 32 characters long, beginning with an English letter (a to z or A to Z) without space and quotation mark, case insensitive.
rule-id	Number of the ACL rule, ranging from 0 to 127. If this argument is not specified, all rules in the specified ACL will be applied.

system-index: Specifies an interior index value which is used when an ACL rule is applied to the port. The index value ranges from 0 to 4294,967,295. This keyword is only available when the ACL rule number is specified in the command. After the specified ACL takes effect, there are three scenarios when you input the index value:

- If you do not input an index value or the index value you input is 0, the system will automatically assign an index whose value is greater than 0;
- If the input index value is not 0 and does not conflict with the interior index used by the system, the system will adopt the index value input by you;
- If the input index value is not 0 but conflicts with the interior index used by the system, the system will reassign an index value.

When the specified ACL rule is not effective, the system will adopt the index value input by you.

Interface *interface-type interface-number* [**reflector**]: Mirrors traffic flows to specific port. *interface-type interface-number* indicates an Ethernet port. With the **reflector** keyword specified, the parameters represent a reflector port, together with corresponding configuration to realize remote traffic mirroring; without the **reflector** keyword, the parameters represent a destination port, used to realize the local traffic mirroring.

mirroring-group *group-id*: Mirrors traffic flows to specific mirroring group.

Description

Use the **mirrored-to** command to start ACLs to identify traffics and perform traffic mirroring for packets that match.

Use the **undo mirrored-to** command to remove traffic mirroring configuration.

This command only applies to the rules whose actions are **permit** in matching the specified ACL, and only mirrors the received traffic flows. If you want to mirror traffic flows to a specified port, the port must be a destination port or reflector port of a mirroring group.

Related command:

display qos-interface mirrored-to, monitor-port.

Only non-type-A I/O Modules support the traffic mirroring configuration.

Example # Mirror packets that match ACL 2000 on port GigabitEthernet 2/0/1 to GigabitEthernet 2/0/4 through traffic mirroring.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] mirroring-group 3 local
[SW7750] mirroring-group 3 monitor-port GigabitEthernet 2/0/4
[SW7750] interface GigabitEthernet 2/0/1
[SW7750-GigabitEthernet2/0/1] qos
[SW7750-qosb-GigabitEthernet2/0/1] mirrored-to inbound ip-group 3000
 interface GigabitEthernet 2/0/4
```

mirroring-group

Syntax **mirroring-group** *group-id* { **local** | **remote-destination** | **remote-source** }

undo mirroring-group { *group-id* | **all** | **local** | **remote-destination** | **remote-source** }

View System view

Parameter *group-id*: Group number of a mirroring group, in the range of 1 to 20.

local: Specifies the mirroring group as a local mirroring group.

remote-destination: Specifies the mirroring group as the destination mirroring group for remote port mirroring.

remote-source: Specifies the mirroring group as the source mirroring group for remote mirroring.

all: Deletes all mirroring groups

Description Use the **mirroring-group** command to configure a mirroring group.

Use the **undo mirroring-group** command to delete a mirroring group.

Example # Configure a mirroring group on the local switch.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] mirroring-group 3 local
```

mirroring-group (only for configuration recovery)

Syntax **mirroring-group** *group-id* { **inbound** | **outbound** } *mirroring-port-list* **mirrored-to** *monitor-port*

View System view

Parameter *group-id*: Group ID of the mirroring group, in the range of 1 to 20.

inbound: Monitors the received packets only.

outbound: Monitors the sending packets only.

mirroring-port-list: Ethernet port list. It means there can be multiple ports. This argument is provide in the form of *port-list*={ *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-8>, where *Interface-type interface-number* means an Ethernet port, and &<1-8> means you can specify eight Ethernet ports or Ethernet port lists.

mirrored-to *monitor-port*: Specifies the destination port.

Description Use the **mirroring-group** command to recover the port mirroring configuration.

After software update, you can use this command to convert the port mirroring configuration configured with the old software version in the configuration file to the command syntax supported by the new software version.

Example # Recover the configuration of mirroring group 2, where Ethernet 2/0/1 through Ethernet 2/0/3 are source ports and Ethernet 2/0/4 is the destination port monitoring only the incoming packets.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] mirroring-group 2 inbound Ethernet 2/0/1 to Ethernet 2/0/3
mirrored-to Ethernet 2/0/4
```

mirroring-group mirroring-port

Syntax **mirroring-group** *group-id* **mirroring-port** *mirroring-port-list* { **both** | **inbound** | **outbound** }

undo mirroring-group *group-id* **mirroring-port** *mirroring-port-list*

View System view/Ethernet port view

Parameter *group-id*: Group number of a mirroring group, in the range of 1 to 20.

mirroring-port *mirroring-port-list*: Specifies a list of source ports, provided in the form of *mirroring-port-list*={ *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-8>, where *Interface-type interface-number* means an Ethernet port, and &<1-8> means you can specify eight source ports or source port lists.

For a centralized I/O Module, if multiple source ports are specified in remote port mirroring configuration, all the source ports must be on the same I/O Module.

both: Mirrors packets both received and sent via the port.

inbound: Mirrors only packets received via the port.

outbound: Mirrors only packets sent via the port.

Description Use the **mirroring-group mirroring-port** command to configure the source port.

Use the **undo mirroring-group mirroring-port** command to remove the configuration of the source port.

Example # Configure GigabitEthernet 2/0/1 as the source port and mirror all packets received via this port.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] mirroring-group 1 mirroring-port GigabitEthernet2/0/1 inbou
nd
```

mirroring-group mirroring-slot

Syntax **mirroring-group** *group-id* **mirroring-slot** *slot-number* { **inbound** | **outbound** | **both** }

undo mirroring-group *group-id* **mirroring-slot** *slot-number* { **inbound** | **outbound** | **both** }

View System view

Parameter *group-id*: Group number of a mirroring group, in the range of 1 to 20.

slot-number: Number of the slot where the mirroring source I/O Module resides.

Description Use the **mirroring-group mirroring-slot** command to configure the mirroring source I/O Module.

Use the **undo mirroring-group mirroring-slot** command to remove the mirroring source I/O Module.

Example # Specify the I/O Module residing in slot 3 as the mirroring source I/O Module and mirror all the packets received on the I/O Module.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] mirroring-group 1 mirroring-slot 3 inbound
```

mirroring-group monitor-port

Syntax **mirroring-group** *group-id* **monitor-port** *monitor-port*

undo mirroring-group *group-id* **monitor-port** *monitor-port*

View System view/Ethernet port view

Parameter *group-id*: Group number of a mirroring group, in the range of 1 to 20.

monitor-port *monitor-port*: Specifies the destination port for port mirroring. *monitor-port* is available in system view only.

Description Use the **mirroring-group monitor-port** command to configure the destination port.

Use the **undo mirroring-group monitor-port** to remove the configuration of the destination port.

Note the following when you configure the destination port:

- LACP must be disabled on the mirroring destination port and STP is recommended to be disabled on the port.
- The destination port for remote mirroring must be an Access port.
- After a port is configured as a reflector port, the switch does not allow you to change the port type and its default VLAN ID.

Example # Configure GigabitEthernet 2/0/4 as the source port and monitor all packets received via this port.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] mirroring-group 1 monitor-port GigabitEthernet2/0/4
```

mirroring-group monitor-slot

Syntax **mirroring-group** *group-id* **monitor-slot** *slot-number*

undo mirroring-group *group-id* **monitor-slot** *slot-number*

View System view

Parameter *group-id*: Group number of a mirroring group, in the range of 1 to 20.

slot-number: Number of the slot where the mirroring destination I/O Module resides.

Description Use the **mirroring-group monitor-slot** command to configure the destination mirroring I/O Module, which must be LS81VSNP or LS82VSNP. In order to mirror a port to a I/O Module, the mirroring group must be active.

Use the **undo mirroring-group monitor-slot** command to remove the configured mirroring destination I/O Module.

Example # Specify the LS81VSNP in slot 4 as the mirroring destination I/O Module.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] mirroring-group 1 monitor-slot 4
```

mirroring-group reflector-port

Syntax **mirroring-group** *group-id* **reflector-port** *reflector-port*

undo mirroring-group *group-id* **reflector-port** *reflector-port*

View System view/Ethernet port view

Parameter *group-id*: Group number of a mirroring group, in the range of 1 to 20.

reflector-port *reflector-port*: Specifies the reflector port. *reflector-port* is available in system view only.

Description Use the **mirroring-group reflector-port** command to specify the reflector port.

Use the **undo mirroring-group reflector-port** command to remove the configuration of the reflector port..

Note the following when you configure the reflector port:

- The reflector port must be an Access port.
- LACP must be disabled on the reflector port.
- The reflector ports are mutually exclusive with STP or DLDP. That is, if STP or DLDP is enabled on a port, you are not recommended to configure it as a reflector port; you are not recommended to enable STP or DLDP on a reflector port.
- After a port is configured as a reflector port, the switch does not allow you to change the port type and its default VLAN ID, or to add it to another VLAN.
- To mirror tagged packets, you need to configure VLAN VPN on the reflector port.

Example # Configure GigabitEthernet 2/0/2 as the reflector port.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] mirroring-group 1 reflector-port GigabitEthernet2/0/2
```

mirroring-group remote-probe vlan

Syntax **mirroring-group** *group-id* **remote-probe vlan** *remote-probe-vlan-id*

undo mirroring-group *group-id* **remote-probe vlan** *remote-probe-vlan-id*

View System view

Parameter *group-id*: Group number of a mirroring group, in the range of 1 to 20.

remote-probe vlan *remote-probe-vlan-id*: Specifies the remote-probe VLAN for the mirroring group.

Description Use the **mirroring-group remote-probe vlan** command to specify the remote-probe VLAN for a mirroring group.

Use the **undo mirroring-group remote-probe vlan** command to remove the configuration of remote-probe VLAN for a mirroring group.

Example # Configure VLAN 100 as the remote-probe VLAN.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] mirroring-group 1 remote-probe vlan 100
```

remote-probe vlan

Syntax **remote-probe vlan enable**

undo remote-probe vlan enable

View VLAN view

Parameter None

Description Use the **remote-probe vlan enable** command to configure the current VLAN as the remote-probe VLAN.

Use the **undo remote-probe vlan enable** command to configure the remote-probe VLAN as a normal VLAN.

Before configuring the remote-probe VLAN, make sure that no Access or Hybrid port belongs to this VLAN. If any Trunk port exists in this VLAN, the port PVID cannot be the ID of remote-probe VLAN. After setting a VLAN as remote-probe VLAN, it is recommended that you do not add Access or Hybrid port to the VLAN.

- *The **undo vlan all** command cannot be used to remove the specified remote-probe VLAN.*
- *After you input the **remote-probe vlan enable** the command, the system will check whether the current VLAN is a dynamic VLAN or not. If it is a dynamic VLAN, the command will fail to be executed, and the system prompts that "Can not set dynamic VLAN as remote-probe VLAN!".*

Example # Configure VLAN 5 as remote-probe vlan.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] vlan 5
[SW7750-vlan5] remote-probe vlan enable
```

60 NDP CONFIGURATION COMMANDS

display ndp

Syntax **display ndp** [**interface** *port-list*]

View Any view

Parameter **interface** *port-list*: Specifies a list of ports. The list can contain consecutive or separated ports, or the combination of the both. You need to provide the *port-list* argument in the form of *interface-type interface-number* [**to** *interface-type interface-number*] &<1-10>, where *interface-type* specifies the port type, and *interface-number* specifies the port number (in the form of slot number/device number/port number).**to**: Specifies a port range. &<1-10> means that you can provide up to ten port indexes/port index ranges for this argument.

Description Use the **display ndp** command to display the global NDP configuration information, including the interval to send NDP packets, the holdtime of NDP information, and the information about the neighbors of all the ports.

Example # Display NDP configuration information.

```
<aaa_0.3Com> display ndp
Neighbor Discovery Protocol is enabled.
Neighbor Discovery Protocol Ver: 1, Hello Timer: 10(s), Aging Timer:
 10(s)
Interface: GigabitEthernet0/0/1
    Status: Enabled, Pkts Snd: 179, Pkts Rvd: 6723, Pkts Err: 0
    Neighbor 1:  Aging Time: 8(s)
       MAC Address : 000f-e200-7502
       Host Name   : 3Com Switch 7757
       Port Name   : GigabitEthernet0/0/1
       Software Ver: 3.10
       Device Name : 3Com Switch 7757
       Port Duplex : AUTO
       Product Ver : S7757-3152
       BootROM Ver : 525

Interface: GigabitEthernet0/0/2
   Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: GigabitEthernet0/0/3
   Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: GigabitEthernet0/0/4
   Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0
```

```
Interface: GigabitEthernet2/0/1
   Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: GigabitEthernet2/0/2
   Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: GigabitEthernet2/0/3
Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0
```

# Display the information about Ethernet0/0/1.

```
<aaa_0.3Com> display ndp interface GigabitEthernet 0/0/1
Interface: GigabitEthernet0/0/1
    Status: Enabled, Pkts Snd: 179, Pkts Rvd: 6723, Pkts Err: 0
    Neighbor 1:  Aging Time: 8(s)
       MAC Address : 000f-e200-7502
       Host Name   : 3Com Switch 7757
       Port Name   : GigabitEthernet0/0/1
       Software Ver: 3.10
       Device Name : 3Com Switch 7757
       Port Duplex : AUTO
       Product Ver : S7757-3152
       BootROM Ver : 525
```

Table 148 Field descriptions of the **display ndp interface** command

Field	Description
Neighbor Discovery Protocol is enabled	NDP is enabled globally on the switch
Neighbor Discovery Protocol Ver: 1	NDP version 1 is running
Hello Timer	The interval to send NDP packets
Aging Timer	The holdtime of the NDP information sent by the local switch
Interface	Port index to specify a specific port
Status	NDP is enabled on the port
Pkts Snd	Number of the NDP packets transmitted through the port
Pkts Rvd	Number of the NDP packets received through the port
Pkts Err	Number of the error NDP packets received through the port
Neighbor 1: Aging Time	The holdtime of the NDP information received from the neighbors connected to the port
MAC Address	MAC address of a neighbor device
Host Name	System name of a neighbor device
Port name	Name of the port connected to the neighbor device
Software Ver	Neighbor device software version
Device Name	Device name of a neighbor device
Port Duplex	Port duplex mode of a neighbor device
Product Ver	Product version of a neighbor device
BootROM Ver	BootROM version of the neighbor device

ndp enable

Syntax **ndp enable** [**interface** *port-list*]

undo ndp enable [**interface** *port-list*]

View System view, Ethernet port view

Parameter **interface** *port-list*: Specifies a list of ports. The list can contain consecutive or separated ports, or the combination of the both. You need to provide the *port-list* argument in the form of *interface-type interface-number* [**to** *interface-type interface-number*] &<1-10>, where *interface-type* specifies the port type, and *interface-number* specifies the port number (in the form of slot number/device number/port number).**to**: Specifies a port range. &<1-10> means that you can provide up to ten port indexes/port index ranges for this argument.

Description In system view:

- Use the **ndp enable** command to enable NDP globally.
- Use the **undo ndp enable** command to disable NDP globally.

When the **ndp enable** command is executed in system view, the NDP feature is enabled globally if the *port-list* argument is not specified, while the NDP feature is enabled on the specified port if the *port-list* argument is specified.

In Ethernet port view:

- Use the **ndp enable** command to enable NDP on a port.
- Use the **undo ndp enable** command to disable NDP on a port.

When this command is used in Ethernet port view, the **interface** keyword cannot be provided and the NDP feature is enabled on the current port only.

By default, NDP is enabled both globally and on a port.

Note that the NDP feature on a port does not take effect until the NDP feature is enabled globally.

Example # Enable NDP globally.

```
<aaa_0.3Com> system-view
System View: return to User View with Ctrl+Z.
[aaa_0.3Com] ndp enable
```

ndp timer aging

Syntax **ndp timer aging** *aging-in-secs*

undo ndp timer aging

View System view

Parameter *aging-in-secs*: Holdtime (in seconds) to be set of the NDP information sent by the local switch. This argument ranges from 5 to 255.

Description Use the **ndp timer aging** command to set the holdtime of the information in the NDP packets sent by the local switch, that is, to specify how long a device will hold the NDP packets received from the local device. After the aging timer expires, the device removes the received NDP neighbor node information.

Use the **undo timer aging** command to restore the default NDP information holdtime.

You can specify how long an adjacent device will hold the NDP information sent by the local device. An adjacent device holds the NDP information of the local switch according to the holdtime carried in the NDP packets received from the local switch and removes the NDP information when the aging timer expires.

The default holdtime is 180 seconds.

Note that NDP information holdtime is longer than the interval to send NDP packets normally. Otherwise, the neighbor information table of an NDP port will become unstable.

Example # Configure the holdtime of the information in NDP packets sent by the local switch to be 60 seconds.

```
<aaa_0.3Com> system-view
System View: return to User View with Ctrl+Z.
[aaa_0.3Com] ndp timer aging 60
```

ndp timer hello

Syntax **ndp timer hello** *timer-in-seconds*

undo ndp timer hello

View System view

Parameter *timer-in-seconds*: Interval (in seconds) to send NDP packets ranging from 5 to 254. By default, the interval to send NDP packets is 60 seconds.

Description Use the **ndp timer hello** command to set the interval to send NDP packets.

Use the **undo ndp timer hello** command to restore the default interval to send NDP packets.

NDP information in a neighbor information table is updated regularly. This enables neighbor information table to contain the actual network topology information. You can use these two commands to adjust the updating frequency of NDP information.

Example # Configure the interval to send NDP packets to be 80 seconds.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ndp timer hello 80
```

reset ndp statistics

Syntax **reset ndp statistics** [**interface** *port-list*]

View User view

Parameter **interface** *port-list*: Specifies a list of ports. The list can contain consecutive or separated ports, or the combination of the both. You need to provide the *port-list* argument in the form of *interface-type interface-number* [**to** *interface-type interface-number*] &<1-10>, where *interface-type* specifies the port type, and *interface-number* specifies the port number (in the form of slot number/device number/port number).**to**: Specifies a port range. &<1-10> means that you can provide up to ten port indexes/port index ranges for this argument.

Description Use the **reset ndp statistics** command to clear NDP statistics.

Example # Clear NDP statistics.

```
<SW7750> reset ndp statistics
```

61 NTDP CONFIGURATION COMMANDS

display ntdp

Syntax **display ntdp**

View Any view

Parameter None

Description Use the **display ntdp** command to display the global NTDP information. The information includes the range (in hop count) within which topology information is collected, the interval to collect topology information (the NTDP timer), the delay time for a device to forward topology-collection requests, the delay time for a topology-collection request to be forwarded through a port, and the time cost during the last topology collection.

Example # Display the global NTDP information.

```
<aaa_0.3Com> display ntdp
 NTDP is running.
 Hops      : 3
 Timer     : 0 min
 Hop Delay : 200 ms
 Port Delay: 20 ms
 Last collection total time: 0ms
```

Table 149 Field descriptions of the **display ntdp** command

Field	Description
NTDP is running.	NTDP is enabled globally on the local device.
Hops	Hop count for topology collection
Timer	Interval to collect topology information
Hop Delay	Delay time for the device to forward topology collection requests
Port Delay	Delay time for a topology-collection request to be forwarded through a port
Last collection total time	Time cost during the last collection

display ntdp device-list

Syntax **display ntdp device-list** [**verbose**]

View Any view

Parameter **verbose**: Displays the detailed device information.

Description Use the **display ntdp device-list** command to display the device information collected through NTDP.

Example # Display the device list collected through NTDP.

```
<aaa_0.3Com> display ntdp device-list
MAC             HOP  IP                  PLATFORM
00e0-fc00-7506  0    100.100.1.1/24      S7757
00e0-fc01-7506  1    16.1.1.1/24         S7757
```

Table 150 Field descriptions of the **display ntdp device-list** command

Field	Description
MAC	MAC address of a device
HOP	Hops to the collecting device
IP	IP address and mask length of the management VLAN interface on the device
PLATFORM	Platform information about a device

# Display the detailed device information collected through NTDP.

```
<aaa_0.3Com> display ntdp device-list verbose

Hostname  : aaa_0.3Com
MAC       : 00e0-fc00-7506
Hop       : 0
Platform  : S7757
IP        : 100.100.1.1/24
Version   :
3Com Comware Platform Software.
   Comware Software, Version 3.10
   Copyright(c) 2004-2007 3Com Corporation All rights reserved. reserved.
S7757-5308
Cluster   :  Administrator switch of cluster aaa

Peer MAC        Peer Port ID            Native Port ID          Speed Duplex
00e0-fc00-3190  Ethernet1/0/22         Ethernet3/0/21          100   FULL

-----------------------------------------------------------------------------
Hostname  : aaa_1.3Com
MAC       : 00e0-fc01-7506
Hop       : 1
Platform  : S7757
IP        : 16.1.1.1/24
Version   :
3Com Comware Platform Software.
   Comware Software, Version 3.10
   Copyright(c) 2004-2007 3Com Corporation All rights reserved.
S7757-5308
Cluster   :  Candidate switch

Peer MAC        Peer Port ID            Native Port ID          Speed Duplex
00e0-fc00-3900  Ethernet3/0/21          Ethernet1/0/22          100   FULL
5600-0000-3334  GigabitEthernet7/0/32   Ethernet1/0/4           100   FULL
```

Table 151 Field descriptions of the **display ntdp device-list verbose** command

Field	Description
Hostname	System name of the device collected through NTDP
MAC	Mac address of the device
Hop	Number of hops from the device to the device which launches the topology collection
Platform	Software platform of the device
IP	IP address of the cluster management VLAN interface on the device (VLAN 1 is the cluster management VLAN of the Switch 7750)
Version	Version of the device
Cluster	The role of the device in the cluster
Peer MAC	MAC address of a neighbor device
Peer Port ID	Name of the peer port connected to the neighbor device
Native Port ID	Name of the local port which a neighbor device is connected to
Speed	Speed of the neighbor device port
Duplex	Duplex mode of the neighbor device port

ntdp enable

Syntax **ntdp enable**

undo ntdp enable

View System view, Ethernet port view

Parameter None

Description In system view:

Use the **ntdp enable** command to enable NTDP globally.

Use the **undo ntdp enable** command to disable NTDP globally.

In Ethernet port view:

Use the **ntdp enable** command to enable NTDP on a port.

Use the **undo ntdp enable** command to disable NTDP on a port.

By default, NTDP is enabled globally and on ports.

Note that the NDTP cannot operate if it is enabled on a port where NDP is disabled.

- *On a management device, NTDP must be enabled globally and on all the ports, and the NTDP parameters must be configured. On a member device, NTDP must be enabled globally and on the corresponding port. When NTDP is running on member devices, it adopts the NTDP parameters from the management device.*

- *NTDP takes effect in the management VLAN only. The Switch 7750 take VLAN 1 as the default VLAN, that is, the NTDP feature of the Switch 7750 takes effect in VLAN 1 only.*

Example # Enable NTDP globally.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ntdp enable
```

ntdp explore

Syntax **ntdp explore**

View User view

Parameter None

Description Use the **ntdp explore** command to start topology information collection manually.

You can use this command to enable the topology information collection manually. NTDP will collect the NDP information of every device and the information about the connections between the local switch and all of its neighbor devices in the specified network scope. The management device or the network administrator uses this information to acquire the network topology, manage and monitor the devices.

Example # Start the topology collection.

```
<aaa_0.3Com> ntdp explore
```

ntdp hop

Syntax **ntdp hop** *hop-value*

undo ntdp hop

View System view

Parameter *hop-value*: Maximum hops for collecting topology information, ranging from 1 to 16. By default, the value is 3.

Description Use the **ntdp hop** command to set a range (in terms of hop count) for topology information collection.

Use the **undo ntdp hop** command to restore the default range for topology information collection.

With the **ntdp hop** command, you can specify to collect the topology information of the devices within a specified range to avoid infinitive collection. The limit is performed by controlling the permitted hops from collection origination. For example, if you set the hop number limit to 2, only the switches less than 2 hops away from the switch starting the topology collection are collected.

Note that this command is only applicable to the topology-collecting device. A broader collection scope requires more memory of the topology-collecting device.

Example # Set the hop count for topology information collection to 5.

```
<aaa_0.3Com> system-view
System View: return to User View with Ctrl+Z.
[aaa_0.3Com] ntdp hop 5
```

ntdp timer

Syntax **ntdp timer** *interval-in- minutes*

undo ntdp timer

View System view

Parameter *interval-in- minutes*: Interval (in minutes) to collect topology information, ranging from 0 to 65,535. This argument defaults to 0, which specifies not to collect topology information.

Description Use the **ntdp timer** command to configure the interval to collect topology information.

Use the **undo ntdp timer** command to restore the default interval.

B y default, the interval to collect topology information is 0 minute, that is, topology information is not collected periodically.

A switch collects topology information once in each period set by the **ntdp timer** command.

Example # Set the interval to collect topology information to 30 minutes.

```
<aaa_0.3Com> system-view
System View: return to User View with Ctrl+Z.
[aaa_0.3Com] ntdp timer 30
```

ntdp timer hop-delay

Syntax **ntdp timer hop-delay** *time*

undo ntdp timer hop-delay

View System view

Parameter

time: Delay time (in milliseconds) for a switch to forward topology-collection request packets. This argument ranges from 1 to 1,000 and defaults to 200.

Description

Use the **ntdp timer hop-delay** command to set the delay time for a switch to forward topology-collection request packets.

Use the **undo ntdp timer hop-delay** command to restore the default delay time.

To avoid network congestion caused by a large amount of topology response packets received by the topology collection device in a short period, a switch delays for specific period before it forwards a received topology-collection request packet through its first ports. You can use the **ntdp timer hop-delay** command to set the delay time.

These two commands are intended for switches that collect topology information. They actually set the hop-delay value for topology-collection request packets sent by these switches. The hop-delay value determines the delay time for a switch receiving topology-collection request packets to forward them through its first port.

Example

Set the delay time for the switch to forward topology-collection request packets through the first port to 300 ms.

```
<aaa_0.3Com> system-view
System View: return to User View with Ctrl+Z.
[aaa_0.3Com] ntdp timer hop-delay 300
```

ntdp timer port-delay

Syntax

ntdp timer port-delay *time*

undo ntdp timer port-delay

View

System view

Parameter

time: Delay time (in milliseconds) for a switch to forward a topology-collection request packet through its successive ports. This argument ranges from 1 to 100 and defaults to 20.

Description

Use the **ntdp timer port-delay** command to set the delay time for a port (on the device whose topology information is collected) to wait to forward topology-collection request packets after the last port (on the device whose topology information is collected) forwards topology-collection request packets.

Use the **undo ntdp timer port-delay** command to restore the default delay time.

By default, the delay time of a port is 20 ms.

To avoid network congestion caused by a large amount of topology response packets received by the topology collection device in short periods, a switch delays for a specific period before it forwards a received topology-collection request packet through the next port. You can use the **ntdp timer port-delay** command to set the delay time.

These two commands are intended for switches that collect topology information. They actually set the port-delay value for topology-collection request packets sent by these switches. The port-delay value determines the delay time for a switch receiving topology-collection request packets to forward them through the next port.

Example # Set the delay time for the switch to forward topology-collection request packets through the successive ports to 40 ms.

```
<aaa_0.3Com> system-view
System View: return to User View with Ctrl+Z.
[aaa_0.3Com] ntdp timer port-delay 40
```

62 CLUSTER CONFIGURATION COMMANDS

add-member

Syntax **add-member** [*member- number*] **mac-address** *H-H-H* [**password** *password*]

View Cluster view

Parameter *member-number*: Member number assigned to the candidate device to be added to a cluster. This argument ranges from 1 to 255.

H-H-H: MAC address of the candidate device (in hexadecimal).

password: Password of the candidate device, a string comprising 1 to 256 characters. The password is required when you add a candidate device to a cluster. However, this argument is not needed if the candidate device is not configured with a password.

Description Use the **add-member** command to add a candidate device to a cluster.

You can add a candidate device to a cluster on the management device only.

If you do not specify the member number when adding a cluster member, the management device assigns the next available member number to it.

After a candidate device is added to a cluster, the level-3 password of the device is replaced by the password of the management device automatically.

Example # Add a candidate device to the cluster, setting the member number to 6. (Assume that the MAC address and level-3 user password of the candidate device are 00E0-fc00-35e7 and 123456.)

```
<aaa_0.3Com> system-view
System View: return to User View with Ctrl+Z.
[aaa_0.3Com] cluster
[aaa_0.3Com-cluster] add-member 6 mac-address 00E0-fc00-35e7 password 123456
```

administrator-address

Syntax **administrator-address** *mac-address* **name** *name*

undo administrator-address

View Cluster view

Parameter *mac-address*: MAC address of the management device.

name *name*: Name of an existing cluster, a string comprising up to 8 characters, which can only be alphanumeric characters, subtraction sign (-), and underline (_).

Description Use the **administrator-address** command to set the MAC address of the management device on a member device.

Use the **undo administrator-address** command to remove a member device from the cluster.

By default, a switch belongs to no cluster.

In order that the member devices identify the management device correctly after the system is restarted, the **administrator-address** command is enabled automatically on the switch to specify the MAC address of the management device in the cluster when the switch is added to the cluster as a member device.

Note that the **undo administrator-address** command is generally used in debugging or restoration. You are recommended to use the **delete-member** command to remove a cluster member from a cluster on the management device.

Example # Remove a member device from the cluster.

```
<aaa_1.3Com> system-view
System View: return to User View with Ctrl+Z
[aaa_1.3Com] cluster
[aaa_1.3Com-cluster] undo administrator-address
```

auto-build

Syntax **auto-build** [**recover**]

View Cluster view

Parameter **recover**: Establishes communication with all the member devices again.

Description Use the **auto-build** command to add the candidate device to the cluster automatically to be a member device.

This command can be executed on a candidate device or a management device.

When you use this command on a candidate device, you will be required to enter the cluster name and build a cluster. The system will collect candidate devices automatically and then it is for the user to decide whether to add the collected candidate devices into the cluster.

When you use this command on a management device, the system will collect candidate devices automatically.

The **recover** keyword is used to recover a cluster. Execute the **auto-build recover** command to look for the down members in the member list and add them to the cluster again.

Note: Ensure that NTDP is enabled, because it is the basis of candidate and member collection. The collection range is also decided through NTDP. You can use the **hop** command in system view to modify the collection range.

If a member device is configured with a level-3 user password different from that of the management device, it cannot be added to the cluster automatically.

CAUTION: *When configuring a cluster, you must ensure that the routing table is not full. Otherwise, the private IP routes of the cluster cannot be advertised, and as a result cluster handshake messages cannot be properly sent or received and devices will repeatedly join or leave the cluster.*

- If the routing table of the administrative device is full upon establishment of a cluster, all candidate devices will repeatedly join or leave the cluster.
- If the routing table of the administrative device is full when a candidate device of a cluster joins the cluster, this device will repeatedly join or leave the cluster.

Example # Set up a cluster automatically.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] cluster
[SW7750-cluster] auto-build

Please input cluster name:aaa
Collecting candidate list, please wait...

Candidate list:

Name                            Hops  MAC Address     Device
3Com                         1     000f-e200-016a  3Com 2016-EI

Add all to cluster?(Y/N)y
%May 30 09:07:30 2006 aaa_0.3Com Switch 7758 CLST/5/LOG:
 Member 000f-e200-016a  is joined in cluster aaa.

 Cluster auto-build Finish!
 1 member(s) added successfully.

[aaa_0.3Com-cluster]
```

build

Syntax **build** *name*

undo build

View Cluster view

Parameter *name*: Cluster name, a string comprising up to 8 characters, which can only be alphanumeric characters, subtraction sign (-), and underline (_).

Description Use the **build** command to configure or modify the cluster name.

Use the **undo build** command to remove a cluster.

If the **build** command is executed on the candidate device, the current switch will be configured as the management device and assigned with a cluster name.

If the **build** command is executed on the management device, the cluster name will be modified.

The member number of a management device is 0.

Example # Configure the current switch to be a management device and specify the cluster name to be aaa.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z
[SW7750] cluster
[SW7750-cluster] build aaa
[aaa_0.3Com-cluster]
```

cluster

Syntax **cluster**

View System view

Parameter None

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

Example # Enter cluster view.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z
[SW7750] cluster
[SW7750-cluster]
```

cluster enable

Syntax **cluster enable**

undo cluster enable

View System view

Parameter None

Description Use the **cluster enable** command to enable the cluster function on a switch.

Use the **undo cluster enable** command to disable the cluster function on a switch.

By default, the cluster function is enabled on all the devices supporting cluster.

You need to create a cluster with the **build** command before using the **cluster enable** command on the management device.

These two commands can be used on any device supporting the cluster function. When you execute the **undo cluster enable** command on a management device, the cluster is removed, and the switch stop operating as a management device. When you execute this command on a member device, the cluster function is disabled on the switch, and the switch quit the cluster. When you execute this command on a switch that belongs to no cluster, the cluster function is disabled on the switch.

Example # Enable the cluster function on a switch.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z
[SW7750] cluster enable
```

cluster switch-to

Syntax **cluster switch-to** { *member-number* | **mac-address** *H-H-H* | **administrator** }

View User view

Parameter *member-number*: Member number of a switch in a cluster, ranging from 0 to 255.

H-H-H: Specifies the MAC address of a member device.

administrator: Redirects from a member device to the management device.

Description Use the **cluster switch-to** command to switch between the management device and member devices for configuration and management.

You can manage member devices in a cluster through the management device, on which you can switch to member view to configure or manage specified member devices, and then use the **quit** command to return to the management device.

Telnet connection is used for switching between the cluster administrative device and member device. When switching between the two views, observe the following rules:

- Authentication is required when you switch between the cluster administrative device view and member device view. The system will authenticate the super password of the level-3 user. If the super password of the device requesting the switchover is inconsistent with that of the device to be logged in, switchover fails. When a candidate device is added to the cluster, its super password is automatically set to the super password of the administrative device. After the cluster is set up, you are recommended not to change the super password of the cluster member (including the administrative device and member device). Otherwise, view switchover may fail because authentication is not passed.

- When you switch from the administrative device view to the member device view, the current user level in member device view is consistent with that in the administrative device view.
- When you switch from the member device view to the administrative device view, the user level is assigned according to the preset level of the administrative device.
- If the number of Telnet users on the device to be logged in reaches the threshold, view switchover fails.

When you use this command on the administrative device, if the member number *n* does not exist or the specified mac-address is not in the member list, the system will display an error message. To end the switchover, enter the **quit** command.

Example # Switch from the management device to the member device numbered 6 and then switch back to the management device.

```
<aaa_0.3Com> cluster switch-to 6
<aaa_0.3Com> quit
<aaa_0.3Com>
```

cluster-mac

Syntax **cluster-mac** *H-H-H*

undo cluster-mac

View Cluster view

Parameters *H-H-H*: Multicast MAC address to be set for the cluster, in hexadecimal format. This argument can be one of the following addresses: 0180-C200-0000, 0180-C200-000A, 0180-C200-0020 to 0180-C200-002F.

Description Use the **cluster-mac** command to configure a multicast MAC address for the cluster.

Use the **undo cluster-mac** command to restore the default multicast MAC address.

The default multicast MAC address is 0180-C200-000A.

Note that, you can only use this command on a management device.

The management device in a cluster is able to periodically send Switch Clustering V2 multicast MAC synchronization packets. After you configure a multicast MAC address on the management device, all the member/candidate devices of the cluster will synchronize to the same multicast MAC address by receiving multicast

MAC synchronization packets. This guarantees that the member/candidate devices of the cluster can receive the multicast packets from the management device.

Examples # Configure multicast MAC address 0180-C200-0028 for the cluster.

```
<aaa_0.3Com> system-view
System View: return to User View with Ctrl+Z.
[aaa_0.3Com] cluster
[aaa_0.3Com-cluster] cluster-mac 0180-C200-0028
```

cluster-mac syn-interval

Syntax **cluster-mac syn-interval** *time-interval*

View Cluster view

Parameters *time-interval*: Interval to send Switch Clustering V2 multicast MAC synchronization packets, ranging from 0 to 30 minutes.

Description Use the **cluster-mac syn-interval** command to set the interval for the management device to send Switch Clustering V2 multicast MAC synchronization packets periodically. You can only use this command on a management device.

By default, this interval is one minute.

If you set this interval to zero on a management device, the management device will not send Switch Clustering V2 multicast MAC synchronization packets to other devices.

Examples # Set the interval for the management device to send Switch Clustering V2 multicast MAC synchronization packets to one minute.

```
<aaa_0.3Com> system-view
System View: return to User View with Ctrl+Z.
[aaa_0.3Com] cluster
[aaa_0.3Com-cluster] cluster-mac syn-interval 1
```

delete-member

Syntax **delete-member** *member-number*

View Cluster view

Parameter *member-number*: Member number of a switch in a cluster, ranging from 0 to 255.

Description Use the **delete-member** command to remove a member device from the cluster.

Perform the operation to remove a member device from a cluster on the management device only. Otherwise, errors occur.

Example # Remove the member device numbered 2 from the cluster.

```
<aaa_0.3Com> system-view
System View: return to User View with Ctrl+Z.
[aaa_0.3Com] cluster
[aaa_0.3Com-cluster] delete-member 2
```

display cluster

Syntax **display cluster**

View Any view

Parameter None

Description Use the **display cluster** command to display the state and statistics of the cluster to which the current switch belongs.

When being executed on a member device, this command displays the information such as cluster name, member number of the current switch, the MAC address and state of the management device, holdtime, and the interval to send packets.

When being executed on a management device, this command displays the information such as cluster name, the number of the member devices in the cluster, cluster state, holdtime and the interval to send packets.

The system will prompt that the device does not belong to any cluster if you execute this command on a switch that does not belong to any cluster.

Example # Display cluster information (assuming that the current switch is a management device).

```
<aaa_0.3Com> display cluster
Cluster name:"aaa"
Role:Administrator

Handshake timer:10 sec
Handshake hold-time:60 sec
IP-Pool:2.2.2.2/24
No logging host configured
No SNMP host configured
FTP server:8.8.8.8
No TFTP server configured

21 member(s) in the cluster, and 1 of them down.
```

# Display cluster information on the member device.

```
<aaa_2.3Com> display cluster
Cluster name:"aaa"
Role:Member
Member number:2
```

```
Handshake timer:10 sec
Handshake hold-time:60 sec

Administrator device mac address:00e0-fc00-7506
Administrator status:Up
```

Table 152 Field descriptions of the **display cluster** command

Field	Description
Cluster name	Name of the cluster
Role	Cluster role of the switch
Member number	Member number of the switch
Handshake timer	Value of handshake timer
Handshake hold-time	Handshake holdtime
Administrator device mac address	MAC address of the management device
Administrator status	State of the management device

display cluster candidates

Syntax **display cluster candidates** [**mac-address** *H-H-H* | **verbose**]

View Any view

Parameter **mac-address** *H-H-H*: Specifies the MAC address of a candidate device.

verbose: Displays the detailed information about all the candidate devices.

Description Use the **display cluster candidates** command to display the information about the candidate devices of a cluster.

Execute this command on management devices only.

Example # Display the information about all the candidate devices.

```
<aaa_0.3Com> display cluster candidates
MAC             HOP   IP                 PLATFORM
0000-0000-004d  3    192.169.121.258/24  3Com 7506R
000f-e200-7502  2    8.8.8.3/24          3Com Switch 7757
000f-e200-1234  1    8.8.8.2/24          3Com S7502
```

Table 153 Field descriptions of the **display cluster candidates** command

Field	Description
MAC	MAC address of a candidate device
Hop	Hops from a candidate device to the management device
IP	IP address of a candidate device
Platform	Platform of a candidate device

# Display the information about a specified candidate device.

```
<aaa_0.3Com-cluster> display cluster candidates mac-address 000f-e200-7502

 Hostname  : S7757
 MAC       : 000f-e200-7502
 Hop       : 1
 Platform  : 3Com Switch 7757
 IP        : 8.8.8.3
```

# Display the detailed information about all the candidate devices.

```
<aaa_0.3Com Switch 7758>display cluster candidates verbose

 Hostname  : 3Com S7502
 MAC       : 000f-e201-0110
 Hop       : 1
 Platform  : 3Com S7502
 IP        :
```

Table 154 Field descriptions of the **display cluster candidates verbose** command

Field	Description
Hostname	Name of a candidate device
MAC	MAC address of a candidate device
Hop	Hops from a candidate device to the management device
IP	IP address of a candidate device
Platform	Platform of a candidate device

display cluster members

Syntax **display cluster members** [*member-number* | **verbose**]

View Any view

Parameter *member-number*: Member number of a switch in a cluster, ranging from 0 to 255.

verbose: Displays the detailed information about all the devices in a cluster.

Description Use the **display cluster members** command to display the information about cluster members.

Execute this command on management devices only.

Example # Display the information about all the devices in the cluster.

```
<aaa_0.3Com> display cluster members
SN   Device              MAC Address     Status Name
0    3Com Switch 7758      00e0-fc00-7506  Admin  aaa_0.3Com
1    3Com S7502       000f-e200-1234  Up     aaa_1.3Com-1
2    3Com Switch 7757      000f-e200-7502  Up     aaa_2.3Com-2
3    3Com Switch 7758      0000-0000-004d  Up     aaa_3.3Com-3
```

Table 155 Field descriptions of the **display cluster members** command

Field	Description
SN	Member number
Device	Device type
MAC Address	MAC address of a device

Table 155 Field descriptions of the **display cluster members** command

Field	Description
Status	State of a device
Name	Name of a device

# Display the detailed information about the management device and all member devices.

```
<aaa_0.3Com> display cluster members verbose
Member number:0
Name: aaa_0.3Com
Device:3Com Switch 7758
MAC Address:00e0-fc00-7506
Member status:Admin
Hops to administrator device:0
IP: 8.8.8.1/24
Version:
3Com Comware Platform Software.
   Comware Software, Version 3.10
   Copyright(c) 2004-2006 3Com Corporation All rights reserved.
S7757-5308

Member number:1
Name:aaa_1.3Com-1
Device:3Com S7502
MAC Address:000f-e200-1234
Member status:Up
Hops to administrator device:
IP: 8.8.8.2/24
Version:
3Com Comware Platform Software.
   Comware Software, Version 3.10
   Copyright(c) 2004-2006 3Com Corporation All rights reserved.
S7757-5308

Member number:2
Name:aaa_2. 3Com-2
Device:3Com Switch 7757
MAC Address:000f-e200-7502
Member status:Up
Hops to administrator device:
IP:8.8.8.3/24
Version:
3Com Comware Platform Software.
   Comware Software, Version 3.10
   Copyright(c) 2004-2006 3Com Corporation All rights reserved.
S7757-5308

Member number:3
Name: aaa_3.3Com-3
Device:3Com Switch 7758
MAC Address:0000-0000-004d
Member status:Up
Hops to administrator device:2
IP: 192.168.1.26/24
Version:
3Com Comware Platform Software.
   Comware Software, Version 3.10
   Copyright(c) 2004-2006 3Com Corporation All rights reserved.
S7757-5308
```

Table 156 Field descriptions of the **display cluster members verbose** command

Field	Description
Member number	Device member number
Name	Name of a device
Device	Device type
MAC Address	MAC address of a device
Member status	State of a device
Hops to administrator device	Hops from the current device to the management device
IP	IP address of a device
Version	Software version of the current device

ftp cluster

Syntax **ftp cluster**

View User view

Parameter None

Description Use the **ftp cluster** command to establish control connection with the public FTP server of the cluster and enter FTP client view.

Example # Connect the FTP clients to the remote FTP server of the cluster.

```
<123_1.3Com> ftp cluster
Trying ...
Press CTRL+K to abort
Connected.
220 FTP service ready.
User(none):hello
331 Password required for hello.
Password:
230 User logged in.
```

ftp-server

Syntax **ftp-server** *ip-address*

undo ftp-server

View Cluster view

Parameter *ip-address*: IP address of the FTP server to be configured for the cluster.

Description Use the **ftp-server** command to configure an FTP server on the management device for the member devices in the cluster.

Use the **undo ftp-server** command to remove the FTP server configured for the member devices in the cluster.

By default, the management device acts as the FTP Server.

You need to configure the IP address of an FTP server first for the member devices in a cluster to access the FTP server through the management device.

Example # Configure the IP address of an FTP server on the management device.

```
<aaa_0.3Com> system-view
System View: return to User View with Ctrl+Z.
[aaa_0.3Com] cluster
[aaa_0.3Com-cluster] ftp-server 1.0.0.9
```

holdtime

Syntax **holdtime** *seconds*

undo holdtime

View Cluster view

Parameter *seconds*: Holdtime (in seconds) ranging from 1 to 255.

Description Use the **holdtime** command to configure the holdtime of a switch.

Use the **undo holdtime** command to restore the default holdtime value.

- If a switch does not receive any information of a peer device during the holdtime, it sets the state of the peer device to "down". When the communication between the two resumes, the corresponding member device is re-added to the cluster (automatically).
- If the downtime does not exceed the holdtime, the member device stays in the normal state and needs not to be added again.

Execute these two commands on management devices only. The member devices in a cluster acquire the holdtime setting from the management device.

Example # Set the holdtime to 30 seconds.

```
<aaa_0.3Com> system-view
System View: return to User View with Ctrl+Z.
[aaa_0.3Com] cluster
[aaa_0.3Com-cluster] holdtime 30
```

ip address

Syntax **ip address** *ip-address* { *mask* | *mask-length* }

undo ip address *ip-address* { *mask* | *mask-length* }

View VLAN interface view

Parameter *ip-address*: IP address of the VLAN interface, expressed in dotted decimal.

mask: Subnet mask of the VLAN interface IP address, expressed in dotted decimal.

mask-length: Length of the subnet mask , namely, the number of "1"s in the subnet mask.

Description Use the **ip address** command to specify an IP address and subnet mask for the VLAN interface.

Use the **undo ip address** command to remove the IP address and subnet mask of the VLAN interface.

By default, the IP address of a VLAN interface is null.

Note that:

- *The Switch 7750 use VLAN 1 as the cluster management VLAN to manage the cluster.*
- *The IP address of the Layer 3 virtual interface of the management VLAN must be configured before a cluster is set up; otherwise, the cluster cannot be set up successfully.*
- *When a cluster is set up, the IP address of the management VLAN interface cannot be modified any more.*

Example # Set the IP address of VLAN interface 1 to 129.12.0.1 and the subnet mask to 255.255.255.0.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface vlan-interface 1
[SW7750-Vlan-interface1] ip address 129.12.0.1 255.255.255.0
```

ip-pool

Syntax **ip-pool** *administrator-ip-address* { *ip-mask* | *ip-mask-length* }

undo ip-pool

View Cluster view

Parameter *administrator-ip-address*: IP address of the management device of a cluster.

ip-mask: Mask of the cluster IP address pool.

ip-mask-length: Mask length of the cluster IP address pool.

Description Use the **ip-pool** command to configure a private IP address range for cluster members on the switch to be configured as the management device.

Use the **undo ip-pool** command to cancel the IP address range configuration.

Before establishing a cluster, you need to configure a private IP address pool for the switches to be added to the cluster. When a candidate device is added to a cluster, the management device assigns a private IP address to it for the candidate device to communicate with other devices in the cluster. This enables you to manage and maintain member devices in a cluster through the management device.

Execute these two commands on switches that belong to no cluster only. The IP address range of an existing cluster cannot be modified.

Example # Configure the IP address range of a cluster.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z
[SW7750] cluster
[SW7750-cluster] ip-pool 10.200.0.1 20
```

logging-host

Syntax **logging-host** *ip-address*

undo logging-host

View Cluster view

Parameter *ip-address*: IP address of the logging host configured for the cluster.

Description Use the **logging-host** command to configure a logging host on the management device for the member devices in the cluster.

Use the **undo logging-host** command to remove the public logging host for the member devices in the cluster.

By default, no logging host is configured.

You need to configure the IP address of a logging host first for the member devices in a cluster to send log information to the logging host through the management device.

Example # Configure the IP address of the logging host on the management device.

```
<aaa_0.3Com> system-view
System View: return to User View with Ctrl+Z
[aaa_0.3Com] cluster
[aaa_0.3Com-cluster] logging-host 10.10.10.9
```

reboot member

Syntax **reboot member** { *member-number* | **mac-address** *H-H-H* } [**eraseflash**]

View Cluster view

Parameter *member-number*: Member number of a switch in a cluster, ranging from 0 to 255.

mac-address *H-H-H*: MAC address of the member device to be rebooted.

eraseflash: Deletes the configuration file when the member device reboots.

Description Use the **reboot member** command to reboot a specified member device on the management device.

Communication between the management and member devices may be interrupted due to some configuration errors. Through the remote control function of member devices, you can control them remotely on the management device. For example, you can reboot a member device that operates improperly and specify to delete the booting configuration file when the member device reboots, and thus restore normal communication between the management and member devices.

The **eraseflash** keyword specifies to delete the booting configuration file when the member device reboots.

Example # Reboot the member device numbered 2.

```
<aaa_0.3Com> system-view
System View: return to User View with Ctrl+Z
[aaa_0.3Com] cluster
[aaa_0.3Com-cluster] reboot member 2
```

snmp-host

Syntax **snmp-host** *ip-address*

undo snmp-host

View Cluster view

Parameter *ip-address*: IP address of a SNMP host to be configured for a cluster.

Description Use the **snmp-host** command to configure an SNMP host for the member devices inside a cluster on the management device.

Use the **undo snmp-host** command to cancel the SNMP host configuration.

By default, no SNMP host is configured.

You need to configure the IP address of an SNMP host first for the cluster, in order that the member devices in a cluster can send trap messages to the SNMP host through the management device.

Example # Configure an SNMP host for the cluster on the management device.

```
<aaa_0.3Com> system-view
System View: return to User View with Ctrl+Z
[aaa_0.3Com] cluster
[aaa_0.3Com-cluster] snmp-host 1.0.0.9
```

tftp cluster get

Syntax **tftp cluster get** *source-file* [*destination-file*]

View User view

Parameter *source-file*: Name of the file to be downloaded from the public TFTP server of the cluster.

destination-file: Name of the downloaded file, which is saved in the switch.

Description Use the **tftp cluster get** command to download files from the specified directory on the public TFTP server to the switch.

Related command: **tftp cluster put**.

Example # Download the file name LANSwitch.app from the public TFTP server of the cluster to the switch and save it as vs.app.

```
<123_1.3Com> tftp cluster get LANSwitch.app vs.app
```

tftp cluster put

Syntax **tftp cluster put** *source-file* [*destination-file*]

View User view

Parameter *source-file*: File to be uploaded to the server.

destination-file: Name of the uploaded file saved in the storage directory of the TFTP server.

Description Use the **tftp put** command to upload the file in the switch to the specified directory in the TFTP server.

Related command: **tftp cluster get**.

Example # Upload the file named vrpcfg.txt in the switch to the public TFTP server of the cluster and save it as temp.txt.

```
<123_1.3Com> tftp cluster put vrpcfg.txt temp.txt
```

tftp-server

Syntax

tftp-server *ip-address*

undo tftp-server

View

Cluster view

Parameter

ip-address: IP address of a TFTP server to be configured for a cluster.

Description

Use the **tftp-server** command to configure a TFTP server for cluster members on the management device.

Use the **undo tftp-server** command to cancel the TFTP server of the cluster members.

By default, no TFTP server is configured.

You need to configure the IP address of the TFTP server for the cluster, in order that the member devices in the cluster can access the TFTP server through the management device.

Execute these two commands on management devices only.

Example

Configure a TFTP server on the management device.

```
<aaa_0.3Com> system-view
System View: return to User View with Ctrl+Z
[aaa_0.3Com] cluster
[aaa_0.3Com-cluster] tftp-server 1.0.0.9
```

timer

Syntax

timer *interval*

undo timer

View

Cluster view

Parameter

interval: Interval (in seconds) to send handshake packets. This argument ranges from 1 to 255.

Description

Use the **timer** command to set the interval to send handshake packets.

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

By default, the interval to send handshake packets is 10 seconds.

Inside a cluster, the connections between member devices and the management device are kept through transmitting handshake packets. Handshake packets in a cluster enable the management device to acquire the information about member states link states.

Execute these two commands on management devices only. All the member devices in a cluster acquire the handshake interval setting from the management device.

Example # Configure the interval to send handshake packets to be 3 seconds.

```
<aaa_0.3Com> system-view
System View: return to User View with Ctrl+Z
[aaa_0.3Com] cluster
[aaa_0.3Com-cluster] timer 3
```

63 POE CONFIGURATION COMMANDS

display poe interface

Syntax **display poe interface** { *interface-type interface-number* | **all** }

View Any view

Parameter *interface-type interface-number*: Port on the switch. Refer to *"Port Basic Configuration Commands" on page 195* for details.

all: Displays the PoE information of all the PoE ports on the switch.

Description Use the **display poe interface** command to view the PoE status of a specific port. If the **all** keyword is specified, the command displays the PoE status of all the PoE ports.

Example # Display the PoE status of Ethernet3/0/1.

```
<SW7750> display poe interface Ethernet 3/0/1
Port power status            :PD searching
Port power mode              :signal
Port PD class                :0
port power priority          :low
Port max power               :15400 mW
Port current power           :0 mW
Port average power           :0 mW
Port peak power              :0 mW
Port current                 :0 mA
Port voltage                 :0.0 V
```

Table 157 Field descriptions of the **display poe interface** command

Field	Description
Port power status	PoE status of the port: Disabled: Power is disabled on the port. PD searching: The port is searching PD. delivering: The port is delivering power to PD. PD disconnected: PD is disconnected. testing: The port is testing the PD. fault: Nonstandard PD is detected or failure occurs.
Port power mode	PoE mode of the port: signal: The port supplies port in the **signal** mode. spare: The port supplies power in the **spare** mode.

Table 157 Field descriptions of the **display poe interface** command

Field	Description
Port PD class	Class of power to the PD
Port power priority	PoE priority of the port: ■ critical: The highest ■ high: High ■ low: Low
Port max power	The maximum available power on the port
Port current power	The current power on the port
Port average power	The average power on the port
Port peak power	The peak power on the port
Port current	The current on the port
Port voltage	The voltage on the port

# Display the PoE status of all ports.

```
<SW7750> display poe interface all
Interface Ethernet3/0/1 power status: delivering
Interface Ethernet3/0/2 power status: PD searching
Interface Ethernet3/0/3 power status: PD searching
Interface Ethernet3/0/4 power status: PD searching
Interface Ethernet3/0/5 power status: PD searching
Interface Ethernet3/0/6 power status: PD searching
Interface Ethernet3/0/7 power status: PD searching
Interface Ethernet3/0/8 power status: PD searching
Interface Ethernet3/0/9 power status: PD searching
Interface Ethernet3/0/10 power status: PD searching
Interface Ethernet3/0/11 power status: PD searching
Interface Ethernet3/0/12 power status: PD searching
Interface Ethernet3/0/13 power status: PD searching
Interface Ethernet3/0/14 power status: PD searching
Interface Ethernet3/0/15 power status: PD searching
Interface Ethernet3/0/16 power status: PD searching
Interface Ethernet3/0/17 power status: delivering
Interface Ethernet3/0/18 power status: PD searching
Interface Ethernet3/0/19 power status: PD searching
Interface Ethernet3/0/20 power status: PD searching
Interface Ethernet3/0/21 power status: PD searching
Interface Ethernet3/0/22 power status: PD searching
Interface Ethernet3/0/23 power status: PD searching
Interface Ethernet3/0/24 power status: PD searching
Interface Ethernet3/0/25 power status: PD searching
Interface Ethernet3/0/26 power status: PD searching
Interface Ethernet3/0/27 power status: PD searching
Interface Ethernet3/0/28 power status: PD searching
Interface Ethernet3/0/29 power status: PD searching
Interface Ethernet3/0/30 power status: PD searching
Interface Ethernet3/0/31 power status: PD searching
Interface Ethernet3/0/32 power status: PD searching
Interface Ethernet3/0/33 power status: PD searching
Interface Ethernet3/0/34 power status: PD searching
Interface Ethernet3/0/35 power status: PD searching
Interface Ethernet3/0/36 power status: PD searching
Interface Ethernet3/0/37 power status: PD searching
Interface Ethernet3/0/38 power status: PD searching
Interface Ethernet3/0/39 power status: PD searching
Interface Ethernet3/0/40 power status: PD searching
Interface Ethernet3/0/41 power status: PD searching
Interface Ethernet3/0/42 power status: PD searching
Interface Ethernet3/0/43 power status: PD searching
Interface Ethernet3/0/44 power status: PD searching
Interface Ethernet3/0/45 power status: PD searching
Interface Ethernet3/0/46 power status: PD searching
Interface Ethernet3/0/47 power status: PD searching
Interface Ethernet3/0/48 power status: PD searching
```

display poe interface power

Syntax **display poe interface power** { *interface-type interface-number* | **all** }

View Any view

Parameter *interface-type interface-number*: Port on the switch. Refer to **interface** on page 205.

all: Displays the power of all PoE ports on the switch.

Description Use the **display poe interface power** command to view the power information of a specific port of the switch. If the **all** keyword is specified, the command displays the power information of all PoE ports on the switch.

Example # Display the power information of the PoE port Ethernet3/0/1.

```
<SW7750> display poe interface power Ethernet 3/0/1
Port power                   :700 mW
```

# Display the power information of all PoE ports.

```
<SW7750> display poe interface power all
Interface Ethernet3/0/1 current power : 700 mw
Interface Ethernet3/0/2 current power : 0 mw
Interface Ethernet3/0/3 current power : 0 mw
Interface Ethernet3/0/4 current power : 0 mw
Interface Ethernet3/0/5 current power : 0 mw
Interface Ethernet3/0/6 current power : 0 mw
Interface Ethernet3/0/7 current power : 0 mw
Interface Ethernet3/0/8 current power : 0 mw
Interface Ethernet3/0/9 current power : 0 mw
Interface Ethernet3/0/10 current power : 0 mw
Interface Ethernet3/0/11 current power : 0 mw
Interface Ethernet3/0/12 current power : 0 mw
Interface Ethernet3/0/13 current power : 0 mw
Interface Ethernet3/0/14 current power : 0 mw
Interface Ethernet3/0/15 current power : 0 mw
Interface Ethernet3/0/16 current power : 0 mw
Interface Ethernet3/0/17 current power : 13900 mw
Interface Ethernet3/0/18 current power : 0 mw
Interface Ethernet3/0/19 current power : 0 mw
Interface Ethernet3/0/20 current power : 0 mw
Interface Ethernet3/0/21 current power : 0 mw
Interface Ethernet3/0/22 current power : 0 mw
Interface Ethernet3/0/23 current power : 0 mw
Interface Ethernet3/0/24 current power : 0 mw
Interface Ethernet3/0/25 current power : 0 mw
Interface Ethernet3/0/26 current power : 0 mw
Interface Ethernet3/0/27 current power : 0 mw
Interface Ethernet3/0/28 current power : 0 mw
Interface Ethernet3/0/29 current power : 0 mw
Interface Ethernet3/0/30 current power : 0 mw
Interface Ethernet3/0/31 current power : 0 mw
Interface Ethernet3/0/32 current power : 0 mw
Interface Ethernet3/0/33 current power : 0 mw
Interface Ethernet3/0/34 current power : 0 mw
Interface Ethernet3/0/35 current power : 0 mw
Interface Ethernet3/0/36 current power : 0 mw
Interface Ethernet3/0/37 current power : 0 mw
Interface Ethernet3/0/38 current power : 0 mw
Interface Ethernet3/0/39 current power : 0 mw
Interface Ethernet3/0/40 current power : 0 mw
Interface Ethernet3/0/41 current power : 0 mw
Interface Ethernet3/0/42 current power : 0 mw
Interface Ethernet3/0/43 current power : 0 mw
Interface Ethernet3/0/44 current power : 0 mw
Interface Ethernet3/0/45 current power : 0 mw
Interface Ethernet3/0/46 current power : 0 mw
Interface Ethernet3/0/47 current power : 0 mw
Interface Ethernet3/0/48 current power : 0 mw
```

display poe powersupply

Syntax **display poe powersupply**

View Any view

Parameter None

Description Use the **display poe powersupply** command to view the parameters of the external PoE power supply units (PSU).

Example # Display the parameters of external PoE PSUs.

```
<SW7750> display poe powersupply
Power Model              :Spring Pms
Power Manufacturer       :Tyco Electronics Com
Power Nominal Value      :2400 W
Power Peak Value         :0 W
Power Average Value      :0 W
Power Current Current    :0 mA
Power Current Voltage    :54.0 V
Power Current Value      :18 W
Power Software Version  :512
Power Hardware Version  :000
```

Table 158 Field descriptions of the **display poe powersupply** command

Field	Description
Power Model	Identification of the PSU manufacturer
Power manufacturer	Name of the power manufacturer
Power Nominal Value	Nominal power of the PSU
Power Peak Value	Peak power of the PSU
Power Average Value	Average power of the PSU
Power Current Current	Current current of the PSU
Power Current Voltage	Current voltage of the PSU
Power Current Value	Current power of the PSU
Power Software Version	Version of the PSU software
Power Hardware Version	Version of the PSU hardware

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 modules that serve as power sourcing equipment (PSE).

Example # Display the parameters of all modules that serve as PSE on the switch.

```
<SW7750> display poe pse
  PSE Information of board 4:
  Power Current Value     :450 W
  Power Max Value         :806 W
  Power Peak Value        :700 W
  Power Average Value     :475 W
  Software Version        :290
  Hardware Version        :000
  CPLD Version            :000
```

Table 159 Field descriptions of the **display poe pse** command

Field	Description
Power Current Value	Current power of the board
Power Max Value	Maximum power of the board
Power Peak Value	Peak power of the board
Power Average Value	Average power of the board
Software Version	Version of the PSE software
Hardware Version	Version of the PSE hardware
CPLD Version	Version of the PSE complex programmable logic device (CPLD)

poe enable

Syntax **poe enable**

undo poe enable

View Ethernet port view and PoE profile 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, the PoE feature on a port is enabled if the PoE feature is enabled on a module.

Example # Enable the PoE feature on Ethernet3/0/1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet3/0/1
[SW7750-Ethernet3/0/1] poe enable
```

poe enable slot

Syntax **poe enable slot** *slot-number*

undo poe enable slot *slot-number*

View System view

Parameter *slot-number*: Number of the slot where the module resides.

Description Use the **poe enable slot** command to enable the PoE feature on a module.

Use the **undo poe enable slot** command to disable the PoE feature on a module.

By default, the PoE feature is disabled on a module.

Note:

- Before enabling the PoE feature on a module, you must ensure that the remaining power output is not less than the maximum power required for the module. Otherwise, PoE cannot be enabled on the module correctly.
- After PoE is enabled on a PoE module, the rated power output shall be reserved for the slot even when the module is removed from the slot. You need to release this power output using the **undo poe enable slot** command.

- If you insert a module which does not support PoE into the slot for which a rated power output is reserved, the reserved power output shall be released.
- If you insert a PoE module of another type into the slot for which a rated power output is reserved, the switch still applies the former PoE configuration to the port.

Example # Enable the PoE feature on the PoE module in slot 3.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] poe enable slot 3
```

poe legacy enable slot

Syntax **poe legacy enable slot** *slot-number*

undo poe legacy enable slot *slot-number*

View System view

Parameter *slot-number*: Number of the slot where the module resides.

Description Use the **poe legacy enable slot** command to enable the module to perform PoE-compatibility detection for the remote PDs.

Use the **undo poe legacy slot** command to disable PoE-compatibility detection for the remote PDs.

By default, PoE-compatibility detection for PDs is disabled on the module.

Through the PoE-compatibility detection, the switch can detect the PDs incompatible with IEEE802.3af and supply power to them.

⚠ ***CAUTION:*** *PoE-compatibility detection process is very slow and has impact on the system performance, so you are recommended not to enable the PoE-compatibility detection on a module if all PDs connected are IEEE802.3af-compatible.*

Example # Enable PoE-compatibility detection on the PoE module in slot 2.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] poe enable slot 2
[SW7750] poe legacy enable slot 2
```

poe max-power

Syntax **poe max-power** *max-power*

undo poe max-power

View Ethernet port view and PoE profile view

Parameter *max-power*: Maximum power distributed to the port, ranging from 1,000 to 15,400 in mW.

Description Use the **poe max-power** command to configure the maximum power supplied by the current port.

Use the **undo poe max-power** command to restore the maximum power supplied by the current port to the default value.

By default, the maximum power that a port can supply is 15,400 mW.

Example # Set the maximum power supplied by Ethernet3/0/1 to 12,000 mW.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet 3/0/1
[SW7750-Ethernet3/0/1] poe max-power 12000
```

poe max-power slot

Syntax **poe max-power** *max-power* **slot** *slot-number*

undo poe max-power slot *slot-number*

View System view

Parameter *max-power*: Maximum power distributed to the module, ranging from 37 to 806 in W.

slot-num: Number of the slot where the module resides.

Description Use the **poe max-power** command to set the maximum power of a module.

Use the **undo poe max-power** command to restore the default maximum power of a module.

By default, the maximum power of a module is 37 W.

Example # Set the maximum power of the module in slot 3 to 400 W.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] poe max-power 400 slot 3
```

poe mode

Syntax **poe mode** { **signal** | **spare** }

undo poe mode

View Ethernet port view and PoE profile view

Parameter **signal**: Supplies power through a signal cable.

spare: Supplies power through a spare cable.

Description Use the **poe mode** command to configure the PoE mode on the current port.

Use the **undo poe mode** command to restore the PoE mode on the current port to the default mode.

By default, the port supplies power through a signal cable.

Note that the Switch 7750s do not support the **spare** mode currently.

Example # Set the PoE mode on Ethernet3/0/1 to **signal**.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet 3/0/1
[SW7750-Ethernet3/0/1] poe mode signal
```

poe power max-value

Syntax **poe power max-value** *max-value*

View System view

Parameter *max-value*: Maximum PoE power output on the switch, ranging from 37 to 2,400 in W.

Description Use the **poe power max-value** command to set the maximum power output on the switch.

By default, the maximum PoE power output on the switch is 2,400 W.

Note that this command works only when the power you specify is greater than the power that has been distributed to the modules.

Example # Set the maximum power output of the switch to 2,000 W.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] poe power max-value 2000
```

poe power-management

Syntax **poe power-management** { **auto** | **manual** } **slot** *slot-number*

View System view

Parameter **auto**: Manages PoE of the switch automatically.

manual: Manages PoE of the switch manually.

slot-number: Number of the slot where the module resides.

Description Use the **poe power-management** command to configure the PoE management mode of the switch.

By default, the PoE management mode of the switch is **auto**.

This command and the PoE priority settings of PoE ports will work together to control the power feeding of the switch when the switch is reaching its full power load in power supply.

- **auto** mode: When the switch is reaching its full load in supplying power, it will first supply power to the PDs that are connected to the ports with critical priority, and secondly supply power to the PDs that are connected to the ports with high priority. For example: Port A has the power priority of **critical**. When the switch is reaching full load and a new PD is now added to the port A, the switch will power down a PD that is connected to a port with the lowest priority and turn to feed this new PD.
- **manual** mode: When the switch is reaching its full load in supplying power externally and a new PD is added, it will neither take the priority into account nor make change to its original power supply status; only the information about the newly added device is provided. For example: Port A has the priority of **critical**. When the switch is reaching full load and a new PD is now connected to port A, the switch does not supply power to this new device.

Example # Configure the PoE management mode of the module in slot 3 of the switch to **auto**.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] poe power-management auto slot 3
```

poe priority

Syntax **poe priority** { **critical** | **high** | **low** }

undo poe priority

View Ethernet port view and PoE profile view

Parameter **critical**: Sets the PoE priority of the port to **critical**.

high: Sets the PoE priority of the port to **high**.

low: Sets the PoE priority of the port to **low**.

Description Use the **poe priority** command to configure the PoE priority of a port.

Use the **undo poe priority** command to restore the default PoE priority.

By default, the PoE priority of a port is **low**.

Note:

This command is used together with the **poe power-management** command, and takes effect when the PoE power output of the switch reaches nearly to its maximum value.

Example # Set the PoE priority of Ethernet3/0/1 to **critical**.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet 3/0/1
[SW7750-Ethernet3/0/1] poe priority critical
```

poe upgrade

Syntax **poe upgrade** { **refresh** | **full** } *filename* **slot** *slot-number*

View System view

Parameter **refresh**: Upgrades the existing valid software in the PSE in the **refresh** mode.

full: Reloads the software to the PSE when there is no valid software in the PSE. *filename*: Upgrade file name, with a length of 1 character to 63 characters.

slot-number: Slot number of a module.

Description Use the **poe upgrade** command to update the processing software in the PSE online.

- *The **full** mode is used only when you cannot use the **refresh** mode.*
- *When the PSE processing software is damaged (that is, all the PoE commands cannot be successfully executed), you can use the **full** mode to update and restore the software.*
- *When the upgrade procedure is interrupted for some unexpected reasons (such as failure which cause restart), if the update in the **full** mode fails after restart, you must update the software in the **full** mode after power-off and restart of the device, and then restart the device manually. In this way, the former PoE configuration is restored.*

Example # Update the processing software in the PSE online.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] poe upgrade refresh 0400_001.S19 slot 2
This will update poe  file on board 2. Continue? [Y/N] y
```

```
Board 2 upgrading poe, please wait...
Load finished!
Start Upgrading...
Frame 0 IO Board 2 upgrade POE Pse succeeded
```

64 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 the PoE power supply units (PSUs) contained in the external PoE power supply system.

Example # Display the AC input state of the PoE PSUs.

```
<SW7750> display poe-power ac-input state
PSU 1 AC Input State : Lack Phrase
PSU 2 AC Input State : Normal
PSU 3 AC Input State : Lack Phrase
```

Table 160 Field descriptions of the **display poe-power ac-input state** command

Field	Description
AC input state of PoE PSU 1	Normal: The AC input is normal. Lack Phrase: The PSU is idle. Under Limit: The AC input voltage is lower than the lower threshold. Upper Limit: The AC input voltage is higher than the upper threshold. Fuse Broken: The fuse is broken. 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 the detailed alarm information about the external PoE PSUs.

Example # Display the detailed alarm information about the external PoE PSUs.

```
<SW7750> display poe-power alarm
PSU alarm detail:

Number of PSUs    : 1
 PSU 1            : Absent         PSU is absent.
 PSU 2            : Normal         PSU is in normal state.
 PSU 3            : Absent         PSU is absent.
```

Table 161 Field descriptions of the **display poe-power alarm** command

Field	Description
The alarm information about PoE PSU1	PSU is in normal state: The PSU operates normally. NOTLINK: The PSU is not linked (the controller fails to communicate with this PSU or the PSU is not inserted). You can clear the failure by powering off the PSU or inserting a PSU. INERROR: PSU input error. Restoring the normal AC input can clear the error. OUTERROR: PSU output error (No normal DC output from the PSU). HIGHVOL: Overvoltage on the PSU (the PSU is shut down because its outputs overvoltage). HIGHTEP: It is overheated in the PSU. FANERROR: The fan fails. CLOSE: The PSU is shut down. CURLIMIT: The current of the PSU is limited. Absent: The PSU is absent.

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 DC output state of the PoE PSUs in-use.

Example # Display the DC output states of the in-use PoE PSUs.

<SW7750> display poe-power dc-output state

```
DC Output State : Normal
```

Table 162 Field descriptions of the **display poe-power dc-output state** command

Field	Description
DC output state of the external PoE PSU	Normal: The DC output is normal. Under Limit: The DC output voltage is lower than the lower threshold. Upper Limit: The DC output voltage is higher than the upper threshold. Fuse Broken: The fuse is broken. Switch Off: The switch is off. Hardware Fault: Hardware fails.

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 values of the external PoE PSUs.

Example # Display the DC output voltage/current values of the external PoE PSUs.

```
<SW7750> display poe-power dc-output value
DC Output Voltage : 53.997
DC Output Current : 0.350 A
```

Table 163 Field descriptions of the **display poe-power dc-output value** command

Field	Description
DC Out Voltage	DC output voltage
DC Output Current	DC output current

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 in the external PoE PSU.

Example # Display the number and current state of the AC power distribution switches.

```
<SW7750> display poe-power switch state
 Switch Number : 0
```

Currently, the Switch 7750 do not use any AC power distribution switch, so the returned value is always 0.

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 basic information about the external PoE PSUs, including the name, the model, the specifications and output power.

Example # Display the information about the PoE PSUs.

```
<SW7750> display supervision-module information
 Supervision Module Version  : 2.6
 Supervision Module Name     : Spring Pms
 Power Type                  : PSE2500-A
 Power Rating Value          : 2400 W
 Power Peak Value            : 1506 W
 Power Average Value         : 1482 W
 Power Current Value         : 1502 W
 PSU Number                  : 1
 PSU 2
      Rating Output Power    : 2500 W (220V)/1250 W(110V)
      Hard Version Info      : NP Series
```

Table 164 Field descriptions 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	Model of the external PoE PSU
Power Rating Value	Rated power of the external PoE PSU
Power Peak Value	Peak power of the external PoE PSU
Power Average Value	Average Power of the external PoE PSU
Power Current Value	Current power of the external PoE PSU
PSU number	Number of PoE PSUs
Rating Output Power	Rated output power of the PoE PSU: 2,500 W for 220 VAC input, 1,250 W for 110 VAC input
Hard Version Info	Hardware version information of the external PoE PSUs

65 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 (in V) in the format of X.X.

- For 220 VAC input, it ranges from 176.0V to 264.0V
- For 110 VAC input, it ranges from 90.0V to 132.0V

Description Use the **poe-power input-thresh lower** command to set the undervoltage alarm threshold of AC input for the external PoE PSUs.

For 220 VAC input, the recommended value is 181.0 V; for 110VAC input, the recommended value is 90.0 V.

Example # Set the undervoltage alarm threshold of AC input for the external PoE PSUs to 181.0 V.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] 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 (in V) in the format of X.X.

- For 220 VAC input, it ranges from 176.0V to 264.0V.
- For 110 VAC input, it ranges from 90.0V to 132.0V.

Description Use the **poe-power input-thresh upper** command to set the overvoltage alarm threshold of AC input for the external PoE PSUs.

For 220 VAC input, the recommended value is 264.0 V; For 110VAC input, the recommended value is 132.0 V.

Example

Set the overvoltage alarm threshold of AC input for the external PoE PSUs to 264.0 V.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] poe-power input-thresh 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 (in volts V) in the format of X.X, in the range of 45.0 to 47.0.

Description

Use the **poe-power output-thresh lower** command to set the undervoltage alarm threshold of DC output for the external PoE PSUs.

For either 220 VAC or 110 VAC input, the recommended threshold is 47.0 V.

Example

Set the undervoltage alarm threshold of DC output for the external PoE PSUs to 47.0 V.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] poe-power output-thresh lower 47.0
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 (in volts V) in the format of X.X, in the range of 55.0 to 57.0.

Description

Use the **poe-power output-thresh upper** command to set the overvoltage alarm threshold of DC output for the external PoE PSUs.

For either 220 VAC or 110 VAC input, the recommended threshold is 55.0 V.

Example

Set the overvoltage alarm threshold of DC output for the external PoE PSUs to 55.0 V.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] poe-power output-thresh upper 55.0
Set upper output-threshold power successfully!
```

66 POE PROFILE CONFIGURATION COMMANDS

PoE profile is a set of PoE configurations in Ethernet port view. You can specify PoE configurations to be applied in Ethernet port view in PoE profiles.

apply poe-profile

Syntax In system view, use the following commands:

apply poe-profile *profilename* **interface** *interface-type interface-number* [**to** *interface-type interface-number*]

undo apply poe-profile *profilename* **interface** *interface-type interface-number* [**to** *interface-type interface-number*]

In Ethernet port view, use the following commands:

apply poe-profile *profilename*

undo apply poe-profile *profilename*

View System view and Ethernet port view

Parameter *profilename*: Name of a PoE profile, a string of 1 to 15 characters. It starts with a letter from a to z or from A to Z, and it cannot be any of reserved keywords like **all**, **interface**, **user**, **undo**, and **mode**.

interface-type interface-number: *interface-type* indicates a port type and *interface-number* indicates a port number.

Description Use the **apply poe-profile** command to apply the existing PoE profile configuration to the specified Ethernet port.

Use the **undo apply poe-profile** command to cancel the PoE profile configuration for the specified Ethernet port.

Only one PoE profile can be in use at any time for each Ethernet port.

The following rules should be obeyed

- *A PoE profile is a group of PoE configurations. Multiple PoE features can be set in a PoE profile. When the* ***apply poe-profile*** *command applies a PoE profile to a port, some PoE features can be applied successfully while some PoE configurations in it cannot.*

- *When the **apply poe-profile** command is used to apply a PoE profile to a port, the PoE profile is applied successfully if one PoE feature in the PoE profile is applied properly.*
- *If one or more features in the PoE profile are not applied properly on a port, the switch prompts explicitly which PoE features in the PoE profile are not applied properly on which ports.*
- *The **display current-configuration** command can be used to query which PoE profiles are applied to a port. However, the command cannot be used to query which PoE features in a PoE profiles are applied successfully.*

Example # Apply the existing PoE profile (profile-test) configuration to Ethernet2/0/1 through Ethernet2/0/9 ports of the switch.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] apply poe-profile profile-test interface Ethernet 2/0/1 to
Ethernet 2/0/9
```

display poe-profile

Syntax **display poe-profile** { **all-profile** | **interface** *interface-type interface-number* | **name** *profilename* }

View Any view

Parameter **all-profile**: Displays all PoE profiles.

interface-type interface-number: *interface-type* indicates a port type and *interface-number* indicates a port number.

profilename: Name of a specified PoE profile.

Description Use the **display poe-profile** command to display detailed configuration information of the created PoE profile for a switch.

Example # Display detailed configuration information for the PoE profile by the name of profile-test.

```
<SW7750> display poe-profile name profile-test
```

poe-profile

Syntax **poe-profile** *profilename*

undo poe-profile *profilename*

View System view

Parameter

profilename: Name of PoE profile, a string with 1 to 15 characters. It starts with a letter from a to z or from A to Z, and it cannot be any of reserved keywords like **all**, **interface**, **user**, **undo**, and **mode**.

Description

Use the **poe-profile** command to create a PoE profile.

Use the **undo poe-profile** command to delete an existing PoE profile.

The following PoE features can be configured in the PoE profile mode:

poe enable

poe mode { **signal** | **spare** }

poe priority { **critical** | **high** | **low** }

poe max-power *max-power*

The maximum number of PoE profiles that can be configured for an S3900 switch is 100.

Example

Create a PoE profile by the name of profile-test.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] poe-profile profile-test
```

67 UDP-HELPER CONFIGURATION COMMANDS

display udp-helper server

Syntax **display udp-helper server** [**interface vlan-interface** *vlan-id*]

View Any view

Parameter *vlan-id*: ID of a VLAN.

Description Use the **display udp-helper server** command to display the information about the configured destination servers connected to a specified VLAN interface and the number of the packets forwarded to each destination server. If you do not specified the *vlan-id* argument, the corresponding information about all the VLAN interfaces is displayed.

Example # Display the information about the configured destination servers connected to VLAN 1 interface and the number of the packets forwarded to the destination servers.

```
<SW7750> 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 server with its IP address being 192.1.1.2 is configured as a destination server and is connected to VLAN 1 interface, and no packets are forwarded to it so far.

reset udp-helper packet

Syntax **reset udp-helper packet**

View User view

Parameter None

Description Use the **reset udp-helper packet** command to clear the statistics about the packets forwarded by UDP-Helper.

Example # Clear the statistics about the packets forwarded by UDP-Helper.

```
<SW7750> reset udp-helper packet
```

udp-helper enable

Syntax **udp-helper enable**

undo udp-helper enable

View System view

Parameter None

Description Use the **udp-helper enable** command to enable the UDP-Helper function.

Use the **undo udp-helper enable** command to disable the UDP-Helper function.

By default, UDP-Helper is disabled.

Example # Enable UDP-Helper.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] 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 a UDP port to be configured as a UDP-Helper destination port, in the range 1 to 65535 (except for 67 and 68).

dns: Specifies the DNS UDP port (port 53) as a UDP-Helper destination port.

netbios-ds: Specifies the NetBIOS-DS UDP port (port 138) as a UDP-Helper destination port.

netbios-ns: Specifies the NetBIOS-NS UDP port (port 137) as a UDP-Helper destination port.

tacacs: Specifies the TACACS UDP port (port 49) as a UDP-Helper destination port.

tftp: Specifies the TFTP UDP port (port 69) as a UDP-Helper destination port.

time: Specifies the time service UDP port (port 37) as a UDP-Helper destination port.

Description

Use the **udp-helper port** command to specify a UDP-Helper destination port.

Use the **undo udp-helper port** command to disable a port from being a UDP-Helper destination port.

With UDP-Helper enabled, UDP broadcast packets with their destination port being the six default UDP ports (that is, port 69, 53, 37, 137, 138, and 49) are forwarded to the configured destination servers by default. After the UDP-Helper function is disabled, all the configured UDP-Helper destination ports are cancelled, including the default UDP ports.

Note that:

- *Before configuring udp-helper port, you must enable UDP-Helper.*
- *When you view the configuration information by using the* ***display current-configuration*** *command, information about default UDP ports is not displayed. Such information is displayed only when a default port is disabled.*

Example

Configure the DNS UDP port as a UDP-Helper destination port.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] 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 device to be configured as a destination server, in dotted decimal notation.

Description

Use the **udp-helper server** command to specify a destination server for the UDP broadcast packets to be forwarded.

Use the **undo udp-helper server** command to remove a configured destination server.

No destination server is configured by default.

Currently, you can configure up to 20 destination servers on a VLAN interface.

Note that if you do not provide the *ip-address* argument when executing the **undo udp-helper server** command, all the destination servers configured on the VLAN interface are removed.

Related command:

display udp-helper server.

Example # Configure the device with its IP address being 192.1.1.2 as a destination server for the UDP broadcast packets to be forwarded on VLAN 1 interface.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 1
[SW7750-Vlan-interface1] udp-helper server 192.1.1.2
```

68 SNMP CONFIGURATION COMMANDS

display snmp-agent

Syntax

display snmp-agent { **local-switch fabricid** | **remote-switch fabricid** }

View

Any view

Parameter

local-switch fabricid: Displays a local switch fabric ID.

remote-switch fabricid: Displays a remote switch fabric ID.

Description

Use the **display snmp-agent** command to view the switch fabric ID of the current device.

An SNMP switch fabric ID identifies an SNMP entity uniquely within an SNMP domain. As an indispensable part of an SNMP entity, an SNMP switch fabric performs the function of sending, receiving and authenticating SNMP message, extracting PDU, packet encapsulation and the communication with SNMP application.

Example

Display the local switch fabric ID of the current device.

```
<SW7750> display snmp-agent local-switch fabricid
SNMP local EngineID: 00000009020000000C025808
```

SNMP local EngineID in the above information represents the ID of the local SNMP switch fabric.

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 information about the currently configured community names for SNMPv1 or SNMPv2c.

Example # Display the currently configured community names.

```
<SW7750> display snmp-agent community
   Community name:public
       Group name:public
       Storage-type: nonVolatile

   Community name:private
       Group name:private
       Storage-type: nonVolatile
```

Table 165 Field descriptions of the **display snmp-agent community** command

Field	Description
Community name	Community name
Group name	Group name
Storage-type	Storage type, including volatile, nonVolatile, permanent, readOnly, and other.

display snmp-agent group

Syntax **display snmp-agent group** [*group-name*]

View Any view

Parameter *groupname*: The group name, ranging from 1 to 32 bytes.

Description Use the **display snmp-agent group** command to view group name, security model, state of various views and storage models.

Example # Display SNMP group name and security model.

```
<SW7750> display snmp-agent group
   Group name: hello
       Security model: v2c noAuthnoPriv
       Readview: ViewDefault
       Writeview: <no specified>
       Notifyview :<no specified>
       Storage-type: nonvolatile
```

The following table describes the output fields.

Table 166 Field descriptions of the **display snmp-agent group** command

Field	Description
Group name	SNMP group name
Security model	Security model of that group, including authorization and encryption (AuthPriv), authorization and no encryption (AuthnoPriv), no authorization and no encryption (noAuthnoPriv).
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

Table 166 Field descriptions of the **display snmp-agent group** command

Field	Description
Storage-type	Storage type, including volatile, nonVolatile, permanent, readOnly and other.

display snmp-agent mib-view

Syntax **display snmp-agent mib-view [exclude | include | viewname** *view-name*]

View Any view

Parameter **exclude**: Displays the SNMP MIB view (excluded).

Include: Displays the SNMP MIB view (included).

Viewname: Displays the SNMP MIB according to the view name.

view-name: SNMP MIB view to be displayed. It is a character string, ranging from 1 to 32 characters.

Description Use the **display snmp-agent mib-view** command to view the MIB view configuration information of the current Ethernet switch.

Example # Display the information about the currently configured MIB view.

```
<SW7750> display snmp-agent mib-view
   View name:system
       MIB Subtree:system
       Subtree mask:
       Storage-type: nonVolatile
       View Type:included
       View status:active
View name:ViewDefault
       MIB Subtree:iso
       Subtree mask:
       Storage-type: nonVolatile
       View Type:included
       View status:active
View name:ViewDefault
       MIB Subtree:snmpUsmMIB
       Subtree mask:
       Storage-type: nonVolatile
       View Type:excluded
       View status:active
View name:ViewDefault
       MIB Subtree:snmpVacmMIB
       Subtree mask:
       Storage-type: nonVolatile
       View Type:excluded
       View status:active
View name:ViewDefault
       MIB Subtree:snmpModules.18
       Subtree mask:
```

```
Storage-type: nonVolatile
View Type:excluded
View status:active
```

Table 167 Field descriptions 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	Includes or excludes access to an MIB object
View status: active/inactive	Indicates the MIB view status: active or inactive

⚠ ***CAUTION:*** *For the above commands, when the SNMP agent is disabled, the system gives the prompt "SNMP agent disabled".*

display snmp-agent statistics

Syntax **display snmp-agent statistics**

View Any view

Parameter None

Description Use the **display snmp-agent statistics** command to view the statistics information about SNMP packets.

This command provides statistics for SNMP operations.

Example # Display the statistics information about SNMP packets.

```
<SW7750> display snmp-agent statistics
  9232 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
  9266 Messages passed from the SNMP entity
  0 SNMP PDUs which had badValue error-status
  0 SNMP PDUs which had genErr error-status
  11 SNMP PDUs which had noSuchName error-status
  0 SNMP PDUs which had tooBig error-status (Maximum packet size 2000)
  33029 MIB objects retrieved successfully
  26 MIB objects altered successfully
  714 GetRequest-PDU accepted and processed
  8514 GetNextRequest-PDU accepted and processed
  10 GetBulkRequest-PDU accepted and processed
  9230 GetResponse-PDU accepted and processed
  1 SetRequest-PDU accepted and processed
  34 Trap PDUs accepted and processed
```

display snmp-agent sys-info

Syntax **display snmp-agent sys-info** [**contact** | **location** | **version**]*

View Any view

Parameter **contact**: Displays the contact information of the current device.

location: Displays the physical location of the current device.

version: Displays the version information about the SNMP running in the system.

Description Use the **display snmp-agent sys-info** command to view the system contact (sysContact) string, system location string, and the current SNMP version.

This command displays all information if you choose no parameter.

Example # Display the sysContact string.

```
<SW7750> display snmp-agent sys-info contact
   The contact person for this managed node:
           3Com Corporation
```

The above information indicates that the contact of this device is 3Com Corporation.

# Display the system location string.

```
<SW7750> display snmp-agent sys-info location
   The physical location of this node:
           Marlborough, MA
```

The above information indicates that the device location is Marlborough, MA.

# Display the current SNMP version.

```
<SW7750> display snmp-agent sys-info version
   SNMP version running in the system:
           SNMPv3
```

The above information indicates that the current SNMP version is SNMPv3.

display snmp-agent usm-user

Syntax **display snmp-agent usm-user** [**switch fabricid** *switch fabricid* | **username** *user-name* | **group** *group-name*]*

View Any view

Parameter *switch fabricid*: Displays the SNMPv3 user information of the specified switch fabric ID, which ranges from 10 to 64 hexadecimal numerals.

username: Displays information about the specified SNMPv3 user, which ranges from 1 to 32 bytes.

groupname: Displays information about users in the specified group name, which ranges from 1 to 32 bytes.

Description Use the **display snmp-agent usm-user** command to view SNMP user information.

If you do not specify a parameter, all the information will be displayed.

Example # Display all user information.

```
<SW7750> display snmp-agent usm-user switch fabricid 1234567890
User name: userv3aaaa
Group name: managev3group
Engine ID: 1234567890
Storage-type: nonVolatile
UserStatus: active
```

Table 168 describes the output fields.

Table 168 Field descriptions of the **display snmp-agent usm-user** command

Field	Description
User name	SNMP user name
Group name	The group name which the SNMP user name belongs to
Engine ID	The character string identifying the SNMP device
Storage-type	Storage type of SNMP information, including volatile, nonVolatile, permanent, readOnly and other.
UserStatus	SNMP user status

enable snmp trap updown

Syntax **enable snmp trap updown**

undo enable snmp trap updown

View Ethernet port view/interface view

Parameter None

Description Use the **enable snmp trap updown** command to enable the sending of port/interface linkUp and linkDown traps.

Use the **undo enable snmp trap updown** command to disable the sending of linkUp and linkDown traps.

By default, the sending of port/interface linkUp and linkDown traps is enabled.

The **enable snmp trap updown** and **snmp-agent trap enable**, **snmp-agent target-host** commands are used at the same time. You can use the **snmp-agent target-host** command to specify the hosts that can receive Trap information. To send Trap information, you must configure at least one **snmp-agent target-host** command.

Example # Enable the port Ethernet 2/0/1 to send linkUp and linkDown SNMP traps, using the community name "public" to the NMS whose IP address is 10.1.1.1.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] snmp-agent trap enable
[SW7750] snmp-agent target-host trap address udp-domain 10.1.1.1 par
ams securityname public
[SW7750] interface ethernet2/0/1
[SW7750-Ethernet2/0/1] enable snmp trap updown
```

snmp-agent

Syntax **snmp-agent**

undo snmp-agent

View System view

Parameter None

Description Use the **snmp-agent** command to enable SNMP Agent.

Use the **undo snmp-agent** command to disable SNMP Agent.

By default, SNMP Agent is disabled.

Example # Disable running SNMP Agent.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] undo snmp-agent
```

snmp-agent community

Syntax **snmp-agent community** { **read** | **write** } *community-name* [[**acl** *acl-number* | **mib-view** *view-name*]*

undo snmp-agent community *community-name*

View System view

Parameter **read**: Indicates that MIB object can only be read. Only the read-only community can query device information.

write: Indicates that MIB object can be read and written. The read-write community can configure the device.

community-name: The community name, a character string of 1 to 32 characters.

view-name: The MIB view name, a character string of 1 to 32 characters.

acl-number: The basic access control list (ACL) number specified by the community, ranging from 2,000 to 2,999.

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 permit read-only access by this community name.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] snmp-agent community read comaccess
```

# Configure community name as mgr and permit read-write access.

```
[SW7750] snmp-agent community write mgr
```

# Remove community name comaccess.

```
[SW7750] undo snmp-agent community comaccess
```

snmp-agent group

Syntax

Versions V1 and V2C:

snmp-agent group { **v1** | **v2c** } *group-name* [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*] [**acl** *acl-number*]

undo snmp-agent group { **v1** | **v2c** } *group-name*

Version V3:

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: Specifies SNMPv1.

v2c: Specifies SNMPv2c.

v3: Specifies SNMPv3.

groupname: 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: Sets read-only view.

read-view: Read-only view name, ranging from 1 to 32 bytes

write-view: Sets read-write view

write-view: Name of read-write view, ranging from 1 to 32 bytes.

notify-view: Sets notify view.

notify-view: Notification view name, ranging from 1 to 32 bytes.

acl: Sets an ACL.

acl-number: Indicates an ACL, ranging from 2,000 to 2,099.

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 with the **snmp-agent group v3** command is not authenticated and encrypted.

Related command: **snmp-agent mib-view**, **snmp-agent usm-user**.

Example # Create SNMPv3 group hello.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] snmp-agent group v3 hello
```

snmp-agent local-switch fabricid

Syntax **snmp-agent local-switch fabricid** *switch fabricid*

undo snmp-agent local-switch fabricid

View System view

Parameter *switch fabricid*: Specifies the switch fabric ID with a character string, only composed of 10 to 64 hexadecimal numbers. Two hexadecimal characters form an octet.

Description Use the **snmp-agent local-switch fabricid** command to set the switch fabric ID of the local SNMP entity.

Use the **undo snmp-agent local-switch fabricid** command to restore the default setting.

By default, the device switch fabric ID is "Enterprise number + device information". Device information is determined according to different products. It can be an IP address, MAC address or user-defined hexadecimal numeral string.

Related command: **snmp-agent usm-user**.

Example # Configure the local device name as 1234512345.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] snmp-agent local-switch fabricid 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 the MIB subtree.

Excluded: Excludes the MIB subtree.

view-name: View name. It is a character string, ranging from 1 to 32 characters.

oid-tree: The OID MIB subtree of the MIB object subtree. It is a character string, ranging from 1 to 255 characters. It can be a character string of the variable OID (such as 1.4.5.3.1), or a variable name (such as system). The character string can include wildcards (such as 1.4.5.*.*.1).

Description Use **snmp-agent mib-view** command to create or update the view information, limiting the MIB objects to be accessed by the NMS.

Use the **undo snmp-agent mib-view** command to cancel the current setting.

By default, the view name is ViewDefault and OID is 1.

Related command: **snmp-agent group**.

Example # Create an SNMP MIB view that consists of all the objects of MIB-II.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] 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*: Maximum size of the SNMP packet (in bytes) that the Agent can send/receive, ranging from 484 to 17,940.

Description Use the **snmp-agent packet max-size** command to set the maximum size of SNMP packet that the Agent can send/receive.

Use **undo snmp-agent packet max-size** command to restore the default size of SNMP packet.

The sizes of the SNMP packets that the Agent can send/receive are different because network environments are different.

Example # Set the maximum size of the SNMP packet that the Agent can send/receive to 1,042 bytes.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] snmp-agent packet max-size 1042
```

snmp-agent sys-info

Syntax **snmp-agent sys-info** { **contact** *sys-contact* | **location** *sys-location* | **version** { { **v1** | **v2c** | **v3** }* | **all** } }

undo snmp-agent sys-info { { **contact** | **location** }* | **version** { { **v1** | **v2c** | **v3** }* | **all** } }

View System view

Parameter **contact**: Sets the contact for system maintenance.

sysContact: The character string describing contact information for system maintenance.

location: Sets the geographical location of the device.

sys-location: The geographical location of the device.

version: Specifies version of running SNMP.

v1: SNMP V1.

v2c: SNMP V2C.

v3: SNMP V3.

all: All SNMP versions, including 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, information for system maintenance and version information of running SNMP.

Use the **undo snmp-agent sys-info location** command to remove the current configuration.

If the device fails, the device maintenance person can use contact information to contact the manufacturer.

By default, the contact information is " 3Com Corporation", the system location is " Marlborough, MA", the SNMP version is SNMP V3.

Related command: **display snmp-agent sys-info**.

Example # Set contact information for system maintenance as Dial System Operator # 1234.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] snmp-agent sys-info contact Dial System Operator # 1234
```

snmp-agent target-host

Syntax **snmp-agent target-host trap address udp-domain** { *ip-address* } [**udp-port** *port-number*] **params securityname** *security-string* [**v1** | **v2c** | **v3** [**authentication** | **privacy**]]

undo snmp-agent target-host *ip-address* **securityname** *security-string*

View System view

Parameter **trap**: Specifies the host to be a Trap host.

address: Specifies the address of the destination host for transmitting SNMP messages.

udp-domain: Specifies transport domain over UDP for the target host.

ip-address: The IPv4 address of the host receiving Trap packets.

port-number: Number of the port receiving Trap packets, ranging from 0 to 65,535 characters.

params: Specifies SNMP target host information to be used in the generation of SNMP messages.

security-string: The community name of SNMP V1 and SNMP V2C, or SNMP V3 user name, ranging from 1 to 32 characters.

v1: Represents SNMPv1.

v2c: Represents SNMPv2C.

v3: RepresentsSNMPv3.

authentication: Configures to authenticate the packet without encryption.

privacy: Configures to authenticate and encrypt the packet.

Description Use **snmp-agent target-host** command to configure destination of SNMP Trap packets.

Use **undo snmp-agent target-host** command to cancel the current setting.

The **snmp-agent target-host** command and the **snmp-agent trap enable** or **enable snmp trap updown** command must be used at the same time on the device to send Trap packets.

1. Use the **snmp-agent trap enable** or **enable snmp trap updown** command to set Trap packets allowed to send (all Trap packets can be sent by default).
2. Use the **snmp-agent target-host** command to set the address of the destination host receiving SNMP Trap packets.

Related command: **snmp-agent trap enable**, **snmp-agent trap source** and **snmp-agent trap life**.

Example # Enable sending SNMP Trap packets to 10.1.1.1 with community name public.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] snmp-agent trap enable standard
[SW7750] 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*] | **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*] | **standard** [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**]* | **system | vrrp** [**authfailure** | **newmaster**]]

View System view

Parameter **bgp** [**backwardtransition** | **established**]*: Configures to send BGP traps.

configuration: Configures to send traps for configuration.

flash: Configures to send traps of Flash.

ospf [*process-id*] [*ospf-trap-list*]: Configures to send traps of the OSPF protocol. *process-id* indicates a process ID. *ospf-trap-list* indicates a list of trap messages allowed to be sent.

standard [**authentication**] [**coldstart**] [**linkdown**] [**linkup**] [**warmstart**]: Configures to send SNMP standard notification or traps.

authentication: Configures to send the authentication trap information of the SNMP protocol when authentication fails.

coldstart: Configures to send the coldstart trap information when the switch restarts.

linkdown: Configures to send SNMP linkDown Trap information when the port is down.

linkup: Configures to send SNMP linkUp Trap information when the port is up.

warmstart: Configures to send SNMP warm start Trap information when SNMP is rebooted.

System: Configures to send the trap information of 3Com-SYS-MAN-MIB (a private MIB).

vrrp [**authfailure** | **newmaster**]: Configures to send VRRP trap information.

Description

Use the **snmp-agent trap enable** command to enable the device to send Trap packets.

Use the **undo snmp-agent trap enable** command to disable the device to send Trap packets.

By default, the device does not send Trap packets.

The **snmp-agent trap enable** and **snmp-agent target-host** commands must be used at the same time. The **snmp-agent target-host** command specifies which hosts can receive Trap message. However, to send Trap message, you must configure **snmp-agent target-host** command.

Example

Enable to send the Trap packet of SNMP authentication failure to 10.1.1.1. The community name is public.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] snmp-agent trap enable standard authentication
[SW7750] snmp-agent target-host trap address udp-domain 10.1.1.1 par
ams securityname public
```

snmp-agent trap ifmib

Syntax **snmp-agent trap ifmib link extended**

undo snmp-agent trap ifmib link extended

View System view

Parameter None

Description Use the **snmp-agent trap ifmib** command to extend the bound variables in the linkup/linkdown trap packet, that is, to add two objects "ifDescr" (interface description) and "ifType" (interface type).

Use the **undo snmp-agent trap ifmib** command to restore the bound variables in a linkup/linkdown trap packet to the standard format defined in IF-MIB.

By default, the bound variables in a linkup/linkdown message are as the standard format defined in IF-MIB.

Example # Extend the format of linkup/linkdown trap packet, that is, add the "ifDescr" (interface description) and "ifType" (interface type) fields to the trap packet.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750]snmp-agent trap ifmib link extended
```

# Restore the linkup/linkdown trap packet format to the standard format defined in IF-MIB.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750]undo snmp-agent trap ifmib link extended
```

snmp-agent trap life

Syntax **snmp-agent trap life** *seconds*

undo snmp-agent trap life

View System view

Parameter *seconds*: Aging time, in seconds, ranging from 1 to 2,592,000.

Description Use the **snmp-agent trap life** command to set aging time for Trap packets. The Trap packets exceeding the aging time are discarded.

Use the **undo snmp-agent trap life** command to restore the default aging time for Trap packets.

By default, the aging time of SNMP Trap packets is 120 seconds.

After the specified aging time has elapsed, the system drops the trap packet.

Related command: **snmp-agent trap enable**, **snmp-agent target-host**.

Example # Set the aging time for Trap packets as 60 seconds.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] snmp-agent trap life 60
```

snmp-agent trap queue-size

Syntax **snmp-agent trap queue-size** *size*

undo snmp-agent trap queue-size

View System view

Parameter *size*: Length of a queue, ranging from 1 to 1,000.

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** and **snmp-agent trap life**.

By default, the length is 100.

Example # Configure the queue length to 200.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] snmp-agent trap queue-size 200
```

snmp-agent trap source

Syntax **snmp-agent trap source** { *interface-type interface-number* }

undo snmp-agent trap source

View System view

Parameter *interface-type*: Interface type.

interface-number: Interface number.

Description Use the **snmp-agent trap source** command to configure the source address for sending Trap message.

Use the **undo snmp-agent trap source** command to cancel the source address for sending Trap message.

The SNMP Trap message sent from a server has a source IP address no matter which interface the Trap message is sent from.

By default, SNMP chooses an outgoing interface.

You can configure this command to trace a specific event using the source address of a Trap packet.

Before setting the IP address of an interface address as the source address of the sent Trap packet, you must configure an IP address for the interface.

Related command: **snmp-agent trap enable**, **snmp-agent target-host**.

Example # Configure the IP address of the VLAN interface 1 as the source address for transmitting the Trap packets.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] snmp-agent trap source Vlan-interface 1
```

snmp-agent usm-user

Syntax

1 Versions V1 and V2C

snmp-agent usm-user { **v1** | **v2c** } *user-name group-name* [**acl** *acl-number*]

undo snmp-agent usm-user { **v1** | **v2c** } *user-name group-name*

1 Version V3

snmp-agent usm-user v3 *user-name group-name* [**authentication-mode** { **md5** | **sha** } *auth-password* [**privacy-mode des56** *priv-password*]] [**acl** *acl-number*]

undo snmp-agent usm-user v3 *user-name group-name* { **local** | **switch fabricid** *switch fabricid-string* }

View System view

Parameter **v1**: Configures to use V1 security model.

v2c: Configures to use V2c security model.

v3: Configures to use V3 security model.

User-name: User name, ranging from 1 to 32 bytes.

Group-name: Group name corresponding to that user, a character string of 1 to 32 characters.

authentication-mode: Specifies the safety level as authentication required. Absence of this parameter indicates that neither authentication nor encryption is required.

md5: Specifies the authentication protocol as HMAC MD5 algorithm.

sha: Specifies the authentication protocol as HMAC SHA algorithm.

auth-password: Authentication password, a character string of 1 to 64 characters.

privacy: Specifies the security level as encrypted.

des56: Specifies the authentication protocol as DES.

Priv-password: Encryption password, a character string of 1 to 64 characters.

acl-number: The basic ACL number, ranging from 2,000 to 2,999.

local: Represents a local entity user.

switch fabricid-string: Engine ID related to the user, ranging from 10 to 64 hexadecimal numerals.

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 the SNMP group.

While using SNMPv3, SNMP switch fabricID (for authentication) is required when you configure a remote user for an agent. If you change switch fabricID after configuring a user, the user corresponding to the original switch fabricID is not effective.

For V1 and V2C, this command will add a new community name. For SNMPv3, it will add a new user for an SNMP group.

Related command: **snmp-agent group**, **snmp-agent community** and **snmp-agent local-switch fabricid**.

Example

Add a user John to SNMPv3 group Johngroup. Configure to authenticate using HMAC-MD5 algorithm, require authentication and set authentication password as hello.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] snmp-agent group v3 Johngroup
[SW7750] snmp-agent usm-user v3 John Johngroup authentication-mode m
d5 hello
```

69 RMON CONFIGURATION COMMANDS

display rmon alarm

Syntax **display rmon alarm** [*entry-number*]

View Any view

Parameter *entry-number*: Alarm entry index, in the range of 1 to 65535. If you do not specify this argument, the configuration of all alarm entries is displayed.

Description Use the **display rmon alarm** command to display the configuration of a specified alarm entry or all the alarm entries.

Related command: **rmon alarm**.

Example # Display the configuration of all the alarm entries.

```
<SW7750> display rmon alarm
Alarm table 1 owned by abc is VALID.
Samples type          : delta
Variable formula      : 1.3.6.1.2.1.2.2.1.11.67111554<ifInUcastPkts.
67111554>
Sampling interval     : 10(sec)
Rising threshold      : 100(linked with event 7)
Falling threshold     : 10(linked with event 8)
  When startup enables  : risingOrFallingAlarm
  Latest value          : 0
```

Table 169 Field descriptions of the **display rmon alarm** command

Field	Description
Alarm table	Alarm entry
abc	Entry creator
VALID	Valid for alarm entries corresponding to the index
Samples type	Sample type: change value or absolute value
Variable formula	Variable formula of the sampled node
Sampling interval	Sampling interval
Rising threshold is 100	Rising threshold is 100
Falling threshold is 10	Falling threshold is 10

Table 169 Field descriptions of the **display rmon alarm** command

Field	Description
When startup enables	Alarm startup type: risingOrFallingAlarm (an alarm is triggered when the rising or falling threshold is reached) risingAlarm (an alarm is triggered when the rising threshold is reached) FallingAlarm (an alarm is triggered when the falling threshold is reached)
Latest value	Latest sampled value

display rmon event

Syntax **display rmon event** [*event-entry*]

View Any view

Parameter *event-entry*: Event entry index, in the range of 1 to 65535. If you do not specify this argument, the configuration of all the event entries is displayed.

Description Use the **display rmon event** command to display the configuration of a specified event entry or all the event entries.

The displayed information includes: event entry index, event entry owner, event description, the action triggered by the event (log or alarm messages), and the time (in seconds) when the latest event is triggered (in terms of the time elapsed since the system is started/initialized).

Related command: **rmon event**.

Example # Display the configuration of all the event entries.

```
<SW7750> display rmon event
Event table 1 owned by abc is VALID.
  Description: null.
  Will cause log-trap when triggered, last triggered at 0days 00h:02
m:27s.
```

Table 170 Field descriptions of the **display rmon event** command

Field	Description
Event table	Event entries
abc	Entry creator
VALID	The entry corresponding to the index is valid
Description	Event description
Will cause log-trap when triggered	The event triggers logs and an trap alarm
last triggered at 0days 00h:02m:27s	Time the latest event is triggered

display rmon eventlog

Syntax **display rmon eventlog** [*event-entry*]

View Any view

Parameter *event-entry*: Event entry index, in the range of 1 to 65535. If you do not specify this argument, the log of all the event entries is displayed.

Description Use the **display rmon eventlog** command to display the log of a specified event entry or all the event entries.

The displayed information includes: the indexes and status of the event entries in the event table, the time (in seconds) when an event log is generated (in terms of the time elapsed since the system is started or initialized), and the event description.

Example # Display the log generated by the event entry numbered 1.

```
<SW7750> display rmon eventlog 1
Event table 1 owned by abc 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 171 Field descriptions of the **display rmon eventlog** command

Field	Description
Event table	Event entries
abc	Entry creator
VALID	The status of the line corresponding to the line is valid
Generates eventLog 1.1 at 0days 00h:01m:39s	Time when the event is triggered. The event may be triggered several times. 1.1 indicates the time event 1 is first triggered
Description	Description of an event log

display rmon history

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

View Any view

Parameter *interface-type*: Interface type.

interface-number: Interface number.

Description Use the **display rmon history** command to display the RMON history information about a specified port. The information about the latest sample, including utilization, the number of errors, the total number of packets and so on, is also displayed.

Related command: **rmon history**.

Example # Display the RMON history information about the RMON port Ethernet2/0/1.

```
<SW7750> display rmon history ethernet 2/0/1
History control entry 1 owned by abc is VALID
  Samples interface     : Ethernet2/0/1<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 172 Field descriptions of the **display rmon eventlog** command

Field	Description
History control entry 1	Index number in the history control table
abc	Entry creator
VALID	The entry corresponding to the index is valid
Samples interface	Sampled interface
Sampling interval	Sampling interval
buckets	Number of records in the history control table
Latest sampled values	Latest sampled information
Dropevents	Event about dropping packets
octets	Number of received or transmitted bytes during sampling duration
packet	Number of received or transmitted packets during sampling duration
broadcastpackets	Number of broadcast packets
multicastpackets	Number of multicast packets
CRC alignment errors	Number of checkerror packets
undersize packets	Number of undersize packets
oversize packets	Number of oversize packets
fragments	Number of undersize and checkerror packets
jabbers	Number of oversize and checkerror packets
collisions	Number of collision packets
utilization	Utilization ratio

display rmon prialarm

Syntax **display rmon prialarm** [*prialarm-entry-number*]

View Any view

Parameter

prialarm-entry-number: Extended alarm entry Index, in the range of 1 to 65535. If you do not specify this argument, the configuration of all the extended alarm entries is displayed.

Description

Use the **display rmon prialarm** command to display the configuration of a specified RMON extended alarm entry or all the RMON extended alarm entries.

Related command:

rmon prialarm.

Example

Display the configuration of the extended RMON alarm entries.

```
<SW7750> display rmon prialarm
Prialarm table 1 owned by abc is VALID.
  Samples type          : delta
  Variable formula      : 1.3.6.1.2.1.2.2.1.10.641
  Description           : ifInOctets.Ethernet2/0/1
  Sampling interval     : 10(sec)
  Rising threshold      : 100(linked with event 2)
  Falling threshold     : 10(linked with event 2)
  When startup enables  : risingOrFallingAlarm
  This entry will exist : forever.
  Latest value          : 0
```

Table 173 Field descriptions of the **display rmon prialarm** command

Field	Description
Prialarm table 1	Index number of a line of the extended alarm table
abc	Creator of this extended alarm entry
VALID	The entry corresponding to the index is valid
Samples type	Sample type: change value or absolute value
Variable formula	Alarm variable of the sampled node
Description	Description of the alarm variable
Sampling interval	Sampling interval
Rising threshold	Rising threshold. An alarm is triggered when the rising threshold is reached
Falling threshold	Falling threshold. An alarm is triggered when the falling threshold is reached
linked with event	Event index corresponding to an alarm
When startup enables	Alarm startup type:
	risingOrFallingAlarm (an alarm is triggered when the rising or falling threshold is reached)
	risingAlarm (an alarm is triggered when the rising threshold is reached)
	FallingAlarm (an alarm is triggered when the falling threshold is reached)
This entry will exist: forever	Existing period. This entry can exist forever or exist in the specified cycle
Latest value	Latest sampled value

display rmon statistics

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

View Any view

Parameter *interface-type*: Interface type.

interface-number: Interface number.

Description Use the **display rmon statistics** command to display the RMON statistics of a specified port.

The displayed information include the number of the following items: collisions, packets with CRC errors, undersize or oversize packets, broadcast packets, multicast packets, received bytes, and received packets.

Related command: **rmon statistics**.

Example # Display the RMON statistics information.

```
<SW7750> display rmon statistics ethernet 3/0/1
Statistics entry 1 owned by abc is VALID.
  Interface : Ethernet3/0/1<ifIndex.201326722>
  etherStatsOctets         : 3776      , etherStatsPkts          : 30
  etherStatsBroadcastPkts  : 0         , etherStatsMulticastPkts : 30
  etherStatsUndersizePkts  : 0         , etherStatsOversizePkts  : 0
  etherStatsFragments      : 0         , etherStatsJabbers       : 0
  etherStatsCRCAlignErrors : 0         , etherStatsCollisions    : 0
  etherStatsDropEvents (insufficient resources): 0
  Packets received according to length (etherStatsPktsXXXtoYYYOctets):
  64     : 5         ,  65-127  : 10         ,  128-255  : 15
  256-511: 0         ,  512-1023: 0          ,  1024-max: 0
```

Table 174 Field descriptions of the **display rmon statistics** command

Field	Description
Statistics entry 3	Index number of the statistics information table
abc	Entry creator
VALID	The entry corresponding to this index is valid
Interface	Interface
etherStatsOctets	Number of received or transmitted bytes
etherStatsPkts	Number of received or transmitted packets
etherStatsBroadcastPkts	Number of broadcast packets
etherStatsMulticastPkts	Number of multicast packets
etherStatsUndersizePkts	Number of undersize packets
etherStatsOversizePkts	Number of oversize packets
etherStatsFragments	Number of undersize and checkerror packets
etherStatsJabbers	Number of oversize and checkerror packets
etherStatsCRCAlignErrors	Number of checkerror packets
etherStatsCollisions	Number of collision packets

Table 174 Field descriptions of the **display rmon statistics** command

Field	Description
etherStatsDropEvents	Event about dropping packets (network resources are insufficient)
Packets received according to length	Number of received packets, which are made statistics by byte length

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: Alarm entry line number, in the range of 1 to 65535.

alarm-variable: Alarm variable, a string comprising 1 to 256 characters in dotted node OID format (such as 1.3.6.1.2.1.2.1.10.1, or ifInOctets.1). Only the variables that can be resolved to ASN.1 INTEGER data type (that is, INTEGER, Counter, Gauge, or TimeTicks) can be used as alarm variables.

sampling-time: Sampling interval (in seconds), in the range of 5 to 65,535.

delta: Specifies to sample increments (that is, the current increment with regard to the latest sample)

absolute: Specifies to sample absolute values.

rising_threshold *threshold-value1*: Specifies the upper threshold. The *threshold-value1* argument ranges from 0 to 2,147,483,647.

event-entry1: Index of the event entry corresponding to the upper threshold, in the range of 1 to 65,535.

falling_threshold *threshold-value2*: Specifies the lower threshold. The *threshold-value2* argument ranges from 0 to 2,147,483,647.

event-entry2: Index of the event entry corresponding to the lower threshold, in the range of 1 to 65,535.

owner *text*: Specifies the owner of the entry. The *text* argument is a string comprising 1 to 127 characters.

Description

Use the **rmon alarm** command to add an alarm entry to the alarm table.

Use the **undo rmon alarm** command to remove an alarm entry from the alarm table.

You can use the **rmon alarm** command to define an alarm entry so that a specific alarm event can be triggered under specific circumstances. The act (such as logging and sending trap messages to NMS) taken after an alarm event occurs is determined by the corresponding alarm entry.

With an alarm entry defined in an alarm group, a network device performs the following operations accordingly:

- Sample the defined alarm variables (alarm-variable) once in each specified period, which is specified by the *sampling-time* argument.
- Comparing the sampled value with the set threshold and performing the corresponding operations, as described in Table 175.

Table 175 Sample value and the corresponding operation

Comparison	Operation
The sample value is larger than or equal to the set upper threshold (*threshold-value1*)	Triggering the event identified by the *event-entry1* argument
The sample value is smaller than the set lower threshold (*threshold-value2*)	Triggering the event identified by the *event-entry2* argument

- *Before adding an alarm entry, you need to use the* ***rmon event*** *command to define the events to be referenced by the alarm entry.*
- *Make sure the node to be monitored exists before executing the* ***rmon alarm*** *command.*

Example

Add the alarm entry numbered 1 as follows:

- The node to be monitored: 1.3.6.1.2.1.16.1.1.1.4.1
- Sampling interval: 10 seconds
- Upper threshold: 50
- The *event-entry1* argument identifies event 1.
- Lower threshold: 5
- The *event-entry2* argument identifies event 2
- Owner: user1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] rmon event 1 log
[SW7750] rmon event 2 none
[SW7750]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 alarm entry numbered 15 from the alarm table.

```
[SW7750] 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*: Event entry line number, in the range of 1 to 65535.

description *string*: Specifies the event description, a string comprising 1 to 127 characters.

log: Logs events.

trap *trap-community*: Defines the event as a trap event and specifies the community name of the NMS that receives the trap messages.

log-trap *log-trapcommunity*: Defines the event as a log and trap event and specifies the community name of the NMS that receives the log messages.

none: Specifies that the event triggers no action.

owner *text*: Specifies the creator of the event entry. The *text* argument is a string comprising 1 to 127 characters.

Description Use the **rmon event** command to add an entry to the event table.

Use the **undo rmon event** command to delete an entry from the event table.

When adding an event entry to an event table, you need to specify the event index. You need also to specify the corresponding actions, including logging the event, sending trap messages to the NMS, and the both, for the network device to perform corresponding operation when an alarm referencing the event is triggered.

Example # Add the event entry numbered 10 to the event table and configure it to be a log event.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] rmon event 10 log
```

rmon history

Syntax **rmon history** *entry-number* **buckets** *number* **interval** *sampling-interval* [**owner** *text*]

undo rmon history *entry-number*

View Ethernet port view

Parameter *entry-number*: History entry index, in the range of 1 to 65535.

buckets *number*: Specifies the size of the history table that corresponds to the entry, in the range of 1 to 65535. Currently the device only supports 1 to 10. If you enter an argument greater than 10, the actual table size is still 10.

interval *sampling-interval*: Specifies the sampling interval (in seconds). The *sampling-interval* argument ranges from 5 to 3,600.

owner *text*: Specifies the owner of the entry, a string comprising 1 to 127 characters.

Description Use the **rmon history** command to add an entry to a history control table.

Use the **undo rmon history** command to delete an entry from a history control table.

You can use the **rmon history** command to sample a specific port. You can also set the sampling interval and the number of the samples that can be saved. After you execute this command, the RMON system samples the port periodically and stores the samples for later retrieval. The sampled information includes utilization, the number of errors, and total number of packets.

You can use the **display rmon history** command to display the statistics of the history control table.

Example # Create the history entry numbered 1 for Ethernet2/0/1 port, with the table size being 10, the sampling interval being 5 seconds, and the owner being user1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750]interface Ethernet 2/0/1
[SW7750-Ethernet2/0/1]rmon history 1 buckets 10 interval 5 owner user1
```

# Remove the history entry numbered 15.

```
[SW7750-Ethernet2/0/1] undo rmon history 15
```

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*: Extended alarm entry index, in the range of 1 to 65535.

prialarm-formula: Expression used to perform operations on the alarm variables, a string comprising 1 to 256 characters. The alarm variables in the expression must be represented by OIDs, for example, (.1.3.6.1.2.1.2.1.10.1)*8. The operations available are addition, subtraction, multiplication and division operations. The operation results are rounded to values that are of long integer type. To prevent invalid operation results, make sure the operation results of each step are valid long integers.

prialarm-des: Alarm description, a string comprising 1 to 256 characters.

sampling-timer: Sampling interval (in seconds), in the range of 10 to 65,535.

delta | absolute | changeratio: Specifies sample type, which can be deltas, absolute values or change ratios.

threshold-value1: Upper threshold, in the range of 0 to 4,294,967,295.

event-entry1: Index of the event entry that corresponds to the upper threshold, in the range of 0 to 65535.

threshold-value2: Lower threshold, in the range of 0 to 4,294,967,295.

event-entry2: Index of the event entry that corresponds to the lower threshold, in the range of 0 to 65535.

forever: Specifies the alarm entry is valid indefinitely.

cycle: Specifies the alarm entry is valid periodically.

cycle-period: Cycle period, in seconds, ranging from 0 to 4,294,967,295.

owner *text*: Specifies the owner of the alarm entry, a string comprising 1 to 127 characters.

Description Use the **rmon prialarm** command to create an extended entry in an extended RMON alarm table.

Use the **undo rmon prialarm** command to remove a specified extended alarm entry.

The maximum number of distances in the table depends on the hardware resources.

- *Before adding an extended alarm entry, you need to use the* ***rmon event*** *command to define the events to be referenced by the entry.*
- *Make sure the node to be monitored exists before executing the* ***rmon event*** *command.*
- *You can define up to 50 extended alarm entries.*

With an extended alarm entry defined in an extended alarm group, the network devices perform the following operations accordingly:

- Sampling the alarm variables referenced in the defined extended alarm expressions (*prialarm-formula*) once in each period specified by the *sampling-timer* argument.
- Performing operations on sampled values according to the defined extended alarm expressions (*prialarm-formula*)
- Comparing the operation result with the set thresholds and perform corresponding operations, as described in Table 176.

Table 176 Operation result and corresponding operation

Comparison	Operation
The operation result is larger than or equal to the set upper threshold (*threshold-value1*)	Triggering the event identified by the *event-entry1* argument
The operation result is smaller than or equal to the set lower threshold (*threshold-value2*)	Triggering the event identified by the *event-entry2* argument

Example # Add the extended alarm entry numbered 2 as follows:

- Perform operations on the corresponding alarm variables using the expression ((1.3.6.1.2.1.16.1.1.1.4.1)*100).
- Sampling interval: 10 seconds
- Upper threshold: 50
- Lower threshold: 5
- Event 1 is triggered when the change ratio is larger than the upper threshold.
- Event 2 is triggered when the change ratio is less than the lower threshold.
- The alarm entry is valid forever.
- Entry owner: user1

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750]interface Ethernet 2/0/1
[SW7750-Ethernet2/0/1] rmon statistics 1
[SW7750-Ethernet2/0/1] quit
[SW7750] rmon prialarm 2 ((.1.3.6.1.2.1.16.1.1.1.4.1)*100) test 10 c
hangeratio rising_threshold 50 1 falling_threshold 5 2 entrytype for
ever owner user1
```

# Remove the extended alarm entry numbered 2 from the extended alarm table.

```
[SW7750] undo rmon prialarm 2
```

rmon statistics

Syntax **rmon statistics** *entry-number* [**owner** *text*]

undo rmon statistics *entry-number*

View Ethernet port view

Parameter *entry-number*: Statistics entry Index, in the range of 1 to 65535.

owner *text*: Specifies the owner of the entry, a string comprising 1 to 127 characters.

Description Use the **rmon statistics** command to add an entry to the statistics table.

Use the **undo rmon statistics** command to remove an entry from the statistics table.

The RMON statistics management function is used to take statistics of the usage of the monitored ports and errors occurred to them. The statistics includes the number of the following items: collisions, packet with CRC errors, undersize (or oversize) packets, broadcast and multicast packets, received packets and bytes and so on.

For each port, only one RMON alarm table entry can be created, that is to say, if one RMON alarm table entry was already created for a given port, creation of another entry with a different index number for the same port will not succeed.

You can use the **display rmon statistics** command to display the statistics entries.

Example # Add the statistics entry numbered 20 to take statistics of Ethernet2/0/1 port.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750]interface Ethernet 2/0/1
[SW7750-Ethernet2/0/1] rmon statistics 20
```

70 NTP CONFIGURATION COMMANDS

display ntp-service sessions

Syntax **display ntp-service sessions** [**verbose**]

View Any view

Parameter **verbose**: Displays the detailed information about all the sessions maintained by the NTP service. When you configure this command without the **verbose** parameter, the Ethernet switch displays the brief information about all 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 device.

CAUTION: *The sessions can be created in all NTP operating modes except the NTP server mode.*

Example # Display the status of all the sessions maintained by the NTP service.

```
<SW7750> display ntp-service sessions
source          reference   stra reach poll  now offset  delay disper
********************************************************************
[12345]1.0.1.11 LOCAL(0)        3    377   64   16   -0.4    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

```
<SW7750> display ntp-service status
 Service status:enabled
 Clock status: unsynchronized
 Clock stratum: 16
 Reference clock ID: none
 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: 0.00 ms
 Reference time: 00:00:00.000 UTC Jan 1 1900(00000000.00000000)
```

The following table describes the displayed fields:

NTP service status information

Field	Meaning
Service status	NTP service status: enabled or disabled
Clock status: unsynchronized	Local clock status: is not synchronized to any remote NTP server
Clock stratum	Indicates the NTP stratum of the local clock
Reference clock ID	Indicates the address of a remote server or the clock source ID when the local system is synchronized with a remote NTP server or a 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 the local clock
Clock offset	Time difference between Offset of the local clock to the NTP server clock
Root delay	Total delay from local device 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.

Example

```
<SW7750> 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 query the local NTP service only.

synchronization: Only allows the peer device to synchronize its clock to the local device.

server: Allows the peer device to perform synchronization and control query to the local device but does not permit the local device to synchronize its clock to the peer device.

peer: Full access. This level of right permits the peer device to perform synchronization and control query to the local device and also permits the local device to synchronize its clock to the peer device.

acl-number: The IP address access control list number, ranging from 2000 to 2999.

Description Use the **ntp-service access** command to set the right to access the local device service.

Use the **undo ntp-service access** command to cancel the access authority settings.

By default, no right limit is configured.

Compared with authentication, setting the right to access and control the NTP services is a basic and brief security measure. From the highest NTP service access-control right to the lowest one are **peer**, **server**, **synchronization**, and **query**. When a device receives an NTP request, it will perform an access control right match and will used first matched right..

Example # Configure to permit the remote switch defined in ACL 2000 to perform time synchronization request, query and synchronization to the local device..

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ntp-service access peer 2000
```

# Configure to permit the remote switch defined in ACL 2000 to perform time synchronization request and query to the local device.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] 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.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] 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*: Specifies the key number from 1 to 4,294,967,295.

value: Specifies the value of the key with 1 to 32 ASCII characters.

Description Use the **ntp-service authentication-keyid** command to set an NTP authentication key.

Use the **undo ntp-service authentication-keyid** command to cancel the NTP authentication key.

By default, no authentication key is configured.

Currently the system supports MD5 authentication only.

Example # Set MD5 authentication key 10 as hello.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
```

```
[SW7750] ntp-service authentication-keyid 10 authentication-mode md5
 hello
```

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 NTP broadcast client mode.

By default, the NTP broadcast client mode is disabled.

Designate an interface on the local device to receive NTP broadcast packets. The local device operates in broadcast client mode. The local device listens to the broadcast packets from the server. When it receives the first broadcast packet, it starts a brief client/server mode to exchange messages with a remote server for estimating the network delay. Thereafter, the local device enters broadcast client mode and continues listening to the broadcast packets and synchronizes the local clock based on the arrived broadcast packets.

Example # Configure to receive NTP broadcast packets through Vlan-interface 1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface vlan-interface1
[SW7750-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 an authentication key.

keyid: Key ID used in broadcast, ranging from 1 to 4,294,967,295.

version: Defines an 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. When no NTP version number is specified, the default version number is 3.

Designate an interface on the local device to broadcast NTP packets. The local device runs in broadcast-server mode and regularly broadcasts packets to its clients.

Example # Configure to broadcast NTP packets through Vlan-interface 1. Encrypt them with Key 4 and set the NTP version number to 3.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface vlan-interface1
[SW7750-Vlan-Interface1] ntp-service broadcast-server authentication-key 4 version 3
```

ntp-service disable

Syntax **ntp-service disable**

undo ntp-service disable

View System view

Parameter None

Description Use the **ntp-service disable** command to disable the NTP service function.

Use **undo ntp-service disable** command to enable this function.

By default, the NTP service is enabled.

Example # Disable NTP service on the device.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ntp-service disable
```

ntp-service in-interface disable

Syntax **ntp-service in-interface disable**

undo ntp-service in-interface disable

View VLAN interface view

Parameter None

Description Use the **ntp-service in-interface disable** command to disable an interface from receiving NTP messages.

Use **undo ntp-service in-interface disable** command to enable an interface to receive NTP messages.

By default, an interface is enabled to receive NTP messages.

Example # Disable Vlan-interface 1 from receiving NTP message.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface vlan-interface1
[SW7750-Vlan-Interface1] ntp-service in-interface disable
```

ntp-service max-dynamic-sessions

Syntax **ntp-service max-dynamic-sessions** *number*

undo ntp-service max-dynamic-sessions

View System view

Parameter *number*: The 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 the maximum number of dynamic sessions that can be created locally.

Use the **undo ntp-service max-dynamic-sessions** command to restore the default value.

By default, a local device allows up to 100 dynamic sessions.

Only the sessions created in NTP peer mode, NTP broadcast client mode and NTP multicast client mode are dynamic sessions. Other sessions are static sessions.

Example # Set the local device to allow up to 50 sessions.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] 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*: Specifies a multicast IP address of Class D.

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 device to receive NTP multicast packets. The local device operates in the multicast client mode. The local device listens to the multicast packets from the server. When it receives the first multicast packet, it starts a brief client/server mode to exchange messages with a remote server for estimating the network delay. Thereafter, the local device enters the multicast client mode and continues listening to the multicast packets and synchronizes the local clock based on the arrived multicast message.

Example # Configure to receive NTP multicast packets to the multicast group address of 224.0.1.1 through Vlan-interface1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface vlan-interface 1
[SW7750-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*: Specifies a multicast IP address of Class D and default to 224.0.1.1.

authentication-keyid: Specifies an authentication key.

keyid: Key ID used in multicast, ranging from 0 to 4,294,967,295.

ttl: Defines the time to live (TTL) of a multicast packet.

ttl-number: Specify the TTL of a multicast packet, ranging from 1 to 255.

version: Defines an NTP version number.

number: Specifies an NTP version number, ranging from 1 to 3.

Description

Use the **ntp-service multicast-server** command to configure NTP multicast server mode. If no IP address is specified, the switch automatically chooses 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 device to transmit NTP multicast packets. The local device 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-interface 1 at 224.0.1.1 and use NTP version 3.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface vlan-interface 1
[SW7750-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 127.127.1.u. Here, u ranges from 0 to 3.

stratum: Specifies which stratum the local clock is located at. The value ranges 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, no NTP master clock is configured. When *ip-address* is not specified, the local clock is set to the NTP master clock by default. When *stratum* is not specified, the local clock is located at stratum 8 by default.

You can use this command to designate an external reference clock or the local clock as an NTP master clock to provide synchronized time to other devices. *ip-address* specifies the IP address of an external clock as 127.127.1.u. If no IP address is specified, the local clock is configured as the NTP master clock by default. You can also specify the stratum at which the NTP master clock is located.

Example # Specify the local clock as the NTP master clock to provide synchronized time for its peers and locate the master clock at stratum 3.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] 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*: Specifies the key number, ranging from 1 to 4,294,967,295.

Description Use the **ntp-service reliable authentication-keyid** command to configure the key as a reliable key.

Use the **undo ntp-service reliable authentication-keyid** command to cancel the current setting.

By default, no reliable key is configured.

When you enable the authentication, you can use this command to configure one or more than one reliable keys. In this case, a client only synchronizes to the server that provides reliable keys.

Example # Enable NTP authentication, adopt MD5 encryption, and designate Key 37 BetterKey and configure it as a reliable key.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ntp-service authentication enable
[SW7750] ntp-service authentication-keyid 37 authentication-mode md5 BetterKey
[SW7750] 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 an interface. This parameter is used to specify an interface together with the *interface-number* parameter.

interface-number: Specifies an interface number. This parameter is used to specify an interface with the *interface-type* parameter.

Description Use the **ntp-service source-interface** command to designate an interface to transmit NTP messages.

Use the **undo ntp-service source-interface** command to cancel the current setting.

By default, the source address depends on the output interface.

You can use this command to designate an interface of which the IP address will be the source IP address in all the NTP packets sent by the local device so that the remote device sends the response message to this interface only.

Example # Configure all the outgoing NTP packets to use the IP address of Vlan-Interface1 as their source IP address.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ntp-service source-interface Vlan-Interface 1
```

ntp-service unicast-peer

Syntax **ntp-service unicast-peer** { *ip-address* | *server-name* } [**version** *number* | **authentication-key** *keyid* | **source-interface** *interface-type interface-number* | **priority**]*

undo ntp-service unicast-peer { *ip-address* | *server-name* }

View System view

Parameter *ip-address*: Specifies the IP address of a remote server.

server-name: Specifies the host name of an NTP server, containing 1 to 20 characters.

version: Defines an NTP version number.

number: NTP version number, ranging from 1 to 3.

authentication-keyid: Defines an authentication key.

keyid: Key ID used for transmitting messages to a remote server, ranging from 1 to 4,294,967,295.

source-interface: Specifies an interface name.

interface-type: Specifies the interface type and determines an interface together with the *interface-number* parameter.

interface-number: Specifies the interface number and determines an interface together with the *interface-type* parameter.

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, no NTP peer mode is configured. When you do not specify a version number, the default version number is 3. When you do not specify **authentication-keyid**, 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 device, which operates in symmetric active mode. *ip-address* specifies a host address other than a broadcast address, multicast address, or the IP address of a reference clock. Under this configuration, a local device can synchronize and be synchronized by a remote server.

Example # Configure the local device to synchronize or to be synchronized by a peer at 128.108.22.44. Set the NTP version to 3. The IP address of the NTP packets is taken from that of VLAN-interface 1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ntp-service unicast-peer 131.108.22.33 version 3 source-int
erface Vlan-Interface 1
```

ntp-service unicast-server

Syntax **ntp-service unicast-server** { *ip-address* | *server-name* } [**version** *number* | **authentication-keyid** *keyid* | **source-interface** *interface-type interface-number* | **priority**]*

undo ntp-service unicast-server { *ip-address* | *server-name* }

View System view

Parameter *ip-address*: Specifies the IP address of a remote server.

server-name: Specifies the host name of an NTP server, containing 1 to 20 characters.

version: Defines an NTP version number.

number: NTP version number, ranging from 1 to 3.

authentication-keyid: Defines an authentication key.

keyid: Key ID used for transmitting messages to a remote server, ranging from 1 to 4,294,967,295.

source-interface: Specifies an interface name.

interface-type: Specifies an interface type and determines an interface together with the *interface-number* parameter.

interface-number: Specifies an interface number and determines an interface together with the *interface-type* parameter.

priority: Designate 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, no NTP server mode is configured. When you do not specify a version number, the default version number is 3. When you do not specify **authentication-keyid**, authentication is disabled.

The command announces to use the remote server at *ip-address* as the local time server. *ip-address* specifies a host address other than a broadcast address, multicast address, or the IP address of a 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.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ntp-service unicast-server 128.108.22.44 version 3
```

71 SSH SERVER CONFIGURATION COMMANDS

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 host key pair (3Com_Host) and the public key of the server key pair (3Com_Server).

Related command: **rsa local-key-pair create**.

Example # Display the public keys of the server key pair and host key pair.

```
<SW7750> display rsa local-key-pair public

=====================================================
Time of Key pair created: 16:51:29  2006/04/27
Key name: 3Com_Host
Key type: RSA encryption Key
=====================================================
Key code:
3047
  0240
    E4B60800 48C19975 3D912FCE 0BBEA711 3E4B94D0
    E8E6A080 F4D5D2DA 4BCBAF07 B9F91198 FE9937C6
    EE0C7AEE 1B8C06F0 8BF01F36 05CF26DB F789A2D8
    23182ECB
  0203
    010001

Host public key for PEM format code:
---- BEGIN SSH2 PUBLIC KEY ----
AAAAB3NzaC1yc2EAAAADAQABAAAAQQDktggASMGZdT2RL84LvqcRPkuU0OjmoID0
1dLaS8uvB7n5EZj+mTfG7gx67huMBvCL8B82Bc8m2/eJotgjGC7L
---- END SSH2 PUBLIC KEY ----

Public key code for pasting into OpenSSH authorized_keys file :
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAQQDktggASMGZdT2RL84LvqcRPkuU0Ojm
oID01dLaS8uvB7n5EZj+mTfG7gx67huMBvCL8B82Bc8m2/eJotgjGC7L rsa-key
```

```
=====================================================
Time of Key pair created: 16:51:55  2006/04/27
Key name: 3Com_Server
Key type: RSA encryption Key
=====================================================
Key code:
3067
  0260
    E1D3BAFE 5E646CF2 241602A1 2FF9AF7F 4AE5A7DE
    02894012 1A733A4B 3ABA2F65 DB8CE292 644BB45C
    2613F773 BC67C912 DCDACBF6 11DF66CA B48A9F0F
    97886142 DB845B18 9C956B16 76D7C8BC 7E355894
    CC2854F0 0D29376C 5F30F7A5 98A64CAD
  0203
    010001
```

display rsa peer-public-key

Syntax **display rsa peer-public-key** [**brief** | **name** *keyname*]

View Any view

Parameter **brief**: Displays brief information about all peer public keys.

keyname: Name of the public key, a string of 1 to 64 characters.

Description Use the **display rsa peer-public-key** command to display information about the peer public keys. If no key name is specified, the command displays detailed information about all peer public keys.

Example # Display brief information about all peer public keys.

```
<SW7750> display rsa peer-public-key brief
Address         Bits   Name
---------------------------
                1024   192.168.0.39
```

# Display the public key named abc.

```
<SW7750> display rsa peer-public-key name abc
=====================================
    Key name: abc
    Key address:
=====================================
Key Code:
308186
  028180
    739A291A BDA704F5 D93DC8FD F84C4274 631991C1 64B0DF17 8C55FA83 3591C7D4
    7D5381D0 9CE82913 D7EDF9C0 8511D83C A4ED2B30 B809808E B0D1F52D 045DE408
    61B74A0E 135523CC D74CAC61 F8E58C45 2B2F3F2D A0DCC48E 3306367F E187BDD9
    44018B3B 69F3CBB0 A573202C 16BB2FC1 ACF3EC8F 828D55A3 6F1CDDC4 BB45504F
  0201
    25
```

display ssh server

Syntax

display ssh server { **status** | **session** }

View

Any view

Parameter

status: Displays SSH status information.

session: Displays SSH session information.

Description

Use the **display ssh server** command to display the status or session information about the SSH server.

Related command:

ssh server authentication-retries, **ssh server timeout**.

Example

Display the status information about the SSH server.

```
<SW7750> display ssh server status
 SSH version : 1.99
 SSH connection timeout : 60 seconds
 SSH server key generating interval : 0 hours
 SSH Authentication retries : 3 times
  SFTP Server: Enable
```

- *If you use the **ssh server compatible-ssh1x enable** command to configure the server to be compatible with the client of SSH1.x version, the SSH version will be displayed as 1.99.*
- *If you use the **undo ssh server compatible-ssh1x enable** command to configure the server to be not compatible with the client of SSH1.x version, the SSH version will be displayed as 2.0.*

# Display the session information about the SSH server.

```
<SW7750> display ssh server session
 Conn   Ver   Encry    State     Retry    SerType  Username
 VTY 0  2.0   AES      started   0        stelnet  kk
VTY 1  2.0   AES      started   0        sFTP     abc
```

Table 177 Field descriptions of the **display ssh server session** command

Field	Description
4) Conn	5) Number of VTY interface used for user login
6) Ver	7) SSH version
8) Encry	9) Encryption algorithm used by SSH. Encry is short for encryption. The encryption algorithms in common use are advanced encryption standard (AES), data encryption standard (DES), and triple DES (3DES).
10) State	11) Current state
12) Retry	13) Number of retries
14) SerType	15) Type of service
16) Username	17) User name

display ssh user-information

Syntax **display ssh user-information** [*username*]

View Any view

Parameter *username*: SSH user name, a string of 1 to 80 characters.

Description Use the **display ssh user-information** command to display information about the current SSH users, including user name, authentication mode, corresponding public key name and authorized service types. If the *username* is specified, the command displays information about the specified user.

Example # Display information about the current user.

```
<SW7750> display ssh user-information
Username            Authentication-type  User-public-key-name  Servi
ce-type
 kk                  rsa                  test                  sftp
```

peer-public-key end

Syntax **peer-public-key end**

View Public key view

Parameter None

Description Use the **peer-public-key end** command to return to system view from public key view.

Related command: **rsa peer-public-key**, **public-key-code begin**.

Example # Exit from public key view.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] rsa peer-public-key 3Com003
[SW7750-rsa-public-key] peer-public-key end
```

protocol inbound

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

View VTY user interface view

Parameter **all**: Supports all protocols, including Telnet and SSH.

ssh: Supports only SSH.

telnet: Supports only Telnet.

Description Use the **protocol inbound** command to configure the protocols supported in the current user interface.

By default, both SSH and Telnet are supported.

CAUTION:

- *When SSH protocol is specified, to ensure a successful login, you must configure the AAA authentication using the* ***authentication-mode scheme*** *command.*
- *The* ***protocol inbound ssh*** *configuration fails if you configured* ***authentication-mode password*** *or* ***authentication-mode none****. When you configured SSH protocol successfully for the user interface, then you cannot configure* ***authentication-mode password*** *or* ***authentication-mode none*** *any more.*

Related command: **user-interface**.

Example # Configure vty0 through vty4 to support SSH only.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] user-interface vty 0 4
[SW7750-ui-vty0-4] authentication-mode scheme
[SW7750-ui-vty0-4] 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 public key edit view and input the client public key.

You can key in a blank space between characters (since the system can remove the blank space automatically), or press <Enter> to continue your input at the next line. But the public key, which is generated randomly by the SSH-supporting client software, should be composed of hexadecimal characters.

Related command: **rsa peer-public-key**, **public-key-code end**.

Example # Enter public key edit view and input client public keys.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] rsa peer-public-key 3Com003
[SW7750-rsa-public-key] public-key-code begin
RSA key code view: return to last view with "public-key-code end".
[SW7750-rsa-key-code] 308186028180739A291ABDA704F5D93DC8FDF84C427463
[SW7750-rsa-key-code] 1991C164B0DF178C55FA833591C7D47D5381D09CE82913
[SW7750-rsa-key-code] D7EDF9C08511D83CA4ED2B30B809808EB0D1F52D045DE4
[SW7750-rsa-key-code] 0861B74A0E135523CCD74CAC61F8E58C452B2F3F2DA0DC
[SW7750-rsa-key-code] C48E3306367FE187BDD944018B3B69F3CBB0A573202C16
[SW7750-rsa-key-code] BB2FC1ACF3EC8F828D55A36F1CDDC4BB45504F020125
[SW7750-rsa-key-code] public-key-code end
[SW7750-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 public key edit view to public key view and save the public keys you set.

After you use this command to terminate the public key editing, public key validity will be checked before the keys are saved.

- If there are illegal characters in the keys, the prompt will be given and the keys will be discarded. Your configuration this time fails.
- If the keys are valid, they will be saved in the local public key list.

Related command: **rsa peer-public-key**, **public-key-code begin**.

Example # Exit from public key edit view and save the public keys.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750]rsa peer-public-key kk
[SW7750-rsa-public-key]public-key-code begin
[SW7750-rsa-key-code] public-key-code end
[SW7750-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 an RSA host key pair and an RSA server key pair.

Note that:

- *After entering this command, you will be prompted to provide the length of the key pair. The length of a server/host key must be in the range 512 to 2048 bits and defaults to 1024. If the key pair already exists, the system will ask you whether you want to overwrite it.*
- *The configuration of this command can survive a reboot. You only need to configure it once.*

*Server key pair (3Com_Server) is not used in SSH2.0. Therefore, when the **rsa local-key-pair create** command is executed, the system only informs you that the RSA host key pair (3Com_Host) is generated, but does not inform you of the information about the server key pair even if the server key pair is generated in the background for the purpose of SSH1.x compatibility. You can use the **display rsa local-key-pair public** command to display the generated key pairs.*

Related command: **rsa local-key-pair destroy**, **display rsa local-key-pair public**, **ssh server compatible-ssh1x enable**.

Example # Generate a local RSA key pair.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750]rsa local-key-pair create
The key name will be: 3Com_Host
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
       It will take a few minutes.
Input the bits in the modulus[default = 1024]:
Generating keys...
.......................................................++++++
........................++++++
.........................++++++++
.........++++++++
.......
```

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 existing RSA key pairs generated locally.

Related command: **rsa local-key-pair create**.

Example # Destroy all existing RSA key pairs generated locally.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] rsa local-key-pair destroy
% The name for the keys which will be destroyed is 3Com_Host .
% Confirm to destroy these keys? [Y/N]:y
.....................
```

rsa peer-public-key

Syntax **rsa peer-public-key** *key-name*

undo rsa peer-public-key *key-name*

View System view

Parameter *key-name*: Name of the peer public key , a string of 1 to 64 characters

Description Use the **rsa peer-public-key** command to enter public key view.

Use the **undo rsa peer-public-key** command to remove the configured peer public key.

After you input the **rsa peer-public-key** command, you will enter public key view. You can use the command along with the **public-key-code begin** command to configure on the server client public keys, which are generated randomly by the SSH-supporting client software.

Related command: **public-key-code begin**, **public-key-code end**.

Example # Enter 3Com002 public key view.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] rsa peer-public-key 3Com002
[SW7750-rsa-public-key]
```

# Delete the peer public key named 192.168.0.39.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] undo rsa peer-public-key 192.168.0.39
% Do you really want to remove the public key named 192.168.0.39 ? [Y/N]:y
[SW7750]
```

rsa peer-public-key import sshkey

Syntax **rsa peer-public-key** *key-name* **import sshkey** *file-name*

undo rsa peer-public-key *key-name*

View System view

Parameter *key-name*: Client public key name, a string of 1 to 64 characters.

file-name: Name of the public key file uploaded to the Flash in advance. This argument is a string of 1 to 136 characters.

Description Use the **rsa peer-public-key import sshkey** command to import a peer public key from the public key file.

Use the **undo rsa peer-public-key** command to remove the setting.

With this command, you need not configure the public key manually. You only need to upload the public key file of the RSA key pair of the peer to the local end by using FTP/TFTP, and then use this command on the local end. This command will transform the format of the public key and configure the public key automatically.

Example # Import a peer public key named 123 from public key file abc.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] rsa peer-public-key 123 import sshkey abc
```

ssh authentication-type default

Syntax **ssh authentication-type default** { **password** | **rsa** | **password-publickey** | **all** }

undo ssh authentication-type default

View System view

Parameter **password**: Specifies the authentication type as password.

rsa: Specifies the authentication type as RSA public key.

password-publickey: Specifies the authentication type as both password and RSA public key, that is, the user can pass the authentication only if both the password and RSA public key are correct.

all: Specifies the authentication type as password or RSA public key, that is, the user can pass the authentication if either the password or RSA public key is correct.

Description Use the **ssh authentication-type default** command to specify a default authentication type for SSH users. After the command is configured, when a SSH user is added, if you do not use the **ssh user authentication-type** command to specify an authentication type for the user, the user needs to pass the default authentication type.

Use the **undo ssh authentication-type default** command to restore the default settings.

By default, the password authentication type is specified.

Related command: **ssh user authentication-type**.

Example # Specifies the default authentication type as password.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] ssh authentication-type default password
```

ssh server authentication-retries

Syntax **ssh server authentication-retries** *times*

undo ssh server authentication-retries

View System view

Parameter *times*: Authentication retry times. It is in the range of 1 to 5 and defaults to 3.

Description Use the **ssh server authentication-retries** command to set the authentication retry times for SSH connections.

Use the **undo ssh server authentication-retries** command to restore the default authentication retry times, which will take effect at next login.

Related command: **display ssh server**.

If you have used the ***ssh user authentication-type*** *command to configure the authentication type to password-publickey, you must set the authentication retry times to a number greater than or equal to 2, for one is counted when a client sends a public key to the server.*

Example # Set the authentication retry number to 4.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] 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 SSH1.x version-supporting client.

Use the **undo ssh server compatible-ssh1x enable** command to make the server not compatible with the SSH1.x version-supporting client.

By default, the server is compatible with the SSH1.x version-supporting client.

Example # Specify the server compatible with the SSH1.x version-supporting client.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] 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 period of the server key, in hours, ranging from 1 to 24.

Description Use the **ssh server rekey-interval** command to set the update interval for the server key.

Use the **undo ssh server rekey-interval** command to cancel the current configuration.

By default, the system does not update the server key.

CAUTION: *This command is only effective on users whose client version is SSH1.x.*

Example # Set the update interval of the server key to 3 hours.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ssh server rekey-interval 3
```

ssh server timeout

Syntax **ssh server timeout** *seconds*

undo ssh server timeout

View System view

Parameter

seconds: Authentication timeout time. It is in the range of 1 to 120 (seconds) and defaults to 60 seconds.

Description

Use the **ssh server timeout** command to set authentication timeout time for SSH connections.

Use the **undo ssh server timeout** command to restore the default timeout time. The default value takes effect at next login.

Related command:

display ssh server.

Example

Set the authentication timeout time to 80 seconds.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ssh server timeout 80
```

ssh user

Syntax

ssh user *username*

undo ssh user *username*

View

System view

Parameter

username: Valid SSH user name. a string of 1 to 80 characters.

Description

Use the **ssh user** command to create an SSH user.

Use the **undo ssh user** command to remove the specified SSH user.

Note that: an SSH user created in this way adopts the default authentication type if you do not use the **ssh user authentication-type** command to specify an authentication type for this user.

Example

Create an SSH user named zhangsan.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750]ssh user zhangsan
```

ssh user assign rsa-key

Syntax

ssh user *username* **assign rsa-key** *keyname*

undo ssh user *username* **assign rsa-key**

View

System view

Parameter

username: SSH user name, a string of 1 to 80 characters.

keyname: Client public key name, a string of 1 to 64 characters.

Description

Use the **ssh user assign rsa-key** command to assign public keys to SSH users.

Use the **undo ssh user assign rsa-key** command to remove the association between the public keys and SSH users. The configuration takes effect at the next login.

If the user already has a public key, the new public key overrides the old one.

Related command: **display ssh user-information**.

Example

Set the client public key for the kk user to key1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ssh user kk 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

username: Valid SSH user name, a string of 1 to 80 characters.

password: Specifies the authentication type as password.

rsa: Specifies the authentication type as RSA public key.

password-publickey: Specifies the authentication type as both password and RSA public key. That is, the user can pass the authentication only if both the password and RSA public key are correct.

*For the **password-publickey** authentication type*

- *SSH1.x client users can access the switch as long as they pass one of the two authentications.*
- *SSH2.0 client users can access the switch only when they pass both the authentications.*

all: Specifies the authentication type as either password or RSA public key. That is, the user can pass the authentication if either the password or RSA public key is correct.

Description

Use the **ssh user authentication-type** command to define on the server the available authentication type for an SSH user.

Use the **undo ssh user authentication-type** command to restore the default setting.

This command defines available authentication type on the server. The actual authentication type, however, is determined by the client.

By default, no authentication type is specified for new users, so they cannot access the switch.

The new authentication type configuration takes effect at the next login.

Related command: **display ssh user-information**.

Example # Set the authentication type for the kk user as password.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ssh user kk authentication-type password
```

72 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 display the association between the server public keys configured on the client and the servers.

Example # Display the association between the server public keys and the servers.

```
<SW7750> display ssh server-info
Server Name(IP)                 Server public key name
________________________________________________________
192.168.0.1                     abc_key01
192.168.0.2                     abc_key02
```

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 public key edit view and set server public keys.

You can key in a blank space between characters (since the system can remove the blank space automatically), or press <Enter> to continue your input at the next line. But the public key, which are generated randomly after you use the **rsa local-key-pair create** command on the server, should be composed of hexadecimal characters.

Related command: **rsa peer-public-key**, **public-key-code end**.

Example # Enter public key edit view and set server public keys.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] rsa peer-public-key 3Com003
[SW7750-rsa-public-key] public-key-code begin
RSA key code view: return to last view with "public-key-code end".
[SW7750-rsa-key-code] 308186028180739A291ABDA704F5D93DC8FDF84C427463
[SW7750-rsa-key-code] 1991C164B0DF178C55FA833591C7D47D5381D09CE82913
[SW7750-rsa-key-code] D7EDF9C08511D83CA4ED2B30B809808EB0D1F52D045DE4
[SW7750-rsa-key-code] 0861B74A0E135523CCD74CAC61F8E58C452B2F3F2DA0DC
[SW7750-rsa-key-code] C48E3306367FE187BDD944018B3B69F3CBB0A573202C16
[SW7750-rsa-key-code] BB2FC1ACF3EC8F828D55A36F1CDDC4BB45504F020125
[SW7750-rsa-key-code] public-key-code end
[SW7750-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 public key edit view to public key view and save the public keys you set.

After you use this command to terminate the public key editing, public key validity will be checked before the keys are saved.

- If there are illegal characters in the keys, the prompt will be given and the keys will be discarded. Your configuration this time fails.
- If the keys are valid, they will be saved in the client list.

Related command: **rsa peer-public-key**, **public-key-code begin**.

Example # Exit from public key edit view and save the public keys.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] rsa peer-public-key 3Com003
[SW7750-rsa-public-key] public-key-code begin
[SW7750-rsa-key-code] public-key-code end
[SW7750-rsa-public-key]
```

rsa peer-public-key

Syntax **rsa peer-public-key** *key-name*

undo rsa peer-public-key *key-name*

View System view

Parameters

Key-name: Name of the public key to be configured , a string of 1 to 64 characters.

Description

Use the **rsa peer-public-key** command to enter public key view.

Use the **undo rsa peer-public-key** command to remove the setting.

After using this command, you will enter public key view. You can use the command along with the **public-key-code begin** command to configure on the client server public keys, which are generated randomly by using the **rsa local-key-pair create** command.

Related commands:

public-key-code begin, **public-key-code end**.

Examples

Enter Switch002 public key view.

```
<SW7750> system-view

System View: return to User View with Ctrl+Z.

[SW7750] rsa peer-public-key Switch002

[SW7750-rsa-public-key]
```

rsa peer-public-key import sshkey

Syntax

rsa peer-public-key *key-name* **import sshkey** *file-name*

undo rsa peer-public-key *key-name*

View

System view

Parameter

key-name: Name of the public key to be configured, a string of 1 to 64 characters.

file-name: Name of the public key file uploaded to the Flash in advance. This argument is a string of 1 to 136 characters.

Description

Use the **rsa peer-public-key import sshkey** command to import a peer public key from the public key file.

Use the **undo rsa peer-public-key** command to remove the setting.

With this command, you need not configure the public key manually. You only need to upload the public key file of the RSA key pair of the peer to the local end by using FTP/TFTP, and then use this command on the local end. This command will transform the format of the public key and configure the public key automatically.

Example

Import a peer public key named 123 from public key file abc.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] rsa peer-public-key 123 import sshkey abc
```

ssh client assign rsa-key

Syntax **ssh client** { *server-ip* | *server-name* } **assign rsa-key** *keyname*

undo ssh client { *server-ip* | *server-name* } **assign rsa-key**

View System view

Parameter *server-ip*: Server IP address.

server-name: Server name, a string of 1 to 80 characters.

keyname: Server public key name, a string of 1 to 64 characters.

Description Use the **ssh client assign rsa-key** command to specify on the client the public key for the server to be connected to guarantee the client can be connected to a reliable server.

Use the **undo ssh client assign rsa-key** command to remove the association between the public keys and servers.

Example # Specify on the client the public key of the server (with IP address 192.168.0.1) as abc.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ssh client 192.168.0.1 assign rsa-key abc
```

ssh client first-time enable

Syntax **ssh client first-time enable**

undo ssh client first-time

View System view

Parameter None

Description Use the **ssh client first-time enable** command to configure the client to run the initial authentication.

Use the **undo ssh client first-time** command to remove the configuration.

In the initial authentication, if the SSH client does not have the public key for the server which it accesses for the first time, the client continues to access the server *and save locally the public key of the server. Then at the next access, the client can authenticate the server with the public key saved locally.*

When the initial authentication function is not available, the client does not access the server if it does not have the public key of the server locally. In this case, you need first to save the public key of the target server to the client in other ways.

By default, the client runs the initial authentication.

Example # Configure the client to run the initial authentication.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] 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** | **aes128** } | **prefer_stoc_cipher** { **des** | **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*: Server IP address.

host-name: Server name, a string of 1 to 20 characters.

port-num: Server port number. It is in the range of 0 to 65,535 and defaults to 22.

prefer_kex: Key exchange algorithm preference. Choose one of the two algorithms available.

dh_group1: Diffie-Hellman-group1-sha1 key exchange algorithm. It is the default algorithm.

dh_exchange_group: Diffie-Hellman-group-exchange-sha1 key exchange algorithm.

prefer_ctos_cipher: Encryption algorithm preference from the client to server. It defaults to AES128.

prefer_stoc_cipher: Encryption algorithm preference from the server to client. It defaults to AES128.

des: DES_cbc encryption algorithm.

aes128: AES_128 encryption algorithm.

prefer_ctos_hmac: HMAC algorithm preference from the client to server. It defaults to SHA1_96.

prefer_stoc_hmac: HMAC algorithm preference from the server to client. It defaults to SHA1_96.

sha1: HMAC-SHA1 algorithm.

sha1_96: HMAC-SHA1_96 algorithm.

md5: HMAC-MD5 algorithm.

md5_96: HMAC-MD5-96 algorithm.

- *DES (Data Encryption Standard) is the standard algorithm for data encryption.*
- *AES (Advanced Encryption Standard) is the advanced encryption standard algorithm.*

Description

Use the **ssh2** command to enable the connection between SSH client and server, define key exchange algorithm preference, encryption algorithm preference and HMAC algorithm preference on the server and client.

Example

Log in to the remote SSH2.0 server with IP address 10.1.1.2 and adopt the default encryption algorithm.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ssh2 10.1.1.2
Username: 123
Trying 10.1.1.2 ...
Press CTRL+K to abort
Connected to 10.1.1.2 ...

The Server is not authenticated. Do you continue access it?(Y/N):y
Do you want to save the server’s public key?(Y/N):n
Enter password:

*******************************************************************
* Copyright (c) 2004-2007 3Com Corporation                        *
* Without the owner’s prior written consent,                      *
* no decompiling or reverse-switch fabricering shall be allowed.  *
*******************************************************************

<SW7750>
```

73 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 enable the secure FTP (SFTP) server.

Use the **undo sftp server enable** command to disable the SFTP server.

By default, the SFTP server is disabled.

Example # Enable the SFTP server.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] sftp server enable
```

ssh user service-type

Syntax **ssh user** *username* **service-type** { **stelnet** | **sftp** | **all** }

undo ssh user *username* **service-type**

View System view

Parameter *username*: Local user name or the user name defined on the remote RADIUS server, a string of 1 to 80 characters.

stelnet: Sets the service type to Telnet.

sftp: Sets the service type to SFTP.

all: Includes Telnet and SFTP two services types.

Description Use the **ssh user service-type** command to specify service type for a user.

Use the **undo ssh user service-type** command to restore the default service type for the SSH user in the system.

The default service type for the SSH user is **stelnet**.

Related command: **display ssh user-information**.

Example # Specify SFTP service for SSH user kk.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ssh user kk service-type sftp
```

74 SFTP CLIENT CONFIGURATION COMMANDS

bye

Syntax **bye**

View SFTP Client view

Parameter None

Description Use the **bye** command to terminate the connection to the remote SFTP server and return to system view.

This command has the same function as the **exit** and **quit** commands.

Example # Terminate the connection to the remote SFTP server.

```
sftp-client> bye
Bye
[SW7750]
```

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 remote SFTP server. If you did not specify the *remote-path* argument, the current path is displayed.

*You can use the **cd..** command to return to the upper level directory.*

You can use the **cd /** command to return to the root directory of the system.

Example # Change current path to new1.

```
sftp-client> cd new1
Received status:Success
Current Directory is:
/new1
```

cdup

Syntax **cdup**

View SFTP Client view

Parameter None

Description Use the **cdup** command to return the current path on the remote SFTP server to the upper directory.

Example # Return to the upper directory.

```
sftp-client> cdup
Received status: Success
Current Directory is:
/
```

delete

Syntax **delete** *remote-file*&<1-10>

View SFTP Client view

Parameter *remote-file*&<1-10>: Name of a file on the server. &<1-10> means that you can provide up to 10 filenames, which are separated by space.

Description Use the **delete** command to delete the specified file from the remote SFTP server.

This command has the same function as the **remove** command.

Example # Delete file test.txt from the server.

```
sftp-client> delete test.txt
The following files will be deleted:
/test.txt
Are you sure to delete it?(Y/N):y
This operation may take a long time.Please wait...
Received status: Success
File successfully Removed
```

dir

Syntax **dir** [**-a** | **-l**] [*remote-path*]

View SFTP Client view

Parameter **-a**: Displays the filenames or the folder names of the specified directory.

-l: Displays in list form detailed information of the files and folder of the specified directory.

remote-path: Name of the directory to be queried.

Description

Use the **dir** command to display the specified directory on the remote SFTP server.

With the **-a** and **-l** keyword not specified, the command displays detailed information of files and folder under the specified directory in a list form.

With the *remote-path* not specified, the command displays the file and folder information of the current working directory.

This command has the same function as the **ls** command.

Example

Display in a list form detailed file and folder information under the current working directory.

```
sftp-client> dir
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06: 52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08: 01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07: 39 pubkey1
-rwxrwxrwx   1 noone    nogroup       225 Sep 28 08: 28 pub1
drwxrwxrwx   1 noone    nogroup         0 Sep 28 08: 24 new1
drwxrwxrwx   1 noone    nogroup         0 Sep 28 08: 18 new2
-rwxrwxrwx   1 noone    nogroup       225 Sep 28 08: 30 pub2
Received status: End of file
Received status: Success
```

exit

Syntax

exit

View

SFTP Client view

Parameter

None

Description

Use the **exit** command to terminate the connection to the remote SFTP server and return to system view.

This command has the same function as the **bye** and **quit** commands.

Example

Terminate the connection to the remote SFTP server.

```
sftp-client> exit
Bye
[SW7750]
```

get

Syntax

get *remote-file* [*local-file*]

View SFTP Client view

Parameter *remote-file*: Name of the source file on the remote SFTP server.

local-file: Name assigned to the file to be saved at the local end.

Description Use the **get** command to download and save a file from a remote server.

If no local file name is specified, the name of the source file is used by default.

Example # Download file tt.bak and save it with name tt.txt.

```
sftp-client>get tt.bak tt.txt....
```

This operation may take a long time, please wait...

```
Remote  file:/tt.bak --->  Local file: tt.txt..
Received status: End of file
Received status: Success
Downloading file successfully ended
```

help

Syntax **help** [**all** | *command-name*]

View SFTP Client view

Parameter **all**: Displays a list of all commands.

command-name: Name of a command.

Description Use the **help** command to get the help information about the specified or all SFTP client commands.

With neither the argument nor the keyword specified, the command displays a list of all commands.

Example # Display the help information about the **get** command.

```
sftp-client> help get
get remote-path [local-path]  Download file.Default local-path is th
e same
                              with remote-path
```

ls

Syntax **ls** [**-a** | **-l**] [*remote-path*]

View SFTP Client view

Parameter **-a**: Displays the filenames or the folder names of the specified directory.

-l: Displays in list form detailed information of the files and folder of the specified directory

remote-path: Name of the directory to be queried.

Description Use the **ls** command to display file and folder information under a specified directory.

With the **-a** and **-l** keyword not specified, the command displays detailed information of files and folder under the specified directory in a list form.

With the *remote-path* not specified, the command displays the file and folder information of the current working directory.

This command functions as the **dir** command.

Example # Display in a list form detailed file and folder information under the current working directory.

```
sftp-client> ls
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey1
-rwxrwxrwx   1 noone    nogroup       225 Sep 28 08:28 pub1
drwxrwxrwx   1 noone    nogroup         0 Sep 28 08:24 new1
drwxrwxrwx   1 noone    nogroup         0 Sep 28 08:18 new2
-rwxrwxrwx   1 noone    nogroup       225 Sep 28 08:30 pub2
Received status: End of file
Received status: Success
```

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 hj on the remote SFTP server.

```
sftp-client>mkdir hj
Received status: Success
New directory created
```

put

Syntax **put** *local-file* [*remote-file*]

View SFTP Client view

Parameter *local-file*: Name of the source file at the local end.

remote-file: Name assigned to the file to be saved on the remote SFTP server.

Description Use the **put** command to upload a local file to the remote SFTP server.

If no name is specified for the file to be saved on the remote SFTP server, the name of the source file is used.

Example # Upload local file bb.txt to the remote SFTP server and save it with the name 1.txt.

```
sftp-client>put bb.txt 1.txt
```

This operation may take a long time, please wait...

```
Local file:bb.txt --->  Remote file: /1.txt
Received status: Success
Uploading file successfully ended
```

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
/
```

quit

Syntax **quit**

View SFTP Client view

Parameter None

Description Use the **quit** command to terminate the connection to the remote SFTP server and exit to system view.

This command has the same function as the **bye** and **exit** commands.

Example # Terminate the connection to the remote SFTP server.

```
sftp-client> quit
Bye
[SW7750]
```

remove

Syntax **remove** *remote-file*&<1-10>

View SFTP Client view

Parameter *remote-file*&<1-10>: Name of a file on an SFTP server. &<1-10> means that you can provide up to 10 filenames, which are separated by space.

Description Use the **remove** command to delete the specified file from the remote SFTP server.

This command has the same function as the **delete** command.

Example # Delete file temp.c from the server.

```
sftp-client> remove temp.c
The following files will be deleted:
/test2.txt
Are you sure to delete it?(Y/N):y
This operation may take a long time.Please wait...

Received status: Success
File successfully Removed
```

rename

Syntax **rename** *oldname newname*

View SFTP Client view

Parameter *oldname*: Original file name or directory name.

newname: New file name or directory name.

Description Use the **rename** command to rename a specified file or directory on an SFTP server.

Example # Rename file temp.bat on the SFTP server to temp.txt.

```
sftp-client> rename temp bat temp.txt
Received status: Success
File successfully renamed
```

rmdir

Syntax **rmdir** *remote-path*&<1-10>

View SFTP Client view

Parameter *remote-path*&<1-10>: Name of the directory on the remote SFTP server. &<1-10> means that you can provide up to 10 filenames that are separated by space.

Description Use the **rmdir** command to delete the specified directory from the remote SFTP server.

Example # Delete directory hello from the remote SFTP server.

```
sftp-client>rmdir hello
Received status: Success
Directory successfully removed
```

sftp

Syntax **sftp** { *host-ip* | *host-name* } [*port-num*] [**prefer_kex** { **dh_group1** | **dh_exchange_group** } | **prefer_ctos_cipher** { **des** | **aes128** } | **prefer_stoc_cipher** { **des** | **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: Name of the server, a string of 1 to 20 characters.

port-num: Port number of the server, in the range 0 to 65,535. The default port number is 22.

prefer_kex: Key exchange algorithm preference. Choose one of the two algorithms available.

dh_group1: Diffie-Hellman-group1-sha1 key exchange algorithm. It is the default key exchange algorithm.

dh_exchange_group: Diffie-Hellman-group-exchange-sha1 key exchange algorithm.

prefer_ctos_cipher: Encryption algorithm preference from the client to server. It defaults to AES128.

prefer_stoc_cipher: Encryption algorithm preference from the server to client. It defaults to AES128.

des: DES_cbc encryption algorithm.

aes128: AES_128 encryption algorithm.

prefer_ctos_hmac: HMAC algorithm preference from the client to server. It defaults to SHA1_96.

prefer_stoc_hmac: HMAC algorithm preference from the server to client. It defaults to SHA1_96.

sha1: HMAC-SHA1 algorithm.

sha1_96: HMAC-SHA1_96 algorithm.

md5: HMAC-MD5 algorithm.

md5_96: HMAC-MD5-96 algorithm.

Description

Use the **sftp** command to establish a connection to the SFTP server and enter SFTP Client view.

Example

Establish a connection to the SFTP server with IP address 10.1.1.2 and use the default encryption algorithms.

```
[SW7750]sftp 10.1.1.2
Input Username: kk
Trying 10.1.1.2 ...
Press CTRL+K to abort
Connected to 10.1.1.2 ...

The Server is not authenticated. Do you continue access it?(Y/N):y
Do you want to save the server’s public key?(Y/N):y
Enter password:

sftp-client>
```

75 FILE SYSTEM MANAGEMENT COMMANDS

You can provide the directory argument in the following two ways in this chapter:

- *In the form of [drive] [path]. In this case, the argument can be a string containing 1 to 64 characters.*
- *By specifying the name of a storage device, such as flash:/ and cf:/.*

You can provide the *file-url* argument in the following two ways in this chapter:

- *In the form of [drive] [path] [file name]. In this case, the argument can be a string containing 1 to 64 characters.*
- *By specifying the name of a storage device, such as flash:/ and cf:/.*

cd

Syntax **cd** *directory*

View User view

Parameter *directory*: Target directory.

Description Use the **cd** command to change the current directory or switch to the directory of a specified storage device.

Make sure the storage device is correctly installed if you want to switch to the storage device by using this command.

Example # Change the current directory to the one named test in the flash.

```
<SW7750> pwd
flash:
<SW7750> cd test
<SW7750> pwd
flash:/test
```

# Enter the root directory of the CF module.

```
<SW7750> cd cf:
<SW7750> pwd
cf:
```

copy

Syntax **copy** *fileurl-source fileurl-dest*

View User view

Parameter *fileurl-source*: Path name and file name of the source file in the Flash.

fileurl-dest: Path name and file name of the destination file in the Flash.

Description Use the **copy** command to copy a file to a specified path with specified name.

You can use this command to copy a file in the current directory to another directory or copy a file in a directory to the current directory. Make sure the path and the file identified by the *fileurl-source* argument exist when executing this command.

If the *fileurl-dest* argument identifies an existing file, the system prompts you for the confirmation to overwrite the existing file.

Example # Display the information about the files in the current directory.

```
<SW7750> dir
Directory of flash:/

   0   -rw-           4   Mar 09 2006 13:59:19   snmpboots
   1   -rw-  16215134    Apr 04 2006 16:36:20   S7750.app
   2   -rw-        553   Jan 21 2006 17:05:55   diaginfo.txt
   3   -rw-       3906   Apr 04 2006 17:23:54   config.cfg
   4   -rw-      11779   Apr 05 2006 10:19:48   test.txt

31877 KB total (15973 KB free)
```

# Copy the file named test.txt, with the destination file name being test2.bak.

```
<SW7750> copy test.txt test2.bak
Copy flash:/test.txt to flash:/test2.bak?[Y/N]:y
.....
%Copy file flash:/test.txt to flash:/test2.bak...Done.
```

# Display the information about the files in the current directory again.

```
<SW7750> dir
Directory of flash:/

   0   -rw-           4    Mar 09 2006 13:59:19   snmpboots
   1   -rw-  16215134    Apr 04 2006 16:36:20   S7750.app
   2   -rw-        553   Jan 21 2006 17:05:55   diaginfo.txt
   3   -rw-       3906   Apr 04 2006 17:23:54   config.cfg
   4   -rw-      11779   Apr 05 2006 10:19:48   test.txt
   5   -rw-      11779   Apr 05 2006 10:23:03   test2.bak

31877 KB total (15961 KB free)
```

delete

Syntax **delete** [**/unreserved**] *file-url*

View User view

Parameter **/unreserved**: Deletes a file completely.

file-url: Path name and file name of a file to be deleted.

Description Use the **delete** command to delete a specified file on a switch.

You can use the * character in this argument as a wildcard.

If you execute the **delete** command with the **/unreserved** keyword specified, the specified file is completely deleted. That is, the file cannot be restored. Otherwise, the specified file is moved to the recycle bin and can be restored using the **undelete** command.

To delete the files in the recycle bin, use the **reset recycle-bin** command.

CAUTION:

- *The **dir** command does not display the information about the files in the recycle bin.*
- *To display the information about all the files, including those in the recycle bin, use the **dir /all** command. Files in the recycle bin are marked by square brackets "[ ]".*
- *For files with the same name, the recycle bin can only hold the latest deleted one.*

Example # Delete the file named test.txt, assuming that it resides in the root directory of the flash.

```
<SW7750> delete flash:/test.txt
Delete flash:/test.txt?[Y/N]:y
...
%Deleted file flash:/test.txt.
```

dir

Syntax **dir** [**/all**] [*file-url*]

View User view

Parameter **/all**: Displays the information about all the files, including those in the recycle bin.

file-ur: Path and the name of a file whose information is to be displayed. You can use the * character as a wildcard in this argument. For example, the **dir** *.txt command displays the information about all the files with the extension of txt in the current directory.

Description

Use the **dir** command to display the information about the specified files or directories in the storage devices on a switch.

You can use the * character as a wildcard.

Example

# Display the information about the file named test2.bak.

```
<SW7750> dir test2.bak
Directory of flash:/

   0   -rw-     11779  Apr 05 2006 10:23:03   test2.bak

31877 KB total (15961 KB free)
```

# Display the information about all the files (including the files in the recycle bin) in directory flash:/hello/.

```
<SW7750> dir /all flash:/hello/
Directory of flash:/hello/

   0   -rw-     11779  Apr 05 2006 10:54:16   tt.txt
   1   -rw-     11779  Apr 05 2006 10:55:10   [tt2.txt]

31877 KB total (15935 KB free)
```

*In the output information of the **dir /all** command, the names of the files in the recycle bin are embraced in brackets.*

execute

Syntax

execute *file-url* [**echo on**]

View

System view

Parameter

File-url: Path and the name of the batch file to be executed. A batch file has an extension of .bat.

echo on: Displays the command line prompt character and command lines in the batch processing file when the batch processing file is executed.

Description

Use the **execute** command to execute a specified batch file.

This command executes command lines in the batch file in sequence.

If you do not specify the **echo on** parameter, the device does not display the prompt character and command lines by default.

Note that

- A batch file cannot contain any invisible character. Otherwise, the command quits the execution and this process is irretrievable.
- A syntax error in a batch file results in error messages.
- This command cannot be executed recursively.

Example # Execute the batch file named test.bat under the directory flash:/.

```
<SW7750> more test.bat
quit
mkdir testdir
copy test.txt test1.txt
move flash:/test1.txt flash:/testdir
cd testdir
dir

<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] execute test.bat
...
%Created dir flash:/testdir.

Copy flash:/test.txt to flash:/test1.txt?[Y/N]:y
....
%Copy file flash:/test.txt to flash:/test1.txt...Done.
Move flash:/test1.txt to flash:/testdir/test1.txt?[Y/N]:y
.
%Moved file flash:/test1.txt to flash:/testdir/test1.txt.
Directory of flash:/testdir/

   0   -rw-        13  Apr 27 2000 17:13:00   test1.txt

14605 KB total (1228 KB free)

<SW7750>
```

# Execute the test.bat batch processing file under the directory flash:/ and display the command line prompt character and command lines in the batch processing file

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] execute test.bat echo on
[SW7750]quit
<SW7750>mkdir testdir
% Created dir testdir

<SW7750>copy test.txt test1.txt
Copy flash:/test.txt to flash:/test1.txt ?[Y/N]:y
% Copied file flash:/test.txt to flash:/test1.txt
<SW7750>move flash:/test1.txt flash:/testdir
Move flash:/test1.txt to flash:/testdir/test1.txt ?[Y/N]:y
% Moved file flash:/test1.txt to flash:/testdir/test1.txt
<SW7750>cd testdir
<SW7750>dir
Directory of flash:/testdir/

-rwxrwxrwx   1 noone    nogroup        17  Jan 07 2001 04:45:42   test1.txt

16125952 bytes total (6568960 bytes free)
```

```
<SW7750>
```

file prompt

Syntax **file prompt** { **alert** | **quiet** }

View System view

Parameter **alert**: Prompts for confirmation before performing file-related operations that have potential risks.

quiet: Disables prompts for file-related operations.

Description Use the **file prompt** command to set the prompt mode for file-related operations.

By default, a switch prompts for confirmation before performing file-related operations that have potential risks.

If you set the prompt mode of the file-related operations to **quiet**, the switch does not prompt for confirmation before performing file-related operations. In this case, the system is more likely to operate improperly if irretrievable file-related operations are performed.

Example # Set the prompt mode to quiet for file-related operations.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] file prompt quiet
```

fixdisk

Syntax **fixdisk** *device*

View User view

Parameter *device*: Device name.

Description Use the **fixdisk** command to restore space on a storage device.

For unavailable memory spaces, you can use this command to restore them.

Example # Restore the memory space on the flash.

```
<SW7750> fixdisk flash:
Fixdisk flash: may take some time to complete.
%Fixdisk unit1>flash: completed.
```

format

Syntax **format** *device*

View User view

Parameter *device*: Device name.

Description Use the **format** command to format a storage device.

Note that all the files on a storage device get lost after the storage device is formatted. The operation is irretrievable. Moreover, the configuration files get lost if you format the flash.

Example # Format the flash.

```
<SW7750> 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*: Name of the directory to be created.

Description Use the **mkdir** command to create a directory in the current directory.

Note that the names of all the directories and files in the same directory must be unique.

Note that the specified directory must exist before you use the above command to create a sub-directory. For example, to create the sub-directory flash:/test/mytest, the test directory must exist.

Example # Create a directory in the current directory, with the name being dd.

```
<SW7750> mkdir dd
...
% Created dir flash:/dd
```

more

Syntax **more** *file-url*

View User view

Parameter *file-url*: Path and file name.

Description Use the **more** command to display the content of a specified file.

Currently, the content of a file can only be displayed in text.

Example # Display the content of the file named test.txt.

```
<SW7750> more test.txt
The file is for test only.
```

move

Syntax **move** *fileurl-source fileurl-dest*

View User view

Parameter *fileurl-source*: Path and file name of the source file.

fileurl-dest: Path and file name of the target file.

Description Use the **move** command to move a file to a specified directory. You can also assign a new name for the file.

If the target file name is the name of an existing file, the system prompts you for the confirmation to overwrite the existing file.

Example # Display the information about the files in flash:/ and flash:/hello.

```
<SW7750> dir
Directory of flash:/

   0   -rw-         4  Mar 09 2006 13:59:19   snmpboots
   1   -rw-  16215134  Apr 04 2006 16:36:20   S7750.app
   2   -rw-       553  Jan 21 2006 17:05:55   diaginfo.txt
   3   -rw-      3906  Apr 04 2006 17:23:54   config.cfg
   4   drw-         -  Apr 05 2006 10:53:23   hello
   5   drw-         -  Apr 10 2005 19:07:59   dd
   6   -rw-     11779  Apr 05 2006 10:23:03   test2.bak
   7   drw-         -  Jan 25 2005 11:08:59   backup

31877 KB total (15935 KB free)
<SW7750> dir flash:/hello/
Directory of flash:/hello/

   0   -rw-     11779  Apr 05 2006 10:54:16   tt.txt
   1   -rw-     11779  Apr 05 2006 11:12:52   tt2.txt

31877 KB total (15935 KB free)
```

# Move the file named tt.txt from flash:/ to flash:/.

```
<SW7750>move flash:/hello/tt.txt flash:/tt.txt
Move flash:/hello/tt.txt to flash:/tt.txt?[Y/N]:y
...
%Moved file flash:/hello/tt.txt to flash:/tt.txt.
```

# Display the information about the files in flash:/ and flash:/hello again.

```
<SW7750> dir
Directory of flash:/

   0   -rw-         4  Mar 09 2006 13:59:19   snmpboots
   1   -rw-  16215134  Apr 04 2006 16:36:20   S7750.app
   2   -rw-       553  Jan 21 2006 17:05:55   diaginfo.txt
   3   -rw-      3906  Apr 04 2006 17:23:54   config.cfg
   4   drw-         -  Apr 05 2006 10:53:23   hello
   5   drw-         -  Apr 10 2005 19:07:59   dd
   6   -rw-     11779  Apr 05 2006 10:23:03   test2.bak
   7   -rw-     11779  Apr 05 2006 11:30:13   tt.txt
   8   drw-         -  Jan 25 2005 11:08:59   backup

31877 KB total (15935 KB free)
<SW7750> dir flash:/hello/
Directory of flash:/hello/

   0   -rw-     11779  Apr 05 2006 11:12:52   tt2.txt

31877 KB total (15934 KB free)
```

pwd

Syntax **pwd**

View User view

Parameter None

Description Use the **pwd** command to display the current path.

Example # Display the current path.

```
<SW7750> pwd
flash:
```

rename

Syntax **rename** *fileurl-source fileurl-dest*

View User view

Parameter *fileurl-source*: File name of the file to be renamed.

fileurl-dest: Target file name.

Description Use the **rename** command to rename a file.

If the target file name or directory name is the same with any existing file name or directory name, you will fail to rename the file.

Example # Display the information about the files in the current directory.

```
<SW7750> dir
Directory of flash:/

   0   -rw-          4   Mar 09 2006 13:59:19   snmpboots
   1   -rw-  16215134    Apr 04 2006 16:36:20   S7750.app
   2   -rw-        553   Jan 21 2006 17:05:55   diaginfo.txt
   3   -rw-       3906   Apr 04 2006 17:23:54   config.cfg
   4   drw-          -   Apr 05 2006 10:53:23   hello
   5   drw-          -   Apr 10 2005 19:07:59   dd
   6   -rw-      11779   Apr 05 2006 10:23:03   test2.bak
   7   -rw-      11779   Apr 05 2006 11:30:13   tt.txt
   8   drw-           -  Jan 25 2005 11:08:59   backup

31877 KB total (15935 KB free)
```

# Rename the file named tt.txt as tt.bak.

```
<SW7750> rename tt.txt tt.bak
Rename flash:/tt.txt to flash:/tt.bak?[Y/N]:y
...
%Renamed file flash:/tt.txt to flash:/tt.bak.
```

# Display the information about the files in the current directory again.

```
<SW7750>dir
Directory of flash:/

   0   -rw-          4   Mar 09 2006 13:59:19   snmpboots
   1   -rw-  16215134    Apr 04 2006 16:36:20   S7750.app
   2   -rw-        553   Jan 21 2006 17:05:55   diaginfo.txt
   3   -rw-       3906   Apr 04 2006 17:23:54   config.cfg
   4   drw-          -   Apr 05 2006 10:53:23   hello
   5   drw-          -   Apr 10 2005 19:07:59   dd
   6   -rw-      11779   Apr 05 2006 10:23:03   test2.bak
   7   -rw-      11779   Apr 05 2006 11:36:06   tt.bak
   8   drw-           -  Jan 25 2005 11:08:59   backup

31877 KB total (15934 KB free)
```

reset recycle-bin

Syntax **reset recycle-bin** [*file-url*] [/**force**]

View User view

Parameter *file-url*: Path and the file name of the file to be deleted.

/force: Does not prompt for the confirmation before deleting all the files in the recycle bin.

Description Use the **reset recycle-bin** command to clear a specified file or all the files in the recycle bin.

You can use the * as a wild module in the *file-url* argument.

The files deleted using the **delete** command are actually moved to the recycle bin. To delete them completely, you can use the **reset recycle-bin** command.

Example # Delete the file named test.txt in the recycle bin.

```
<SW7750> reset recycle-bin flash:/test.txt
Clear flash:/test.txt ?[Y/N]:y
Clear file from flash will take long time if needed...
...
%Cleared file flash:/test.txt.
```

rmdir

Syntax **rmdir** *directory*

View User view

Parameter *directory*: Name of a directory.

Description Use the **rmdir** command to delete a directory.

As only empty directories can be deleted, you need to clear a directory before deleting it.

Example # Delete the directory named hello.

```
<SW7750> rmdir hello
The files in the recycle-bin under this directory will be deleted pe
rmanently, Remove flash:/hello?[Y/N]:y
...
%Removed directory flash:/hello.
```

umount

Syntax **umount cf:**

View User view

Parameter None

Description Use the **umount cf:** command to disable the CF module. After you execute this command, you need to re-install the CF module to use it again.

This command can be executed successfully only when the CF module is correctly installed.

Example # Disable the CF module.

```
<SW7750>umount cf:
%Umount cf: succeed.Current directory is changed to flash:.
```

# Verify the above operation by displaying the information about the CF module.

```
<SW7750> dir cf:
% Wrong device  "cf:"
```

undelete

Syntax **undelete** *file-url*

View User view

Parameter *file-url*: Path and the file name of a file in the recycle bin.

Description Use the **undelete** command to restore a deleted file in the recycle bin.

If the name of the file to be restored is the same as that of an existing file, the system prompts you for the confirmation to overwrite the latter.

Example # Restore the deleted file with its path and file name being flash:/hello/tt2.txt.

```
<SW7750> undelete flash:/hello/tt2.txt
Undelete flash:/hello/tt2.txt?[Y/N]:y
...
%Undeleted file flash:/hello/tt2.txt.
```

76 BIMS CONFIGURATION COMMANDS

bims boot request

Syntax **bims boot request**

undo bims boot request

View System view

Description Use the **bims boot request** command to enable the BIMS device to access the branch intelligent management system (BIMS) center at startup.

Use the **undo bims boot request** command to disable the BIMS device to access the BIMS center automatically at startup.

If a user forcibly disables the BIMS device to access the BIMS center at startup, when the device is restarted, it will not send messages to BIMS server. Therefore BIMS center cannot detect that the device is restarted and the waiting for restart message will be displayed on the interface.

By default, the BIMS device accesses the BIMS center immediately at startup if the BIMS is enabled on the device.

Related command: **bims request**.

Example # Configure the BIMS device to access the BIMS center at startup.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] bims boot request
```

bims device-id

Syntax **bims device-id** *string*

undo bims device-id

View System view

Parameter *string*: Unique identifier of the BIMS device, up to 30 characters, among which the characters "0 to 9", "a to z", "A to Z", "-", "_", "@", and "." can be configured.

Description Use the **bims device-id** command to configure the unique identifier of the BIMS device at the BIMS center.

Use the **undo bims device-id** command to delete the identifier.

By default, no identifier is assigned to the BIMS device.

Related command: **bims interval**.

Example # Set the unique identifier of the BIMS device at the BIMS center to R2102311042W033000076.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] bims device-id R2102311042W033000076
```

bims enable

Syntax **bims enable**

undo bims enable

View System view

Description Use the **bims enable** command to enable BIMS.

Use the **undo bims enable** command to disable BIMS.

By default, BIMS is not enabled.

Example # Enable BIMS.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] bims enable
bims is enable
```

bims interval

Syntax **bims interval** *number*

undo bims interval

View System view

Parameter *number*: Interval for accessing the BIMS center, in the range 10 to 10080 minutes.

Description Use the **bims interval** command to configure the interval for accessing the BIMS center. When the interval is set to 0, the BIMS device does not access the BIMS center regularly.

Use the **undo bims interval** command to delete the interval specified for accessing the BIMS center.

By default, no BIMS center accessing interval is set.

Related command:

bims specify-time.

Example

Set the interval for accessing the BIMS center to 120 minutes.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] bims interval 120
```

bims ip address

Syntax

bims ip address *ip-address* [**port** *portnumber*]

undo bims ip address

View

System view

Parameter

ip-address: IP address of the BIMS center.

portnumber: Port number used by the BIMS center.

Description

Use the **bims ip address** command to configure the IP address and port number of the BIMS center.

Use the **undo bims ip address** command to delete the configuration.

By default, the IP address of the BIMS center is not configured. If you do not specify a port number when configuring the IP address of the BIMS center, port 80 applies by default.

CAUTION: *The port number configured on the BIMS device must be consistent with that configured on the BIMS center.*

Related command:

bims interval.

Example

Set the IP address and port number of the BIMS center to 129.33.72.66 and 81 respectively.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] bims ip address 129.33.72.66 port 81
```

bims request

Syntax

bims request

View System view

Description Use the **bims request** command to have the BIMS device access the BIMS center.

Related command: **bims boot request**.

Example # Access the BIMS center.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] bims request
```

bims sharekey

Syntax **bims sharekey** { **simple** | **cipher** } *sharekey*

undo bims sharekey

View System view

Parameter *sharekey*: Shared Key between the BIMS device and the BIMS center. It is 16 bits long.

simple: Displays the shared key in clear text.

cipher: Displays the shared key in ciphertext. Two key configuration modes are available:

- Clear text: A self-defined string of 1 to 16 characters. It is automatically generated by the system. For example, if you enter "123", the system automatically generate the key "7-CZB#/YX]KQ=^Q'MAF4<1!!".
- Cipher text: A string of 24 characters. It is directly entered by the user, for example, "7-CZB#/YX]KQ=^Q'MAF4<1!!".

The key in clear text is used regardless of the configuration mode selected. Thus, you are recommended to use the clear text mode for configuration.

Description Use the **bims sharekey** command to configure the shared key between the BIMS device and the BIMS center.

Use the **undo bims sharekey** command to delete the shared key.

By default, no shared key is configured between the BIMS device and the BIMS center.

Related command: **bims ip address**.

Example # Set the shared key between the BIMS device and the BIMS center to 1234567812345678. It is to be displayed in clear text.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] bims sharekey simple 1234567812345678
```

bims source ip-address

Syntax **bims source ip-address** *ip-address*

undo bims source ip-address

View System view

Parameter *ip-address*: Source IP address in the packets sent by the BIMS device.

Description Use the **bims source ip-address** command to configure a source IP address for the packets sent by the BIMS device. It can be the IP address of a port on the device.

Use the **undo bims source ip-address** command to delete the source IP address configured for the BIMS device.

By default, no source IP address is configured for the packets sent by the BIMS device. The BIMS device and BIMS center use the source IP address configured for communication.

Example # On the BIMS device set the source IP address to 10.153.72.66.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] bims source ip-address 10.153.72.66
```

bims specify-time

Syntax **bims specify-time** *start-time* [[*end-time*] **period** *numberdays*]

undo bims specify-time

View System view

Parameter *start-time*: Start time of a period during which the device accesses the BIMS center.

end-time: End time of a period during which the device accesses the BIMS center.

Both *start-time* and *end-time* are in the format of *hh:mm yyyy/mm/dd.*

hh:mm yyyy/mm/dd: The first and second *hh:mm yyyy/mm/dd* arguments respectively specify the start time and end time for accessing the BIMS center. If only the first argument is specified, the BIMS device accesses the BIMS center at that time once.

numberdays: Period in days for accessing the BIMS center.

Description

Use the **bims specify-time** command to configure the BIMS device to access the BIMS center at the specified time and if desired, configure the device to access the BIMS center at regular intervals from then on during a specified period.

Use the **undo bims specify-time** command to delete the setting.

The precision of the timer is one minute. The device will access BIMS center in one minute after the specified time comes.

By default, the access time is not specified.

Related command: **bims interval**.

Example

Configure the router to access the BIMS center at 01:01 on December 12, 2004, and from then on, to access the BIMS center at seven-day intervals until December 12, 2005 01:01. If the current time hasn’t reached the specified start time, after the above configuration, the router will access the BIMS center at 01:01 on December 12, 2004 and next time at 01:01 on December 19, 2004 after a 7*24 hours interval.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] bims specify-time 01:01 2004/12/12 01:01 2005/12/12 period 7
```

77 INFORMATION CENTER 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: Channel name. By default, the name of channel 0 to channel 9 is (in turn) **console**, **monitor**, **loghost**, **trapbuffer**, **logbuffer**, **snmpagent**, **channel6**, **channel7**, **channel8**, **channel9**.

Description Use the **display channel** command to display the settings of an information channel.

If no argument is provided, the settings of all channels are displayed.

Example # Show details about the information channel 0.

```
<SW7750> display channel 0
channel number:0, channel name:console
MODU_ID   NAME     ENABLE   LOG_LEVEL     ENABLE   TRAP_LEVEL    ENABLE    DEBUG_LEVEL
ffff0000 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 display the operation status of information center, the configuration of information channels, and the format of time stamp.

If the information records in the current log/trap buffer are less than the buffer size specified by a user, this command displays the actual log/trap information.

Related command: **info-center enable**, **info-center loghost**, **info-center logbuffer**, **info-center console channel**, **info-center monitor channel**, **info-center trapbuffer**, **info-center snmp channel**, and **info-center timestamp**.

Example # Display information about information center.

```
<SW7750> 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:2, channel number:4, channel name:logbuffer
        dropped messages:0, overwritten 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, overwritten messages:0
Information timestamp setting:
        log - date, trap - date, debug - boot
```

Table 178 Field descriptions of the **display info-center** command

Field	Description
Information Center:	Information center is enabled.
Log host:	Information about the log host, including its IP address, name and number of information channel, language and level of the log host
Console:	Information about the console port, including name and channel of its information channel
Monitor:	Information about the monitor port, including name and channel of its information channel
SNMP Agent:	Information about SNMP Agent, including name and number of its information channel
Log buffer:	Information about the log buffer, including its state (enabled or disabled), its maximum size, current size, current messages, information channel name and number, dropped messages, and overwritten messages
Trap buffer:	Information about the trap buffer, including its state (enabled or disabled), maximum size, current size, current messages, channel number and name, dropped messages, and overwritten messages
Information timestamp setting	Information about time stamp setting, describing log information, trap information, and the time stamp format of the debugging information

display logbuffer

Syntax **display logbuffer** [**level** *severity* | **size** *buffersize*]* [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View Any view

Parameter

level *severity*: Specifies an information severity level. The *severity* argument ranges from 1 to 8.

Table 179 Severity definitions made on the information center

Severity	Value	Description
emergencies	1	Emergent errors
alerts	2	Errors that need to be corrected immediately
critical	3	Critical errors
errors	4	Errors that need to be considered but are not critical
warnings	5	Warnings that prompt possible errors
notifications	6	Information that needs to be noticed
informational	7	Normal prompting information
debugging	8	Debugging information

size *buffersize*: Specifies the size of the log buffer (number of messages the log buffer holds) you want to display. The *buffersize* argument ranges from 1 to 1024 and defaults to 256.

|: Filters output log information with a regular expression.

begin: Displays the log information beginning with the specified characters.

exclude: Displays the log information excluding the specified characters.

include: Displays the log information including the specified characters.

regular-expression: Regular expression.

Table 180 Special characters in regular expression.

Special characters	Description	Usage restrictions
_	The underscore, functions similar to a wildcard, can represent the following characters: ^ -- Caret $ -- Dollar sign | -- Alternation sign [-- Left bracket , -- Comma ( ) -- Left/right parenthesis { } -- Left/right brace] -- Right bracket Space Start/stop character	If the first character of a regular expression is not '_', the number of '_' used in the expression is not restricted, but is restricted by the length of command line. If the first character is '_', the number of consecutive "_" should less than 5; If the '_' characters are not consecutive, the output information will be filtered by the first group of '_', and the remain '_' characters will not be processed.
(	The left parenthesis, the push-onto-the-stack flag in programming	You are recommended not to use this character to establish a regular expression.

Description

Use the **display logbuffer** command to display the state of logbuffer and the information recorded in logbuffer.

Example # Display the state of logbuffer and the log information recorded in the logbuffer.

```
<SW7750> 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
```

...... (Omitted)

display logbuffer summary

Syntax **display logbuffer summary** [**level** *severity*]

View Any view

Parameter **Level** *severity*: Specifies an information severity level. The *severity* argument ranges from 1 to 8.

Description Use the **display logbuffer summary** command to display the statistics of the log buffer.

Example # Display summary information recorded in logbuffer.

```
<SW7750> display logbuffer summary
SLOT EMERG ALERT  CRIT ERROR  WARN NOTIF  INFO DEBUG
    0     0     0     0     0     0     0     0     0
    1     0     0     0     0     0     0     0     0
```

display trapbuffer

Syntax **display trapbuffer** [**size** *buffersize*]

View Any view

Parameter **size** *buffersize*: Specifies the size of the trap buffer (number of messages the buffer holds) you want to display. The *buffersize* argument ranges from 1 to 1024 and defaults to 256.

Description Use the **display trapbuffer** command to display the status of the trap buffer and the trap information recorded in the trap buffer.

Executing the command with the **size** *buffersize* parameters will display the latest trap records.

Example # Display the trapbuffer status and the trap information in trapbuffer.

```
<SW7750> display trapbuffer
Trapping Buffer Configuration and contents:enabled
allowed max buffer size : 1024
actual buffer size : 256
channel number : 3 , channel name : trapbuffer
dropped messages : 0
overwritten messages : 0
current messages : 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/BOARD 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/BOARD STATE CHANGE TO NORMAL:
 Trap 1.3.6.1.4.1.2011.2.23.1.12.1.11: frameIndex is 0, slotIndex 0.
```

...(Omitted)

info-center channel

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: Channel name, a string up to 30 characters, excluding "-", "/" or " ". And the first character must not be a number.

Description Use **info-center channel name** command to name a channel specified by the *channel-number* as *channel-name*.

Use **undo info-center channel** command to restore the default channel name.

By default, the name of channel 0 to channel 9 is (in turn) **console**, **monitor**, **loghost**, **trapbuffer**, **logbuffer**, **snmpagent**, **channel6**, **channel7**, **channel8**, **channel9**.

Note that the channel names must not be the same with each other.

Example # Name the channel 0 as execconsole.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] 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: Channel name, by default, the name of channel 0 to channel 9 is (in turn) **console**, **monitor**, **loghost**, **trapbuffer**, **logbuffer**, **snmpagent**, **channel6**, **channel7**, **channel8**, **channel9**.

Description Use the **info-center console channel** command to configure the channel through which the log information is output to the console.

Use the **undo info-center console channel** command to restore the default channel through which the log information is output to the console.

By default, Ethernet switches output log information to the console.

This command takes effect only after the information center function is enabled.

Related command: **info-center enable**, **display info-center**.

Example # Configure to output log information to the console through channel 7.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] info-center console channel 7
```

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 information center function.

Use the **info-center enable** command to disable the information center function.

The switch can output system information to the log host, the console, and other destinations only when the information center function is enabled.

By default, the information center function is enabled.

Related command: **display info-center**, **info-center loghost**, **info-center logbuffer**, **info-center console channel**, **info-center monitor channel**, **info-center trapbuffer**, **info-center snmp channel**.

Example # Enable the information center function.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] info-center enable
% information center is enabled
```

info-center logbuffer

Syntax **info-center logbuffer** [**channel** { *channel-number* | *channel-name* } | **size** *buffersize*]* [**| exclude** *regular-expression*]

undo info-center logbuffer [**channel** | **size** | **| exclude** *regular-expression*]

View System view

Parameter **channel**: Configure the channel to output information to buffer.

channel-number: Channel number, ranging from 0 to 9, that is, system has ten channels.

channel-name: Channel name, by default, the name of channel 0 to channel 9 is (in turn) **console**, **monitor**, **loghost**, **trapbuffer**, **logbuffer**, **snmpagent**, **channel6**, **channel7**, **channel8**, **channel9**.

size *buffersize*: Specifies the size of the log buffer (number of messages the buffer holds). The *buffersize* argument ranges from 0 to 1024 and defaults to 512.

|: Filters output log information with a regular expression.

exclude: Displays the log information excluding the specified characters.

regular-expression: Regular expression.

For special characters used in the regular expression, refer to Table 180.

Description Use the **info**-**center logbuffer** command to configure information output to the log buffer.

Use the **undo info**-**center logbuffer** command to cancel the configuration.

By default, the system outputs information to the log buffer, which can hold 512 records.

This command takes effect only when the information center function is enabled for the system.

Related command: **info-center enable** and **display info-center**.

Example # Send log information to log buffer and sets the size of log buffer to 50.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] info-center logbuffer size 50
```

info-center loghost

Syntax **info-center loghost** *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: Channel name, by default, the name of channel 0 to channel 9 is (in turn) **console**, **monitor**, **loghost**, **trapbuffer**, **logbuffer**, **snmpagent**, **channel6**, **channel7**, **channel8**, **channel9**.

facility *local-number*: Specifies the logging facility of the log host, which ranges from local0 to local7, with the corresponding value ranging from 16 to 23; and defaults to local7, with the corresponding value being 23.

language: Sets the logging language.

chinese,**english**: Switches language used in log file between Chinese and English.

Description Use the **info-center loghost** command to enable information output to loghost by setting the IP address of the loghost.

Use the **undo info-center loghost** command to cancel the configuration.

By default, the system does not output information to loghost.

This command works only when the information center function is enabled for the system.

*Be sure to set the correct IP address in the **info-center loghost** command. A loopback IP address will cause an error message prompting invalid address.*

Related command: **info-center enable** and **display info-center**.

Example # Configure the Ethernet switch to send information to the workstation Unix whose IP address is 202.38.160.1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] 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 type.

interface-number: Interface number.

Description Use the **info**-**center loghost source** command to configure the source interface through which information is sent to the loghost.

Use the **undo info**-**center loghost source** command to cancel the source interface configuration.

Related command: **info-center enable** and **display info-center**.

Example # Specify source address of the packets sent to loghost as the address of the VLAN 1 interface.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] 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, by default, the name of channel 0 to channel 9 is (in turn) **console**, **monitor**, **loghost**, **trapbuffer**, **logbuffer**, **snmpagent**, **channel6**, **channel7**, **channel8**, **channel9**.

Description Use the **info**-**center monitor channel** command to set the channel through which information is output to user terminals.

Use the **undo info**-**center monitor channel** command to restore the default channel through which the information is output to user terminals.

By default, the system outputs information to user terminal.

This command takes effect only when the information center function is enabled.

Related command: **info-center enable** and **display info-center**.

Example # Configure channel 0 to output log information to user terminal.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] 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.

channel-name: Channel name, by default, the name of channel 0 to channel 9 is (in turn) **console**, **monitor**, **loghost**, **trapbuffer**, **logbuffer**, **snmpagent**, **channel6**, **channel7**, **channel8**, **channel9**.

Description Use the **info**-**center snmp channel** command to set the channel through which information is output to the SNMP.

Use the **undo info**-**center snmp channel** command to restore the default channel through which information is output to the SNMP.

By default, the system outputs information to SNMP Agent through channel 5.

Related command: **snmp-agent** and **display info-center**.

Example # Configure the system to output information to the SNMP agent through channel 6.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] info-center snmp channel 6
```

info-center source

Syntax **info-center source** { *module-name* | **default** } **channel** { *channel-number* | *channel-name* } [**debug** { **level** *severity* | **state** *state* }* | **log** { **level** *severity* | **state** *state* }* | **trap** { **level** *severity* | **state** *state* }*]*

undo info-center source { *module-name* | **default** } **channel** { *channel-number* | *channel-name* }

View System view

Parameter *modu-name*: Module name. Refer to Table 181 for the detail.

Table 181 Modules generating the information

Module name	Description
8021X	802.1x module
ACCOUNT	L3+ real time accounting module
ACL	Access control list module
ADBM	Address base module
AM_USERB	Access management module
ARP	Address resolution protocol module
BGP	Border gateway protocol module
CFAX	Configuration agent module
CFM	Configuration file management module
CLNP	Connectionless network protocol module
CLNSECHO	Connectionless network protocol echo module
CLST	Cluster management module
CMD	Command line module
DEV	Device management module
DHCP	Dynamic host configuration protocol module
DHCPS	DHCP server module
DHCPSNP	DHCP snooping module
DIAG	Diagnosis module
DLDP	Device link detection protocol module
DNS	Domain name system module
ENTEXMIB	Entity extended MIB module
ENTITY	ENTITY module
ESIS	End system to intermediate system routing protocol module
ETH	Ethernet module
FIB	Forwarding information base module
FTPS	FTP server module
HA	High availability module
HABP	3Com authentication bypass protocol module
HTTPD	HTTP server module
HWCM	3Com Configuration Management proprietary MIB module

Table 181 Modules generating the information

Module name	Description
HWP	NQA module
IFNET	Interface management module
IGSP	IGMP snooping module
IP	Internet protocol module
IPX	IPX protocol module
ISIS	Intermediate system-to-intermediate system intra-domain routing information exchange protocol module
L2INF	Layer 2 interface management module
LACL	Lanswitch access control list module
LARP	Address resolution protocol module
LETH	Ethernet debugging module
LQOS	Lanswitch quality of service module
LS	Local server module
MIX	Dual main control network management module
MODEM	MODEM module
MPM	Multicast port management module
MSDP	Multicast source discovery protocol module
MSTP	Multiple spanning tree protocol module
NAT	Network address translation module
NDP	Neighbor discovery protocol module
NETSTREA	Traffic statistic module
NTDP	Network topology discovery protocol module
NTP	Network time protocol module
OSPF	Open shortest path first module
RDS	Radius module
RM	Routing management module
RMON	Remote monitor module
RMX	IPX routing module
RRPP	Rapid ring protection protocol module
RSA	Revest, Shamir and Adleman encryption module
RTA	L3+ plug-in module traffic accounting module
RTPRO	Routing protocol module
SC	Server control module
SHELL	User interface module
SNMP	Simple network management protocol module
SOCKET	Socket module
SSH	Secure shell module
SYSM	System management module
SYSMIB	System MIB module
TAC	Terminal access controller module
TELNET	Telnet module
TFTPC	TFTP client module

Table 181 Modules generating the information

Module name	Description
TUNNEL	Packets transparent transmission module
UDPH	UDP helper module
USERLOG	User log module
VFS	Virtual file system module
VLAN	Virtual local area network module
VRRP	VRRP (virtual router redundancy protocol) module
VTY	VTY (virtual type terminal) module
default	Default settings of all modules

default: Defaults the settings of all modules.

channel-number: Number of information channel to be used.

channel-name: Channel name, by default, the name of channel 0 to channel 9 is (in turn) **console**, **monitor**, **loghost**, **trapbuffer**, **logbuffer**, **snmpagent**, **channel6**, **channel7**, **channel8**, **channel9**.

log: Specifies to output log information.

trap: Specifies to output trap information.

debug: Specifies to output debugging information.

level: Specifies an information severity level.

severity: Information severity level. The information below this level will not be output.

Information at different levels is as follows:

emergencies: Level 1 information, which cannot be used by the system.

alerts: Level 2 information, to be reacted immediately.

critical: Level 3 information, critical information.

errors: Level 4 information, error information.

warnings: level 5 information, warning information.

notifications: Level 6 information, showed normally and important.

informational: Level 7 information, notice to be recorded.

debugging: Level 8 information, generated during the debugging progress.

The default information level of each channel is shown in the following table.

Table 182 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
Channel6	debugging	debugging	debugging
Channel7	debugging	debugging	debugging
Channel8	debugging	debugging	debugging
Channel9	debugging	debugging	debugging

The default information state of each channel is shown in the following table.

Table 183 Default information switch state of each channel

Channel	Log information switch	Trap information switch	Debug information switch
Console	Enable	Enable	Enable
Terminal	Enable	Enable	Enable
Log host	Enable	Enable	Disable
Trapbuffer	Disable	Enable	Disable
Logbuffer	Enable	Disable	Disable
SNMPagent	Disable	Enable	Disable
Channel6	Enable	Enable	Disable
Channel7	Enable	Enable	Disable
Channel8	Enable	Enable	Disable
Channel9	Enable	Enable	Disable

state: Sets the information state.

state: Can be **on** or **off**.

Description

Use the **info-center source** command to specify the information source in the information center and the output direction.

Use the **undo info-center source** command to cancel the configuration of information source and output direction.

This command can be used for filtering of log, trap or debugging information. For example, it can control information output from the IP module to any direction. You can configure to output information with severity higher than "warning" to the log host, and information with severity higher than "informational" to the log buffer. You can also configure to output trap information to the log host at the same time.

The **info-center source** command determines the output direction according to channel name or channel number. Each output direction is assigned with a default information channel at present, as shown in the following table.

Table 184 Information channel in each output direction by default

Output direction	Information channel name
Console	console
Monitor	monitor
Info-center loghost	loghost
Log buffer	logbuffer
Trap buffer	trapbuffer
Snmpagent	snmpagent

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 # Enable the log information of VLAN module in SNMP channel and allow the output of the information with a level higher than emergencies.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] 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**: Specifies log information.

trap: Specifies trap information.

debugging: Specifies debugging information.

boot: Specifies to adopt the time elapsed since system boot, which is in the format of "xxxxxx.yyyyyy", where xxxxxx is the high 32 bits and yyyyyy the low 32 bits of the elapsed milliseconds.

date: Specifies to adopt the current system date and time, which is in format "yyyy/mm/dd-hh:mm:ss:ms" for Chinese environment and "Mmm dd hh:mm:ss:ms yyyy" for English environment.

none: Specifies not to include time stamp in specified output information.

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 restore the default settings.

By default, the **date** time stamp is adopted for all types of information.

Example # Configure the debugging information timestamp format as boot.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] info-center timestamp debugging boot
```

info-center trapbuffer

Syntax **info-center trapbuffer** [**channel** { *channel-number* | *channel-name* } | **size** *buffersize*]*

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). This argument ranges from 0 to 1,024 and defaults to 256.

channel: Sets the channel through which information is sent to the trap buffer.

channel-number: Channel number, ranging from 0 to 9, that is, the system has ten channels.

channel-name: Channel name. By default, the name of channel 0 to channel 9 is (in turn) **console**, **monitor**, **loghost**, **trapbuffer**, **logbuffer**, **snmpagent**, **channel6**, **channel7**, **channel8**, **channel9**.

Description Use the **info-center trapbuffer** command to enable information output to the trap buffer.

Use the **undo info-center trapbuffer** command to disable information output to the trap buffer.

This command takes effect only after the information center function is enabled.

Related command: **info-center enable** and **display info-center**.

Example # Send information to the trap buffer and sets the size of buffer to 30.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750] 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.

```
<SW7750> 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.

```
<SW7750> 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 displaying function is disabled.

Related commands: "System Debugging Commands" on page 1027.

Example # Enable the terminal display debugging.

```
<SW7750> terminal debugging
% Current terminal debugging is on
```

terminal logging

Syntax **terminal logging**

undo terminal logging

View User view

Parameter none

Description Use the **terminal logging** command to enable terminal log information display.

Use the **undo terminal logging** command to disable terminal log information display.

By default, this function is enabled for console users and terminal users.

Example # Disable the terminal log display.

```
<SW7750> undo terminal logging
% Current terminal logging is off
```

terminal monitor

Syntax **terminal monitor**

undo terminal monitor

View User view

Parameter none

Description Use the **terminal monitor** command to enable the debugging/log/trap information terminal display function.

Use the **undo terminal monitor** command to disable these functions.

By default, these functions are enabled for console users and terminal users.

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 / undo terminal logging** and **terminal trapping / undo terminal trapping** respectively to enable or disable the corresponding functions.

Example # Disable the terminal monitor.

```
<SW7750> undo terminal monitor
% Current terminal monitor is off
```

terminal trapping

Syntax **terminal trapping**

undo terminal trapping

View User view

Parameter None

Description Use the **terminal trapping** command to enable terminal trap information display.

Use the **undo terminal trapping** command to disable this function.

By default, this function is enabled.

Example # Enable trap information display.

```
<SW7750> terminal trapping
% Current terminal trapping is on
```

78 FTP Server Configuration Commands

display ftp-server

Syntax **display ftp-server**

View Any view

Parameter None

Description Use the **display ftp-server** command to display the FTP server-related settings of a switch when it operates as an FTP server.

You can use this command to verify FTP server-related configurations.

Example # Display the FTP server-related settings of the switch (assuming that the switch is operating as an FTP server).

```
<SW7750> display ftp-server
   FTP server is running
   Max user number       1
   User count  0
   Timeout value(in minute)       30
```

Table 185 Field descriptions of the **display ftp-server** command

Field	Description
FTP server is running	The FTP server is started
Max user number 1	The FTP server can accommodate up to one user.
User count	The current login user number
Timeout value (in minute)	The connection idle time

display ftp-user

Syntax **display ftp-user**

View Any view

Parameter None

Description Use the **display ftp-user** command to display the settings of the current FTP user, including the user name, host IP address, port number, connection idle time, and work directory.

Example # Display FTP user settings.

```
<SW7750> display ftp-user
Username        Host IP     Port        Idle        Homedir
3Com     10.110.3.5  1074        2       flash:/3Com
```

# If the user name exceeds ten characters, characters behind the tenth will be displayed in a new line in the left-aligning mode. Take username username@test for example, the result is:

```
<SW7750> display ftp-user
Username        Host IP     Port        Idle        Homedir
username@t  10.110.3.5  1074        2       flash:/3Com
est
```

ftp server enable

Syntax **ftp sever enable**

undo ftp sever

View System view

Parameter None

Description Use the **ftp server enable** command to enable the FTP server for users to log in.

Use the **undo ftp server** command to disable the FTP server.

By default, the FTP server is disabled to avoid potential security risks.

Example # Enable the FTP server.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ftp server enable
% Start FTP server
```

ftp timeout

Syntax **ftp timeout** *minutes*

undo ftp timeout

View System view

Parameter *minutes:* Connection idle time (in minutes) ranging from 1 to 35,791.

Description

Use the **ftp timeout** command to set the connection idle time.

Use the **undo ftp timeout** command to restore the default connection idle time.

The default connection idle time is 30 minutes.

If a FTP connection between an FTP server and an FTP client breaks down abnormally and the FTP server is not acknowledged with this, the FTP server keeps the connection as usual.

You can set a connection idle time, so that the FTP server considers a FTP connection to be invalid and terminate it if no data exchange occurs on it in a specific period known as connection idle time.

Example

Set the connection idle time to 36 minutes.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ftp timeout 36
```

79 FTP CLIENT CONFIGURATION COMMANDS

- *You need to use the* ***ftp*** *command to enter FTP client view for configurations under this view. For details, refer to section "ftp" on page 1001 .*
- *After you execute the commands in this section, the output information varies with the FTP server software you use. Examples in this section are for your reference only.*

ascii

Syntax **ascii**

View FTP client view

Parameter None

Description Use the **ascii** command to specify that files be transferred in the ASCII mode.

By default, files are transferred in the ASCII mode.

Example # Specify to transfer files in the ASCII mode.

```
[ftp] ascii
200 Type set to A.
```

binary

Syntax **binary**

View FTP client view

Parameter None

Description Use the **binary** command to specify that files be transferred in the binary mode.

Example # Specify to transfer files in the binary mode.

```
[ftp] binary
200 Type set to I.
```

bye

Syntax **bye**

View FTP client view

Parameter None

Description Use the **bye** command to terminate the control connection and data connection with the remote FTP server and quit to user view.

This command has the same effect as that of the **quit** command.

Example # Terminate the connections with the remote FTP server and return to user view.

```
[ftp] bye
221 Server closing.
<SW7750>
```

cd

Syntax **cd** *pathname*

View FTP client view

Parameter *pathname*: Path name

Description Use the **cd** command to change the work directory on the remote FTP server.

Note that you can use this command to enter the authorized directories only.

Example # Change the work directory to **flash:/temp**.

```
[ftp] cd flash:/temp
250 CWD command successful.
```

# Display the current work directory.

```
[ftp] pwd
257 "flash:/temp" is current directory.
```

cdup

Syntax **cdup**

View FTP client view

Parameter None

Description Use the **cdup** command to go to the parent directory of the current directory.

Example # Change the work directory to **flash:/temp**.

```
[ftp] cd flash:/temp
250 CWD command successful.
```

# Change the work directory to the parent directory.

```
[ftp] cdup
200 CDUP command successful.
```

# Display the current directory.

```
[ftp] pwd
257 "flash:" is current directory.
```

close

Syntax **close**

View FTP client view

Parameter None

Description Use the **close** command to terminate an FTP connection without quitting FTP client view.

This command has the same effect as that of the **disconnect** command.

Example # Terminate the FTP connection without quitting FTP client view.

```
[ftp] close
221 Server closing.
[ftp]
```

delete

Syntax **delete** *remotefile*

View FTP client view

Parameter *remotefile*: Name of the file to be deleted.

Description Use the **delete** command to delete a specified remote file.

Example # Delete file **temp.c**.

```
[ftp] delete temp.c
250 DELE command successful.
```

dir

Syntax **dir** [*filename* [*localfile*]]

View FTP client view

Parameter *filename*: Name of the file to be queried.

localfile: Name of the local file where the query result is to be saved.

Description Use the **dir** command to query specified files on a remote FTP server, or to display file information in the current directory. The output information, which includes the name, size and creation time of files, will be saved in a local file.

If you do not specify the *filename* argument, the information about all the files in the current directory is displayed.

Example # Display the information about all the files in the current directory on the remote FTP server.

```
[ftp] dir
200 PORT command okay
150 File Listing Follows in ASCII mode
-rwxrwxrwx   1 noone    nogroup   430585 Dec 21  2005 4.app
-rwxrwxrwx   1 noone    nogroup   430585 Dec 21  2005 5.app
-rwxrwxrwx   1 noone    nogroup   430585 Dec 23  2005 6. app
-rwxrwxrwx   1 noone    nogroup   430585 Dec 21  2005 6. app.bak
-rwxrwxrwx   1 noone    nogroup   638912 Nov 15  2005 abc.BTM
drwxrwxrwx   1 noone    nogroup        0 Dec 15  2005 TEST
-rwxrwxrwx   1 noone    nogroup  3212176 Jul 14  2005 21.bin
226 Transfer finished successfully.
FTP: 5346 byte(s) received in 6.782 second(s) 788.00 byte(s)/sec.
```

# Display the information about the file named **4.app** and save the output information in the file named **temp1**.

```
[ftp] dir 4.app temp1
200 PORT command okay
150 File Listing Follows in ASCII mode
-rwxrwxrwx   1 noone    nogroup   430585 Dec 21  2004 4. app
226 Transfer finished successfully.
FTP: 70 byte(s) received in 0.122 second(s) 573.00 byte(s)/sec.
```

disconnect

Syntax **disconnect**

View FTP client view

Parameter None

Description

Use the **disconnect** command to terminate a FTP connection without quitting FTP client view.

This command has the same effect as that of the **close** command.

Example

Terminate the FTP connection without quitting FTP client view.

```
[ftp] disconnect
221 Server closing.
[ftp]
```

ftp

Syntax

ftp [**cluster** | *ftp-server* [*port-number*]]

View

User view

Parameter

cluster: Cluster FTP server.

ftp-server: Host name or the IP address of an FTP server. Note that the host name can be a string comprising 1 to 20 characters.

*port-numbe*r: Port number of the FTP server, ranging from 0 to 65535. The default is 21.

Description

Use the **ftp** command to establish a control connection with an FTP server and enter FTP client view.

Example

Connect to the FTP server whose IP address is 2.2.2.2.

```
<SW7750> ftp 2.2.2.2
Trying ...
Press CTRL+K to abort
Connected.
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
User(none):switch
331 Give me your password, please
Password:
230 Logged in successfully
[ftp]
```

The above information is output when you use the WFTPD software as the FTP server software. The output information may be different if you use other FTP server software.

get

Syntax

get *remotefile* [*localfile*]

View

FTP client view

Parameter *remotefile*: Name of a file on an FTP server.

localfile: Name of a local file.

Description Use the **get** command to download a remote file and save it as a local file.

If you do not specify the *localfile* argument, the downloaded file is saved using its original name.

⚠ ***CAUTION:*** *When using the* ***get*** *command to download files from a remote FTP server, make sure the number of the characters containing in the path and file name is within the system-acceptable range*

Example # Download file **temp.c**.

```
[ftp] get temp.c
200 Port command okay.
150 Opening ASCII mode data connection for temp.c.
...226 Transfer complete.
FTP: 2162 byte(s) received in 4.163 second(s) 519.33 byte(s)/sec.
```

lcd

Syntax **lcd**

View FTP client view

Parameter None

Description Use the **lcd** command to display the local work directory on the FTP client.

Example # Display the local work directory.

```
[ftp] lcd
% Local directory now flash:/temp
```

ls

Syntax **ls** [*remotefile* [*localfile*]]

View FTP client view

Parameter *remotefile*: Name of the remote file to be queried.

Localfile: Name of the local file where the querying result is to be saved.

Description Use the **ls** command to display the name of a specified file on a remote FTP server. This command does not support extended parameters, such as -a.

If you do not specify the *remotefile* argument, the names of all the files in the current remote directory are displayed.

***CAUTION:** The **ls** command only displays file names, while the **dir** command displays file information in more detail, including file size, creation date and so on.*

Example # Display the names of all the files in the current directory on the remote FTP server.

```
[ftp] ls
227 Entering Passive Mode (2,2,2,2,4,9).
125 ASCII mode data connection already open, transfer starting for *.
s7500.app
test.cfg
s7500-1.app
another.bat
test
default.diag
226 Transfer complete.
FTP: 189 byte(s) received in 0.011 second(s) 17.18Kbyte(s)/sec.
```

mkdir

Syntax **mkdir** *pathname*

View FTP client view

Parameter *Pathname*: Name of the directory to be created.

Description Use the **mkdir** command to create a directory on an FTP server.

This command is available only to the FTP clients that are assigned the permission to create directories on FTP servers.

Example # Create the directory **flash:/lanswitch** on the FTP server.

```
[ftp] mkdir flash:/lanswitch
257 "flash:/ lanswitch" new directory created.
```

open

Syntax **open** { *ip-address* | *server-name* } [*port*]

View FTP client view

Parameter *ip-address*: IP address of an FTP server.

server-name: Host name of the FTP server, a string comprising 1 to 20 characters.

port: Port number on the remote FTP server, ranging from 0 to 65535. The default value is 21.

Description Use the **open** command to establish a control connection with an FTP server.

Related command: **close**.

Example # Establish a control connection with the FTP server whose IP address is 1.1.1.1.

```
[ftp]open 1.1.1.1
Trying ...
Press CTRL+K to abort
Connected.
220-
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
User(none):abc
331 Give me your password, please
Password:
230 Logged in successfully
```

passive

Syntax **passive**

undo passive

View FTP client view

Parameter None

Description Use the **passive** command to set the data transfer mode to the passive mode.

Use the **undo passive** command to set the data transfer mode to the active mode.

By default, the passive mode is adopted.

Example # Set the data transfer mode to the passive mode.

```
[ftp] passive
% Passive is on
```

put

Syntax **put** *localfile* [*remotefile*]

View FTP client view

Parameter *localfile*: Name of a local file to be uploaded.

remotefile: File name, which the local file is to be saved as.

Description Use the **put** command to upload a local file to an FTP server.

If you do not specify the *remotefile* argument, the local file is saved on the FTP server using the original name.

Example # Upload the local file named **temp.c** to the FTP server.

```
[ftp] put temp.c
200 Port command okay.
150 Opening ASCII mode data connection for config.cfg.

 Operation may take a long time, please wait...
 226 Transfer complete.
FTP: 2162 byte(s) sent in 12.115 second(s) 178.45byte(s)/sec.
```

pwd

Syntax **pwd**

View FTP client view

Parameter None

Description Use the **pwd** command to display the work directory on an FTP server.

Example # Display the work directory on the FTP server.

```
[ftp] pwd
257 "flash:/temp" is current directory.
```

quit

Syntax **quit**

View FTP client view

Parameter None

Description Use the **quit** command to terminate an FTP connection and quit to user view.

This command has the same effect as that of the **bye** command.

Example # Terminate the FTP connection and return to user view.

```
[ftp] quit
221 Windows FTP Server (WFTPD, by Texas Imperial Software) says goodbye
<SW7750>
```

remotehelp

Syntax **remotehelp** [*protocol-command*]

View FTP client view

Parameter *protocol-command*: FTP protocol command.

Description Use the **remotehelp** command to display the on-line help of an FTP protocol command.

This command works only when the FTP server provides the on-line help information about FTP protocol commands.

CAUTION:

- *This command is always valid when a 3Com switch operates as an FTP server.*
- *If you use other FTP server software, refer to related instructions to make sure whether it provides on-line help information about FTP protocol commands.*

Example # Display the syntax of the **user** command.

```
[ftp] remotehelp user
214 Syntax: USER <sp> <username>
```

rmdir

Syntax **rmdir** *pathname*

View FTP client view

Parameter *pathname*: Name of a directory on an FTP server.

Description Use the **rmdir** command to remove a directory on an FTP server.

Note that you can only use this command to remove directories that are empty.

Example # Remove directory **flash:/temp1** on the FTP server. (Assume that the directory is empty.)

```
[ftp] rmdir flash:/temp1
200 RMD command successful.
```

user

Syntax **user** *username* [*password*]

View FTP client view

Parameter *username*: Name of the user to switch to.

password: Password corresponding to the user.

Description

Use the **user** command to switch to a specified user.

Example

Switch to the user named **tom**, assuming that the corresponding password is **111**.

```
[ftp] user tom 111
331 Give me your password, please
230 Logged in successfully
```

verbose

Syntax

verbose

undo verbose

View

FTP client view

Parameter

None

Description

Use the **verbose** command to enable the verbose function, which displays the execution and response information of when a command is executed.

Use the **undo verbose** command to disable the verbose function.

The verbose function is enabled by default.

Example

Enable the verbose function.

```
[ftp] verbose
% Verbose is on
```

80 TFTP CONFIGURATION COMMANDS

tftp get

Syntax **tftp** { **cluster |** *tftp-server* } **get** *source-file* [*dest-file*]

View User view

Parameter **cluster**: Cluster TFTP server.

tftp-server: IP address or the host name of a TFTP server.

source-file: Name of the file to be downloaded from the TFTP server.

dest-file: File name, which the downloaded file is to be saved as.

Description Use the **tftp get** command to download a file from a TFTP server to the local switch.

Related command: **tftp put**.

Example # Download the file named **abc.txt** from the TFTP server whose IP address is 1.1.1.1 and save it as **efg.txt**.

```
<SW7750> tftp 1.1.1.1 get abc.txt efg.txt
  File will be transferred in binary mode.
  Downloading file from remote tftp server, please wait......
  TFTP:       35 bytes received in 0 second(s).
  File downloaded successfully.
```

tftp put

Syntax **tftp** { **cluster |** *tftp-server* } **put** *source-file* [*dest-file*]

View User view

Parameter **cluster***:* Cluster TFTP server.

tftp-server: IP address or the host name of a TFTP server.

source-file: Name of the file to be uploaded to the TFTP server.

dest-file: File name, which the uploaded file is to be saved as.

Description Use the **tftp put** command to upload a file to a specified directory on a TFTP server.

Related command: **tftp get**.

Example # Upload the file named **config.cfg** to the TFTP server whose IP address is 1.1.1.1 and save it as **temp.cfg**.

```
<SW7750> tftp 1.1.1.1 put config.cfg temp.cfg
  File will be transferred in binary mode.
  Copying file to remote tftp server. Please wait... /
  TFTP:      962 bytes sent in 0 second(s).
  File uploaded successfully.
```

tftp-server acl

Syntax **tftp-server acl** *acl-number*

undo tftp-server acl

View System view

Parameter *acl-number*: Basic ACL number ranging from 2000 to 2999.

Description Use the **tftp-server acl** command to specify the ACL adopted for the connection between a TFTP client and a TFTP server.

Use the **undo tftp-server acl** command to cancel all the ACLs adopted.

Example # Specify to adopt ACL 2000 on the TFTP client.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] tftp-server acl 2000
```

81 DNS CONFIGURATION COMMANDS

display dns domain

Syntax **display dns domain**

View Any view

Parameter None

Description Use the **display dns domain** command to display the information in the DNS suffix list.

Related command: **dns domain**.

Example # Display the information in the DNS suffix list.

```
<SW7750> display dns domain
No.         Domain-name
0           aaa.com
```

Table 186 Field descriptions of the **display dns domain** command

Field	Description
No.	Sequence number
Domain-name	Domain name suffix

display dns dynamic-host

Syntax **display dns dynamic-host**

View Any view

Parameter None

Description Use the **display dns dynamic-host** command to display information about the dynamic DNS cache.

The DNS Client saves successful DNS resolution results to the DNS cache. When receiving a name query, the DNS Client first looks up the DNS cache for a match. If a match is found, it returns the corresponding IP address to the user program. If not, it sends a query to the DNS Server.

Example # Display the information in the dynamic DNS cache.

```
<SW7750> display dns dynamic-host
No. Domain-name            IpAddress            TTL      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 187 Description on the field of the **display dns dynamic-host** command

Field	Description
No.	Sequence number
Domain-name	Domain name
IpAddress	IP address corresponding to the domain name
TTL	Time for the entry to be stored in the cache (in seconds)
Alias	Alias name for the domain name, up to 4

display dns server

Syntax **display dns server** [**dynamic**]

View Any view

Parameter **Dynamic**: Displays the DNS server information dynamically obtained by DHCP or other protocols.

Description Use the **display dns server** command to display the DNS server information.

Related command: **dns server**.

Example # Display the DNS server information.

```
<SW7750> display dns server
Domain-server        IpAddress
     0          169.254.65.125
     1          169.254.66.15
```

Table 188 Field descriptions of the **display dns server** command

Field	Description
Domain-server	Sequence number of the DNS server. The system automatically numbers the configured DNS servers starting from 0.
IpAddress	IP address of the DNS server

display ip host

Syntax **display ip host**

View Any view

Parameter None

Description Use the **display ip host** command to display the hostnames and corresponding IP addresses in the static DNS list.

Example # Display the hostnames and corresponding IP addresses in the static DNS list.

```
<SW7750> display ip host
Host            Age     Flags       Address
My          0       static      1.1.1.1
Aa          0       static      2.2.2.4
```

Table 189 Field descriptions of the **display ip host** command

Field	Description
Host	Hostname
Age	Time to live. It is always 0, meaning the static entries will never age out. A static name-to-address mapping entry can only be manually removed.
Flags	Type flag for the name-to-address mapping entry. It is "static" for static entries.
Address	IP address of the host

dns domain

Syntax **dns domain** *domain-name*

undo dns domain [*domain-name*]

View System view

Parameter *domain-name*: DNS suffix, a string of 1 to 60 characters, including alphanumeric characters, hyphens (-), underscores (_), and dots (.).

Description Use the **dns domain** command to configure a DNS suffix.

Use the **undo dns domain** command to delete one or all DNS suffixes.

No DNS suffix is configured by default.

You can configure up to 10 DNS suffixes. When using the **undo dns domain** command, if you specify a DNS suffix, only the specified DNS suffix is removed, otherwise, all statically configured suffixes are removed.

Related command: **display dns domain**.

The DNS resolution function supported by Switch 7750 should be used together with a DNS Server. Different DNS Servers may have differences in DNS implementation. For example, the Switch 7750 supports a domain name which includes "_", while Windows 2000 Server may be unable to resolve the "_".

Example # Configure com as a DNS suffix.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] dns domain com
```

dns resolve

Syntax **dns resolve**

undo dns resolve

View System view

Parameter None

Description Use the **dns resolve** command to enable dynamic DNS resolution.

Use the **undo dns resolve** command to disable dynamic DNS resolution.

Dynamic DNS resolution is disabled by default.

Example # Enable dynamic DNS resolution.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] dns resolve
```

dns server

Syntax **dns server** *ip-address*

undo dns server [*ip-address*]

View System view

Parameter *ip-address*: IP address of a DNS server.

Description Use the **dns server** command to configure a DNS server IP address.

Use the **undo dns server** to remove a configured DNS server IP address.

No DNS server IP address is configured by default.

You can configure up to 6 DNS servers.

Related command: **display dns server**.

Example # Configure a DNS server with the IP address 172.16.1.1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] dns server 172.16.1.1
```

ip host

Syntax **ip host** *hostname ip-address*

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

View System view

Parameter *Hostname*: Hostname, a string of 1 to 30 characters, including alphanumeric characters, hyphens (-), or dots (.).

ip-address: IP address of the specified host, in dotted decimal notation.

Description Use the **ip host** command to add a hostname-to-IP address mapping entry in the static DNS list.

Use the **undo ip host** command to remove a mapping entry from the static DNS list.

By default, there is no entry in the static DNS list.

As one hostname can mapped to only one IP address, when you add multiple hostname-to-address mapping entries with the same hostname, only the last one will be valid.

Related command: **display ip host**.

Example # Configure a mapping entry from the host named aaa to the IP address 10.110.0.1

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ip host aaa 10.110.0.1
```

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 DNS cache.

Related command: **display dns dynamic-host**.

Example # Clear the dynamic DNS cache.

```
<SW7750> reset dns dynamic-host
```

82 BASIC SYSTEM CONFIGURATION COMMANDS

clock datetime

Syntax **clock datetime** *HH:MM:SS YYYY/MM/DD*

View User view

Parameter *HH:MM:SS*: Current time, where *HH* ranges from 0 to 23, *MM* and *SS* range from 0 to 59.

YYYY/MM/DD: Current date, where *YYYY* is the year ranging from 2000 to 2099, *MM* is the month ranging from 1 to 12, and *DD* is the day the range of which is related with the month.

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

In an environment that needs to obtain exact absolute time, it is required to use this command to set the current date and time of the Ethernet switch.

Related command: **display clock**.

Example # Set the current date and time of the Ethernet switch to 0:0:0 2001/01/01.

```
<SW7750> clock datetime 0:0:0 2001/01/01
```

clock summer-time

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

clock summer-time *zone-name* **repeating** { *start-time start-date end-time end-date* | *start-time start-year start-month start-week start-day end-time end-year end-month end-week end-day* } *offset-time*

undo clock summer-time

View User view

Parameter *zone-name*: Name of the summer time, 1 to 32 characters long.

one-off: Sets the summer time for only one year (the specified year).

repeating: Sets the summer time for every year starting from the specified year.

start-time start-date: Start time and start date of the summer time, in the form of HH:MM:SS YYYY/MM/DD.

end-time end-date: End time and end date of the summer time, in the form of HH:MM:SS YYYY/MM/DD.

start-year: Start year, in the range of 2000 to 2099.

start-month: Start month, the value of which is January, February, March, April, May, June, July, August, September, October, November, and December.

start-week: Start week, the value of which is first, second, third, fourth, fifth, and last.

start-day: Start day, the value of which is Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Sunday.

end-year: End year, which should be the same year as the start year, ranges from 2000 to 2099.

end-month: End month, the value of which is January, February, March, April, May, June, July, August, September, October, November, and December.

end-week: End week, the value of which is first, second, third, fourth, fifth, and last.

end-day: End day, the value of which is Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Sunday.

offset-time: Offset of the summer time relative to the standard time.

Description

Use the **clock summer-time** command to set the name and time range of the summer time.

Use the **undo clock summer-time** to cancel the settings.

After the setting, you can use the **display clock** command to check the results. The time of the log and debugging information adopts the local time that has been adjusted by the time zone and summer time.

Related command: **clock timezone**.

Example

Set the summer time named z2, which starts from 06:00:00 2002/06/08, ends until 06:00:00 2002/09/01, and is one hour ahead of the standard time.

```
<SW7750> clock summer-time z2 one-off 06:00:00 2005/06/08 06:00:00 2
002/09/01 01:00:00
```

# Set the summer time named z2, which starts from 06:00:00 06/08, ends until 06:00:00 09/01, and is one hour ahead of the standard time every year from 2002 on.

```
<SW7750> 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, in length of 1 to 32 characters.

add: Sets the time zone to a time before the UTC time.

minus: Sets the time zone to a time behind the UTC time.

HH:MM:SS: Time to be subtracted from the UTC time, in the form of HH:MM:SS.

Description

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

Use the **undo clock timezone** command to restore the local time zone to the default UTC (universal time coordinated) time zone.

After the setting, you can use the **display clock** command to check the results. The log information time and the debugging information time adopt the local time that has been adjusted by the time zone and the summer time.

Related command:

clock summer-time.

Example

Set the local time zone named z5, which is five hours ahead of the UTC time.

```
<SW7750> clock timezone z5 add 05:00:00
```

language-mode

Syntax

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

View

User view

Parameter

chinese: Sets the CLI language environment to Chinese.

English: Sets the CLI language environment to English.

Description Use the **language-mode** command to toggle between the language modes (that is, language environments) of the command line interface (CLI) to meet your requirement.

By default, the CLI language mode is english.

Example # Toggle from the english mode to the chinese mode.

```
<SW7750> language-mode chinese
```

quit

Syntax **quit**

View Any view

Parameter None

Description Use the **quit** command to return from current view to lower level view, or exit the system if current view is user view.

The following lists the three levels of views available (from lower level to higher level):

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

Related command: **return** and **system-view**.

Example # Return from system view to user view.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] quit
<SW7750>
```

return

Syntax **return**

View System view and higher level views

Parameter None

Description Use the **return** command to return from current view to user view. The composite key <Ctrl+Z> has the same effect with the **return** command.

Related command: **quit**.

Example # Return from interface view to user view.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet 1/0/1
[SW7750-Ethernet1/0/1] return
<SW7750>
```

sysname

Syntax **sysname** *sysname*

undo sysname

View System view

Parameter *sysname*: System name of the Ethernet switch. It is a character string in length of 1 to 30 characters. By default, it is 3Com.

Description Use the **sysname** command to set the system name of the Ethernet switch. Changing the system name will affect the CLI prompt. For example, if the system name of the switch is 3Com, the prompt for user view is <SW7750>.

Use the **undo sysname** command to restore the default system view of the Ethernet switch.

Example # Set the system name of the Ethernet switch to 3ComLANSwitch.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] sysname 3ComLANSwitch
[SW7750LANSwitch]
```

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** and **return**.

Example # Enter system view from user view.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750]
```

83 SYSTEM STATUS/INFORMATION DISPLAY COMMANDS

display clock

Syntax **display clock**

View Any view

Parameter None

Description Use the **display clock** command to display the current date and time of the system, so that you can adjust them if they are wrong.

The maximum date and time that can be displayed by this command is 23:59:59 9999/12/31.

Related command: **clock datetime**.

Example # Display the current date and time of the system.

```
<SW7750> 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 190 Field descriptions of the **display clock** command

Field	Description
18:36:31 beijing Sat 2002/02/02	Current date and time of the system
Time Zone	Configured time zone information
Summer-Time	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, which can be Ethernet, GigabitEthernet, AUX, VLAN-interface and so on.

interface-numbe: Interface number.

module-name: Module name.

Description

Use the **display debugging** command to display enabled debugging.

If you want to view the current enabled debugging, you can execute the **display debugging** command. Executing this command without any parameter will display all enabled debugging.

Related command: **debugging**.

Example

Display all enabled debugging.

```
<SW7750> display debugging
IP packet debugging is on.
```

The above information indicates that the IP packets debugging is enabled.

display version

Syntax

display version

View

Any view

Parameter

None

Description

Use the **display version** command to display the information (such as the version information) about the switch system.

Specifically, you can use this command to check the software version and issue time, the basic hardware configuration, and some other information about the switch.

Example

Display the version of the system.

```
<SW7750> display version
3Com Comware Platform Software
Comware software, Version 3.10, Release E3226
Copyright (c) 2004-2007 3Com Corporation All rights reserved.
3Com Switch 7758 uptime is 0 week, 1 day, 0 hour, 32 minutes
SRPG 0:  uptime is 0 weeks,1 days,0 hours,32 minutes
3Com S7750 with 1 MPC8245 Processor
256M    bytes SDRAM
32768K  bytes Flash Memory
512K    bytes NVRAM Memory
PCB Version      :   VER.B
BootROM Version  :   530
CPLD Version     :   004
Second CPLD Ver  :   005
Software Version :   S7758-E3226
Patch Version    :   None
```

```
I/O Module 1:  uptime is 0 weeks,1 days,0 hours,29 minutes
3Com S7750 I/O Module with 1 MPC8241 Processor
128M    bytes SDRAM
0K      bytes Flash Memory
0K      bytes NVRAM Memory
PCB Version      :   VER.B
BootROM Version  :   527
CPLD Version     :   002
Software Version :   S7758-E3226
Patch Version    :   None
......
```

84 System Debugging 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 debugging.

timeout *interval*: Sets the timeout time for all debugging, in the range of 1 to 1,440 (in minutes). After the setting, all debugging is valid in the specified period which starts from the time when the debugging is enabled. After the period, all debugging will be disabled.

module-name: Module name.

debugging-option: Debugging option.

Description

Use the **debugging** command to enable system debugging.

Use the **undo debugging** command to disable system debugging.

By default, all debugging is disabled for the system.

Ethernet switches provide various debugging functions for technical support specialists and senior maintenance personnel to do network fault diagnostics.

Enabling debugging will generate a great deal of debugging information and thus will affect the efficiency of the system, especially after enabling all debugging through the **debugging all** command, the system may collapse. Therefore, it is recommended not to use the **debugging all** command. The **undo debugging all** command brings great convenience for you to disable all debugging at a time instead of disabling them one by one.

Related command:

display debugging.

Example

Enable IP packet debugging.

```
<SW7750> debugging ip packet
```

display diagnostic-information

Syntax **display diagnostic-information** [*module-name*]

View Any view

Parameter *module-name*: Module name. See the following table for details:

Table 191 Module name list

Module name	Description
ARP	ARP module information
DHCP	DHCP module information
DRV	Driver information
ETHERNET	Ethernet module information
FTTH	FTTH information
IGMP	Multicast information
IP	IP module information
L2INF	Interface management information
LACP	Link aggregation information
MEMORY	Memory information
QUEUE	Queue management information
RXTX	Packet transmission information
STP	STP information
SYSTEM	System status information

Description Use the **display diagnostic-information** command to display operation information about all or specified functional modules.

When the system goes wrong, you need to collect much information to locate the fault. However, each module has its corresponding display command, which make it difficult for you to collect all the information needed at a time. In this case, you can use **display diagnostic-information** command to collect the operation information about all or specified module. For displaying all information at a time costs a long time and is not convenient to view, this command provides two modes for you to collect the information

- Output information to the Console.
- Output information to a file.

You can choose one according to the prompt of the system.

Example # Display operation information about ARP module, output the information to the file diaginfo.txt and save the file to the Flash memory.

```
<SW7750 > display diagnostic-information ARP
Redirect it to file?[Y/N]y
 Please input the file name(*.txt)[flash:/diaginfo.txt]:
 This operation may take a few minutes, continue?[Y/N]y
```

```
Writing diagnostic information to flash:/diaginfo.txt now.
......
<SW7750>
```

terminal debugging

Syntax **terminal debugging**

undo terminal debugging

View User view

Parameter None

Description Use the **terminal debugging** command to enable terminal display for debugging information.

Use the **undo terminal debugging** command to disable terminal display for debugging information.

By default, terminal display for debugging information is disabled.

Related command: **debugging**.

Example # Enable terminal display for debugging information.

```
<SW7750> terminal debugging
```

85 NETWORK CONNECTIVITY TEST COMMANDS

ping

Syntax **ping** [**-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** | **ip**]* *host-ip*

ping ipx *ipx-address* [**-c** *count* | **-s** *packetsize* | **-t** *timeout*]*

ping clns *nsap-address*

View Any view

Parameter **-a** *ip-address*: Sets the source IP address to send the ICMP ECHO-REQUEST packets.

-c *count*: Specifies how many times the ICMP ECHO-REQUEST packet will be sent. The *count* argument is the times, which ranges from 1 to 4,294,967,295 and defaults to 5.

-d: Sets the socket to DEBUGGING mode. By default, it is non-DEBUGGING mode.

-f: Specifies to discard a packet directly instead of fragmenting it if its length is greater than the MTU (maximum transmission unit) of the interface.

-h *ttl*: Sets the TTL (time to live) value of the echo request packets in the range of 1 to 255. By default, the TTL value is 255.

-i *interface-type interface-number*: Specifies the interface that sends ICMP ECHO-REQUEST packets by its interface type and number. After the interface is specified, the TTL of the ICMP ECHO-REQUEST packet is set to 1 to test the directly-connected device (the IP address of the device is in the same network segment as that of the interface).

-n: Specifies to regard the *host* argument as an IP address without performing domain name resolution. By default, the *host* argument is first regarded as an IP address; if it is not an IP address, domain name resolution is performed.

-p *pattern*: Specifies the padding byte pattern of the ICMP ECHO-REQUEST packets. The *pattern* argument is a byte in hexadecimal. For example, -p ff fills a packet with only ff. By default, the system fills a packet with 0x01, 0x02, and so on, until 0x09; then it repeats this procedure from 0x01 again.

-q: Specifies to display only the statistics and not to display the details. By default, all the information including the details and statistics will be displayed.

-r: Specifies to record the routes. By default, the system does not record any route.

-s *packetsize*: Specifies the size (in bytes) of each ECHO-REQUEST packet (excluding the IP and ICMP headers). The *packetize* argument ranges from 20 to 32,000 and defaults to 56 bytes.

-t *timeout*: Sets the timeout time (in ms) waiting for an ECHO-RESPONSE packet after an ECHO-REQUEST packet is sent. The *timeout* argument ranges defaults to 2,000 ms.

-tos *tos*: Sets the ToS value of the echo request packets in the range of 0 to 255. By default, this value is 0.

-v: Specifies to display other ICMP packets received (that is, non-ECHO-RESPONSE packets). By default, except for the ECHO-RESPONSE packets, other ICMP packets are not displayed.

ip: Chooses IP ICMP packet.

host-ip: Domain name or IP address of the destination host, 1 to 30 characters long.

ipx: Chooses IPX packet.

ipx-address: IPX address of the destination host.

clns: Chooses CLNS ECHO packets.

nsap-address: NSAP address of the destination host.

Description

Use the **ping** command to check the connectivity of IP network or IPX network, and the reachability of a host.

The process of executing of the **ping** command in the IP network: First, the source host sends an ICMP ECHO-REQUEST packet to the destination host. If the connection to the destination network is normal, the destination host receives this packet and responds with an ICMP ECHO-REPLY packet.

You can use the **ping** command to check the network connectivity and the quality of a network line. This command can output the following information:

- Response status of the destination to each ICMP ECHO-REQUEST packet. If no response packet is received within the timeout time, including the number of bytes, packet sequence number, TTL and response time of the response packet. If no response packet is received within the timeout time, the message "Request time out" is displayed instead.
- Final statistics, including the numbers of sent packets and received response packets, the irresponsive packet percentage, and the minimum, average and maximum values of response time.

You can set a relatively long timeout time waiting for response packet if the network transmission is slow.

Related command: **tracert**.

Example # Check the reachability of the host with IP address 202.38.160.244.

```
<SW7750> ping 202.38.160.244
ping 202.38.160.244 : 56 data bytes, press CTRL_C to break
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 packet transmitted
5 packet received
0.00% 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* | **-w** *timeout*] * *host*

tracert clns [**-m** *max-TTL* | **-n** *num-packet* | **-t** *timeout* | **-v**]* *nsap-address*

View Any view

Parameter **-a** *source-ip*: Sets the source IP address used by this command.

-f *first-TTL*: Sets the initial TTL of the packets to be sent, so that this command displays the addresses of only those gateways on the path whose hop counts are not smaller than the hop count specified by the *first-TTL* argument. For example, if the *first-TTL* argument is three, the command displays the addresses of the gateways from the third hop. The *first-TTL* argument ranges from 1 to 255 and defaults to 1.

-m *max-TTL*: Sets the maximum TTL value of the packets to be sent. After the command sends a packet with the maximum TTL, it will not send any more packets. With this argument, this command displays the addresses of only those gateways from the source destination to the hop count specified by the argument. For example, if the *max-TTL* argument is 5, the command displays the addresses of the gateways from the source to the fifth count. The *max-TTL* argument ranges from 1 to 255 and defaults to 30.

-p *port*: Sets the destination port of the packets to be sent. The *port* argument ranges from 0 to 65535 and defaults to 33434. Generally, you need not change the argument.

-q *num-packet*: Sets the number of packets to be sent every time. The *nqueries* argument ranges from 0 to 65,535 and defaults to 3.

-w *timeout*: Sets the timeout time to wait for ICMP error packets. The *timeout* argument ranges from 0 to 65,535 and defaults to 5,000 (in milliseconds).

host: IP address of the destination host or the host name of the remote system, 1 to 30 characters long.

clns: Connectionless network service, a suit of protocols in OSI system, including CLNP, ISIS and ESIS.

-m *max-TTL*: Sets a maximum TTL value. The *max-TTL* argument ranges from 1 to 255 and defaults to 30.

-n *num-packet*: Indicates the integral number of the sent test packets. The *num-packet* argument ranges from 0 to 65535 and defaults to 3.

-t *timeout*: Sets the timeout time of the **tracert** command. The *timeout* argument, in seconds, ranges from 0 to 65535 and defaults to 5.

-v: Explains the error if the response packet error occurs. If no error occurs, after you execute the command, the result is the same as the command is executed without **-v**.

nsap-address: NSAP address of the destination host.

Description

Use the **tracert** command to trace the gateways the test packets passes through during its journey from the source to the destination. This command is mainly used to check the network connectivity. It can help you locate the trouble spot of the network.

The executing procedure of the **tracert** command is as follows: First, the source sends a packet with the TTL of 1, and the first hop device returns an ICMP error message indicating that it cannot forward this packet because of TTL timeout. Then, the source resends a packet with the TTL of 2, and the second hop device also returns an ICMP TTL timeout message. This procedure goes on and on until a packet gets to the destination or the maximum TTL is reached. During the procedure, the system records the source address of each ICMP TTL timeout message in order to offer the path that the packets pass through to the destination.

If you find that the network is in trouble by using the **ping** command, you can use the **tracert** command to find where the trouble is in the network.

The **tracert** command can output the IP addresses of all the gateways the packets pass through to the destination. It output the string "***" if a gateway times out.

Example

Trace the gateways the packets pass through during its journey to the destination with IP address 18.26.0.115.

```
<SW7750> tracert 18.26.0.115
tracert to allspice.lcs.mit.edu (18.26.0.115), 30 hops max, 40 bytes
 packet
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
```

86 DEVICE MANAGEMENT COMMANDS

boot boot-loader

Syntax **boot boot-loader** { **primary** | **backup** } *file-url*

View User view

Parameter **primary**: Specifies an application as primary boot application.

backup: Specifies an application as backup boot application.

file-url: Path + name of an APP file in the Flash memory or CF module.

Description Use the **boot boot-loader** command to specify the APP file that will be adopted when the switch reboots next time.

You can use this command to specify a primary and backup boot application for a switch. The boot process is as following:

- Normally, primary boot application is adopted for boot.
- When the primary boot application goes wrong, the switch automatically uses the backup boot application to startup.
- If the switch can not boot through primary and backup boot applications, it chooses an application in the Flash randomly for boot. If the switch still can not boot, then the switch fails to boot.

The Boot ROM with the version not below 400 supports double applications boot.

Example # Specify the S7750.APP as the main application adopted when the active Fabric reboots next time.

```
<SW7750> boot boot-loader primary S7750.APP slot 0
```

# Specify the S7750.APP as the main application file adopted when the standby Fabric reboots next time.

```
<SW7750> boot boot-loader primary slot1#flash:/S7750.APP slot 1
```

boot bootrom

Syntax **boot bootrom** *file-url* **slot** *slot-list*

View User view

Parameter *file-url*: Path + name of a Boot ROM file (that is, a .btm file) in the Flash memory.

slot *slot-list*: Specifies the slot number list, which is provided in the format of *slot-list*= { *slot-number* [**to** *slot-number*] } & <1-N>, where &<1-N> means that you can specify up to N slot numbers or slot number ranges. For the Switch 7757, and 7758, N is 7 and for the Switch 7754, N is 4.

Description Use the **boot bootrom** command to update the Boot ROM.

Example # Update the Boot ROM of the module in slot 1 of the switch using the file named S7750.btm.

```
<SW7750> boot bootrom S7750.btm slot 1
```

boot bootrom default

Syntax **boot bootrom default** [**slot** *slot-list*]

View User view

Parameter *slot-list*: Slot number list, provided in the format of *slot-list* = [*slot-number* [**to** *slot-number*]]&<1-N>, where &<1-N> means that you can specify up to N slot numbers or slot number ranges. For the Switch 7757, and 7758, N is 7 and for the Switch 7754, N is 4.

Description Use the **boot bootrom default** command to upgrade the Boot ROM by using the current boot file.

Example # Use the current boot file to upgrade the Boot ROM of all service modules that working normally.

```
<SW7750> boot bootrom default
```

bootrom-update security-check enable

Syntax **bootrom-update security-check enable**

undo bootrom-update security-check enable

View System view

Parameter None

Description Use the **bootrom-update security-check enable** command to enable the validity check function when upgrading Boot ROM.

Use the **undo bootrom-update security-check enable** command to disable the validity check function when upgrading Boot ROM.

By default, validity check function is enabled during Boot ROM upgrade.

Switch 7750s have many modules. Every module has its own Boot ROM application. Wrongly upgrading the Boot ROM causes serious results. The validity checking is used to avoid the above wrong operation.

Example

Enable the validity check function.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] bootrom-update security-check enable
```

display boot-loader

Syntax

display boot-loader

View

Any view

Parameter

None

Description

Use the **display boot-loader** command to display the APP file that is adopted when the switch boots this time and next time.

Example

Display the APP that will be adopted when the switch reboots.

```
<SW7750> display boot-loader
The primary app to boot of board 0 at the next time is: flash:/ccc.a
pp
The backup app to boot of board 0 at the next time is: flash:/ddd.ap
p
The app to boot of board 0 at this time is: flash:/ccc.app
```

Table 192 Field descriptions of the **display boot-loader** command

Field	Description
The primary app to boot of module 0 at the next time	Primary boot file used by the device for reboot next time
The backup app to boot of module 0 at the next time	Backup boot file used by the device for reboot next time
The app to boot of module 0 at this time	Boot file used by the device for boot this time

display cpu

Syntax

display cpu [**slot** *slot-number*]

View

Any view

Parameter **slot** *slot-number*: Specifies a slot. The CPU status of the module on the slot is displayed.

Description Use the **display cpu** command to display the CPU usage of a specified switch.

Example # Display the CPU usage of the module on slot 0 of the switch.

```
<SW7750> display cpu slot 0
Board 0 CPU busy status:
         18% in last 5 seconds
         19% in last 1 minute
     19% in last 5 minutes
```

Table 193 Field descriptions of the **display cpu** command

Field	Description
CPU busy status	Indicates that the following lines describe the CPU occupancies in different time periods.
18% in last 5 seconds	The CPU usage in the last five seconds is 18%.
19% in last 1 minute	The CPU usage in the last one minute is 19%.
19% in last 5 minutes	The CPU usage in the last five minutes is 19%.

display device

Syntax **display device** [**detail** | [**shelf** *shelf-no*] [**frame** *frame-no*] [**slot** *slot-number*]]

View Any view

Parameter **detail**: Detail information about the specified switch.

shelf-no: Shelf number of a switch.

frame-no: Frame number of a switch.

slot-number: Slot number of a switch.

Description Use the **display device** command to display the information, such as the module type and operating status, about each module (main module and sub module) of a specified switch.

You can use this command to display the following information about each module: slot number, sub slot number, versions of PCB, FPGA, hardware and Boot ROM software, address learning mode, interface module type, and patch version.

Example # Display module information of the Switch 7750.

```
<SW7750> display device
3Com Switch 7758 switch fabric
 Slot No.  Brd Type    Brd Status   Subslot Num    Sft Ver         Patch Ver
 0         LS81SRPG    Master       0              S7758-E3226    None
 1         NONE        Absent       Absent         None            None
 2         LS813C16888    Normal       0              S7758-E3226    None
 3         3C16860    Normal       0              S7758-E3226    None
 4         NONE        Absent       Absent         None            None
 5         NONE        Absent       Absent         None            None
 6         LS81VSNP    Normal       0              S7758-E3226    None
 7         NONE        Absent       Absent         None            None
```

# Display the information about the module in slot 0.

```
<SW7750> display device slot 0
Slot  0 info:
  Status          :   Master
  Type            :   LS81SRPG
  Software Ver    :   S7758-E3226
  Patch Ver       :   None
  PCB Ver         :   VER.B
  FPGA Ver        :   004
  BootRom Ver     :   530
  CPLD Ver        :   004
  Chip  0
    Learning Mode:  IVL
```

display environment

Syntax **display environment**

View Any view

Parameter none

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

Example # Display the environment information.

```
<SW7750> display environment
System temperature information (degree centigrade):
----------------------------------------------------
 Board    Temperature         Lower limit      Upper limit
 1        30                  10               70
 3        43                  10               80
 5        33                  10               70
```

display fan

Syntax **display fan** [*fan-id*]

View Any view

Parameter *fan-id*: ID number of a fan.

Description Use the **display fan** command to view the working state of the built-in fans.

You can check whether the fans are working normally through the command.

Example # Display the working state of the fans.

```
<SW7750> display fan
 Fan  1 State: Normal
```

The above information indicates that fan works normally.

display memory

Syntax **display memory** [**slot** *slot-number* | **limit**]

View Any view

Parameter **slot** *slot-number* Specifies a slot number, the usage state of the memory on the slot will be displayed.

limit: Displays the memory configuration information of the device.

Description Use the **display memory** command to display the memory usage of a specified switch.

Example # Display the memory usage on slot 0 of the switch.

```
<SW7750> display memory slot 0
System Total Memory(bytes): 197932416
Total Used Memory(bytes): 65234704
Used Rate: 32%
```

Table 194 Field descriptions of the **display memory** command

Field	Description
System Total Memory(bytes)	Total memory size of the system, in unit of bytes
Total Used Memory(bytes)	Used memory size of the system, in unit of bytes
Used Rate	Percentage of the used memory

# Display the current configuration information of the switch.

```
<SW7750> display memory limit
Current memory limit configuration information:
  system memory safety: 40 (MBytes)
  system memory limit: 30 (MBytes)
  auto-establish enabled

Free Memory: 108120672 (Bytes)

The state information about connection:
  The times of disconnect: 0
  The times of reconnect: 0
  The current state: Normal
```

display power

Syntax **display power** [*power-id*]

View Any view

Parameter *power-id*: Power ID.

Description Use the **display power** command to view the state of the power supply of the switch.

Example # Display the state of the power supply.

```
<SW7750> 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 display information about scheduled reboot.

Related command: **reboot**, **schedule reboot at**.

Example # Display the information about scheduled reboot.

```
<SW7750> display schedule reboot
System will reboot at 16:00:00 2004/11/1 (in 2 hours and 5 minutes).
```

display transceiver alarm interface

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

View Any view

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

Description Use the **display transceiver alarm interface** command to display the current alarm information of a single or all transceivers.

If no error occurs, **None** is displayed.

Table 195 shows the alarm information that may occur for the four types of transceivers.

Table 195 Field descriptions of **display transceiver alarm interface**

Field	Remarks
GBIC/SFP	
RX loss of signal	RX signal is lost.
RX power high	RX power is high.
RX power low	RX power is low.
TX fault	TX fault
TX bias high	TX bias current is high.
TX bias low	TX bias current is low.
TX power high	TX power is high.
TX power low	TX power is low.
Temp high	Temperature is high.
Temp low	Temperature is low.
Voltage high	Voltage is high.
Voltage low	Voltage is low.
Transceiver info I/O error	Transceiver information read and write error
Transceiver info checksum error	Transceiver information checksum error
Transceiver type and port configuration mismatch	Transceiver type does not match port configuration.
Transceiver type not supported by port hardware	Transceiver type is not supported on the port.
XFP	
RX loss of signal	RX signal is lost.
RX not ready	RX is not ready
RX CDR loss of lock	RX clock cannot be recovered.
RX power high	RX power is high.
RX power low	RX power is low.
TX not ready	TX is not ready.
TX fault	TX fault
TX CDR loss of lock	TX clock cannot be recovered.
TX bias high	TX bias current is high.
TX bias low	TX bias current is low.
TX power high	TX power is high.
TX power low	TX power is low.
Module not ready	Module is not ready.
APD supply fault	APD (Avalanche Photo Diode) supply fault
TEC fault	TEC (Thermoelectric Cooler) fault
Wavelength unlocked	Wavelength of optical signal exceeds the manufacturer’s tolerance.
Temp high	Temperature is high.

Table 195 Field descriptions of **display transceiver alarm interface**

Field	Remarks
Temp low	Temperature is low.
Voltage high	Voltage is high.
Voltage low	Voltage is low.
Transceiver info I/O error	Transceiver information read and write error
Transceiver info checksum error	Transceiver information checksum error
Transceiver type and port configuration mismatch	Transceiver type does not match port configuration.
Transceiver type not supported by port hardware	Transceiver type is not supported on the port.
XENPAK	
WIS local fault	WIS (WAN Interface Sublayer) local fault
Receive optical power fault	Receive optical power fault
PMA/PMD receiver local fault	PMA/PMD (Physical Medium Attachment/Physical Medium Dependent) receiver local fault
PCS receive local fault	PCS (Physical Coding Sublayer) receiver local fault
PHY XS receive local fault	PHY XS (PHY Extended Sublayer) receive local fault
RX power high	RX power is high.
RX power low	RX power is low.
Laser bias current fault	Laser bias current fault
Laser temperature fault	Laser temperature fault
Laser output power fault	Laser output power fault
TX fault	TX fault
PMA/PMD receiver local fault	PMA/PMD receiver local fault
PCS receive local fault	PCS receive local fault
PHY XS receive local fault	PHY XS receive local fault
TX bias high	TX bias current is high.
TX bias low	TX bias current is low.
TX power high	TX power is high.
TX power low	TX power is low.
Temp high	Temperature is high.
Temp low	Temperature is low.
Transceiver info I/O error	Transceiver information read and write error
Transceiver info checksum error	Transceiver information checksum error
Transceiver type and port configuration mismatch	Transceiver type does not match port configuration.
Transceiver type not supported by port hardware	Transceiver type is not supported on the port.

For pluggable transceivers supported by Switch 7750 Ethernet switches, refer to 3Com Switch 7750 Family Installation Manual.

Examples # Display the alarm information of the transceiver on interface GigabitEthernet 2/0/1.

```
<SW7750> display transceiver alarm interface gigabitethernet 2/0/1
GigabitEthernet2/0/1 transceiver current alarm information:
  TX fault
```

Table 196 Field descriptions of display transceiver alarm interface

Field	Description
transceiver current alarm information	Current alarm information of the transceiver
TX fault	TX fault

display transceiver diagnosis interface

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

View Any view

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

Description Use the **display transceiver diagnosis interface** command to display the currently measured value of digital diagnosis parameters of a single or all anti-spoofing transceivers customized by 3Com.

Examples # Display the currently measured value of digital diagnosis parameters of the anti-spoofing pluggable optical transceiver customized by 3Com on interface GigabitEthernet 2/0/2.

```
<SW7750> display transceiver diagnosis interface gigabitethernet 2/0
/2
GigabitEthernet2/0/2 transceiver diagnostic information:
  Current diagnostic parameters:
    Temp(°C)  Voltage(V)  Bias(mA)  RX power(dBM)  TX power(dBM)
    35        3.26        6.18      -35.64         -5.17
```

Table 197 Field descriptions of display transceiver diagnosis interface

Field	Description
transceiver diagnostic information	Digital diagnosis information of the transceiver carried by an interface
Current diagnostic parameters	Current diagnostic parameters
Temp.(°C)	Digital diagnosis parameter-temperature, in °C, with the precision to 1°C.
Voltage(V)	Digital diagnosis parameter-voltage, in V, with the precision to 0.01 V.
Bias(mA)	Digital diagnosis parameter-bias current, in mA, with the precision to 0.01 mA.
RX power(dBM)	Digital diagnosis parameter-RX power, in dBM, with the precision to 0.01 dBM.
TX power(dBM)	Digital diagnosis parameter-TX power, in dBM, with the precision to 0.01 dBM.

display transceiver interface

Syntax

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

View

Any view

Parameters

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

Description

Use the **display transceiver interface** command to display main parameters of a single or all transceivers.

Examples

Display main parameters of the pluggable transceiver on interface GigabitEthernet 2/0/3.

```
<SW7750> display transceiver interface gigabitethernet 2/0/3
GigabitEthernet2/0/3 transceiver information:
  Transceiver Type                   : 1000_BASE_LX_SFP
  Connector Type                     : LC
  Wavelength(nm)                     : 1310
  Transfer Distance(km)              : 10(9um)
  Digital Diagnostic Monitoring      : YES
  Vendor Name                        : 3Com
  Ordering Name                      : SFP-GE-LX10-SM1310
```

Table 198 Field descriptions of the **display transceiver interface** command

Field	Description
transceiver information	Transceiver information of the interface
Transceiver Type	Transceiver type
Connector Type	Type of the connectors of the transceiver: ■ Optical connectors, including SC (SC connector, developed by NTT) and LC (LC connector, 1.25 mm/RJ45 optical connector developed by Lucent). ■ Other connectors, including RJ-45 and CX4.
Wavelength(nm)	■ Optical transceiver: central wavelength of the laser sent, in nm. If the transceiver supports multiple wavelengths, every two wavelength values are separated by a comma. ■ Electrical transceiver: displayed as N/A.
Transfer distance(xx)	Transfer distance, with xx representing km for single-mode transceivers and m for other transceivers. If the transceiver supports multiple transfer medium, every two values of the transfer distance are separated by a comma. The corresponding transfer medium is included in the bracket following the transfer distance value. The following are the transfer media: ■ 9 um: 9/125 um single-mode fiber ■ 50 um: 50/125 um multi-mode fiber ■ 62.5 um: 62.5/125 um multi-mode fiber ■ TP: Twisted pair ■ CX4: CX4 cable

Table 198 Field descriptions of the **display transceiver interface** command

Field	Description
Digital Diagnostic Monitoring	Whether the digital diagnosis function is supported, where: ■ YES: supported ■ NO: not supported
Vendor Name	Vendor name or vendor name specified of the transceiver: ■ The anti-spoofing transceiver customized by 3Com: **3Com** is displayed. ■ Other transceivers: The original vendor name is displayed.
Ordering Name	■ Ordering name of the transceiver

display transceiver manuinfo interface

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

View Any view

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

Description Use the **display transceiver manuinfo interface** command to display part of the electrical label information of a single or all anti-spoofing pluggable transceivers customized by 3Com.

Examples # Display part of the electrical label information of the anti-spoofing pluggable transceiver customized by 3Com on interface GigabitEthernet 2/0/4.

```
<SW7750> display transceiver manuinfo interface gigabitethernet 2/0/
4
GigabitEthernet2/0/4 transceiver manufacture information:
  Manu. Serial Number  : 213410A0000054000251
  Manufacturing Date   : 2007-07-28
  Vendor Name          : 3Com
```

Table 199 Field descriptions of display transceiver manuinfo interface

Field	Description
Manu. Serial Number	Serial number generated during debugging and testing
Manufacturing Date	Debugging and testing date.. The date takes the value of the system clock of the computer that performs debugging and testing.
Vendor Name	Vendor name specified, that is, 3Com.

display uplink monitor

Syntax **display uplink monitor**

View Any view

Parameter

None

Description

Use the **display uplink monitor** command to view information about Layer 3 connectivity between the local device and the remote device.

Related command:

uplink monitor.

Example

View information about Layer 3 connectivity between the local device and the remote device.

```
<SW7750> display uplink monitor
UpLink monitor information
No.  Dest_IP_Addr     Dest_MAC_Addr   Vlan      Port  ErrCnt   Last_Err_Time
1  192.168.0.35     ----.----.----     1         -     135  04/29 16:15:04
```

The above information shows there are 135 Layer 3 connectivity errors between the local device and the remote device whose IP address is 192.168.0.35.

loadsharing enable

Syntax

loadsharing enable

undo loadsharing enable

View

System view

Parameter

None

Description

Use the **loadsharing enable** command to enable system load sharing.

Use the **undo loadsharing enable** command to disable system load sharing.

By default, system load sharing function is disabled.

With system load sharing enabled, when an I/O Module receives traffic to be cross-card forwarded, load sharing is performed between the active Fabric and the standby Fabric.

- *Only unicast traffic supports load sharing.*
- *Only 32Gbps and 64Gbps Switch Fabrics support load sharing.*
- *Only I/O Modules of XGbus type support load sharing.*

Example

Enable system load sharing.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] loadsharing enable
```

pause-protection

Syntax **pause-protection** { **enable** | **disable** } **slot** *slot-number*

View System view

Parameter **enable**: Enables pause frame protection mechanism.

disable: Disables pause frame protection mechanism.

slot *slot-number*: Specifies a slot where module is to seat in.

Description Use the **pause-protection** command to enable/disable pause frame protection mechanism.

Pause frame protection mechanism is disabled by default.

Pause frames, which can be utilized as packets to attack a network, are used in traffic controlling. A switch that has pause frame protection mechanism enabled discards the detected pause frames that are utilized to attack the network it resides and logs these attacks in the log buffer. If the switch experiences successive pause frame attacks, it sends messages to the console to warn users.

CAUTION: *Only A type modules support pause frame protection mechanism and the related commands. A type modules include: 3C16860, 3C16861, LS81FS24A, 3C16858, and 3C16859.*

Example # Enable pause frame protection mechanism on the module in slot 7.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] pause-protection enable slot 7
```

qe monitor

Syntax **qe monitor** { **enable** | **disable** }

View System view

Parameter **enable**: Enables queue traffic monitoring.

disable: Disables queue traffic monitoring.

Description Use the **qe monitor** command to enable/disable queue traffic monitoring.

Queue traffic monitoring is disabled by default.

With queue traffic monitoring enabled on a switch, the switch monitors the queue traffic and relieves blocks in the output queue of its interfaces.

The criterion used to distinguish a block is that the queue is full and the traffic of the corresponding interface is less than the specified threshold.

Refer to the **qe monitor overflow-threshold** on page 1053 for information about how to set a threshold.

Example # Enable queue traffic monitoring.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] qe monitor enable
```

qe monitor errpkt

Syntax **qe monitor errpkt** { **all** | **none** | **runt** }

View Ethernet port view

Parameter **all**: Specifies to detect all error packets on current interface.

none: Specifies not to detect error packets on current interface.

runt: Specifies to detect error packets that are of runt type on current interface. Error packets that are of runt type refer to frames whose data segment is less than 64 bytes without CRC errors.

Description Use the **qe monitor errpkt** command to configure error packets detection function on current interface.

A switch does not detect error packets on current interface by default.

If the switch receives a great number of error packets, it will not be able to send/receive packets properly. With error packets monitoring enabled, the switch collects information about received error packets regularly. If error packets are detected, it takes protection measures to ensure that its interfaces send/receive packets properly.

Example # Specify to detect error packets that are of runt type on Ethernet4/0/1 interface.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet 4/0/1
[SW7750-Ethernet4/0/1] qe monitor errpkt runt
```

qe monitor errpkt check-time

Syntax **qe monitor errpkt check-time** *interval*

View System view

Parameter *interval*: Specifies the interval for detecting error packets. The *interval* argument ranges from 1 to 3600 (in seconds) and defaults to 5.

Description Use the **qe monitor errpkt check-time** command to set the interval for detecting error packets.

If the switch receives a great number of error packets, it will not be able to send/receive packets properly. With error packets monitoring enabled, the switch collects information about received error packets at intervals. If error packets are detected, it takes protection measures to ensure that its interfaces send/receive packets properly.

Example # Set the interval for detecting error packets to 50 seconds.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] qe monitor errpkt check-time 50
```

qe monitor inner-bad

Syntax **qe monitor inner-bad** { **enable** | **disable** }

View System view

Parameter **enable**: Enables error packet monitoring on internal ports.

disable: Disables error packet monitoring on internal ports.

Description Use the **qe monitor inner-bad enable** command to enable error packet monitoring on internal ports.

Use the **qe monitor inner-bad disable** command to disable error packet monitoring on internal ports.

By default, error packet monitoring on internal ports is enabled.

If detecting that an internal port receives error packets, the system clears the queues under this port.

- *This command is applicable to type-A I/O Modules only.*
- *Type-A I/O Modules refer to the following I/O Modules: 3C16860, 3C16861, LS81FS24A, 3C16858, 3C16859, 3C16860, 3C16861, LS81FS24, 3C16858, and 3C16859.*

Example # Enable error packet monitoring on internal ports.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] qe monitor inner-bad enable
```

qe monitor overflow-threshold

Syntax **qe monitor overflow-threshold** *threshold*

View System view

Parameter *threshold*: Integer that sets the overall traffic threshold, ranging from 0 to 4294967295 (in bps).

Description Use the **qe monitor overflow-threshold** command to specify the overall traffic threshold used in queue traffic monitoring.

The overall traffic threshold defaults to 300,000,000 bps (300 Mbps).

With queue traffic monitoring enabled, the switch monitors the queue traffic and relieves blocks in the output queue of its interfaces.

The criterion used to distinguish a block is that the queue is full and the traffic of the corresponding interface is less than the specified threshold.

Example # Set the overall traffic threshold used in queue traffic monitoring to 90 Mbps.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] qe monitor overflow-threshold 90000000
```

rdram

Syntax **rdram** { **enable** | **disable** }

View System view

Parameter **enable**: Enables rambus dynamic random access memory (RDRAM) of the device.

disable: Disables RDRAM of the device.

Description Use the **rdram enable** command to enable RDRAM of the device.

Use the **rdram disable** command to disable RDRAM of the device.

By default, RDRAM of the device is disabled.

Example # Disable RDRAM of the device.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] rdram disable
```

reboot

Syntax **reboot** [**slot** *slot-number*]

View User view

Parameter **slot** *slot-number*: Specifies the slot number.

Description Use the **reboot** command to restart the whole system or the specified module.

Example # Restart the switch.

```
<SW7750> reboot
System is checking configuration now. Please wait ...
 This command will reboot the system. The current configuration has
not been saved and will be lost if you continue. Continue? [Y/N]
```

schedule reboot at

Syntax **schedule reboot at** *hh:mm* [*yyyy/mm/dd*]

undo schedule reboot

View User view

Parameter *hh:mm*: Reboot time, where *hh* (hour) ranges from 0 to 23, and *mm* (minute) ranges from 0 to 59.

yyyy/mm/dd: Reboot date, where *yyyy* (year) ranges from 2,000 to 2,099, *mm* (month) ranges from 1 to 12, and the range of *dd* (day) depends on the specific month.

Description Use the **schedule reboot at** command to schedule a reboot on the current switch and set the reboot date and time.

Use the **undo schedule reboot** command to cancel the scheduled reboot.

By default, no scheduled reboot is set on the switch.

There is at most one minute defer for scheduled reboot, that is, the switch will reboot within one minute after reaching the specified reboot date and time.

After you execute the **schedule reboot at** command with a future date specified, the switch will reboot at the specified time with at most one minute delay.

After you execute the **schedule reboot at** command without specifying a date, the switch will:

- Reboot at the specified time on the current day if the specified time is later than the current time.

- Reboot at the specified time on the next day if the specified time is earlier than the current time.

Note that the specified date can not be 30 days later than the current date. And after you execute the command, the system will prompt you to confirm. Enter "Y" or "y" for your setting to take effect, and your setting will overwrite the old one (if available).

If you adjust the system time by the **clock** command after executing the **schedule reboot at** command, the **schedule reboot at** command will be invalid and the scheduled reboot will not happen.

Related command: **reboot**, **display schedule reboot**.

Example # Suppose the current time is16:21, schedule a reboot so that the switch reboots at 22:00 on the current day.

```
<SW7750> schedule reboot at 22:00
Reboot system at 22:00 2005/04/06(in 5 hours and 39 minutes)
confirm?[Y/N]:y
<SW7750>
%Apr  6 16:21:03 2005 S7758 CMD/5/REBOOT:
aux0: schedule reboot parameters at 16:21:00 2005/04/06. And system
will reboot
at 22:00:2005 04/06/2005.
```

schedule reboot delay

Syntax **schedule reboot delay** { *hhh:mm* | *mmm* }

undo schedule reboot

View User view

Parameter *hhh:mm*: Reboot waiting delay, in the format of "hour:minute". *hh* ranges from 0 to 720, and *mm* ranges from 0 to 59.

mmm: Reboot waiting delay, ranging from 0 to 43,200 minutes.

Description Use the **schedule reboot delay** command to schedule a reboot on the switch, and set the reboot waiting delay.

Use the **undo schedule reboot** command to cancel the scheduled reboot.

By default, no scheduled reboot is set on the switch.

There is at most one minute defer for scheduled reboot, that is, the switch will reboot within one minute after waiting for the specified delay.

You can set the reboot waiting delay in two formats: the hour:minute format and the absolute minutes format, and both must be less than or equal to 30 × 24 × 60 (that is, 30 days).

After you execute the command, the system will prompt you to confirm. Enter "Y" or "y" for your setting to take effect. Your setting will overwrite the old one (if available).

If you adjust the system time by the **clock** command after executing the **schedule reboot delay** command, the **schedule reboot delay** command will be invalid and the scheduled reboot will not happen.

Related command: **reboot**, **schedule reboot at**, **undo schedule reboot at**, and **display schedule reboot**.

Example # Suppose the current time is 16:26, schedule a reboot so that the switch reboots after 88 minutes.

```
<SW7750> schedule reboot delay 88
Reboot system at 17:54 2005/04/06(in 1 hours and 28 minutes)
confirm?[Y/N]:y
<SW7750>
%Apr  6 16:26:38 2005 S7758 CMD/5/REBOOT:
aux0: schedule reboot parameters at 16:26:34 2005/04/06. And system will reboot
at 17:54:2005 04/06/2005.
```

set backboard enhance

Syntax **set backboard enhance**

undo set backboard enhance

View System view

Parameter None

Description Use the **set backboard enhance** command to set the running mode of cross-card HG clock to enhanced mode (frequency: 187MHz).

Use the **undo set backboard enhance** command to restore the default running mode of cross-card HG clock, that is, standard mode (frequency: 127 MHz).

By default, the cross-card HG clock runs in standard mode.

Example # Set the running mode of the HG clock between LS81GT48B and LS81VSNP modules to enhanced mode.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] set backboard enhance
```

temperature-limit

Syntax **temperature-limit** *slot-number down-value up-value*

undo temperature-limit *slot-number*

View User view

Parameter *slot-number*: Physical module slot number.

down-value: Lower temperature limit, ranging from 0 to 70, in centigrade.

up-value: Upper temperature limit, in centigrade, ranging from 20 to 90, and must be greater than the *down-value*.

Description Use the **temperature-limit** command to configure temperature alarm threshold.

Use the **undo temperature-limit** command to restore temperature alarm threshold to the default.

Example # Set the lower temperature limit of module 0 to 10, and upper temperature limit to 75.

```
<SW7750> temperature-limit 0 10 75
Success temperature limit set successfully
```

uplink monitor

Syntax **uplink monitor ip** *ip-address*

undo uplink monitor ip

View Ethernet port view

Parameter *ip-address*: IP address of a interface on the Layer 3 device in the remote peer. The interface connects with the local device.

Description Use the **uplink monitor ip** command to enable the Layer 3 connectivity detection function on the current port, and specify the IP address to be detected, that is the IP address of the interface on the remote device that connects with the local device.

Use the **undo uplink monitor ip** to disable the Layer 3 connectivity detection function.

By default, Layer 3 connectivity detection function is disabled on all ports.

This function requires no Layer 3 device existing between the local peer and the remote peer.

Example # Enable Layer 3 connectivity detection function on Ethernet4/0/1, and specify the IP address to be detected as 1.1.1.1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet 4/0/1
[SW7750-Ethernet4/0/1] uplink monitor ip 1.1.1.1
```

87 REMOTE-PING CLIENT COMMANDS

count

Syntax **count** *times*

undo count

View remote-ping test group view

Parameter *times*: Number of probes in each test. The *times* argument ranges from 1 to 15.

Description Use the **count** command to set the number of probes in each test.

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

For tests except jitter test, only one packet is sent in a probe. In a jitter test, you can use the **jitter-packetnum** command to set the number of packets to be sent in a probe.

By default, the number of probes in each test is 1.

Related command: **frequency**

Example # Set the number of probes made in an ICMP test to 10.

```
<7750> system-view
System View: return to User View with Ctrl+Z
[7750] remote-ping administrator icmp
[7750-remote-ping-administrator-icmp] test-type icmp
[7750-remote-ping-administrator-icmp] count 10
```

datasize

Syntax **datasize** *size*

undo datasize

View remote-ping test group view

Parameter *size*: Size of a test packet in bytes. The value range varies with the test types.

Table 200 Value range of the remote-ping test packets

Test type	Value range	Default
Jitter	68 to 8100	68
ICMP	4 to 8100	56
Udpprivate	4 to 8100	100
Udppublic	4 to 8100	100

The packet size configuration applies to ICMP, UDP, and jitter tests only.

Description

Use the **datasize** command to configure the size of a test packet in a test.

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

Example

Set the size of ICMP test packets to 50 bytes.

```
<7750> system-view
System View: return to User View with Ctrl+Z.
[7750] remote-ping administrator icmp
[7750-remote-ping-administrator-icmp] test-type icmp
[7750-remote-ping-administrator-icmp] datasize 50
```

destination-ip

Syntax

destination-ip *ip-address*

undo destination-ip

View

remote-ping test group view

Parameter

ip-address: Destination IP address of a remote-ping test.

Description

Use the **destination-ip** command to configure a destination IP address of an remote-ping test.

Use the **undo destination-ip** command to remove the configured destination IP address.

By default, no destination IP address is configured for an remote-ping test.

Related command: **destination-port**

The destination address can be an IP address or a host name in HTTP test, while in other types of tests, it must be an IP address.

Example

Set the destination IP address of an ICMP test to 169.254.10.3.

```
<7750> system-view
System View: return to User View with Ctrl+Z
[7750] remote-ping administrator icmp
[7750-remote-ping-administrator-icmp] test-type icmp
[7750-remote-ping-administrator-icmp] destination-ip 169.254.10.3
```

destination-port

Syntax

destination-port *port-number*

undo destination-port

View

remote-ping test group view

Parameter

port-number: Destination port number for an remote-ping test, in the range of 1 to 65535.

Description

Use the **destination-port** command to configure a destination port number for an remote-ping test.

Use the **undo destination-port** command to remove the configured destination port number.

By default, no destination port number is configured for a test.

Related command: **destination-ip**

- *The **destination-port** command has effect on jitter, TCP-Private, and UDP-Private tests only.*
- *You are not recommended to perform a TCP, UDP, or jitter test to a known port (ports with a number ranging from 1 to 1023). Otherwise, the remote-ping test will fail or the corresponding service of the port will become unavailable.*

Example

Set the destination port number for a tcpprivate test to 9000.

```
<7750> system-view
System View: return to User View with Ctrl+Z
[7750] remote-ping administrator tcp
[7750-remote-ping-administrator-tcp] test-type tcpprivate
[7750-remote-ping-administrator-tcp] destination-port 9000
```

display remote-ping

Syntax

display remote-ping { **results** | **history** } [*administrator-name operation-tag*]

View

Any view

Parameters

results: Displays results of the last test.

history: Displays the history records of tests.

administrator-name: Name of the administrator who created the remote-ping test operation, a string of 1 to 32 characters.

operation-tag: Operation tag, a string of 1 to 32 characters.

Description

Use the **display remote-ping** command to display the result of the last remote-ping test or the history of remote-ping tests.

Without *administrator-name test-operation-tag* specified, the command displays the results of all test groups; without *administrator-name test-operation-tag* specified, the command displays the results of the specified test group.

Related command: **test-enable**

Example

Display the result of the test group with the administrator name being administrator, and the operation tag being icmp.

```
[7750-remote-ping-administrator-icmp] display remote-ping results administrator
icmp
  remote-ping entry(admin administrator, tag icmp) test result:
      Destinationip address:10.2.2.2
      Send operation times: 10             Receive response times: 10
      Min/Max/Average Round Trip Time: 1/2/1
      Square-Sum of Round Trip Time: 13
      Last succeeded test time: 2004-11-25 16:28:55.0
    Extend result:
      SD Maximal delay: 0                  DS Maximal delay: 0
      Packet lost in test: 0%
      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
      Other operation errors:0
```

Table 201 Description of the **display remote-ping result** command fields

Filed	Description
Destination ip address	Destination IP address
Send operation times	Number of probes made
Receive responds times	Number of received response packets
Min/Max/Average Round Trip Time	Minimum/maximum/average round trip time
Square-Sum of Round Trip Time	Square sum of round trip time
Last succeeded test time	Completion time of the last successful test
SD Maximal delay	Maximum delay from the source to the destination
DS Maximal delay	Maximum delay from the destination to the source
Packet lost in test	Average packet loss ratio
Disconnect operation number	Number of times the test was disconnected by the remote end
System busy operation number	Number of times the test failed because the system was busy
Operation sequence errors	Number of out-of-sequence packets received
Other operation errors	Number of other errors
Operation timeout number	Number of time-out occurrences in a test
Connection fail number	Number of failures to connect with the remote end
Drop operation number	Number of system resource allocation failures

# Display the history records of remote-ping tests.

```
[7750-remote-ping-administrator-icmp] display remote-ping history administrator i
cmp
  remote-ping entry(admin administrator, tag icmp) history record:
    Index     Response    Status      LasrRC      Time
```

```
      1          1         1          0    2004-11-25 16:28:55.0
      2          1         1          0    2004-11-25 16:28:55.0
      3          1         1          0    2004-11-25 16:28:55.0
      4          1         1          0    2004-11-25 16:28:55.0
      5          1         1          0    2004-11-25 16:28:55.0
      6          2         1          0    2004-11-25 16:28:55.0
      7          1         1          0    2004-11-25 16:28:55.0
      8          1         1          0    2004-11-25 16:28:55.0
      9          1         1          0    2004-11-25 16:28:55.9
     10          1         1          0    2004-11-25 16:28:55.9
```

Table 202 Description of the **display remote-ping history** command fields

Field	Description
Response	Round trip time in the case of a successful test, timeout time in the case of test timeout, or 0 in the case of a test failure (in milliseconds)
Status	Test result values, including: 1: responseReceived: Response received 2: unknown: Unknown error. 3: internalError: System internal error 4: requestTimeOut: Request timed out 5: unknownDestinationAddress: Unknown destination address 6: noRouteToTarget: Destination unreachable 7: interfaceInactiveToTarget: Interface to destination address inactive 8: arpFailure: ARP operation failed. 9: maxConcurrentLimitReached: Maximum limit of concurrent accesses reached 10: unableToResolveDnsName: Unable to resolve DNS domain name 11: invalidHostAddress: Invalid host address
LasrRC	Last response code received (this code is based on the specific implementation). With ICMP echo enabled on the system, receiving ICMP response which includes ICMP_ECHOREPLY(0) indicates the probe succeeds. ICMP response is often defined in a file including ip_icmp.
Time	Test completion time

# Display the result of the test group with the administrator name being administrator, and the operation tag being http.

```
[7750-remote-ping-administrator-http] display remote-ping results administrator
 http
  remote-ping entry(admin administrator, tag http) test result:
      Destination ip address:192.168.0.152
      Send operation times: 10              Receive response times: 10
      Min/Max/Average Round Trip Time: 47/87/74
      Square-Sum of Round Trip Time: 57044
      Last succeeded test time: 2000-4-2 20:41:50.4
  Extend result:
      SD Maximal delay: 0                 DS Maximal delay: 0
      Packet lost in test: 0%
      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
      Other operation errors: 0
    Http result:
      DNS Resolve Time: 0                HTTP Operation Time: 675
      DNS Resolve Min Time: 0            HTTP Test Total Time: 748
      DNS Resolve Max Time: 0            HTTP Transmission Successful Times: 10
      DNS Resolve Failed Times: 0        HTTP Transmission Failed Times: 0
      DNS Resolve Timeout Times: 0       HTTP Transmission Timeout Times: 0
      TCP Connect Time: 73               HTTP Operation Min Time: 27
      TCP Connect Min Time: 5            HTTP Operation Max Time: 80
      TCP Connect Max Time: 20
      TCP Connect Timeout Times: 0
```

Table 203 Description of the **display remote-ping result** command fields

Field	Description
DNS Resolve Time	Time used for a DNS resolution
HTTP Operation Time	Total time used to establish an HTTP connection
DNS Resolve Min Time	Minimal time used for a DNS resolution
HTTP Test Total Time	Total time used for an HTTP test
DNS Resolve Max Time	Maximum time used for a DNS resolution
HTTP Transmission Successful Times	Number of successful HTTP transmissions
DNS Resolve Failed Times	Number of failed DNS resolutions
HTTP Transmission Failed Times	Number of failed HTTP transmissions
DNS Resolve Timeout Times	DNS resolution timeout times
HTTP Transmission Timeout Times	HTTP transmission timeout times
TCP Connect Time	Total time used to establish a TCP connection
HTTP Operation Min Time	Minimum time used to establish an HTTP connection
TCP Connect Min Time	Minimum time used to establish a TCP connection
HTTP Operation Max Time	Maximum time used to establish an HTTP connection
TCP Connect Max Time	Maximum time used to establish a TCP connection
TCP Connect Timeout Times	TCP connection timeout times

# Display the result of the test group with the administrator name being administrator, and the operation tag being Jitter.

```
[7750-remote-ping-administrator-Jitter] display remote-ping results
administrator Jitter
remote-ping entry(admin administrator, tag Jitter) test result:
      Destination ip address:10.2.2.2
      Send operation times: 100             Receive response times: 100
      Min/Max/Average Round Trip Time: 9/21/13
      Square-Sum of Round Trip Time: 18623
      Last succeeded test time: 2000-4-2 8:14:58.2
  Extend result:
      SD Maximal delay: 10                  DS Maximal delay: 10
      Packet lost in test: 0%
      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
      Other operation errors: 0
    Jitter result:
      RTT Number:100
      Min Positive SD:1                    Min Positive DS:1
      Max Positive SD:6                    Max Positive DS:8
      Positive SD Number:38                Positive DS Number:25
      Positive SD Sum:85                   Positive DS Sum:42
      Positive SD average:2                Positive DS average:1
      Positive SD Square Sum:267           Positive DS Square Sum:162
```

```
Min Negative SD:1                    Min Negative DS:1
Max Negative SD:6                    Max Negative DS:8
Negative SD Number:30                Negative DS Number:24
Negative SD Sum:64                   Negative DS Sum: 41
Negative SD average:2                Negative DS average:1
Negative SD Square Sum:200           Negative DS Square Sum:161
SD lost packets number:0             DS lost packet number:0
Unkown result lost packet number:0
```

Table 204 Description of the **display remote-ping result** command fields

Field	Description
RTT Number	Number of received response packets
Min Positive SD	Minimum positive jitter delay from the source to the destination
Min Positive DS	Minimum positive jitter delay from the destination to the source
Max Positive SD	Maximum positive jitter delay from the source to the destination
Max Positive DS	Maximum positive jitter delay from the destination to the source
Positive SD Number	Number of positive jitter delays from the source to the destination
Positive DS Number	Number of positive jitter delays from the destination to the source
Positive SD Sum	Sum of positive jitter delays from the source to the destination
Positive DS Sum	Sum of positive jitter delays from the destination to the source
Positive SD average	Average of positive jitter delays from the source to the destination
Positive DS average	Average of positive jitter delays from the destination to the source
Positive SD Square Sum	Sum of the square of positive jitter delays from the source to the destination
Positive DS Square Sum	Sum of the square of positive jitter delays from the destination to the source
Min Negative SD	Minimum absolute value of negative jitter delays from the source to the destination
Min Negative DS	Minimum absolute value of negative jitter delays from the destination to the source
Max Negative SD	Maximum absolute value of negative jitter delays from the source to the destination
Max Negative DS	Maximum absolute value of negative jitter delays from the destination to the source
Negative SD Number	Number of negative jitter delays from the source to the destination
Negative DS Number	Number of negative jitter delays from the destination to the source
Negative SD Sum	Sum of absolute values of negative jitter delays from the source to the destination
Negative DS Sum	Sum of absolute values of negative jitter delays from the destination to the source
Negative SD average	Average of negative jitter delays from the source to the destination

Table 204 Description of the **display remote-ping result** command fields

Field	Description
Negative DS average	Average of negative jitter delays from the destination to the source
Negative SD Square Sum	Sum of the square of negative jitter delays from the source to the destination
Negative DS Square Sum	Sum of the square of negative jitter delays from the destination to the source
SD lost packets number	Number of lost packets from the source to the destination
DS lost packet number	Number of lost packets from the destination to the source
Unknown result lost packet number	Number of lost packets for unknown reasons

# Display the result of the test group with the administrator name being administrator, and the operation tag being dns.

```
[7750] display remote-ping results administrator dns
remote-ping entry(admin administrator, tag dns) test result:
      Destination ip address:10.2.2.2
      Send operation times: 10              Receive response times: 10
      Min/Max/Average Round Trip Time: 6/10/8
      Square-Sum of Round Trip Time: 756
      Last succeeded test time: 2006-11-28 11:50:40.9
  Extend result:
      SD Maximal delay: 0                   DS Maximal delay: 0
      Packet lost in test: 0%
      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
      Other operation errors: 0
    Dns result:
      DNS Resolve Current Time: 10         DNS Resolve Min Time: 6
      DNS Resolve Times: 10                DNS Resolve Max Time: 10
      DNS Resolve Timeout Times: 0         DNS Resolve Failed Times: 0
```

Table 205 Description of the **display remote-ping result** command fields

Field	Description
DNS Resolve Current Time	Default time used for a DNS resolution
DNS Resolve Min Time	Minimum time used for a DNS resolution
DNS Resolve Times	Number of DNS resolutions
DNS Resolve Max Time	Maximum time used for a DNS resolution
DNS Resolve Timeout Times	DNS resolution timeout times
DNS Resolve Failed Times	Number of failed DNS resolutions

The description on a specific field is available for the test results of all types of tests, so that not the description on the output information of all types of tests is provided here.

dns-server

Syntax **dns-server** *ip-address*

undo dns-server

View remote-ping test group view

Parameter *ip-address*: IP address to be assigned to a domain name server (DNS).

Description Use the **dns-server** command to configure the IP address of a DNS server.

Use the **undo dns-server** command to remove the IP address of a DNS server.

By default, no DNS server IP address is configured.

- *This command applies to DNS and HTTP tests only.*
- *For an HTTP test, if configuring the destination address as the host name, you must configure the IP address of the DNS server to resolve the host name into an IP address, which is the destination IP address of this HTTP test*

Example # Set 192.168.1.1 as the IP address of the DNS server.

```
<7750> system-view
System View: return to User View with Ctrl+Z
[7750] remote-ping administrator dns
[7750-remote-ping-administrator-dns] test-type dns
[7750-remote-ping-administrator-dns] dns-server 192.168.1.1
```

dns resolve-target

Syntax **dns resolve-target** *domain-name*

undo dns resolve-target

View remote-ping test group view

Parameter *domain-name*: Domain name to be resolved, in the range of 1 to 60 characters.

Description Use the **dns resolve-target** command to configure a domain name to be resolved.

Use the **undo resolve-target** command to remove a domain name to be resolved.

By default, no dns resolve-target information is configured.

This command applies to DNS tests only.

Example # Configure the domain name to be resolved as www.test.com.

```
<7750> system-view
System View: return to User View with Ctrl+Z
[7750] remote-ping administrator dns
[7750-remote-ping-administrator-dns] test-type dns
[7750-remote-ping-administrator-dns] dns resolve-target www.test.com
```

filename

SyntaExamplex

filename *file-name*

undo filename

View

remote-ping test group view

Parameter

file-name: Name of the file to be downloaded/uploaded in FTP tests, a string of 1 to 255 characters.

Description

Use the **filename** command to specify a file to be downloaded/uploaded in FTP tests.

Use the **undo filename** command to remove the configured file name.

By default, no file name is configured for FTP tests.

Related commands: **username**, **password**, and **ftp-operation**

The filename command applies to FTP tests only.

Example

Specify to transmit **config.txt** between remote-ping client and FTP server in an FTP test.

```
<7750> system-view
System View: return to User View with Ctrl+Z
[7750] remote-ping administrator ftp
[7750-remote-ping-administrator-ftp] test-type ftp
[7750-remote-ping-administrator-ftp] filename config.txt
```

frequency

Syntax

frequency *interval*

undo frequency

View

remote-ping test group view

Parameter

interval: Automatic test interval in seconds. It ranges from 0 to 65,535.

Description

Use the **frequency** command to configure the time interval of performing automatic tests.

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

If *interval* is configured greater than 0, the system performs automatic tests at this interval.

interval defaults to 0, which means no automatic test is performed by default.

Related command: **count**

- *The **frequency** command does not apply to DHCP tests.*
- *The **frequency** command supports fabric only when the test type of this test group is ICMP. With fabric enabled, you are allowed to configure the **frequency** command and use the **display** command to check your configuration, but unless the test type is ICMP, your configuration does not take effect until fabric is disabled.*

Example

Set the automatic test interval to 10 seconds in an ICMP test.

```
<7750> system-view
System View: return to User View with Ctrl+Z
[7750] remote-ping administrator icmp
[7750-remote-ping-administrator-icmp] test-type icmp
[7750-remote-ping-administrator-icmp] frequency 10
```

ftp-operation

Syntax

ftp-operation { **get** | **put** }

View

remote-ping test group view

Parameters

get: Specifies the test operation as download from the FTP server.

put: Specifies the test operation as upload to the FTP server.

Description

Use the **ftp-operation** command to configure the FTP operation mode, which can be **get** and **put**.

By default, the FTP operation mode is **get**.

Related commands: **username** and **password**

The ftp-operation command applies to FTP tests only.

Example

Set the FTP operation mode to **put** in an FTP test.

```
<7750> system-view
System View: return to User View with Ctrl+Z
[7750] remote-ping administrator ftp
[7750-remote-ping-administrator-ftp] test-type ftp
[7750-remote-ping-administrator-ftp] ftp-operation put
```

history-records

Syntax

history-records *number*

undo history-records

View remote-ping test group view

Parameter Number: Maximum number of history records that can be saved in a test group, in the range of 0 to 50, and 50 by default.

Description Use the **history-records** command to set the maximum number of history records that can be saved in a test group.

Use the **undo history-records** to restore the default.

By default, up to 50 records can be saved in a test group.

Example # Set the maximum number of history records that can be saved to 10.

```
<7750> system-view
System View: return to User View with Ctrl+Z
[7750] remote-ping administrator icmp
[7750-remote-ping-administrator-icmp] test-type icmp
[7750-remote-ping-administrator-icmp] history-records 10
```

http-operation

Syntax **http-operation** { **get** | **post** }

View remote-ping test group view

Parameters **get**: Specifies the test operation to be download from the HTTP server.

post: Specifies the test operation to be uploaded to the HTTP server.

Description Use the **http-operation** command to configure the HTTP operation mode.

By default, the HTTP operation mode is **get**.

The http-operation command applies to HTTP tests only.

Example # Set the HTTP operation mode to **post** in an HTTP test.

```
<7750> system-view
System View: return to User View with Ctrl+Z
[7750] remote-ping administrator http
[7750-remote-ping-administrator-http] test-type http
[7750-remote-ping-administrator-http] http-operation post
```

http-string

Syntax **http-string** *string version*

undo http-string

View remote-ping test group view

Parameters *string*: HTTP operation string used to specify the webpage to be accessed, in the range 1 to 255 characters.

version: HTTP version, in the range 1 to 255 characters. At present, this argument can only be HTTP/1.0, where HTTP must be capitalized.

Description Use the **http-string** command to configure the HTTP operation string and version in an HTTP test.

Use the **undo http-string** command to remove the configured HTTP operation string and version.

By default, HTTP operation string and version are not configured.

The **http-string** command applies to HTTP tests only.

Related commands: **http-operation**

Example # Set the webpage to be accessed by an HTTP test as /index.htm and the HTTP version as HTTP/1.0.

```
<7750> system-view
[7750] remote-ping administrator http
[7750-remote-ping-administrator-http] test-type http
[7750-remote-ping-administrator-http] http-string /index.htm
HTTP/1.0
```

remote-ping

Syntax **remote-ping** *administrator-name operation-tag*

undo remote-ping *administrator-name operation-tag*

View System view

Parameters *administrator-name*: Name of the administrator to create a remote-ping test group, a string of 1 to 32 characters.

operation-tag: Operation tag, a string of 1 to 32 characters.

Description Use the **remote-ping** command to create an remote-ping test group and enter remote-ping test group view. If the specified remote-ping test group already exists, this command leads you to remote-ping test group view directly.

Use the **undo remote-ping** command to delete the test group.

Example

Create an remote-ping test group of which the administrator name is **administrator** and operation tag is **ICMP**.

```
<7750> system-view
System View: return to User View with Ctrl+Z
[7750] remote-ping administrator icmp
[7750-remote-ping-administrator-icmp]
```

remote-ping-agent enable

Syntax

remote-ping-agent enable

undo remote-ping-agent enable

View

System view

Parameters

None

Description

Use the **remote-ping-agent enable** command to enable the remote-ping client function.

Use the **undo remote-ping-agent enable** command to disable the remote-ping client function.

By default, the remote-ping client function is disabled.

You can perform tests only after you enable the remote-ping client function.

Related command: **remote-ping-server enable**

Example

Enable remote-ping client.

```
<7750> system-view
System View: return to User View with Ctrl+Z
[7750] remote-ping-agent enable
```

jitter-interval

Syntax

jitter-interval *interval*

undo jitter-interval

View

remote-ping test group view

Parameter

interval: Interval in milliseconds between jitter test packets. The value is in the range of 10 to 1000.

Description

Use the **jitter-interval** command to configure the interval between sending jitter test packets.

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

By default, the interval between sending jitter test packets is 20 milliseconds.

Related command: **jitter-packetnum**

The jitter-interval command applies to jitter tests only.

Example # Set the interval between sending jitter test packets to 30 milliseconds.

```
<7750> system-view
System View: return to User View with Ctrl+Z
[7750] remote-ping administrator jitter
[7750-remote-ping-administrator-jitter] test-type jitter
[7750-remote-ping-administrator-jitter] jitter-interval 30
```

jitter-packetnum

Syntax **jitter-packetnum** *number*

undo jitter-packetnum

View remote-ping test group view

Parameter *number*: Number of packets to be transmitted in one probe for a jitter test, in the range of 10 to 100.

Description Use the **jitter-packetnum** command to configure the number of packets to be sent in one probe for a jitter test.

Use the **undo jitter-packetnum** command to restore the default.

By default, 10 packets are sent in a probe for a jitter test.

Related command: **jitter-interval**

This command applies to jitter tests only.

Example # Configure to send 30 packets in a probe for a jitter test.

```
<7750> system-view
System View: return to User View with Ctrl+Z
[7750] remote-ping administrator jitter
[7750-remote-ping-administrator-jitter] test-type jitter
[7750-remote-ping-administrator-jitter] jitter-packetnum 30
```

password

Syntax

password *password*

undo password

View

remote-ping test group view

Parameter

password: Password for logging in to an FTP server, a string of 1 to 32 characters.

Description

Use the **password** command to configure a password for logging in to the FTP server.

Use the **undo password** command to remove the configured password.

By default, the password for logging in to the FTP server is not configured.

Related commands: **username** and **ftp-operation**

- *To perform an FTP test successfully, the configured password must be consistent with the FTP user password configured on the server.*
- *This command applies to FTP tests only.*

Example

Set the password for logging into the FTP server as **remote-ping** in an FTP test.

```
<7750> system-view
System View: return to User View with Ctrl+Z
[7750] remote-ping administrator ftp
[7750-remote-ping-administrator-ftp] test-type ftp
[7750-remote-ping-administrator-ftp] password remote-ping
```

probe-failtimes

Syntax

probe-failtimes *times*

undo probe-failtimes

View

remote-ping test group view

Parameter

times: Number of consecutive failed probes, in the range of 1 to 15.

Description

Use the **probe-failtimes** command to configure the number of consecutive times the probe fails before the switch sends out a trap message.

Use the **undo probe-failtimes** command to restore the default.

By default, the switch sends a trap about probe failure each time when a probe fails.

Example # Configure the switch to send a trap after the probe in an ICMP test fails for three consecutive times.

```
<7750> system-view
System View: return to User View with Ctrl+Z
[7750] remote-ping administrator icmp
[7750-remote-ping-administrator-icmp] test-type icmp
[7750-remote-ping-administrator-icmp] probe-failtimes 3
```

send-trap

Syntax **send-trap** { **all** | { **probefailure** | **testcomplete** | **testfailure** }***** }

undo send-trap { **all** | { **probefailure** | **testcomplete** | **testfailure** }***** }

View remote-ping test group view

Parameters **probefailure**: Sends a trap when a probe fails.

testcomplete: Sends a trap after a test is finished.

testfailure: Sends a trap when a test fails.

all: Sends a trap when any of the above-mentioned scenarios occurs.

Description Use the **send-trap** command to enable debugging for a trap.

Use the **undo send-trap** command to disable debugging for a trap.

By default, no trap is output.

Example # Send a trap message after an ICMP test is finished.

```
<7750> system-view
System View: return to User View with Ctrl+Z
[7750] remote-ping administrator icmp
[7750-remote-ping-administrator-icmp] test-type icmp
[7750-remote-ping-administrator-icmp] send-trap testcomplete
```

source-interface

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

undo source-interface

View remote-ping test group view

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

Description For ICMP tests, use the **source-interface** command to specify a source interface for sending ICMP requests. The corresponding IP address of the specified interface is used as the source IP address of ICMP requests. For DHCP tests, use the **source-interface** command to specify an interface for DHCP probes.

For ICMP tests, use the **undo source-interface** command to remove the specified source interface, and its corresponding IP address is no longer used as the source IP address of ICMP requests. For DHCP tests, use the **undo source-interface** command to remove the specified interface for DHCP probes.

By default, no source interface is specified for ICMP tests and no interface is configured for DHCP probes.

- *For DHCP tests, this command is required. For ICMP tests, this command is optional. This command does not apply to other tests.*
- *For ICMP tests, if a source IP address has been configured with the **source-ip** command, the **source-interface** command cannot change the configured IP address.*
- *The interface to be specified in this command can be only a VLAN interface.*
- *The interface to be specified must be Up; otherwise the test will fail.*

Example # Configure the source interface that sends test packets in DHCP tests as VLAN-interface 1.

```
<7750> system-view
System View: return to User View with Ctrl+Z
[7750] remote-ping administrator dhcp
[7750-remote-ping-administrator-dhcp] test-type dhcp
[7750-remote-ping-administrator-dhcp] source-interface Vlan-interface 1
```

source-ip

Syntax **source-ip** *ip-address*

undo source-ip

View remote-ping test group view

Parameter *ip-address*: Source IP address for a test.

Description Use the **source-ip** command to configure the source IP address for the test.

Use the **undo source-ip** command to remove the configured source IP address.

By default, the IP address of the interface that sends test packets serves as the source IP address.

- *For FTP tests, this command is required. This command does not apply to DHCP tests. For other tests, this command is optional.*
- *The specified source IP address by this command cannot be of an interface on a remote device, and the interface must be Up; otherwise the test will fail.*

Example # Configure the source IP address as 169.254.10.2 for this ICMP test.

```
<7750> system-view
System View: return to User View with Ctrl+Z
[7750] remote-ping administrator icmp
[7750-remote-ping-administrator-icmp] test-type icmp
[7750-remote-ping-administrator-icmp] source-ip 169.254.10.2
```

source-port

Syntax **source-port** *port-number*

undo source-port

View remote-ping test group view

Parameter *port-number*: Source port number, in the range of 1 to 65,535.

Description Use the **source-port** command to configure the source port number for this test.

Use the **undo source-port** command to remove the configured source port number.

This command does not apply to ICMP, DHCP, and DNS tests.

Example # Configure the source port number as 8000 for this ICMP test.

```
<7750> system-view
System View: return to User View with Ctrl+Z
[7750] remote-ping administrator icmp
[7750-remote-ping-administrator-icmp] test-type icmp
[7750-remote-ping-administrator-icmp] source-port 8000
```

test-type

Syntax **test-type** *type*

View remote-ping test group view

Parameter *type*: Test type. It can be any of the following keywords:

- **dhcp**: Indicates a DHCP test.
- **dns**: Indicates a DNS test.
- **ftp**: Indicates an FTP test.
- **http**: Indicates an HTTP test.
- **icmp**: Indicates an ICMP test.
- **jitter**: Analyzes the delay change of UDP packet transmission.
- **snmpquery**: Indicates an SNMP test.
- **tcpprivate**: Indicates a TCP test on a specified (unknown) port.

- **tcppublic**: Indicates a TCP test on port 7.
- **udpprivate**: Indicates a UDP test on a specified (unknown) port.
- **udppublic**: Indicates a UDP test on port 7.

The default type is **icmp**.

Description

Use the **test-type** command to configure the test type.

Example

Configure the test type as an FTP test.

```
<7750> system-view
System View: return to User View with Ctrl+Z
[7750] remote-ping administrator ftp
[7750-remote-ping-administrator-ftp] test-type ftp
```

test-enable

Syntax

test-enable

undo test-enable

View

remote-ping test group view

Parameters

None

Description

Use the **test-enable** command to enable a remote-ping test.

Use the **undo test-enable** command to disable a remote-ping test.

Related command: **display remote-ping**

*The result of the remote-ping test cannot be displayed automatically, and you need to use the **display remote-ping** command to display the test result.*

Example

Perform a remote-ping test on an ICMP test group with the administrator name and operation tag being administrator and icmp respectively.

```
<7750> system-view
System View: return to User View with Ctrl+Z
[7750] remote-ping administrator icmp
[7750-remote-ping-administrator-icmp] test-type icmp
[7750-remote-ping-administrator-icmp] destination-ip 169.254.10.3
[7750-remote-ping-administrator-icmp] test-enable
```

test-failtimes

Syntax

test-failtimes *times*

undo test-failtimes

View

remote-ping test group view

Parameter

times: Number of times of consecutive test failure, in the range of 1 to 15.

Description

Use the **test-failtimes** command to configure the number of consecutive times a remote-ping test fails before the switch sends out a trap message.

Use the **undo test-failtimes** command to restore the default.

By default, the switch sends a trap about test failure each time when a test fails.

Example

Configure the switch to send out a trap message after an ICMP test fails for three consecutive times.

```
<7750> system-view
System View: return to User View with Ctrl+Z
[7750] remote-ping administrator icmp
[7750-remote-ping-administrator-icmp] test-type icmp
[7750-remote-ping-administrator-icmp] test-failtimes 3
```

timeout

Syntax

timeout *time*

undo timeout

View

remote-ping test group view

Parameter

time: Timeout time for one probe, in the range of 1 to 60, in seconds.

Description

Use the **timeout** command to set the timeout time for a probe. That is, the value of the probe timer that is started after the remote-ping client sends out a test packet.

Use the **undo timeout** command to restore the default value.

By default, the probe timeout time is 3 seconds.

Example

Set the timeout time for one probe in an ICMP test to 10 seconds.

```
<7750> system-view
System View: return to User View with Ctrl+Z
[7750] remote-ping administrator icmp
[7750-remote-ping-administrator-icmp] test-type icmp
[7750-remote-ping-administrator-icmp] timeout 10
```

tos

Syntax

tos value

undo tos

View remote-ping test group view

Parameter *value*: ToS value in a remote-ping test packet header, in the range of 0 to 255.

Description Use the **tos** command to configure the ToS value in a remote-ping test packet header.

Use the **undo tos** command to remove the ToS value in a remote-ping test packet header.

By default, no ToS value is configured.

This command does not apply to DHCP tests.

Example # Set the ToS value in the header of an ICMP test packet to 1.

```
<7750> system-view
System View: return to User View with Ctrl+Z
[7750] remote-ping administrator icmp
[7750-remote-ping-administrator-icmp] test-type icmp
[7750-remote-ping-administrator-icmp] tos 1
```

username

Syntax **username** *name*

undo username

View remote-ping test group view

Parameter *name*: Username for logging in to an FTP server, a string of 1 to 32 characters.

Description Use the **username** command to configure a username for logging in to the FTP server.

Use the **undo username** command to remove the configured username.

By default, no username for logging in to the FTP server is configured.

Related commands: **password** and **ftp-operation**

- *To perform an FTP test successfully, the configured username must be consistent with the username configured on the FTP server.*
- *This command applies to FTP tests only.*

Example # Configure the username for logging into the FTP server in an FTP test as **administrator**.

```
<7750> system-view
System View: return to User View with Ctrl+Z
```

```
[7750] remote-ping administrator ftp
[7750-remote-ping-administrator-ftp] test-type ftp
[7750-remote-ping-administrator-ftp] username administrator
```

88 REMOTE-PING SERVER COMMANDS

- *A remote-ping server is required for only jitter, TCP, and UDP tests.*
- *You are not recommended to configure remote-ping jitter/UDP/TCP servers on ports 1 through 1023 (well-known ports); otherwise, remote-ping probes may fail or the services corresponding to these ports may be unavailable.*

remote-ping-server enable

Syntax **remote-ping-server enable**

undo remote-ping-server enable

View System view

Parameters None

Description Use the **remote-ping-server enable** command to enable the remote-ping server function.

Use the **undo remote-ping-server enable** command to disable the remote-ping server function.

By default, the remote-ping server function is disabled.

Related commands: **remote-ping-agent enable**, **remote-ping-server tcpconnect**, and **remote-ping-server udpconnect**.

Example # Enable a remote-ping server.

```
<7750> system-view
System View: return to User View with Ctrl+Z
[7750] remote-ping-server enable
```

remote-ping-server tcpconnect

Syntax **remote-ping-server tcpconnect** *ip-address port-number*

undo remote-ping-server tcpconnect *ip-address port-number*

View System view

Parameters *ip-address*: IP address from which a remote-ping server performs TCP listening.

port-number: Port from which a remote-ping server performs TCP listening. The value ranges from 1 to 65535. Note that the ports with a number greater than 50000 or some special ports (that is, those used for fixed functions, such as port 1701) cannot be configured.

Description Use the **remote-ping-server tcpconnect** command to enable TCP listening.

Use the **undo remote-ping-server tcpconnect** command to disable TCP listening.

When performing a TCP connection test on a specified port of a remote-ping client, you must enable TCP listening on the server if a 3Com Switch 7750 serves as a remote-ping server; otherwise, the test may fail.

Related command: **remote-ping-server enable**

⚠ ***CAUTION:*** *The port number used by remote-ping server for TCP listening cannot be set to a number greater than 50000 or to some special port numbers that are for fixed functions, such as 1701.*

Example # Enable TCP listening, using 169.254.10.2 as the IP address and 9000 as the port number.

```
<7750> system-view
System View: return to User View with Ctrl+Z
[7750] remote-ping-server tcpconnect 169.254.10.2 9000
```

remote-ping-server udpecho

Syntax **remote-ping-server udpecho** *ip-address port-number*

undo remote-ping-server udpecho *ip-address port-number*

View System view

Parameters *ip-address*: IP address from which a remote-ping server performs UDP listening.

port-number: Port from which a remote-ping server performs UDP listening. The value ranges from 1 to 65535. Note that the ports with a number greater than 49999 or some special ports (that is, those used for fixed functions, such as port 1701) cannot be configured.

Description Use the **remote-ping-server udpecho** command to enable UDP listening on a remote-ping server.

Use the **undo remote-ping-server udpecho** command to disable UDP listening.

When performing a jitter test or a UDP connection test on a specified port of a remote-ping client, you must enable UDP listening on the server if a Switch 7750 serves as a remote-ping server; otherwise, the test may fail.

Related command: **remote-ping-server enable**

⚠ ***CAUTION:*** *The port number used by remote-ping server for UDP listening cannot be set to a number greater than 49999 or to some special port numbers that are for fixed functions, such as 1701.*

Example # Enable UDP listening, using 169.254.10.2 as the IP address and 9000 as the port number.

```
<7750> system-view
System View: return to User View with Ctrl+Z
[7750] remote-ping-server udpecho 169.254.10.2 9000
```

89 RRPP Configuration Commands

This board is supported if you have the special order modules listed in the Switch 7750 Family Configuration Guide, in the chapter entitled "RPPP Configuration."

control-vlan

Syntax **control-vlan** *vlan-id*

View RRPP domain view

Parameter *vlan-id*: Control VLAN ID, in the range of 2 to 4093.

Description Use the **control-vlan** command to specify the control VLAN for the RRPP domain.

You can configure the control VLAN of the primary ring. The control VLAN of the subring is assigned by the system automatically and its ID is the control VLAN ID of the primary ring plus 1.

A control VLAN is a special VLAN used to transfer RRPP packets. The port on each switch for connecting the switch with the Ethernet ring belongs to the control VLAN, and only the ports connected to the Ethernet ring can be added to the control VLAN. It is not allowed to configure an IP address for the interface of the control VLAN.

CAUTION:

- *A specified control VLAN cannot be removed by using the undo vlan all command.*
- *The control VLAN of an RRPP domain cannot be a static VLAN already created on the switch. If you configure a dynamic VLAN as the control VLAN of an RRPP domain, the VLAN becomes a static VLAN automatically.*
- *You are not recommended to configure a VLAN as both an RRPP control VLAN and a remote-probe VLAN. (Refer to* ***remote-probe vlan*** *on page 814.)*
- *You are not recommended to configure a VLAN as both an RRPP control VLAN and an isolate-user-VLAN/sub VLAN. (Refer to "Isolate-User-VLAN Configuration Commands" on page 131 and* ***subvlan*** *on page 136 for more information.)*

Example # Configure VLAN 100 as the control VLAN of the RRPP domain 1.

```
<SW7750> system-view
[SW7750] rrpp domain 1
[SW7750-rrpp-domain1] control-vlan 100
```

display rrpp brief

Syntax **display rrpp brief**

View Any view

Parameter None

Description Use the **display rrpp brief** command to display the brief information of all RRPP domains configured on the switch, including the RRPP enable state, RRPP domain configuration, and Ethernet rings in the domains.

Example # Display the brief information of the RRPP domains.

```
<SW7750> display rrpp brief
Abbreviations for Switch Node Mode :
M - Master , T - Transit , E - Edge , A - Assistant-Edge

RRPP Protocol Status : Enabled
Number of RRPP Domains : 2
Domain Index : 1
Control Vlan : major 4093    sub 4094
Hello Timer : 1 sec Fail Timer : 3 sec
Ring  Ring   Node  Primary/Common          Secondary/Edge     Is
ID    Level  Mode  Port                     Port              Enabled
-------------------------------------------------------------------------
1     0      M     GigabitEthernet 2/0/1       GigabitEthernet 2/0/2       Yes

Domain Index : 2
Control Vlan : major 2003     sub 2004
Hello Timer : 1 sec Fail Timer : 3 sec
Ring  Ring   Node  Primary/Common          Secondary/Edge    Is
ID    Level  Mode  Port                    Port              Enabled
----------------------------------------------------------------------
1     0      T     GigabitEthernet 2/0/11      GigabitEthernet 2/0/12      No
```

display rrpp statistics

Syntax **display rrpp statistics domain** *domain-id* [**ring** *ring-id*]

View Any view

Parameter *domain-id*: RRPP domain ID, in the range of 1 to 8.

ring-id: RRPP ring ID, in the range of 1 to 64.

Description Use the **display rrpp statistics** command to display the RRPP packet statistics.

Example # Display the packet statistics of primary ring 10 in RRPP domain1 (the current switch is the master node of ring 10).

```
<SW7750> display rrpp statistics domain 1 ring 10
RRPP Ring     : 10
Ring Level    : 0
Node Mode     : Master
Is Activated  : No
Primary port  : -
Packet             LINK        LINK        COMMON      COMPLETE    Packet
 Direct HEALTH      UP          DOWN        FDB         FDB         Total
-------------------------------------------------------------------------
 Send   0           0           0           0           0           0
 Rcv    0           0           0           0           0           0
Secondary port: -
Packet             LINK        LINK        COMMON      COMPLETE    Packet
 Direct HEALTH      UP          DOWN        FDB         FDB         Total
-------------------------------------------------------------------------
 Send   0           0           0           0           0           0
 Rcv    0           0           0           0           0           0
```

# Display the packet statistics of secondary ring 20 in RRPP domain1 (the current switch is an edge node of secondary ring 20).

```
<SW7750> display rrpp statistics domain 1 ring 20
RRPP Ring     : 20
Ring Level    : 1
Node Mode     : Edge
Is Activated  : No
Primary port  : -
Packet             LINK        LINK        COMMON      COMPLETE    Packet
 Direct HEALTH      UP          DOWN        FDB         FDB         Total
-------------------------------------------------------------------------
 Send   0           0           0           0           0           0
 Rcv    0           0           0           0           0           0
Secondary port: -
Packet             LINK        LINK        COMMON      COMPLETE    Packet
 Direct HEALTH      UP          DOWN        FDB         FDB         Total
-------------------------------------------------------------------------
 Send   0           0           0           0           0           0
 Rcv    0           0           0           0           0           0
```

display rrpp verbose

Syntax **display rrpp verbose domain** *domain-id* [**ring** *ring-id*]

View Any view

Parameter *domain-id*: RRPP domain ID, in the range of 1 to 8.

ring-id: RRPP ring ID, in the range of 1 to 64.

Description Use the **display rrpp verbose** command to display the RRPP configuration details on the switch. If you do not specify the RRPP ring ID, the command displays the details of all rings in the specified domain. Otherwise, the command displays the details of the specified ring.

Example # Display the details of primary ring 10 in RRPP domain 1 (the current switch is the master node in ring 10).

```
<SW7750> display rrpp verbose domain 1 ring 10
Domain Index  : 1
Control VLAN  : major 2003    sub 2004
Hello Timer   : 1  sec  Fail Timer : 3  sec
RRPP Ring     : 10
Ring Level    : 0
Node Mode     : Master
Ring State    : -
Is Enabled    : No    Is Activated  : No
Primary port  : -    Port status: -
Secondary port: -    Port status: -
```

# Display the details of primary ring 10 in RRPP domain 1 (the current switch is the transit node in ring 10).

```
<SW7750> display rrpp verbose domain 1 ring 10
Domain Index  : 1
Control VLAN  : major 2003    sub 2004
Hello Timer   : 1  sec  Fail Timer : 3  sec
RRPP Ring     : 10
Ring Level    : 0
Node Mode     : Transit
Ring State    : -
Is Enabled    : No    Is Activated  : No
Primary port  : -    Port status: -
Secondary port: -    Port status: -
```

# Display the details of secondary ring 20 in RRPP domain 1 (the current switch is the transit node in secondary ring 20).

```
<SW7750> display rrpp verbose domain 1 ring 20
Domain Index  : 1
Control VLAN  : major 2003    sub 2004
Hello Timer   : 1  sec  Fail Timer : 3  sec
RRPP Ring     : 20
Ring Level    : 1
Node Mode     : Transit
Ring State    : -
Is Enabled    : No    Is Activated  : No
Primary port  : -    Port status: -
Secondary port: -    Port status: -
```

# Display the details of secondary ring 20 in RRPP domain 1 (the current switch is the edge node in secondary ring 20).

```
<SW7750> display rrpp verbose domain 1 ring 20
Domain Index  : 1
Control VLAN  : major 2003    sub 2004
Hello Timer   : 1  sec  Fail Timer : 3  sec
RRPP Ring     : 20
Ring Level    : 1
Node Mode     : Edge
Ring State    : -
Is Enabled    : No    Is Activated  : No
```

```
Common port   : -    Port status: -
Edge port     : -    Port status: -
```

reset rrpp statistics

Syntax **reset rrpp statistics domain** *domain-id* [**ring** *ring-id*]

View User view

Parameter *domain-id*: RRPP domain ID, in the range of 1 to 8.

ring-id: RRPP ring ID, in the range of 1 to 64.

Description Use the **reset rrpp statistics** command to clear the statistics information of the specified RRPP domain.

If you specify the RRPP ring ID, the command clears the RRPP packet statistics information of the specified ring in the specified domain. Otherwise, the command clears the RRPP packet statistics information of all the rings in the specified domain.

Related command: **display rrpp statistics**.

Example # Clear the packet statistics of ring 10 in RRPP domain 1 on the current switch.

```
<SW7750> reset rrpp statistics domain 1 ring 10
```

# Clear the packet statistics of all rings in RRPP domain 1 on the current switch.

```
<SW7750> reset rrpp statistics domain 1
```

ring

Syntax **ring** *ring-id* **node-mode** { **master** | **transit** } [**primary-port** *pri-port*] [**secondary-port** *sec-port*] **level** *level-value*

ring *ring-id* **node-mode** { **edge** | **assistant-edge** } [**common-port** *comm-port*] [**edge-port** *edge-port*]

undo ring *ring-id*

View RRPP domain view

Parameter *ring-id*: Ethernet ring network ID, in the range of 1 to 64.

master: Defines the current switch as the master node on the Ethernet ring network.

transit: Defines the current switch as the transit node on the Ethernet ring network.

primary-port pri-port: Specifies a primary port.

secondary-port *sec-port*: Specifies a secondary port.

level-value: RRPP ring level, 0 for primary ring and 1 for secondary ring.

edge: Specifies the current switch as an edge node on the Ethernet ring network.

assistant-edge: Specifies the current switch as an assistant edge node on the Ethernet ring network.

common**-port** *comm-port*: Specifies a common port.

edge-port edge-port: Specifies an edge port.

Description

Use the **ring** command to configure the node role for the current switch and the port role for the port connecting to the Ethernet ring.

Use the **undo ring** command to remove the role configuration.

For an edge node or an assistant edge node, make sure you have removed the secondary ring configuration before removing the primary ring configuration.

Node roles

- Master node: The node that initiates loop detection and prevents data loops. Each ring has one and only one master node.
- Transit node: Nodes on a ring other than the master node are all transit nodes.
- Edge node: A node on the primary ring and a secondary ring at the same time is an edge node. An edge node serves as a transit node on a primary ring and an edge node on a secondary ring. In an RRPP domain, a secondary ring has two edge nodes. You must specify one of them as assistant edge node.

In the same RRPP domain, different rings must have different Ring IDs.

Port roles

Of the two ports that connect the master node and a transit node to an Ethernet ring, one is the primary port and the other the secondary port. The port roles are determined by user configuration.

- The primary port and secondary port of the master node

The primary port of the master node transmits the loop detection packet, and the secondary port of the master node receives the loop detection packet.

When an Ethernet ring is in the healthy state, the secondary port of the master node allows only packets of control VLAN to pass, but logically blocks packets of data VLAN.

When the Ethernet ring is in the broken state, the secondary port of the master node stops blocking the data VLAN and begins to forwards packets of data VLAN.

- The primary and secondary ports on a transit node are functionally the same.
- Of the two ports connecting an edge node to a subring, one is the common port and the other is the edge port of the node. The common port connects

the edge node to the primary ring and a subring at the same time. An edge port is connected only with a subring.

- *RRPP and loopback test functions are mutually exclusive. You must disable the loopback test on the primary/secondary port of the master/transit node and the common/edge port of the edge node.*
- *An aggregation port cannot be configured as a primary/secondary port of the master/transit node and a common/edge port of the edge node.*

Example

# Configure the current switch as the master node on primary ring 10 in RRPP domain 1, GigabitEthernet2/0/5 as the primary port, and GigabitEthernet 2/0/6 as the secondary port.

```
<SW7750> system-view
[SW7750] rrpp domain 1
[SW7750-rrpp-domain1] ring 10 node-mode master primary-port GigabitE
thernet2/0/5 secondary-port GigabitEthernet 2/0/6 level 0
```

# Configure the current switch as the transit node on primary ring 10 in RRPP domain 1, GigabitEthernet2/0/5 as the primary port, and GigabitEthernet 2/0/6 as the secondary port.

```
<SW7750> system-view
[SW7750] rrpp domain 1
[SW7750-rrpp-domain1] ring 10 node-mode transit primary-port Gigabit
Ethernet2/0/5 secondary-port GigabitEthernet 2/0/6 level 0
```

# Configure the current switch as the master node on secondary ring 20 in RRPP domain 1, GigabitEthernet2/0/10 as the primary port, and GigabitEthernet 2/0/11 as the secondary port.

```
<SW7750> system-view
[SW7750] rrpp domain 1
[SW7750-rrpp-domain1] ring 20 node-mode master primary-port GigabitE
thernet 0/10 secondary-port GigabitEthernet 0/11 level 1
```

# Configure the current switch as a transit node on secondary ring 20 in RRPP domain 1, GigabitEthernet2/0/10 as the primary port, and GigabitEthernet 2/0/11 port as secondary port.

```
<SW7750> system-view
[SW7750] rrpp domain 1
[SW7750-rrpp-domain1] ring 20 node-mode transit primary-port Gigabit
Ethernet 2/0/10 secondary-port GigabitEthernet 2/0/11 level 1
```

# Configure the current switch as an edge node on secondary ring 20 in RRPP domain 1, GigabitEthernet2/0/5 as the common port, and GigabitEthernet 2/0/10 as the edge port.

```
<SW7750> system-view
[SW7750] rrpp domain 1
[SW7750-rrpp-domain1] ring 20 node-mode edge common-port GigabitEthe
rnet 2/0/5 edge-port GigabitEthernet 2/0/10
```

# Configure the current switch as an assistant edge node on secondary ring 20 in RRPP domain 1, GigabitEthernet2/0/6 as a common port, and GigabitEthernet 2/0/11 as an edge port.

```
<SW7750> system-view
[SW7750] rrpp domain 1
[SW7750-rrpp-domain1] ring 20 node-mode assistant-edge common-port G
igabitEthernet 2/0/6 edge-port GigabitEthernet 2/0/11
```

# Remove the node role configured for the current switch on RRPP ring 10, and the role configured for the port connecting to the Ethernet ring.

```
<SW7750> system-view
[SW7750] rrpp domain 1
[SW7750-rrpp-domain1] undo ring 10 enable
[SW7750-rrpp-domain1] undo ring 10
```

ring enable

Syntax **ring** *ring-id* **enable**

undo ring *ring-id* **enable**

View RRPP domain view

Parameter *ring-id*: RRPP ring ID, in the range of 1 to 64.

Description Use the **ring enable** command to enable an RRPP ring for the current switch.

Use the **undo ring enable** command to disable an RRPP ring on the current switch.

To enable the RRPP domain of the current switch, you must enable RRPP and the RRPP ring at the same time.

RRPP and STP are mutually exclusive on the port to prevent the possible conflict when the RRPP and STP calculate the blocked/unblocked status of the port.

Related command: **rrpp enable**.

Example # Enable Ethernet ring 10 on RRPP domain 1.

```
<SW7750> system-view
[SW7750] rrpp domain 1
[SW7750-rrpp-domain1] ring 10 enable
```

# Disable Ethernet ring 10 on RRPP domain 1.

```
<SW7750> system-view
[SW7750] rrpp domain 1
[SW7750-rrpp-domain1] undo ring 10 enable
```

rrpp domain

Syntax **rrpp domain** *domain-id*

undo rrpp domain *domain-id*

View System view

Parameter *domain-id*: RRPP domain ID, in the range of 1 to 8.

Description Use the **rrpp domain** command to create an RRPP domain and enter RRPP domain view.

Use the **undo rrpp domain** command to delete an RRPP domain.

Before deleting an RRPP domain, make sure that no RRPP ring exists in the domain. Otherwise, the deletion operation will fail.

Example # Create RRPP domain 1.

```
<SW7750> system-view
[SW7750] rrpp domain 1
New domain created.
[SW7750-rrpp-domain1]
```

# Delete RRPP domain 1.

```
<SW7750> system-view
[SW7750] undo rrpp domain 1
```

rrpp enable

Syntax **rrpp enable**

undo rrpp enable

View System view

Parameter None

Description Use the **rrpp enable** command to enable the RRPP protocol on the current switch.

Use the **undo rrpp enable** command to disable the RRPP protocol on the current switch.

To enable an RRPP ring of the current switch, you must enable RRPP and the RRPP ring at the same time.

Related command: **ring enable**.

Example # Enable the RRPP protocol.

```
<SW7750> system-view
[SW7750] rrpp enable
```

# Disable the RRPP protocol.

```
<SW7750> system-view
[SW7750] undo rrpp enable
```

timer

Syntax **timer hello-timer** *hello-value* **fail-timer** *fail-value*

undo timer

View RRPP domain view

Parameter *hello-value*: Time interval in seconds at which the primary port of the master node sends the health detection packet, in the range of 1 to 10. The default value is 1 second.

fail-value: Timeout time in seconds at which the secondary port of the master node receives the health detection packet, in the range of 3 to 30. The default value is 3 seconds.

Description Use the **timer** command to configure the time values of the Hello timer and Fail timer in the RRPP domain.

Use the **undo timer** command to restore the default time values.

The Fail timer value cannot be less than three times the Hello timer value.

Example # Set the time interval at which the primary port of the master node in RRPP domain 1 sends the health detection packet to 2 seconds, and set the timeout time for the secondary port of the master node in the RRPP domain 1 to receive health detection packets to 7 seconds.

```
<SW7750> system-view
[SW7750] rrpp domain 1
[SW7750-rrpp-domain1] timer hello-timer 2 fail-timer 7
```

# Restore the default timer values for RRPP domain 1.

```
<SW7750> system-view
[SW7750] rrpp domain 1
[SW7750-rrpp-domain1] undo timer
```

90 Netstream Configuration Commands

Currently, the LS81VSNP modules installed in Switch 7750s support the Netstream feature. In this manual, the LS81VSNP module is called I/O Module.

display ip netstream cache

Syntax **display ip netstream cache slot** *slot-number*

View Any view

Parameter *slot-number*: Slot number of an I/O Module.

Description Use the **display ip netstream cache** command to display the Netstream configuration and status of the Netstream cache on the I/O Module in a specified slot.

Example # Display information about the Netstream cache of the I/O Module in slot 3.

```
<SW7750> display ip netstream cache slot 6
IP netstream cache information in slot 6
  Stream active timeout(minute)  : 30
  Stream inactive timeout(second): 60
  Active stream entry            : 0
  Stream entry been counted      : 0
  Last statistics reset time     : none

 Protocol           Total  Packets   Stream   Packets
                  Streams     /Sec     /Sec   /stream
 ----------------------------------------------------
 Total                  0        0        0         0
```

Table 206 Field descriptions of the **display ip netstream cache** command

Field	Description
Stream active timeout(minute) : 30	The current active aging time is 15 minutes.
Stream inactive timeout(second): 60	The current inactive aging time is 60 seconds.
Active stream entry : 50	The Netstream cache contains 50 active stream entries.
Stream entry been counted : 0	Netstream has no stream entries.
Last statistics reset time : none	The statistics have never been cleared.
Protocol, Total Streams, Packets/sec, Stream/sec, Packets/stream	Protocol type, total number of streams, packet per second, stream per second, and average number of packets per stream.

display ip netstream export

Syntax **display ip netstream export slot** *slot-number*

View Any view

Parameter *slot-number*: Slot number of an I/O Module.

Description Use the **display ip netstream export** command to display information about Netstream export packets on the I/O Module in a specified slot.

Example # Display information about Netstream export packets of the I/O Module in slot 6.

```
<SW7750> display ip netstream export slot 6
IP netstream export information in slot 6
IP netstream is enabled in slot : 3
 Version 9 export information:
Stream destination IP(UDP): 10.10.0.10 (30000)
  Stream source address:     3.3.3.3
  Exported stream number:      16
  Exported UDP datagram number(failed number):      16(0)

 Version 9 AS aggregation information:
  Stream destination IP(UDP):  10.10.0.11 (30000)
  Exported stream number:      16
  Exported UDP datagram number(failed number):  2(0)
```

Table 207 Field descriptions of the **display ip netstream export** command

Field	Description
IP netstream export information in slot 6	Information about Netstream export packets on the I/O Module in slot 6 will be followed.
IP netstream is enabled in slot : 3	Slot number of a module where Netstream is enabled
Version 9 export information:	The following is information about version 9 Netstream export packets
Stream destination IP(UDP):	Destination IP address and UDP port number of Netstream export packets
Not destination address for exported packet.	This information is displayed if you do not configure the destination IP address for Netstream export packets.
Exported stream number:	Number of sent stream entries
Exported UDP datagram number(failed number):	Number of sent UDP packets (Number of UDP packets failed in sending)
Version 9 AS aggregation information:	The following is information about version 9 Netstream export packets when AS aggregation is enabled. This information is not displayed if AS aggregation is not enabled.

enable

Syntax **enable**

undo enable

View Netstream aggregation view

Parameter None

Description Use the **enable** command to enable the aggregation mode corresponding to current aggregation view.

Use the **undo enable** command to disable the aggregation mode.

By default, no aggregation mode is enabled.

Related command: **ip netstream aggregation**.

Example # Enable the AS aggregation mode of Netstream.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ip netstream aggregation as
[SW7750-aggregation-as] enable
```

# Disable the AS aggregation mode of Netstream.

```
[SW7750-aggregation-as] undo enable
```

ip netstream aggregation

Syntax **ip netstream aggregation** { **as** | **protocol-port** | **destination-prefix** | **prefix** | **source-prefix** }

View System view

Parameter **as**: Specifies the view for AS (autonomous system) aggregation mode. In this mode, the Netstream streams are classified by: source and destination AS numbers, outbound interface index.

protocol-port: Specifies the view for protocol-port aggregation mode. In this mode, the Netstream streams are classified by: protocol number, source and destination ports.

source-prefix: Specifies the view for source-prefix aggregation mode. In this mode, the Netstream streams are classified by: source AS number, source mask length and source prefix.

destination-prefix: Specifies the view for destination-prefix aggregation mode. In this mode, the Netstream streams are classified by: destination AS number, destination mask length, destination prefix, and outbound interface index.

prefix: Specifies the view for source- and destination-prefix aggregation mode. In this mode, the Netstream streams are classified by: source and destination AS numbers, source and destination mask lengths, source and destination prefixes, and outbound interface index.

Description Use the **ip netstream aggregation** command to enter a Netstream aggregation view.

Under the aggregation view, you can enable/disable the aggregation function in the corresponding mode, and set the source IP address, the destination IP address and port number for Netstream export packets in version 9 format.

Related commands: **enable**, **ip netstream export host**, and **ip netstream export source**.

Example # Enter Netstream AS aggregation view.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ip netstream aggregation as
[SW7750-aggregation-as]
```

ip netstream export dscp

Syntax **ip netstream export dscp** *dscp-value*

undo ip netstream export dscp

View System view

Parameter *dscp-value*: Differentiated services code point (DSCP) value, ranging from 0 to 63, with 0 as the default value.

Description Use the **ip netstream export dscp** command to configure the DSCP value of Netstream export packets. Netstream export packets will be classified by their DSCP values.

Use the **undo ip netstream export dscp** command to restore the default DSCP value.

Example # Set the DSCP value of Netstream export packets to 60.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ip netstream export dscp 60
```

ip netstream export host

Syntax **ip netstream export host** *ip-address udp-port*

undo ip netstream export host

View System view or Netstream aggregation view

Parameter *ip-address*: IP address of the destination host for Netstream export packets, in dotted decimal notation.

udp-port: UDP port number of the destination host for Netstream export packets.

Description Use the **ip netstream export host** command to configure the IP address and UDP port number of the destination host for Netstream export packets.

Use the **undo ip netstream export host** command to restore the default IP address and port number.

By default:

- The destination IP address is 0.0.0.0 and the destination port number is 0 in system view.
- The destination IP address and port number in aggregation view are those configured in system view.

You can configure different destination IP addresses and port numbers for different aggregation modes.

Related command: **ip netstream aggregation** and **ip netstream export source**.

Example # Configure the destination IP address and UDP port number for Netstream export packets to 172.16.105.48 and 50000 respectively.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ip netstream export host 172.16.105.48 50000
```

ip netstream export source

Syntax **ip netstream export source** *ip-address*

undo ip netstream export source

View System view or Netstream aggregation view

Parameter *ip-address*: IP address, in dotted decimal notation.

Description Use the **ip netstream export source** command to configure the source IP address of Netstream export packets, which will be used as the source address of UDP packets.

Use the **undo ip netstream export source** command to restore the default setting.

By default, the source IP address is 0.0.0.0, which indicates that the IP address of the corresponding outbound interface is used as the source IP address.

You can configure different source IP addresses for different aggregation modes.

Related commands: **ip netstream aggregation** and **ip netstream export host**.

Example

Configure the source IP address of Netstream export packets to 3.3.3.3.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ip netstream export source 3.3.3.3
```

ip netstream export version

Syntax

ip netstream export version *version-number* [**origin-as** | **peer-as**]

undo ip netstream export version

View

System view

Parameter

version-number: Version number for Netstream export packets. Currently, you can configure version 5 or version 9.

origin-as: Use original AS numbers as the AS numbers for individual IP addresses.

peer-as: Use peer AS numbers as the AS numbers for individual IP addresses.

Description

Use the **ip netstream export version** command to configure the version and the AS option for Netstream export packets in non-aggregation mode.

Use the **undo ip netstream export version** command to restore the default configuration.

By default, version 5 is used and the AS option is **peer-as**.

Netstream can use three versions of Netstream export packets to send aged stream entries: version 5, version 8 and version 9. But currently, only version 5 and version 9 are configurable:

- If version 5 is configured: the system sends normal stream entries through version 5 packets and sends aggregated stream entries through version 8 packets.
- If version 9 is configured: the system sends all aged stream entries through version 9 packets.

Example

Configure to use version 5 Netstream export packets and use original AS numbers as the AS numbers for individual IP addresses.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ip netstream export version 5 origin-as
```

ip netstream inbound source

Syntax

ip netstream inbound source *srcslot-number* **to** *dstslot-number* [**acl** *acl-number*]

undo ip netstream inbound source *srcslot-number* **to** *dstslot-number*

View System view

Parameter *srcslot-number*: Slot number of an interface module.

dstslot-number: Slot number of an I/O Module.

acl-number: Index of an ACL.

Description Use the **ip netstream inbound source** command to mirror the inbound packets on an interface module to an I/O Module and enable Netstream, a packet statistics function.

Use the **undo ip netstream inbound source** command to stop the mirroring and disable Netstream.

If the **acl** keyword is used in the **ip netstream inbound source** command, the streams on the interface module that match the ACL will be mirrored onto the I/O Module, which in turn collect packet statistics.

By default, Netstream is disabled.

With ACL rules, up to 100 streams can be mirrored for Netstream statistics collection in the system.

Example # Mirror the inbound packets on the module in slot 3 to the I/O Module in slot 6 and enable Netstream.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ip netstream inbound source 3 to 6
```

ip netstream outbound source

Syntax **ip netstream outbound source** *srcslot-number* **to** *dstslot-number*

undo ip netstream outbound source *srcslot-number* **to** *dstslot-number*

View System view

Parameter *srcslot-number*: Slot number of an interface module.

dstslot-number: Slot number of an I/O Module.

Description Use the **ip netstream outbound source** command to mirror the outbound packets on an interface module to an I/O Module and enable Netstream.

Use the **undo ip netstream outbound** command to stop the mirroring and disable Netstream.

By default, Netstream is disabled.

Example # Mirror the outbound packets on the module in slot 3 to the I/O Module in slot 6 and enable Netstream.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ip netstream outbound source 3 to 6
```

ip netstream template refresh

Syntax **ip netstream template refresh** *packets*

undo ip netstream template refresh

View System view

Parameter *Packets*: Threshold for the number of Netstream packets, ranging from 1 to 600, in packets.

Description Use the **ip netstream template refresh** command to configure a packet threshold for updating the template of version 9 Netstream packets. When the number of transmitted packets exceeds the configured threshold, the system sends the newest template to the NSC (Netstream collector).

Use the **undo ip netstream template refresh** command to restore the default packet threshold.

By default, the packet threshold is 20.

Example # Set the packet threshold for updating the template to 100.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] 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*: Template aging time, ranging from 1 to 3,600, in minutes.

Description Use the **ip netstream template timeout** command to configure a template aging time. When the time for transmitting Netstream packets exceeds the configured aging time, the system sends the newest template to the NSC and counts time again.

Use the **undo ip netstream template timeout** command to restore the default aging time.

By default, the template aging time is 30 minutes.

Example

Set the template aging time to 60 minutes.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ip netstream template timeout 60
```

ip netstream timeout active

Syntax

ip netstream timeout active *minutes*

undo ip netstream timeout active

View

System view

Parameter

minutes: Active aging time for Netstream entries in minutes, in the range of 5 to 60.

Description

Use the **ip netstream timeout active** command to configure the active aging time for Netstream entries.

Use the **undo ip netstream timeout active** command to restore the default active aging time.

By default, the active aging time is 30 minutes.

A stream entry will be aged out when the active time of this stream (the time elapsed since the stream entry was created) exceeds the time limit you set here.

Related command:

ip netstream timeout inactive.

Example

Configure the active aging time for Netstream entries to 60 minutes.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] 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 for Netstream entries in seconds, in the range of 60 to 600.

Description Use the **ip netstream timeout inactive** command to configure the inactive aging time for Netstream entries.

Use the **undo ip netstream timeout inactive** command to restore the default inactive aging time.

By default, the inactive aging time for Netstream entries is 60 seconds.

A stream entry will be aged out when the inactive time of the stream (the time elapsed since the last packet of the stream passed the switch) exceeds the time limit you set here.

Related command: **ip netstream timeout active**.

Example # Configure the inactive aging time for Netstream entries to 150 seconds.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] ip netstream timeout inactive 150
```

reset ip netstream statistics

Syntax **reset ip netstream statistics slot** *slot-number*

View User view

Parameter *slot-number*: Slot number of an I/O Module.

Description Use the **reset ip netstream statistics** command to clear the Netstream statistics and output statistics on a specified I/O Module and age out all the stream entries in the Netstream cache.

*Executing the **reset ip netstream statistics** command will forcibly age out the current stream entries in the NP. This forcible aging procedure may take a long time and stops the creation of any new entry until all current entries are aged out.*

Example # Clear the Netstream statistics and age all the stream entries in the Netstream cache on the I/O Module in slot 6.

```
<SW7750> reset ip netstream statistics slot 6
```

91 POLICY ROUTING CONFIGURATION COMMANDS

Currently, the LS81VSNP modules installed in Switch 7750s support the policy routing feature. In this manual, the LS81VSNP module is called I/O Module.

display qos-vlan traffic-redirect

Syntax **display qos-vlan** [*vlan-id*] **traffic-redirect**

View Any view

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

Description Use the **display qos-vlan traffic-redirect** command to display policy routing configuration.

Use the **display qos-vlan** *vlan-id* **traffic-redirect** command to display policy routing configuration on a specified VLAN interface.

Example # Display policy routing configuration on all VLAN interfaces.

```
<SW7750> display qos-vlan traffic-redirect
Vlan 1 traffic-redirect
 Inbound:
   Matches: Acl 2001 rule 0  running
     Redirected to: next-hop 13.53.3.3 slot 5
Vlan 2 traffic-redirect
 Inbound:
   Matches: Acl 2000 rule 0  running
     Redirected to: next-hop 3.3.3.3 slot 6
```

# Display policy routing configuration on VLAN-interface 2.

```
<SW7750> display qos-vlan 2 traffic-redirect
Vlan 2 traffic-redirect
 Inbound:
   Matches: Acl 2000 rule 0  running
     Redirected to: next-hop 3.3.3.3 slot 6
```

traffic-redirect inbound ip-group

Syntax

1 Redirect packets to a specified VLAN interface

traffic-redirect inbound ip-group { *acl-number* | *acl-name* } [**rule** *rule* [**system-index** *index*]] **interface vlan-interface** *interface-number* [**remark** { **dscp** *dscp* | { **precedence** *precedence* | **tos** *tos* }* }] **slot** *slot-number*

undo traffic-redirect inbound ip-group { *acl-number* | *acl-name* } [**rule** *rule*]

1 Redirect packets to a specified IP address

traffic-redirect inbound ip-group { *acl-number* | *acl-name* } [**rule** *rule* [**system-index** *index*]] **next-hop** *ipaddr* &1-3 [**remark** { **dscp** *dscp* | { **precedence** *precedence* | **tos** *tos* }* }] **slot** *slot-number*

undo traffic-redirect inbound ip-group { *acl-number* | *acl-name* } [**rule** *rule*]

View

VLAN view

Parameters

acl-number: ACL number, ranging from 2000 to 3999.

acl-name: ACL name, a string of 1 to 32 characters.

rule *rule*: Specifies a rule in the ACL. The *rule* argument represents the number of an ACL rule and ranges from 0 to 127. If **rule** *rule* is not provided, all rules in the specified ACL will be applied.

system-index *index*: Specifies a system index for the specified ACL rule. The two parameters are optional. The *index* argument ranges from 0 to 4,294,967,295. When an ACL rule is applied, the system automatically assigns a system index to the rule for search purpose. But you can also manually specify a system index for an ACL rule when executing these commands. Generally, you are not recommended to do so.

interface vlan-interface *interface-number*: Specifies the VLAN interface to which packets are redirected. The *interface-number* argument is the index of a VLAN interface, which ranges from 1 to 4094.

dscp *dscp*: Specifies the value of differential services code point. The *dscp* argument ranges from 0 to 63 and defaults to 0. Packets can be classified by their DSCP values.

precedence *precedence*: Specifies a precedence, which will be used to remark packets. The *precedence* argument ranges from 0 to 7 and defaults to 0.

tos *tos*: Specifies the value of type of service. The *tos* argument ranges from 0 to 15 and defaults to 0. Packets can be classified by their ToS values.

slot *slot-number*: Specifies the slot number of an I/O Module.

next-hop *ipaddr* &1-3: Specifies the IP address(es) to which packets are redirected. You can specify at most three IP addresses in one command line.

Description

Use the **traffic-redirect inbound ip-group** command to redirect inbound packets that match a specified ACL or ACL rule on an I/O Module.

Use the **undo traffic-redirect inbound ip-group** command to remove the inbound packet redirection configuration.

You can redirect packets to a specified VLAN interface or specified IP addresses.

If all specified IP addresses are unreachable, the packets will be forwarded depending on their destination IP addresses, but the action defined by the **remark** keyword (if any) will still be performed.

CAUTION:

- *With ACL rules, up to 100 streams can be redirected in the system.*
- *Up to 3,000* ***traffic-redirect inbound ip-group*** *commands can be configured.*
- *Totally up to 3,000* ***traffic-redirect inbound ip-group*** *and* ***traffic-redirect outbound ip-group*** *commands can be configured.*

Example

Configure to redirect the inbound packets that match ACL 2100 on I/O Module in slot 5 to 10.13.152.1 (the next hop).

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] vlan 3
[SW7750-vlan3] traffic-redirect inbound ip-group 2100 next-hop 10.13
.152.1 slot 5
```

traffic-redirect outbound ip-group

Syntax

1 Redirect packets to a specified VLAN interface

traffic-redirect outbound ip-group { *acl-number* | *acl-name* } [**rule** *rule* [**system-index** *index*]] **interface vlan-interface** *interface-number* [**remark** { **dscp** *dscp* | { **precedence** *precedence* | **tos** *tos* }*}] **slot** *slot-number*

undo traffic-redirect outbound ip-group { *acl-number* | *acl-name* } [**rule** *rule*]

1 Redirect packets to a specified IP address

traffic-redirect outbound ip-group { *acl-number* | *acl-name* } [**rule** *rule* [**system-index** *index*]] **next-hop** *ipaddr* &1-3 [**remark** { **dscp** *dscp* | { **precedence** *precedence* | **tos** *tos* } *}] **slot** *slot-number*

undo traffic-redirect outbound ip-group { *acl-number* | *acl-name* } [**rule** *rule*]

View

VLAN view

Parameter

acl-number: ACL number, ranging from 2000 to 3999.

acl-name: ACL name, a string of 1 to 32 characters.

rule *rule*: Specifies a rule in the ACL. The *rule* argument represents the number of an ACL rule and ranges from 0 to 127. If **rule** *rule* is not provided, all rules in the specified ACL will be applied.

system-index *index*: Specifies a system index for the specified ACL rule. The two parameters are optional. The *index* argument ranges from 0 to 4,294,967,295. When an ACL rule is applied, the system automatically assigns a system index to the rule for search purpose. But you can also manually specify a system index for an ACL rule when executing these commands. Generally, you are not recommended to do so.

interface vlan-interface *interface-number*: Specifies the VLAN interface to which packets are redirected. The *interface-number* argument is the index of a VLAN interface, which ranges from 1 to 4094.

dscp *dscp*: Specifies the value of differential services code point. The *dscp* argument ranges from 0 to 63 and defaults to 0. Packets can be classified by their DSCP values.

precedence *precedence*: Specifies a precedence, which will be used to remark packets.. The *precedence* argument ranges from 0 to 7 and defaults to 0.

tos *tos*: Specifies the value of type of service. The *tos* argument ranges from 0 to 15 and defaults to 0. Packets can be classified by their ToS values.

slot *slot-number*: Specifies the slot number of an I/O Module.

next-hop *ipaddr* &1-3: Specifies the IP address(es) to which packets are redirected. You can specify at most three IP addresses in one command line.

Description

Use the **traffic-redirect outbound ip-group** command to redirect outbound packets that match a specified ACL or ACL rule on an I/O Module.

Use the **undo traffic-redirect outbound ip-group** command to disable the outbound packet redirection configuration.

You can redirect packets to a specified VLAN interface or IP addresses.

If all specified IP addresses are unreachable, the packets will be forwarded depending on their destination IP addresses, but the action defined by the **remark** keyword (if any) will still be performed.

CAUTION:

- *Up to 100 ACL rule-filtered streams can be redirected in the system.*
- *Up to 3,000* ***traffic-redirect outbound ip-group*** *commands can be configured.*
- *Totally up to 3,000* ***traffic-redirect inbound ip-group*** *and* ***traffic-redirect outbound ip-group*** *commands can be configured.*

Example # Configure to redirect the outbound packets that match ACL 2100 on the I/O Module in slot 5 to 10.13.152.2 (the next hop).

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] vlan 3
[SW7750-vlan3] traffic-redirect outbound ip-group 2100 next-hop 10.1
3.152.2 slot 5
```

92 TELNET PROTECTION CONFIGURATION COMMANDS

attack-protection

Syntax **attack-protection** [*ip-address*]

undo attack-protection

View System view

Parameter *ip-address*: Sets special ARP Telnet protection for the specified Layer-3 interface.

Description Use the **attack-protection** command to set global Telnet protection. After you execute this command, the system protects all the Layer-3 interfaces in the Up state.

Use the **undo attack-protection** command to cancel the global Telnet protection.

Use the **attack-protection** *ip-address* command to set special ARP Telnet protection. If the Layer-3 interface corresponding to the specified IP address is in the UP state, Telnet protection is enabled on this Layer-3 interface. If the corresponding Layer-3 interface does not exist or is in the Down state, the system saves this configuration as the special ARP settings and enables Telnet protection when the corresponding Layer-3 interface is in the UP state.

Use the **undo attack-protection** *ip-address* command to cancel the special ARP Telnet protection.

Example # Configure global Telnet protection.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] attack-protection
```

# Configure special ARP Telnet protection.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] attack-protection 192.168.0.1
```

attack-protection disable-defaultroute

Syntax **attack-protection disable-defaultroute**

undo attack-protection disable-defaultroute

View System view

Parameter None

Description Use the **attack-protection disable-defaultroute** command to disable the default-route Telnet protection function.

Use the **undo attack-protection disable-defaultroute** command to enable the default-route Telnet protection function.

By default, default-routing Telnet protection is disabled.

After you enable the NAT function, You cannot configure default-routing Telnet protection.

Example # Enable default-route Telnet login protection.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] undo attack-protection disable-defaultroute
```

attack-protection icmp

Syntax **attack-protection icmp** [*ip-address*]

undo attack-protection icmp

View System view

Parameter *ip-address*: Configures to protect ICMP packets for the specified source IP address.

Description Use the **attack-protection icmp** command to enable ICMP protection.

Use the **undo attack-protection icmp** command to disable ICMP protection.

Before enabling ICMP protection, you need to enable ICMP protection, and then configure global Telnet protection, special ARP Telnet protection, and default-routing Telnet protection.

By default, ICMP protection is disabled.

Example # Protect ICMP packets addressed from the source IP address 192.168.0.100.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] attack-protection icmp 192.168.0.100
```

attack-protection snmp

Syntax **attack-protection snmp** [*ip-address*]

undo attack-protection snmp

View System view

Parameter *ip-address*: Configures to protect SNMP packets for the specified source IP address.

Description Use the **attack-protection snmp** command to enable SNMP protection.

Use the **undo attack-protection snmp** command to disable SNMP protection.

Before enabling SNMP protection, you need to enable SNMP protection, and then configure global Telnet protection, special ARP Telnet protection, and default-routing Telnet protection.

By default, SNMP protection is disabled.

Example # Protect SNMP packets addressed from the source IP address 192.168.0.100.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] attack-protection snmp 192.168.0.100
```

attack-protection telnet

Syntax **attack-protection telnet** [*ip-address*]

undo attack-protection telnet

View System view

Parameter *ip-address*: Configures to protect Telnet packets for the specified source IP address.

Description Use the **attack-protection telnet** command to enable Telnet protection.

Use the **undo attack-protection telnet** command to disable Telnet protection.

Before enabling Telnet protection, you need to enable Telnet protection, and then configure global Telnet protection, special ARP Telnet protection, and default-routing Telnet protection.

By default, Telnet protection is disabled.

Example # Protect Telnet packets addressed from the source IP address 192.168.0.100.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] attack-protection telnet 192.168.0.100
```

93 SMART LINK CONFIGURATION COMMANDS

display smart-link flush

Syntax **display smart-link flush**

View Any view

Parameter None

Description Use the **display smart-link flush** command to view the information about how the Smart Link device processes flush messages.

Example # Display the information about how the Smart Link device processes flush messages.

```
<SW7750> display smart-link flush
Flush interface :Ethernet2/0/1

 Count of flush packets received              : 1
 Time of last flush packet received           : 22:52:23 2006/04/01
 Source MAC of last flush packet received     : 000f-e20f-5566
 Device ID of last flush packet received      : 000f-e20f-5566
 Control VLAN ID of last flush packet received : 1
```

Table 208 Field descriptions of the **display smart-link flush** command

Field	Description
Flush interface	Interface that receives the latest legal flush message
Count of flush packets received	Total number of flush messages received
Time of last flush packet received	Time when the last legal flush message is received
Source MAC of last flush packet received	Source MAC address in the last legal flush message received
Device ID of last flush packet received	Bridge MAC address of the device from which the last legal flush message was received
Control VLAN ID of last flush packet received	Control VLAN ID in the last legal flush message received

A legal fulsh message refers to the message whose control VLAN ID is consistent with the receiving control VLAN ID configured on the receiving port.

display smart-link group

Syntax **display smart-link group** { *group-id* | **all** }

View Any view

Parameter *group-id*: Smart link group ID, in the range of 1 to 48.

all: Displays the information about all Smart Link groups.

Description Use the **display smart-link group** command to display the information about the specific Smart Link group or all the Smart Link groups.

Example # Display the information about Smart Link group 1.

```
<SW7750> display smart-link group 1
 Smart Link Group 1 information:
 Device ID: 000f-e212-3456              Control-VLAN ID: 1
 Member                    Role    State    Flush-count Last-flush-time
--------------------------------------------------------------------------
 Ethernet2/0/1             MASTER  ACTVIE   1           16:37:20 2006/04/21
 AGG-1                     SLAVE   STANDBY  2           17:45:20 2006/04/21
```

Table 209 Field descriptions of the **display smart-link group** command

Field	Description
Member	Member of the Smart Link group
Role	Port role of a Smart Link group member: master or slave.
Status	Port status of a Smart Link group member when the link of this member port is up: active or standby.
Flush-count	Number of sent flush messages
Last-flush-time	Time when the last flush message is sent. If no flush message is sent, "NA" will be displayed.

flush enable control-vlan

Syntax **flush enable control-vlan** *vlan-id*

undo flush enable

View Smart Link group view

Parameter *vlan-id*: Control VLAN ID, in the range of 1 to 4,094.

Description Use the **flush enable control-vlan** command to enable the function of sending flush messages in the specified control VLAN.

Use the **undo flush enable control-vlan** command to disable the function of sending flush messages to the specified control VLAN.

By default, no control VLAN is specified.

Example # Configure to send flush messages within control VLAN 1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] smart-link group 1
[SW7750-smlk-group1] flush enable control-vlan 1
```

link-aggregation group

Syntax **link-aggregation group** *group-id* { **master** | **slave** }

undo link-aggregation group *group-id*

View Smart Link group view

Parameter *group-id*: Link aggregation group ID, in the range of 1 to 384 (only link aggregation groups configured manually or statically are available).

master: Configures the specified link aggregation group as the master port of the Smart Link group.

slave: Configures the specified link aggregation group as the slave port of the Smart Link group.

Description Use the **link-aggregation group** command to configure a link aggregation group as a member of the Smart Link group.

Use the **undo link-aggregation group** command to remove the specified link aggregation group from the current Smart Link group.

Smart Link and STP cannot be enabled on an Ethernet port at the same time. Make sure that STP is not enabled on the port of the link aggregation group before configuring the link aggregation group as a member of the Smart Link group.

Example # Configure link aggregation group 8 as the slave port of Smart Link group 1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] smart-link group 1
[SW7750-smlk-group1] link-aggregation group 8 slave
```

port

Syntax **port** *interface-type interface-number* { **master** | **slave** }

undo port *interface-type interface-number*

View Smart Link group view

Parameter *interface-type*: Port type.

interface-number: Port number.

master: Configures the specified port as the master port of the Smart Link group.

slave: Configures the specified port as the slave port of the Smart Link group.

Description

Use the **port** command to configure the specified port as a member of the Smart Link group.

Use the **undo port** command to remove the specified port from the Smart Link group.

Either a single port or a link aggregation group configured manually or statically can serve as a member for a Smart Link group. However, a link aggregation group configured dynamically cannot serve as a member for a Smart Link group. This command is not applicable to member ports in a link aggregation group.

Smart Link and STP cannot be enabled on an Ethernet port at the same time. Make sure that STP is not enabled on the port of the link aggregation group before configuring the link aggregation group as a member of the Smart Link group.

Example

Configure Ethernet2/0/6 as the slave port of Smart Link group 1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] smart-link group 1
[SW7750-smlk-group1] port Ethernet 2/0/6 slave
```

port smart-link group

Syntax

port smart-link group *group-id* { **master** | **slave** }

undo port smart-link group *group-id*

View

Ethernet port view

Parameter

group-id: Smart link group ID, in the range of 1 to 48.

master: Configures the port as the master port of the Smart Link group.

slave: Configures the port as the slave port of the Smart Link group.

Description

Use the **port smart-link group** command to configure the current port as a member of the Smart Link group.

Use the **undo port smart-link group** command to remove the current port from the specified Smart Link group.

Either a single port or a link aggregation group configured manually or statically can serve as a member for a Smart Link group. However, a link aggregation group configured dynamically cannot serve as a member for a Smart Link group. This command is not applicable to member ports in a link aggregation group.

Smart Link and STP cannot be enabled on an Ethernet port at the same time. Make sure that STP is not enabled on the port of the link aggregation group before configuring the link aggregation group as a member of the Smart Link group.

Example # Configure Ethernet2/0/3 as the master port of Smart Link group 1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet 2/0/3
[SW7750-Ethernet2/0/3] port smart-link group 1 master
```

reset smart-link packets counter

Syntax **reset smart-link packets counter**

View User view

Parameter None

Description Use the **reset smart-link packets counter** command to clear the flush message statistics of Smart Link.

Example # Clear the flush message statistics of Smart Link.

```
<SW7750> reset smart-link packets counter
```

smart-link flush enable

Syntax

- In Ethernet port view:

smart-link flush enable control-vlan *vlan-id*

undo smart-link flush enable

- In system view:

smart-link flush enable control-vlan *vlan-id* **port** *interface-type interface-number* [**to** *interface-type interface-number*]

undo smart-link flush enable port *interface-type interface-number* [**to** *interface-type interface-number*]

View Ethernet port view/system view

Parameter *vlan-id*: Control VLAN ID, in the range of 1 to 4,094.

Description Use the **smart-link flush enable control-vlan** command to enable the current/specified port to process flush messages received on the specified control VLAN.

Use the **undo smart-link flush enable** command to disable the port from processing flush messages.

- The command executed in Ethernet port view has effect on the current port only.
- The command executed in system view has effect on the specified port only.

By default, no control VLAN is specified.

If you configure different control VLANs on the same port, only the last one takes effect.

The VLAN configured as a control VLAN for sending or receiving flush messages must exist. You cannot directly remove the control VLAN. When a dynamic VLAN is configured as a control VLAN for the Smart Link group, this VLAN will become a static VLAN, and related prompt information is displayed.

Example # Enable Ethernet2/0/4 to process flush messages received from control VLAN 1..

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet 2/0/4
[SW7750-Ethernet2/0/4] smart-link flush enable control-vlan 1
```

# Enable Ethernet2/0/5 through Ethernet2/0/10 to process flush messages received from control VLAN 1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] smart-link flush enable control-vlan 1 port Ethernet 2/0/5
to Ethernet 2/0/10
```

smart-link group

Syntax **smart-link group** *group-id*

undo smart-link group *group-id*

View System view

Parameter *group-id*: Smart link group ID, in the range of 1 to 48.

Description Use the **smart-link group** command to create a Smart Link group and enter Smart Link group view. If the specified Smart Link group exists, this command leads you into Smart Link group view directly.

Use the **undo smart-link group** command to remove the specified Smart Link group.

After creating a Smart Link group, you must configure member ports for this Smart Link group.

Related command: **port smart-link group**, **link-aggregation group**, and **port**.

Make sure that the Smart Link group has no members before executing the undo ***smart-link group*** *command.*

Example # Create a Smart Link group.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] smart-link group 1
New Smart Link Group has been created.
[SW7750-smlk-group1]
```

94 MONITOR LINK CONFIGURATION COMMANDS

display monitor-link group

Syntax **display monitor-link group** { *group-id*| **all** }

View Any view

Parameter *group-id*: Monitor Link group ID, ranging 1 to 96.

all: Specifies all the Monitor Link groups.

Description Use the **display monitor-link group** command to display Monitor Link group information.

Example # Display the information about Monitor Link group 1.

```
<SW7750> display monitor-link group 1
Monitor link group 1 information:
Member  Role       Status     Last-up-time          Last-down-time
----------------------------------------------------------------------
SMLK-2  UPLINK     UP         16:37:20 2006/4/21   16:37:20 2006/4/20
AGG-1   DOWNLINK   UP
```

Table 210 Field descriptions of the **display monitor-link group** command

Field	Description
Member	Member of the Monitor Link group
Role	Role of Monitor Link group member port: UPLINK or DOWNLINK
Status	Status of Monitor Link group member port: UP or DOWN
Last-up-time	Last time the port is up
Last-down-time	Last time the port is down

link-aggregation group

Syntax **link-aggregation group** *group-id*{ **uplink** | **downlink** }

undo link-aggregation group *group-id*

View Monitor Link group view

Parameter *group-id*: Link aggregation group ID, ranging from 1 to 384 (A link aggregation group can be a manual or static link aggregation group only).

uplink: Configures the specified link aggregation group as the uplink port of the Monitor Link group

downlink: Configures the specified link aggregation group as the downlink port of the Monitor Link group

Description Use the **link-aggregation group** command to configure the specified link aggregation group as a Monitor Link group member.

Use the **undo link-aggregation group** command to remove the specified link aggregation group from the current Monitor Link group.

In Monitor Link, a Monitor Link group member can be a single port, a manual or static link aggregation group, but not a dynamic link aggregation group. Uplink port can also be a Smart Link group.

Use this command only on the link aggregation groups that are not Smart Link group members.

A port or a link aggregation group cannot serve as a member port for two Smart Link groups. On the other hand, a port or a link aggregation group cannot serve as a member of a Smart Link group and a Monitor Link group at the same time. However, a Smart Link group can serve as the uplink member port of a Monitor Link group.

Example # Configure link aggregation group 8 as the downlink port of the Monitor Link group.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] monitor-link group 1
[SW7750-mtlk-group1] link-aggregation group 8 downlink
```

monitor-link group

Syntax **monitor-link group** *group-id*

undo monitor-link group *group-id*

View System view

Parameter *group-id*: Monitor Link group ID, ranging from 1 to 96.

Description Use the **monitor-link group** command to create a Monitor Link group and enter Monitor Link group view.

Use the **undo monitor-link group** command to remove a Monitor Link group.

After the Monitor Link group is configured, member ports of the Monitor Link group need to be configured.

Related command: **port monitor-link group**, **link-aggregation group**, **smart-link group**, and **port**.

Make sure that the Monitor Link group has no members before executing the undo ***monitor-link group*** *command.*

Example # Create a Monitor Link group.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] monitor-link group 1
 New Monitor Link Group has been created.
[SW7750-mtlk-group1]
```

port

Syntax **port** *interface-type interface-number* { **uplink** | **downlink** }

undo port *interface-type interface-number*

View Monitor Link group view

Parameter *interface-type*: Port type.

interface-number: Port number.

uplink: Configures the specified port as the uplink port of the Monitor Link group

downlink: Configures the specified port as the downlink port of the Monitor Link group

Description Use the **port** command to configure the specified port as a member of the Monitor Link group.

Use the **undo port** command to remove the specified port from the current Monitor Link group.

In Monitor Link, a Monitor Link group member can be a single port, a static link aggregation group, but not a dynamic link aggregation group. The uplink port of a Monitor Link group can also be a Smart Link group.

Do not use this command on member ports of a link aggregation group or a Smart Link group.

A port or a link aggregation group cannot serve as a member port for two Smart Link groups. On the other hand, a port or a link aggregation group cannot serve as a member for a Smart Link group and a Monitor Link group at the same time. However, a Smart Link group can serve as the uplink member port of a Monitor Link group.

Example # Configure Ethernet2/0/7 as a downlink port of the Monitor Link group

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] monitor-link group 1
[SW7750-mtlk-group1] port Ethernet 2/0/7 downlink
```

port monitor-link group

Syntax **port monitor-link group** *group-id*{ **uplink** | **downlink** }

undo port monitor-link group *group-id*

View Ethernet port view

Parameter *group-id*: Monitor Link group ID, ranging 1 to 96.

uplink: Configures the port as the uplink port of the specified Monitor Link group

downlink: Configures the port as the downlink port of the specified Monitor Link group

Description Use the **port monitor-link group** command to configure the current port as a member of the specified Monitor Link group.

Use the **undo port monitor-link group** command to remove the current port from the specified Monitor Link group.

In Monitor Link, a Monitor Link group member can be a single port, a static link aggregation group, but not a dynamic link aggregation group. Uplink port can also be a Smart Link group.

Do not use this command on member ports of a link aggregation group or a Smart Link group.

A port or a link aggregation group cannot serve as a member port for two Smart Link groups. On the other hand, a port or a link aggregation group cannot serve as a member for a Smart Link group and a Monitor Link group at the same time. However, a Smart Link group can serve as the uplink member port of a Monitor Link group.

Example # Configure Ethernet2/0/8 as a downlink port of Monitor Link group 1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Ethernet 2/0/8
[SW7750-Ethernet2/0/8] port monitor-link group 1 downlink
```

smart-link group

Syntax **smart-link group** *group-id* **uplink**

undo smart-link group *group-id*

View Monitor Link group view

Parameter *group-id*: Smart Link group ID, ranging 1 to 48.

uplink: Configures the specified Smart Link group as the uplink port of the Monitor Link group

Description Use the **smart-link group** command to configure the specified Smart Link group as the uplink port of the Monitor Link group.

Use the **undo smart-link group** command to remove the configuration.

A Smart Link group can belong to only one Monitor Link group and can be configured only as an uplink port of the Monitor Link group.

Example # Configure Smart Link group 1 as the uplink port of Monitor Link group 1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] monitor-link group 1
[SW7750-mtlk-group1] smart-link group 1 uplink
```

95 COMMANDS FOR BOOT ROM UPGRADE WITH APP FILE

boot bootrom default

Syntax **boot bootrom default** [**slot** *slot-number-lis*t]

View User view

Parameter *slot-number-list*: Specifies a slot number list of the switch. *slot-number-list* = { *slot-number* [**to** *slot-number*] }&<1-N>. &<1-N> means you can enter the previous parameters up to N times. For the Switch 7757, and 7758, N is 7 and for the Switch 7754, N is 4.

Description Use the **boot bootrom default** command to use the current startup file to upgrade the Boot ROMs.

Example # Use the current startup file to upgrade the Boot ROMs of all normal I/O Module modules in position.

```
<SW7750> boot bootrom default
```

boot bootrom file-url

Syntax **boot bootrom** *file-url* [**slot** *slot-number-lis*t]

View User view

Parameter *file-url*: Specifies the Boot ROM file path and file name in the Flash memory.

slot-number-list: Specifies a slot number list of the switch. *slot-number-list* = { *slot-number* [**to** *slot-number*] }&<1-N>. &<1-N> means you can enter the previous parameters up to N times. For the Switch 7757, and 7758, N is 7 and for the Switch 7754, N is 4.

Description Use the **boot bootrom** *file-url* command to use the specified App file to upgrade the Boot ROMs.

Example # Use the specified App file (**abcd.app**) to upgrade the Boot ROMs of slot 1 I/O Module modules in position.

```
<SW7750> boot bootrom abcd.app slot 1
```

boot boot-loader primary

Syntax **boot boot-loader primary** *file-url*

View User view

Parameter *file-url*: Specifies the Boot ROM file path and file name in the Flash memory.

Description Use the **boot boot-loader primary** command to specify the primary startup file at next booting.

Example # Specify the App file **abcd.app** as the primary startup file for next booting and use it to upgrade the Boot ROMs.

```
<SW7750> boot boot-loader primary abcd.app
```

96 INTER-CARD LINK STATE ADJUSTMENT CONFIGURATION COMMANDS

set inlink

Syntax **set inlink** { **auto** | **fix** }

View System view

Parameter **auto**: Sets the inter-card links are established in the auto negotiation mode.

fix: Sets the inter-card links are established the fix mode.

Description Use the **set inlink** command to set the mode in which inter-card links are established. By default, inter-card links are established in the auto negotiation mode.

Example # Configure the inter-card links to be established in the fix mode.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] set inlink fix
```

97 INTERNAL CHANNEL MONITOR COMMANDS

monitor inner-channel

Syntax

monitor inner-channel [**reboot-lpu** | **reboot-switch**]

undo monitor inner-channel [**reboot-lpu** | **reboot-switch**]

View

System view

Parameter

reboot-lpu: Restarts a service module.

reboot-switch: Restarts a switch.

Description

Use the **monitor inner-channel** command to enable the function of monitoring internal channels.

Use the **undo monitor inner-channel** command to disable the function of monitoring internal channels.

By default, the function of monitoring internal channels is enabled.

An internal channel refers to the interface channel between the Fabric and the service modules. The Fabric sends handshake packets to each service module every second. After receiving the handshake packets, the service modules reports the result to the Fabric. In this case, the Fabric knows that the service modules are operating normally. Through this process, the Fabric can judge whether each service module in the device operates normally.

Switch 7750s support this feature. Through this feature, you can monitor internal channels.

You can also set the maximum number of times the Fabric fails to receive handshake packets. If the number of times the Fabric fails to receive handshake packets exceeds the upper limit, the switch resets the processing chip automatically. When the Fabric receives handshake packets, it resets the counter automatically.

You can also set whether to restart the service module or the switch when the number of times the Fabric fails to receive handshake packets exceeds the upper limit.

Example

Enable the function of monitoring internal channels

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] monitor inner-channel
```

monitor inner-channel

Syntax **monitor inner-channel upper-limit** *upper-timers*

undo monitor inner-channel

View System view

Parameter *upper-times:* Specifies the upper limit.

Description Use the **monitor inner-channel upper-limit** command to set the maximum number of times of monitoring internal channels.

Use the **undo monitor inner-channel** command to disable the function of setting the maximum number of times of monitoring internal channels.

The default value is 10.

An internal channel refers to the interface channel between the Fabric and the service modules. The Fabric sends handshake packets to each service module every second. After receiving the handshake packets, the service modules reports the result to the Fabric. In this case, the Fabric knows that the service modules are operating normally. Through this process, the Fabric can judge whether each service module in the device operates normally.

Switch 7750s support this feature. Through this feature, you can monitor internal channels.

You can also set the maximum number of times the Fabric fails to receive handshake packets. If the number of times the Fabric fails to receive handshake packets exceeds the upper limit, the switch resets the processing chip automatically. When the Fabric receives handshake packets, it resets the counter automatically.

Example # Set the upper limit to 50.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] monitor inner-channel upper-limit 50
```

98 SWITCH CHIP AUTO-RESET CONFIGURATION COMMANDS

monitor slot

Syntax

monitor slot *slot-id* **enable**

monitor slot *slot-id* **disable**

View

System view

Parameter

slot-id: Slot ID. The value range depends on the products (Switch 7754: 0 to 3; Switch 7757: 0 to 6; Switch 7758: 0 to 7).

Description

Use the **monitor slot enable** command to enable switch chip auto-reset.

Use the **monitor slot disable** command to disable switch chip auto-reset.

By default, switch chips cannot be reset automatically when the internal channel handshake fails.

In actual application, a switch may fail to process services normally due to internal channel block or because the switch chip is busy.

Switch 7750s support the function of resetting switch chips automatically. In case that the function of monitoring internal channels is enabled, when the internal channel handshake between a module and the backplane fails, the switch resets the switch chip automatically to resume the corresponding module.

When the function of resetting switch chips is disabled, even if the switch finds that the internal channel handshake fails, it cannot reset the switch chip automatically.

Example

Enable switch chip auto-reset for the module in slot 2.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] monitor inner-channel
[SW7750] monitor slot 2 enable
```

99 CPU USAGE THRESHOLD CONFIGURATION COMMAND

cpu-usage-threshold

Syntax **cpu-usage-threshold** *value* [**slot** *slot-id*]

undo cpu-usage-threshold [**slot** *slot-id*]

View System view

Parameter *value*: Upper limit of the CPU usage threshold, ranging from 1 to 99.

slot-id: Slot ID. The value range depends on the products (Switch 7754: 0 to 3; Switch 7757: 0 to 6; Switch 7758: 0 to 7).

Description Use the **cpu-usage-threshold** command to enable CPU usage threshold configuration.

Use the **undo cpu-usage-threshold** command to disable this function.

By default, this function is disabled.

Switch 7750 Ethernet switches support CPU usage threshold configuration. When the CPU usage exceeds the configured threshold, the switch sends trap messages and log messages, according to which the network administrator can modify the switch configuration.

Switch 7750 Ethernet switches also support configuration of the CPU usage threshold of the specified module. You can specify **slot** *slot-number* to configure the CPU usage threshold of the specified module. When the CPU usage of the module in the specified slot exceeds the configured threshold, the switch sends trap messages and log messages to the network administrator.

If you set CPU thresholds for both all the modules and the specified module, the CPU threshold of the specified module is determined by the latter one. For example, if you set the CPU usage threshold of all the modules to 88 and set that of the module in slot 2 to 77, the CPU usage threshold of the module in slot 2 is 77.

Example # Enable CPU usage threshold configuration on the module in slot 2 and set the upper limit to 88.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] cpu-usage-threshold 88 slot 2
```