Switch 7750
Configuration Guide

Version 3.1.5

http://www.3com.com/

CONTENTS

IP ROUTING PROTOCOL OPERATION

MULTICAST PROTOCOL

QoS/ OPERATION

STP OPERATION

AAA AND RADIUS OPERATION

SYSTEM MANAGEMENT

ABOUT THIS GUIDE

This guide describes the 3Com® Switch 7750 and how to configure it in version 3.0 of the software.

Conventions

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

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.

Table 2 lists the text conventions used in this book.

Table 2   Text Conventions

Convention	Description
Screen displays	This typeface represents information as it appears on the screen.
Keyboard key names	If you must press two or more keys simultaneously, the key names are linked with a plus sign (+), for example: Press Ctrl+Alt+Del
The words "enter" and type"	When you see the word "enter" in this guide, you must type something, and then press Return or Enter. Do not press Return or Enter when an instruction simply says "type."

Table 2 Text Conventions

Convention	Description
Words in *italics*	Italics are used to:
	■ Emphasize a point.
	■ Denote a new term at the place where it is defined in the text.
	■ Identify command variables.
	■ Identify menu names, menu commands, and software button names. Examples:
	From the *Help* menu, select *Contents*.
	Click *OK*.
Words in **bold**	Boldface type is used to highlight command names. For example, "Use the **display user-interface** command to…"

1

SYSTEM ACCESS

This chapter covers the following topics:

- Product Overview
- Configuring the Switch 7750
- Setting Terminal Parameters
- Command Line Interface

Product Overview

The 3Com Switch 7750 is a large capacity, modularized wire speed Layer 2/Layer 3 switch. It is designed for IP metropolitan area networks (MAN), large-sized enterprise networks, and campus network users.

The Switch 7750 has an integrated chassis structure. The chassis contains a card area, fan area, power supply area, and a power distribution area. In the card area, there are seven slots. Slot 0 is prepared specially for the switch Fabric module. The remaining slots are for interface modules. You can install different interface modules for different networks; the slots support a mixed set of modules.

The Switch 7750 supports the following services:

- MAN, enterprise/campus networking
- Multicast service and multicast routing functions and audio and video multicast service.

Features

Table 3 lists and describes the function features that the Switch 7750 supports.

Table 3   Function Features

Features	Support
VLAN	VLANs compliant with IEEE 802.1Q standard Port-based VLAN Protocol-based VLAN GARP VLAN Registration Protocol (GVRP)
STP protocol	Spanning Tree Protocol (STP) Multiple Spanning Tree Protocol (MSTP), compliant with IEEE 802.1D/IEEE 802.1s Standard
Flow control	IEEE 802.3x flow control (full-duplex) Back-pressure based flow control (half-duplex)
Broadcast suppression	Broadcast suppression
Multicast	GARP Multicast Registration Protocol (GMRP) Internet Group Management Protocol (IGMP) Snooping Internet Group Management Protocol (IGMP) Protocol-Independent Multicast-Dense Mode (PIM-DM) Protocol-Independent Multicast-Sparse Mode (PIM-SM)

Table 3   Function Features (continued)

Features	Support
IP routing	Static route RIP V1/v2 IP routing policy
DHCP Relay	Dynamic Host Configuration Protocol (DHCP) Relay
Link aggregation	Link aggregation
Mirror	Port-based mirroring
Security features	Multi-level user management and password protection 802.1X authentication Packet filtering AAA and RADIUS/HWTACACS
Quality of Service (QoS)	Traffic classification Bandwidth control Priority Queues of different priority on the port Queue scheduling: supports Strict Priority Queueing (SP)
Management and maintenance	Command line interface configuration Configuration through the console port Remote configuration by Telnet Configuration through dialing the modem SNMP System log Level alarms Output of the debugging information PING and Tracert Remote maintenance with Telnet, modem
Loading and updating	Loading and upgrading software using the XModem protocol Loading and upgrading software using the File Transfer Protocol (FTP) and Trivial File Transfer Protocol (TFTP)

Configuring the Switch 7750

On the Switch 7750, you can set up the configuration environment through the console port. To set up the local configuration environment:

1 Plug the DB-9 or DB-25 female plug of the console cable into the serial port of the PC or the terminal where the switch is to be configured.

2 Connect the RJ-45 connector of the console cable to the console port of the switch, as shown in Figure 1.

Figure 1   Setting Up the Local Configuration Environment Through the Console Port

RS-232 Serial port

Console port

Console cable
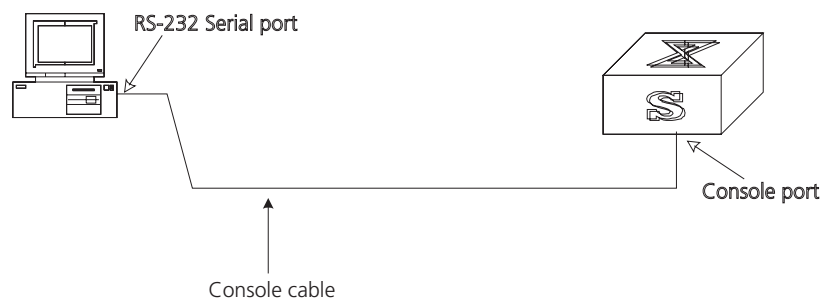
Setting Terminal Parameters

To set terminal parameters:

1 Start the PC and select *Start > Programs > Accessories > Communications > HyperTerminal*. The HyperTerminal window displays the Connection Description dialog box, as shown in Figure 2.

Figure 2   Set Up the New Connection
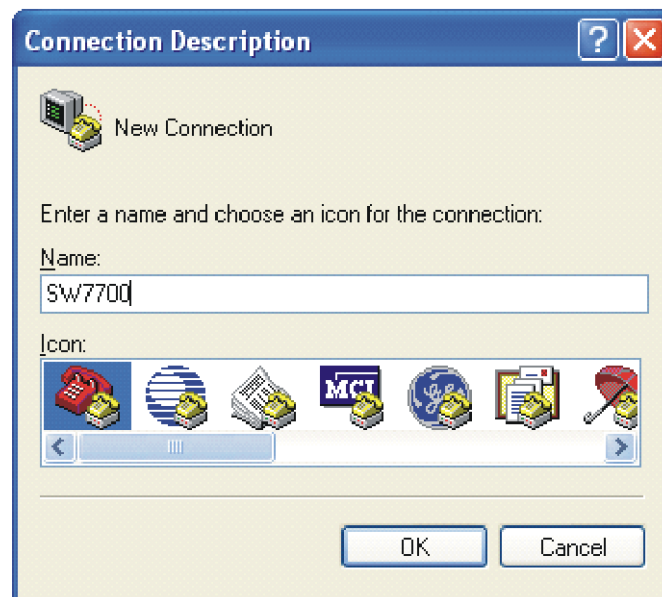
2 Enter the name of the new connection in the *Name* field and click *OK*. The dialog box, shown in Figure 3 displays.

3 Select the serial port to be used from the *Connect using* dropdown menu.

Figure 3   Properties Dialog Box

4 Click *OK*. The Port Settings tab, shown in Figure 4, displays and you can set serial port parameters. Set the following parameters:

- Baud rate = 9600
- Databit = 8
- Parity check = none
- Stopbit = 1
- Flow control = none

Figure 4   Set Communication Parameters
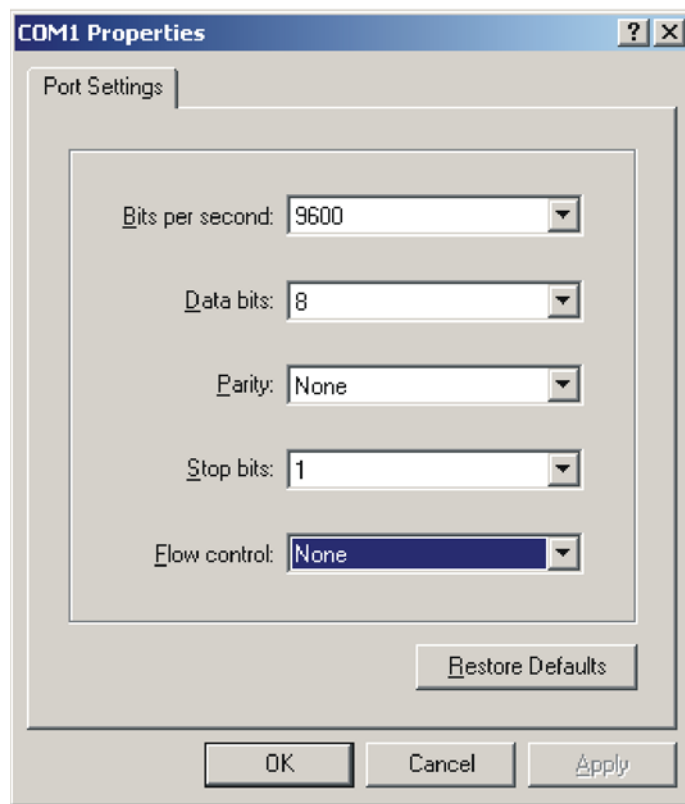
5 Click *OK*. The HyperTerminal dialogue box displays, as shown in Figure 5.

6 Select *Properties*.

Figure 5   HyperTerminal Window
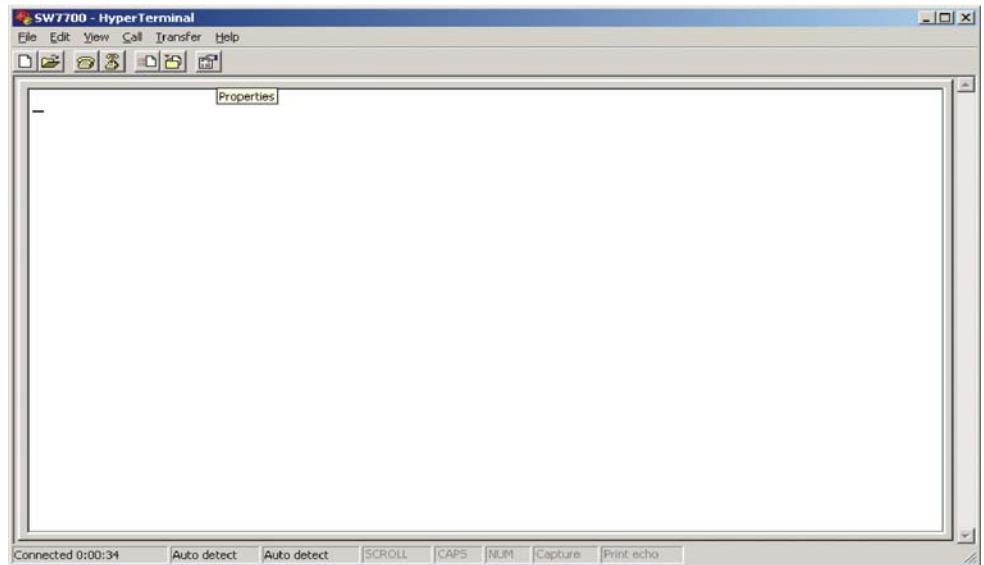
7 In the Properties dialog box, select the *Settings* tab, as shown in Figure 6.

8 Select *VT100* in the *Emulation* dropdown menu.

9 Click *OK*.

Figure 6   Settings Tab
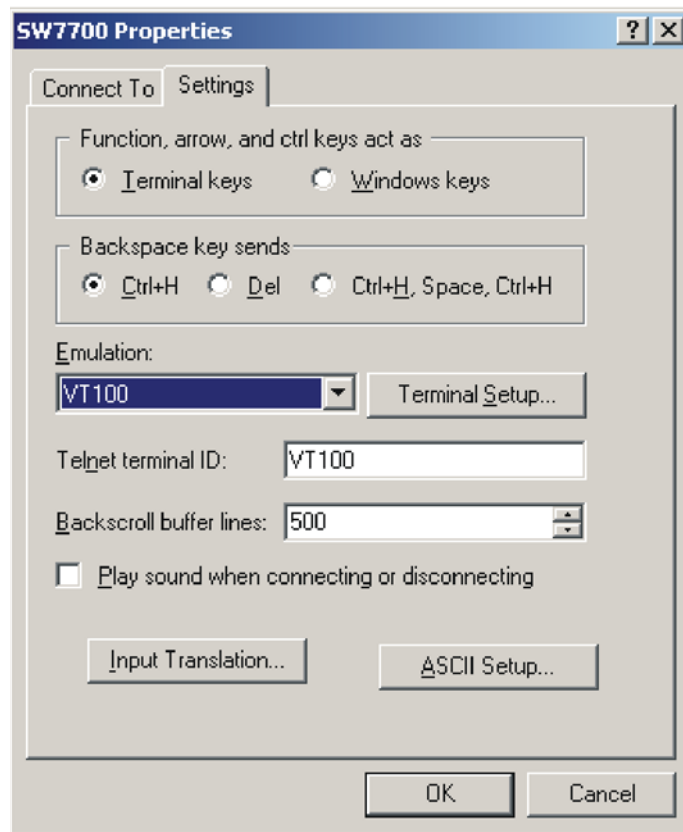
Setting the Terminal Parameters is described in the following sections:

- Configuring Through Telnet
- Configuring Through a Dial-up Modem
- Configuring the User Interface

Configuring Through Telnet

Before you can telnet to a Switch 7750 and configure it, you must:

1 Configure the IP address of a VLAN interface for the Switch 7750 through the console port (using the **ip address** command in VLAN interface view)

2 Add the port (that connects to a terminal) to this VLAN (using the **port** command in VLAN view)

3 Log in to the Switch 7750

Tasks for Configuring through Telnet are described in the following sections:

- Connecting the PC to the Switch 7750
- Connecting Two Switch 7750 Systems

Connecting the PC to the Switch 7750

To connect the PC and Switch 7750 through Telnet:

1 Authenticate the Telnet user through the console port before the user logs in by Telnet.

> [i] *By default, a password is required for authenticating the Telnet user to log in the Switch 7750. If a user logs in by Telnet without a password, the user sees the message:* `Login password has not been set!`

2 Enter system view, return to user view by pressing *Ctrl+Z*.

```
<SW7750>system-view
[SW7750]user-interface vty 0 4
[SW7750-ui-vty0]set authentication password simple/cipher xxxx
```

(xxxx is the preset login password of Telnet user)

3 To set up the configuration environment, connect the Ethernet port of the PC to that of the Switch 7750 through the LAN. See Figure 7.

Figure 7 Setting Up the Configuration Environment Through Telnet
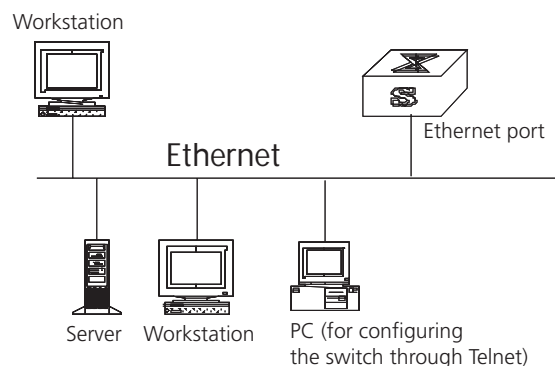
4 Run Telnet on the PC by selecting *Start > Run* from the Windows desktop and entering *Telnet* in the *Open* field, as shown in Figure 8. Click *OK*.

Figure 8   Run Telnet
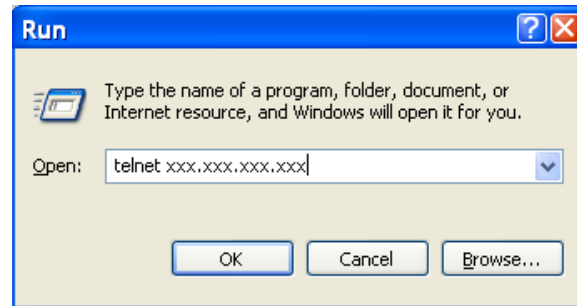
The terminal displays *Login authentication* and prompts you for the logon password.

5 Enter the password. The terminal displays the command line prompt (`<SW7750>`).

If the message, `All user interfaces are used, please try later!` appears, try to reconnect later. At most, 5 Telnet users are allowed to log on to a Switch 7750 simultaneously.

6 Use the appropriate commands to configure the Switch 7750 or to monitor the operational state. Enter `?` to get immediate help. For details on specific commands, refer to the chapters in this guide.

> *When configuring the Switch 7750 by Telnet, do not modify the IP address unless necessary, because the modification might terminate the Telnet connection. By default, after passing the password authentication and logging on, a Telnet user can access the commands at login level 0.*

Connecting Two Switch 7750 Systems

Before you can telnet the Switch 7750 to another Switch 7750, as shown in Figure 9, you must:

1 Configure the IP address of a VLAN interface for the Switch 7750 through the console port (using the `ip address` command in VLAN interface view)

2 Add the port (that connects to a terminal) to this VLAN (using the `port` command in VLAN view)

3 Log in to the Switch 7750

After you telnet to a Switch 7750, you can run the `telnet` command to log in and configure another Switch 7750.

Figure 9   Provide Telnet Client Service

PC   Telnet client   Telnet server
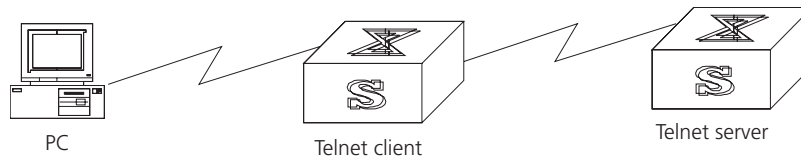
1 Authenticate the Telnet user through the console port on the Telnet Server (Switch 7750) before login.

> *By default, a password is required for authenticating the Telnet user to log in the Switch 7750. If a user logs into Telnet without password, the system displays the following message:* `Login password has not been set!`

2 Enter system view, return to user view by pressing *Ctrl+Z*.

```
<SW7750>system-view
[SW7750]user-interface vty 0
[SW7750-ui-vty0]set authentication password simple/cipher xxxx (xxxx
is the preset login password of Telnet user)
```

3 Log in to the Telnet client (Switch 7750). For the login process, see "Connecting the PC to the Switch 7750".

4 Perform the following operations on the Telnet client:

```
<SW7750>telnet xxxx
```

(XXXX can be the hostname or IP address of the Telnet Server. If it is the hostname, you must use the **ip host** command to specify it.

5 Enter the preset login password. The Switch 7750 prompt (`<SW7750>`) displays. If the message, `All user interfaces are used, please try later!` displays, try to connect later.

6 Use the appropriate commands to configure the Switch 7750 or view its operational state. Enter **?** to get immediate help. For details on a specific command, refer to the appropriate chapter in this guide.

Configuring Through a Dial-up Modem   To configure your router through a dial-up modem:

1 Authenticate the modem user through the console port of the Switch 7750 before the user logs in to the switch through a dial-up modem.

> *By default, a password is required for authenticating the modem user to log in to the Switch 7750. If a user logs in through the modem without a password, the user sees an error message.*

```
<SW7750>system-view
[SW7750]user-interface aux 0
[SW7750-ui-aux0]set authentication password simple/cipher xxxx (xxxx
is the preset login password of the Modem user.)
```

2 Using the **modem** command, you can configure the console port to modem mode.

```
[SW7750-ui-aux0]modem
```

3 To set up the remote configuration environment, connect the modems to a PC (or a terminal) serial port and to the Switch 7750 console port, as shown in Set Up Remote Configuration Environment.

Figure 10 Set Up Remote Configuration Environment
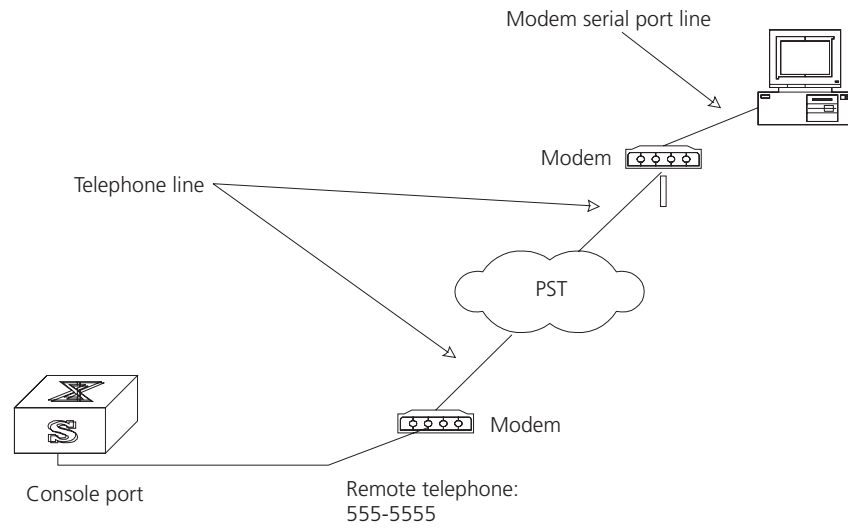
4 Dial for a connection to the switch, using the terminal emulator and modem on the remote end. Dial the telephone number of the modem connected to the Switch 7750. See Figure 11 and Figure 12.

Figure 11 Set the Dialed Number

Figure 12 Dial the Remote PC
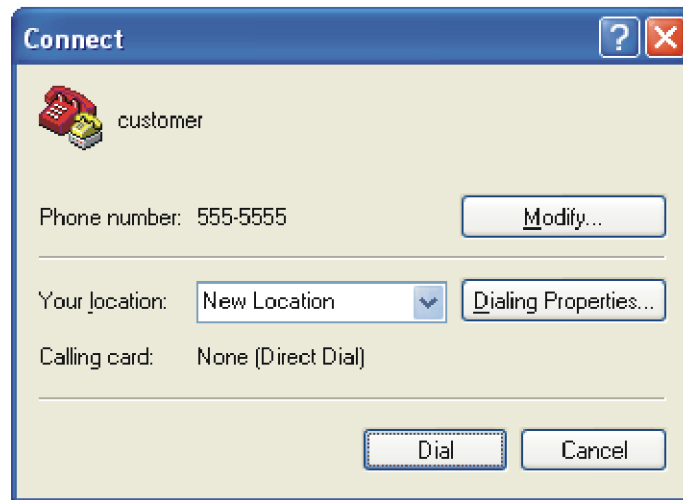
5 Enter the preset login password on the remote terminal emulator and wait for the `<SW7750>` prompt.

6 Use the appropriate commands to configure the Switch 7750 or view its operational state. Enter **?** to get immediate help. For details on a specific command, refer to the appropriate chapter in this guide.

[i] *By default, after login, a modem user can access the commands at Level 0.*

Configuring the User Interface

User interface configuration is another way to configure and manage port data.

The Switch 7750 supports the following configuration methods:

■ Local configuration through the console port

■ Remote configuration through Telnet on the Ethernet port

■ Remote configuration through a modem through the console port.

There are two types of user interfaces:

■ AUX user interface is used to log in the Switch 7750 through a dial-up modem. A Switch 7750 can only have one AUX port.

■ VTY user interface is used to telnet the Switch 7750.

[i] *For the Switch 7750, the AUX port and Console port are the same port. There is only the type of AUX user interface.*

The user interface is numbered by absolute number or relative number.

To number the user interface by absolute number:

■ The AUX user interface is the first interface — user interface 0.

■ The VTY is numbered after the AUX user interface. The absolute number of the first VTY is the AUX user interface number plus 1.

To number the user interface by relative number, represented by *interface* + *number* assigned to each type of user interface:

- AUX user interface = AUX 0.
- The first VTY interface = VTY 0, the second one = VTY 1, and so on.

Tasks for configuring the user interface are described in the following sections:

- Entering the User Interface View
- Configuring the Attributes of the AUX (Console) Port
- Configuring the Terminal Attributes
- Managing Users
- Configuring the Attributes of a Modem
- Configuring Redirection
- Displaying and Debugging User Interface

Entering the User Interface View

Use the `user-interface` command (see Table 4) to enter a user interface view. You can enter a single user interface view or multi-user interface view to configure one or more user interfaces.

Perform the following configuration in system view.

Table 4   Enter User Interface View

Operation	Command
Enter a single user interface view or multi user interface views	**user-interface** [*type*] *first-number* [*last-number*]

Configuring the Attributes of the AUX (Console) Port

Use the `speed`, `flow control`, `parity`, `stop bit`, and `data bit` commands (see Table 5) to configure these attributes of the AUX (Console) port.

Perform the following configurations in user interface (AUX user interface only) view.

Table 5   Configure the Attributes of the AUX (Console) Port

Operation	Command
Configure the transmission speed on AUX (Console) port. By default, the transmission speed is 9600bps	**speed** *speed-value*
Restore the default transmission speed on AUX (Console) port	**undo speed**
Configure the flow control on AUX (Console) port. By default, no flow control is performed on the AUX (Console) port	**flow-control** { **hardware** | **none** | **software** }
Restore the default flow control mode on AUX (Console) port	**undo flow-control**
Configure parity mode on the AUX (Console) port. By default, there is no parity bit on the AUX (Console) port	**parity** { **even** | **mark** | **none** | **odd** | **space** }
Restore the default parity mode	**undo parity**

Table 5   Configure the Attributes of the AUX (Console) Port

Operation	Command
Configure the stop bit of AUX (Console) port. By default, AUX (Console) port supports 1 stop bit	`stopbits { 1	1.5	2 }`
Restore the default stop bit of AUX (Console) port	`undo stopbits`
Configure the data bit of AUX (Console) port. By default, AUX (Console) port supports 8 data bits.	`databits { 7	8 }`
Restore the default data bit of AUX (Console) port	`undo databits`

Configuring the Terminal Attributes

The following commands can be used for configuring the terminal attributes, including enabling/disabling terminal service, disconnection upon timeout, lockable user interface, configuring terminal screen length and history command buffer size.

Perform the following configuration in user interface view. Perform the `lock` command in user view.

Enabling and Disabling Terminal Service   After the terminal service is disabled on a user interface, you cannot log in to the Switch 7750 through the user interface. However, if a user is logged in through the user interface before disabling the terminal service, the user can continue operation. After the user logs out, the user cannot log in again. In this case, the user can log in to the Switch through the user interface only when the terminal service is enabled again. Use the commands described in Table 6 to enable or disable terminal service.

Table 6   Enabling and Disabling Terminal Service

Operation	Command
Enable terminal service	`shell`
Disable terminal service	`undo shell`

By default, terminal service is enabled on all the user interfaces.

Note the following points:

- For the sake of security, the `undo shell` command can only be used on the user interfaces other than the AUX user interface.

- You cannot use this command on the user interface through which you log in.

- You must confirm your privilege before using the `undo shell` command in any legal user interface.

Configuring idle-timeout   By default, idle-timeout is enabled and set to 10 minutes on all the user interfaces. The `idle-timeout` command is described in Table 7.

Table 7   Idle Timeout

Operation	Command
Configure idle-timeout	`idle-timeout` *minutes* [*seconds*] (`idle-timeout` 0 means disabling idle-timeout.)
Restore the default idle-timeout	`undo idle-timeout`

Locking the User Interface   The `lock` command locks the current user interface and prompts the user to enter a password. This makes it impossible for others to operate in the interface after the user leaves. The `lock` command is described in Table 8.

Table 8   Lock User Interface

Operation	Command
Lock user interface	`lock`

Setting the Screen Length   If a command displays more than one screen of information, you can use the `screen length` command to determine how many lines are displayed on a screen so that information can be separated in different screens and you can view it more conveniently. The `screen-length` command is described in Table 9.

Table 9   Setting Screen Length

Operation	Command
Set the screen length	`screen-length` *screen-length* (`screen-length` 0 indicates to disable screen display separation function.)
Restore the default screen length	`undo screen-length`

By default, the terminal screen length is 24 lines.

Setting the History Command Buffer Size

Table 10 describes the `history-command max-size` command. By default, the size of the history command buffer is 10.

Table 10   Set the History Command Buffer Size

Operation	Command
Set the history command buffer size	**history-command max-size** *value*
Restore the default history command buffer size	`undo history-command max-size`

Managing Users

The management of users includes: the setting of the user logon authentication method, the level of command a user can use after logging on, the level of command a user can use after logging on from the specific user interface, and the command level.

Configuring the Authentication Method   The `authentication-mode` command configures the user login authentication method that allows access to an unauthorized user. Table 11 describes the `authentication-mode` command.

Perform the following configuration in user interface view.

Table 11   Configure Authentication Method

Operation	Command
Configure the authentication method	`authentication-mode { password	scheme [command-authorization] }`
Configure no authentication	`authentication-mode none`

By default, terminal authentication is not required for users who log in through the console port, whereas a password is required for authenticating modem and Telnet users when they log in.

To configure authentication for modem and Telnet users:

1 Configure local password authentication for the user interface.

When you set the password authentication mode, you must also configure a login password to log in successfully. Table 12 describes the `set authentication password` command.

Perform the following configuration in user interface view.

Table 12   Configure the Local Authentication Password

Operation	Command
Configure the local authentication password	`set authentication password{ cipher|simple} password`
Remove the local authentication password	`undo set authentication password`

Configure for password authentication when a user logs in through a VTY 0 user interface and set the password to 3Com:

```
[SW7750]user-interface vty 0
[SW7750-ui-vty0]authentication-mode password
[SW7750-ui-vty0]set authentication password simple 3Com
```

2 Configure the local or remote authentication username and password.

Use the `authentication-mode scheme` command to perform local or remote authentication of username and password. The type of the authentication depends on your configuration. For detailed information, see "AAA and RADIUS Operation"

Perform username and password authentication when a user logs in through the VTY 0 user interface and set the username and password to zbr and 3Com respectively:

```
[SW7750-ui-vty0]authentication-mode scheme
[SW7750-ui-vty0]quit
[SW7750]local-user zbr
[SW7750-luser-zbr]service-type telnet
```

3 Authorize users to use the command lines

The `authentication-mode scheme command-authorization` command indicates that you must be authorized to use the command lines on the TACACS

authentication server before executing the other commands. Commands that different users can execute are defined on the TACACS authentication server.

For example, the user tel@hwtac passes the authentication of the TACACS server 192.168.6.1 and logs into the switch through the port vty0. As the **authentication-mode scheme command-authorization** command is configured for the vty0 port on the switch, the NAS sends a request for authorization to the AAA server when you perform the **display current-configuration** command. If the reply indicates that the authorization succeeds, the user can execute the command.

4 Set the Switch 7750 to allow user access without authentication.

```
[SW7750-ui-vty0]authentication-mode none
```

i> *By default, the password is required for authenticating the modem and Telnet users when they log in. If the password has not been set, when a user logs in, the following message displays,* Login password has not been set!

If the **authentication-mode none** *command is used, the modem and Telnet users are not required to enter a password.*

Set the Command Level after Login   The following command is used for setting the command level used after a user logs in.

Perform the following configuration in local-user view.

Table 13   Set Command Level Used After a User Logs In

Operation	Command
Set command level used after a user logging in	**service-type** { [**level** level | **telnet** [**level** level]] | **telnet** [**level** level |[**level** level]]}
Restore the default command level used after a user logging in	**undo service-type** { [**level** | **telnet** [**level**]] | **telnet** [**level** | [**level**]] }

By default, a Telnet user can access the commands at Level 1 after logon.

Setting the Command Level Used after a User Logs in from a User Interface

Use the **user privilege level** command to set the command level, after a user logs in from a specific user interface, so that a user is able to execute the commands at that command level. Table 14 describes the **user privilege level** command.

Perform the following configuration in user interface view.

Table 14   Set Command Level After User Login

Operation	Command
Set command level used after a user logging in from a user interface	**user privilege level** level
Restore the default command level used after a user logging in from a user interface	**undo user privilege** level

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

When a user logs in to the switch, the command level that the user can access depends on two points. One is the command level that the user can access, the other is the set command level of the user interface. If the two levels are different, the former is taken. For example, the command level of VTY 0 user interface is 1, however, user Tom has the right to access commands of level 3; if Tom logs in from VTY 0 user interface, he can access commands of level 3 and lower.

Setting Command Priority   The `command-privilege level` command sets the priority of a specified command in a certain view. The command levels include visit, monitoring, configuration, and management, which are identified with command level 0 through 3, respectively. An administrator assigns authority according to user requirements. See Table 15.

Perform the following configuration in system view.

Table 15   Set Command Priority

Operation	Command
Set the command priority in a specified view.	**command-privilege level** *level* **view** *view command*
Restore the default command level in a specified view.	**undo command-privilege view** *view command*

Configuring the Attributes of a Modem

You can use the commands described in Table 16 to configure the attributes of a modem when logging in to the Switch through the modem.

Perform the following configuration in user interface view.

Table 16   Configure Modem

Operation	Command
Set the interval since the system receives the RING until CD_UP	**modem timer answer** seconds
Restore the default interval since the system receives the RING until CD_UP	**undo modem timer answer**
Configure auto answer	**modem auto-answer**
Configure manual answer	**undo modem auto-answer**
Configure to allow call-in	**modem call-in**
Configure to bar call-in	**undo modem call-in**
Configure to permit call-in and call-out.	**modem both**
Configure to disable call-in and call-out	**undo modem both**

Configuring Redirection

The send Command   can be used for sending messages between user interfaces. See Table 17.

Perform the following configuration in user view.

Table 17   Configure to Send Messages Between User Interfaces

Operation	Command
Configure to send messages between different user interfaces.	**send** { **all** | number | type number }

The auto-execute Command   is used to run a command automatically after you log in. The command is automatically executed when you log in again. See Table 18.

This command is usually used to execute the **telnet** command automatically on a terminal, which connects the user to a designated device.

Perform the following configuration in user interface view.

Table 18   Configure Automatic Command Execution

Operation	Command
Configure to automatically run the command	**auto-execute command** text
Configure not to automatically run the command	**undo auto-execute command**

⚠ **!**   *CAUTION: After applying the* **auto-execute** *command, the user interface can no longer be used to carry out the routine configurations for the local system.*

Make sure that you will be able to log in to the system in some other way and cancel the configuration before you use the **auto-execute** *command and save the configuration.*

Telnet 10.110.100.1 after the user logs in through VTY0 automatically.:

```
[SW7750-ui-vty0]auto-execute command telnet 10.110.100.1
```

When a user logs on by VTY 0, the system will run **telnet 10.110.100.1** automatically.

Displaying and Debugging User Interface

After creating the previous configuration, execute the **display** command in all views to display the user interface configuration, and to verify the effect of the configuration. Execute the **free** command in user view to clear a specified user interface.

Table 19   Display and Debug User Interface

Operation	Command
Clear a specified user interface	**free user-interface** [type] number
Display the user application information of the user interface	**display users** [**all**]
Display the physical attributes and some configurations of the user interface	**display user-interface** [type number] [number] [**summary**]

Command Line Interface	The Switch 7750 provides a series of configuration commands and command line interfaces for configuring and managing the Switch 7750. The command line interface has the following features.

- Local configuration through the console port.

- Local or remote configuration through Telnet.

- Remote configuration through a dial-up Modem to log in to the Switch 7750.

- Hierarchy command protection to prevent unauthorized users from accessing the switch.

- Access to online Help by entering **?**.

- Network test commands, such as Tracert and Ping, for rapid troubleshooting of the network.

- Detailed debugging information to help with network troubleshooting.

- Ability to log in and manage other Switch 7750s directly, using the **telnet** command.

- FTP service for the users to upload and download files.

- Ability to view previously executed commands.

- The command line interpreter that searches for a target not fully matching the keywords. You can enter the whole keyword or part of it, as long as it is unique and not ambiguous.

Configuring a Command Line Interface is described in the following sections:

- Command Line View

- Features and Functions of the Command Line

Command Line View   The Switch 7750 provides hierarchy protection for the command lines to prevent unauthorized users from accessing the switch illegally.

There are four levels of commands:

- Visit level — involves commands for network diagnosis tools (such as **ping** and **tracert**), command of the switch between different language environments of user interface (language-mode) and the **telnet** command. Saving the configuration file is not allowed on this level of commands.

- Monitoring level — includes the **display** command and the **debugging** command for system maintenance, service fault diagnosis, and so on. Saving the configuration file is not allowed on this level of commands.

- Configuration level — provides service configuration command, such as the **routing** command and commands on each network layer that are used to provide direct network service to the user.

- Management level — influences the basic operation of the system and the system support module which plays a support role for service. Commands at this level involve file system commands, FTP commands, TFTP commands, XModem downloading commands, user management commands, and level setting commands.

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

To prevent unauthorized users from illegal intrusion, users are identified when switching from a lower level to a higher level with the `super` [level] command. User ID authentication is performed when users at a lower level switch to users at a higher level. Only when the correct password is entered three times, can the user switch to the higher level. Otherwise, the original user level remains unchanged.

Command views are implemented according to requirements that are related to one another. For example, after logging in to the Switch 7750, you enter user view, in which you can only use some basic functions, such as displaying the operating state and statistics information. In user view, key in `system-view` to enter system view, in which you can key in different configuration commands and enter the corresponding views.

The command line provides the following views:

- User view
- System view
- Ethernet Port view
- VLAN view
- VLAN interface view
- Local-user view
- User interface view
- FTP client view
- Cluster view
- PIM view
- RIP view
- Route policy view
- Basic ACL view
- Advanced ACL view
- Layer-2 ACL view
- RADIUS server group view
- HWTACACS view
- ISP domain view

Table 20 describes the function features of different views.

For all views, use the **quit** command to return to system view and use the **return** command to return to user view.

Table 20 Function Feature of Command View

Command view	Function	Prompt	Command to enter
User view	Show basic information about operation and statistics	`<SW7750>`	Enter immediately after connecting the switch
System view	Configure system parameters	`[SW7750]`	Enter **system-view** in user view
Ethernet Port view	Configure Ethernet port parameters	`[SW7750-Etherne t1/0/1]`	100M Ethernet port view Enter **interface ethernet1/0/1** in system view
		`[SW7750-Gigabit Ethernet1/0/1]`	Gigabit Ethernet port view Enter **interface gigabitethernet 1/0/1** in system view
VLAN view	Configure VLAN parameters	`[SW7750-Vlan1]`	Enter **vlan 1** in System view
VLAN interface view	Configure IP interface parameters for a VLAN or a VLAN aggregation	`[SW7750-Vlan-in terface1]`	Enter **interface vlan-interface 1** in System view
Local-user view	Configure local user parameters	`[SW7750-user-user1]`	Enter **local-user user1** in System view
User interface view	Configure user interface parameters	`[SW7750-ui0]`	Enter **user-interface 0** in System view
FTP Client view	Configure FTP Client parameters	`[ftp]`	Enter **ftp** in user view
PIM view	Configure PIM parameters	`[SW7750-PIM]`	Enter **pim** in system view
RIP view	Configure RIP parameters	`[SW7750-rip]`	Enter **rip** in system view
Route policy view	Configure route policy parameters	`[SW7750-route-policy]`	Enter **route-policy policy1 permit node 10** in System view
Basic ACL view	Define the rule of basic ACL	`[SW7750-acl-basic-2000]`	Enter **acl number 2000** in System view
Advanced ACL view	Define the rule of advanced ACL	`[SW7750-acl-adv -3000]`	Enter **acl number 3000** in system view
Layer-2 ACL view	Define the rule of layer-2 ACL	`[SW7750-acl-link-4000]`	Enter **acl number 4000** in system view
RADIUS scheme view	Configure radius parameters	`[SW7750-radius-1]`	Enter **radius scheme 1** in system view
HWTACACS view	Configure HWTACACS parameters	`[SW7750-hwtacacs-1]`	Enter **hwtacacs scheme1** in system view

Table 20   Function Feature of Command View (continued)

Command view	Function	Prompt	Command to enter
ISP domain view	Configure ISP domain parameters	[SW7750-isp-163 .net]	Enter **domain isp-163.net** in system view

**Features and Functions
of the Command Line**

Tasks for configuring the features and functions of the command line are described as follows:

- Online Help
- Common Command Line Error Messages
- History Command
- Editing Features of the Command Line
- Displaying Features of the Command Line

Online Help

The command line interface provides full and partial online Help modes.

You can get the help information through these online help commands, which are described as follows.

- Enter **?** in any view to get all the commands in that view and corresponding descriptions.

```
<SW7750>?
User view commands:
   boot              Set boot option
   cd                Change current directory
   clock             Specify the system clock
   copy              Copy from one file to another
   debugging         Enable system debugging functions
   delete            Delete a file
   dir               List files on a file system
   display           Display current system information
Enter a command with a ?, separated by a space. If this position is
for keywords, then all the keywords and the corresponding brief
descriptions will be listed.
<SW7750>ping ?
-a   Select source IP address
-c   Specify the number of echo requests to send
-d   Specify the SO_DEBUG option on the socket being used
-h   Specify TTL value for echo requests to be sent
-I   Select the interface sending packets
-n Numeric output only. No attempt will be made to lookup host
addresses for symbolic names
-p No more than 8 "pad" hexadecimal characters to fill out the sent
packet. For example, -p f2 will fill the sent packet with f and 2
repeatedly
-q Quiet output. Nothing is displayed except the summary lines at
startup time and when finished
-r Record route. Includes the RECORD_ROUTE option in the ECHO_REQUEST
packet and displays the route
-s   Specifies the number of data bytes to be sent
-t   Timeout in milliseconds to wait for each reply
```

```
-v Verbose output. ICMP packets other than ECHO_RESPONSE that are
received are listed
STRING<1-20>  IP address or hostname of a remote system
Ip   IP Protocol
```

■ Enter a command with a **?**, separated by a space. If this position is for parameters, all the parameters and their brief descriptions will be listed.

```
[Quidway] interface vlan ?
  <1-4094>  VLAN interface number
[Quidway] interface vlan 1 ?
<cr>
```

<cr> indicates no parameter in this position. The next command line repeats the command, you can press Enter to execute it directly.

■ Enter a character string with a **?**, and list all the commands beginning with this character string.

```
<SW7750>pi?
ping
```

■ Input a command with a character string and **?**, and list all the key words beginning with this character string in the command.

```
<SW7750>display ver?
  version
```

Common Command Line Error Messages

All the commands that are entered by users can be correctly executed if they have passed the grammar check. Otherwise, error messages are reported to users. Common error messages are listed in Table 21.

Table 21   Common Command Line Error Messages

Error messages	Causes
Unrecognized command	Cannot find the command. Cannot find the keyword. Wrong parameter type. The value of the parameter exceeds the range.
Incomplete command	The command is incomplete.
Too many parameters	You entered too many parameters.
Ambiguous command	The parameters you entered are not specific.

History Command

The command line interface provides a function similar to DosKey. The commands entered by users can be automatically saved by the command line interface and you can invoke and execute them at any time. By default, the history command buffer can store 10 history commands for each user. The operations are shown in Table 22.

Table 22   Retrieve History Command

Operation	Key	Result
Display history command	**display history-command**	Displays history commands by the user who is entering them.
Retrieve the previous history command	Up cursor key <> or <Ctrl+P>	Retrieves the previous history command, if there is any.

Table 22   Retrieve History Command

Operation	Key	Result
Retrieve the next history command	Down cursor key <> or <Ctrl+N>	Retrieves the next history command, if there is any.

Editing Features of the Command Line

The command line interface provides a basic command editing function and supports editing multiple lines. A command cannot be longer than 256 characters. See Table 23.

Table 23   Editing Functions

Key	Function
Common keys	Inserts at the cursor position and the cursor moves to the right, if the edition buffer still has free space.
Backspace	Deletes the character preceding the cursor and the cursor moves backward.
Left cursor key < or *Ctrl+B*	Moves the cursor a character backward
Right cursor key > or *Ctrl+F*	Moves the cursor a character forward
Up cursor key ^ or *Ctrl+P* Down cursor key v or *Ctrl+N*	Retrieves the history command.
Tab	Press *Tab* after typing the incomplete key word and the system will execute the partial help: If the key word matching the typed one is unique, the system will replace the typed one with the complete key word and display it in a new line. If there is not a matched key word or the matched key word is not unique, the system will do no modification but displays the originally typed word in a new line.

Displaying Features of the Command Line

If information to be displayed exceeds one screen, the pause function allows users three choices, as described in Table 24.

Table 24   Display Functions

Key or Command	Function
Press *Ctrl+C* when the display pauses	Stop displaying and executing command.
Enter a space when the display pauses	Continue to display the next screen of information.
Press *Enter* when the display pauses	Continue to display the next line of information.

2

PORT CONFIGURATION

This chapter covers the following topics:

- Ethernet Port Overview
- Configuring Link Aggregation

Ethernet Port Overview

The following features are found in the Ethernet ports of the Switch 7750:

- 10BASE-T/100BASE-TX Gigabit Ethernet ports support MDI/MDI-X auto-sensing, and can be configured to operate in half/full duplex mode or auto-negotiation mode to negotiate the duplex mode and speed with other network devices. This also allows you to use the optimal mode automatically.

- 100BASE-FX-MMF Ethernet ports operate in 100 Mbps full duplex mode. The duplex mode can be configured as full (full duplex) or auto (auto-negotiation). The speed can be set to 100 (100 Mbps) or auto (auto-negotiation).

- 1000BASE-X Gigabit Ethernet ports work in gigabit full duplex mode. The duplex mode can be configured as full (full duplex) or auto (auto-negotiation). The speed can be set to 1000 (1000Mbps) or auto (auto-negotiation).

- 10/100/1000BASE-T Gigabit Ethernet ports support MDI/MDI-X auto-sensing, and the modes are 1000 Mbps full duplex, 100 Mbps half/full duplex, and 10 Mbps half/full duplex. These modules also support auto-negotiation

- 10GBASE-R-XENPAK 10-Gigabit Ethernet ports work in 10-gigabit full duplex mode. The duplex mode can be configured as full (full duplex) or auto (autonegotiation), and the speed can be set to 10000 (10000 Mbps) or auto (autonegotiation).

Configuring an Ethernet Port Overview is described in the following sections:

- Configuring Ethernet Ports
- Example: Configuring the Default VLAN ID of the Trunk Port
- Troubleshooting VLAN Port Configuration

Configuring Ethernet Ports

Tasks for configuring Ethernet ports are described in the following sections:

- Entering Ethernet Port View
- Enabling and Disabling Ethernet Ports
- Setting Description Character String for Ethernet Port
- Setting Duplex Attribute of the Ethernet Port
- Setting the Speed of the Ethernet Port
- Setting Cable Type for Ethernet Port

- Setting Flow Control for Ethernet Port
- Permitting/Forbidding Jumbo Frames on the Ethernet port
- Setting Ethernet Port Broadcast Suppression Ratio
- Setting the Link Type for an Ethernet Port
- Adding the Ethernet Port to a VLAN
- Setting the Default VLAN ID for Ethernet Port
- Copying a Port Configuration to Other Ports
- Displaying and Debugging Ethernet Ports

Entering Ethernet Port View

Before configuring the Ethernet port, enter Ethernet port view.

Perform the following configuration in system view.

Table 25   Enter Ethernet Port View

Operation	Command
Enter Ethernet port view	**interface** {Gigabit | Ethernet} slot/subslot/port

i> *The submodule on the fabric for the 4-slot chassis is always set to 1.*

Enabling and Disabling Ethernet Ports

The following command can be used for disabling or enabling the port. After configuring the related parameters and protocol of the port, you can use the following command to enable the port.

Perform the following configuration in Ethernet port view.

Table 26   Enable/Disable an Ethernet Port

Operation	Command
Disable an Ethernet port	**shutdown**
Enable an Ethernet port	**undo shutdown**

i> *By default, the port is enabled.*

Setting Description Character String for Ethernet Port

You can use the following command to identify the Ethernet ports.

Perform the following configuration in Ethernet port view.

Table 27   Set Description Character String for Ethernet Port

Operation	Command
Set description character string for Ethernet port.	**description** text
Delete the description character string of Ethernet.	**undo description**

i> *By default, the port description is a null character string.*

Setting Duplex Attribute of the Ethernet Port

Set the port to full duplex to send and receive data packets at the same time. Set the port to half-duplex to either send or receive only. If the port has been set to auto-negotiation mode, the local and peer ports will automatically negotiate the duplex mode.

Perform the following configuration in Ethernet port view.

Table 28   Set Duplex Attribute for Ethernet Port

Operation	Command
Set duplex attribute for Ethernet port.	`duplex { auto	full	half }`
Restore the default duplex attribute of Ethernet port.	`undo duplex`

The 100 Mbps TX Ethernet port can operate in full-duplex, half-duplex, or auto-negotiation mode. The Gigabit TX Ethernet port can operate in full duplex, half duplex, or auto-negotiation mode. When the port operates at 1000 Mbps, the duplex mode can be set to full (full duplex) or auto (auto-negotiation).

*The optical 100M/Gigabit/10Gigabit Ethernet ports support full duplex mode and can be configured to operate in **full** (full duplex) or **auto** (auto-negotiation) mode. By default, the port is in **auto** (auto-negotiation) mode.*

Setting the Speed of the Ethernet Port

You can use the following command to set the speed on the Ethernet port. If the speed is set to auto (auto-negotiation) mode, the local and peer ports will automatically negotiate the port speed.

Perform the following configuration in Ethernet port view.

Table 29   Set Speed on Ethernet Port

Operation	Command
Set 100M Ethernet port speed	`speed { 10	100	auto }`
Set Gigabit Ethernet port speed	`speed { 10	100	1000	auto }`
Restore the default speed on Ethernet port	`undo speed`

Setting Cable Type for Ethernet Port

The Ethernet port supports the straight-through (MDI) and cross-over (MDIX) network cables. The Switch 7750 only supports auto (auto-sensing). If you set another duplex type, an error message displays. By default, the cable type is auto (auto-recognized). The system will automatically recognize the type of cable connecting to the port.

Perform the following configuration in Ethernet port view. The settings only take effect on 10/100BASE-T and 10/100/1000BASE-T ports.

Table 30   Set the Type of the Cable Connected to the Ethernet Port

Operation	Command
Set the type of the cable connected to the Ethernet port.	`mdi { auto }`
Restore the default type of the cable connected to the Ethernet port.	`undo mdi`

Setting Flow Control for Ethernet Port

If congestion occurs in the local switch after enabling flow control in both the local and the peer switch, then the switch will inform its peer to pause sending packets. Once the peer switch receives this message, it will pause packet sending, and vice versa. In this way, packet loss is effectively reduced. The flow control function of the Ethernet port can be enabled or disabled through the following command.

Perform the following configuration in Ethernet port view.

Table 31   Set Flow Control for Ethernet Port

Operation	Command
Enable Ethernet port flow control	`flow-control`
Disable Ethernet port flow control	`undo flow-control`

i>   *By default, Ethernet port flow control is disabled.*

Permitting/Forbidding Jumbo Frames on the Ethernet port

Using the `jumbo frame enable` command, you can allow jumbo frames (1523 to to 9216 bytes) to pass through the specified Ethernet port. Note that packets up to 1522 bytes, including the IEEE 802.1Q tagging are always allowed to pass through Ethernet ports.

Jumbo frames are only allowed for Ethernet Type II frames. Most network equipment, including NICs, switches, and routers are not capable of supporting jumbo frames and will always discard these packets.

Perform the following configuration in Ethernet port view.

Table 32   Permitting/Forbidding Jumbo Frame to Pass Through the Ethernet Port

Operation	Command
Permit jumbo frame to pass through the Ethernet port.	`jumboframe enable` [*jumboframe_value*]
Forbid jumbo frame to pass through the Ethernet port.	`undo jumboframe enable`

i>   *By default, jumbo frames are disabled.*

Setting Ethernet Port Broadcast Suppression Ratio

You can use the following commands to restrict the broadcast traffic. Once the broadcast traffic exceeds the value set by the user, the system maintains an appropriate broadcast packet ratio by discarding the overflow traffic. This is done to suppress broadcast storm, avoid suggestion, and ensure the normal service.

The parameter is taken the maximum wire speed ratio of the broadcast traffic allowed on the port. The smaller the ratio is, the less broadcast traffic is allowed. If the ratio is 100%, do not perform broadcast storm suppression on the port.

Perform the following configuration in Ethernet port view.

Table 33 Setting Ethernet Port Broadcast Suppression Ratio

Operation	Command
Set Ethernet port broadcast suppression ratio	**broadcast-suppression pct**
Restore the default Ethernet port broadcast suppression ratio	**undo broadcast-suppression**

By default, 100% broadcast traffic is allowed to pass through, that is, no broadcast suppression will be performed.

> *Note that in the Switch 7750, you can only use the command at the port on a 20-port 10/100/1000BASE-T Gigabit Ethernet card or a 20-port 1000BASE-X Gigabit Ethernet card.*

Setting the Link Type for an Ethernet Port

An Ethernet port can operate in three different link types, access, hybrid, and trunk. The access port carries one VLAN only and is used for connecting to the user's computer.

The trunk port can belong to more than one VLAN and receive/send the packets on multiple VLANs. The hybrid port can also carry more than one VLAN and receive/send the packets on multiple VLANs. The difference between the hybrid port and the trunk port is that the hybrid port allows the packets from multiple VLANs to be sent without tags, but, the trunk port only allows the packets from the default VLAN to be sent without tags.

Perform the following configuration in Ethernet port view.

Table 34 Set Link Type for Ethernet Port

Operation	Command
Set the port to access port	**port link-type access**
Set the port to hybrid port	**port link-type hybrid**
Set the port to trunk port	**port link-type trunk**
Restore the default link type, that is, the access port.	**undo port link-type**

> *A port on a switch can be configured as an access port, a hybrid port, or a trunk port. However, to reconfigure between hybrid and trunk link types, you must first restore the default, or access link type.*

The default link type is the access link type.

Adding the Ethernet Port to a VLAN

The following commands are used for adding an Ethernet port to a specified VLAN. Access ports can be added to only one VLAN, while hybrid and trunk ports can be added to multiple VLANs.

Perform the following configuration in Ethernet port view.

Table 35   Adding the Ethernet Port to Specified VLANs

Operation	Command
Add the current access port to a specified VLAN	**port access vlan** vlan_id
Add the current hybrid port to specified VLANs	**port hybrid vlan** vlan_id_list { **tagged** | **untagged** }
Add the current trunk port to specified VLANs	**port trunk permit vlan** { vlan_id_list | **all** }
Remove the current access port from to a specified VLAN.	**undo port access vlan**
Remove the current hybrid port from to specified VLANs.	**undo port hybrid vlan** vlan_id_list
Remove the current trunk port from specified VLANs.	**undo port trunk permit vlan** { vlan_id_list | **all** }

> **i** > *The access port will be added to an existing VLAN other than VLAN 1. The VLAN to which a Hybrid port is added must exist. The VLAN to which a Trunk port is added cannot be VLAN 1.*

After adding the Ethernet port to the specified VLANs, the local port can forward packets from these VLANs. The hybrid and trunk ports can be added to multiple VLANs, thereby, implementing the VLAN intercommunication between peers. For the hybrid port, you can tag VLAN packets to process packets in different ways, depending on the target device.

Setting the Default VLAN ID for Ethernet Port

Since the access port can only be included in one VLAN, its default VLAN is the one to which it belongs. The hybrid port and the trunk port can be included in several VLANs, however, it is necessary to configure the default VLAN ID. If the default VLAN ID has been configured, the packets without VLAN Tag will be forwarded to the port that belongs to the default VLAN. When sending the packets with VLAN Tag, if the VLAN ID of the packet is identical to the default VLAN ID of the port, the system will remove VLAN Tag before sending this packet.

Perform the following configuration in Ethernet port view.

Table 36   Set the Default VLAN ID for the Ethernet Port

Operation	Command
Set the default VLAN ID for the hybrid port.	**port hybrid pvid vlan** vlan_id
Set the default VLAN ID for the trunk port	**port trunk pvid vlan** vlan_id
Restore the default VLAN ID of the hybrid port to the default value	**undo port hybrid pvid**
Restore the default VLAN ID of the trunk port to the default value	**undo port trunk pvid**

> **i** > ■ *A Trunk port and isolate-user-vlan cannot be configured simultaneously. A hybrid port and* isolate-user-vlan *can be configured simultaneously. However, if the default VLAN has been mapped in isolate-user-vlan, you cannot modify the default VLAN ID until the mapping relationship has been removed.*

■ *To guarantee proper packet transmission, the default VLAN ID of local hybrid port or Trunk port should be identical to that of the hybrid port or Trunk port on the peer switch. The VLAN of hybrid port and trunk port is VLAN 1 by default. The access port is the VLAN to which it belongs.*

Copying a Port Configuration to Other Ports

To keep the configuration of other ports consistent with a specified port, you can copy the configuration of that specified port to other ports. Port configuration involves the following settings:

■ STP setting — includes STP enabling/disabling, link attribute (point-to-point or not), STP priority, path cost, max transmission speed, loop protection, root protection, edge port or not.

■ QoS setting — includes traffic limiting, priority marking, default 802.1p priority, bandwidth assurance, congestion avoidance, traffic redirection, traffic statistics.

■ VLAN setting — includes permitted VLAN types, default VLAN ID.

■ Port setting — includes port link type, port speed, duplex mode. LACP setting includes LACP enabling/disabling.

Perform the following configuration in system view.

Table 37   Copying a Port Configuration to Other Ports

Operation	Command
Copy port configuration to other ports	**copy configuration source** { interface-type interface-number | interface-name | **aggregation-group** agg-id } **destination** { interface_list [**aggregation-group** agg-id] | **aggregation-group** agg-id }

Note that if the copy source is an aggregation group, use the port with the lowest ID as the source. If the copy destination is an aggregation group, make the configurations of all group member ports identical with that of the source.

Displaying and Debugging Ethernet Ports

After configuration, execute the **display** command in all views to display the current configuration of Ethernet port parameters, and to verify the configuration.

Execute the **reset** command in user view to clear the statistics from the port.

Table 38   Display and Debug Ethernet Port

Operation	Command
Display all the information of the port	**display interface** {interface_type | interface_type interface_num | interface_name}
Display hybrid port or trunk port	**display port** { **hybrid** | **trunk** }
Clear the statistics information of the port	**reset counters interface** [interface_type | interface_type interface_num | interface_name]

Example: Configuring the Default VLAN ID of the Trunk Port

In this example, the Ethernet Switch (Switch A) is connected to the peer (Switch B) through the trunk port Ethernet1/0/1. This example shows the default VLAN ID for the trunk port and verifies the **port trunk pvid vlan** command. As a typical application of the **port trunk pvid vlan** command, the trunk port will transmit the packets without tag to the default VLAN.

Figure 13 Configure the Default VLAN for a Trunk Port

Switch A   Switch B

The following configurations are used for Switch A, configure Switch B in a similar way:

1 Enter the Ethernet port view of Ethernet1/0/1.

```
[SW7750]interface ethernet1/0/1
```

2 Set the Ethernet1/0/1 as a trunk port and allow VLAN 2, 6 through 50, and 100 to pass through.

```
[SW7750-Ethernet1/0/1]port link-type trunk
[SW7750-Ethernet1/0/1]port trunk permit vlan 2 6 to 50 100
```

3 Create the VLAN 100.

```
[SW7750]vlan 100
```

4 Configure the default VLAN ID of Ethernet1/0/1 as 100.

```
[SW7750-Ethernet1/0/1]port trunk pvid vlan 100
```

Troubleshooting VLAN Port Configuration   If the default VLAN ID configuration fails, take the following steps:

1 Execute the **display interface** or **display port** command to check if the port is a trunk port or a hybrid port. If it is neither of them, configure it as a trunk port or a hybrid port.

2 Configure the default VLAN ID.

Configuring Link Aggregation   Link aggregation means aggregating several ports together to implement the outgoing/incoming payload balance among the member ports and to enhance connection reliability.

IEEE802.3ad-based link aggregation control protocol (LACP) implements dynamic link aggregation and disaggregation and exchanges information with the peer through LACP data unit (LACPDU). When LACP is enabled on it, the port notifies the peer, by sending LACPDUs with the port's system priority, system MAC, port priority, port number and operation key.

When the peer receives this port information, it compares the received information with the information stored at other ports to determine which ports can be aggregated so that the two parties can agree on adding ports to, or deleting ports from, a dynamic aggregation group.

The operation key is a configuration set generated by LACP based on port setting (speed, duplex mode, basic configuration and management key). When LACP is enabled, the management key of a dynamic aggregation port is 0 by default, but the management key of a static aggregation port includes the aggregation group ID. For a dynamic aggregation group, all member ports must have the same operation key, while for a manual or static aggregation group, only the active member ports must have the same operation key.

The basic configuration of member ports in an aggregation group must be the same. That is, if one is a trunk port, others must be trunk ports also. If a port turns into an access port, then others must change to access ports.

Basic configuration includes the following types of settings:

■ STP — Includes STP enabling/disabling, link attribute (point-to-point or not), STP priority, path cost, max transmission speed, loop protection, root protection, edge port or not

■ QoS — Includes traffic limiting, priority marking, default 802.1p priority, bandwidth assurance, congestion avoidance, traffic redirection, traffic statistics

■ VLAN — Includes permitted VLAN types and the default VLAN ID

■ Port — Includes port link type

The Switch 7750 supports a maximum of sixty four load-balance groups, with each group containing a maximum of eight 1000M ports or sixteen 100M ports. For the 48-port 10/100BASE-T auto-sensing fast Ethernet interface card, a port grouped in first 24 ports cannot be aggregated with the one grouped in the last 24 ports.

Configuring Link Aggregation is described in the following sections:

■ Types of Link Aggregation

■ Load Sharing

■ Configuring Link Aggregation

■ Example: Link Aggregation Configuration

Types of Link Aggregation

The types of link aggregation are described in the following sections:

■ Manual and Static LACP Aggregation

■ Dynamic LACP aggregation

Manual and Static LACP Aggregation

Both manual aggregation and static LACP aggregation require manual configuration of aggregation groups. They prohibit automatic adding or deleting of member ports by the system. A manual or static LACP aggregation group must contain at least one member port, and you must delete the aggregation group, instead of the port, if the group contains only one port. At a manual aggregation port, LACP is disabled and you are not allowed to enable it. LACP is enabled at a static aggregation port. When a static aggregation group is deleted, its member ports form one or several dynamic LACP aggregation groups and LACP remains enabled on them. You are not allowed to disable LACP protocol at a static aggregation group.

In a manual or static LACP aggregation group, its ports may be in an active or inactive state. However, only the active ports can receive user service packets. The active port with the minimum port number serves as the master port, while others act as sub-ports.

In a manual aggregation group, the system sets the ports to active or inactive state based on these rules:

- The system sets the port with the highest priority to active state, and others to inactive state based on the following descending order of priority levels:
    - full duplex/high speed
    - full duplex/low speed
    - half duplex/high speed
    - half duplex/low speed
- The system sets ports to inactive state if they cannot aggregate with the active port with the lowest port number due to a hardware limit, for example, if trans-board aggregation is not available.
- The system sets ports to inactive state if their basic configurations are different from the basic configuration of the active port with the lowest port number.

In a static LACP aggregation group, the system sets the ports to active or inactive state based on these rules:

- The system sets the port with the highest priority to active state, and others to inactive state based on the following descending order of priority levels:
    - full duplex/high speed
    - full duplex/low speed
    - half duplex/high speed
    - half duplex/low speed
- If the Switch 7750 is connected to a peer device on which the maximum number of ports in a link aggregation is smaller than on the Switch 7750, the Switch 7750 sets to active the number of ports that correspond to the peer's maximum. The Switch 7750 sets its extra ports to inactive.
- The system sets ports to inactive if they cannot aggregate with the active port with the lowest port number because of a hardware limit, for example, if trans-board aggregation is not available.
- The system sets ports to inactive if their basic configurations are different from the basic configuration of the active port with lowest port number.

Since a defined number of ports can be supported in an aggregation group, then if the active ports in an aggregation group exceed the port quantity threshold for that group, the system shall set some ports with smaller port numbers (in ascending order) as selected ports and others as standby ports. Both selected and standby ports can transceive LACP protocol, but standby ports cannot forward user service packets.

Dynamic LACP aggregation

Dynamic LACP aggregation allows automatic adding/deleting by the system but prohibits manual configuration of users. Dynamic LACP aggregation can be established for a single port; this is called single port aggregation. LACP is enabled on dynamic aggregation ports. Only ports with the same speed, duplex mode and basic configuration and connected to the same device can be aggregated dynamically.

Only a defined number of ports can be supported in an aggregation group. If the ports in an aggregation group exceed the port quantity threshold for that group, the system will set some ports with smaller system IDs (system priority + system MAC address) and port IDs (port priority + port number) as selected ports and others as standby ports. If not, all member ports are selected ports. Both selected and standby ports can transceive LACP protocol, but standby ports cannot forward user service packets. Among the selected ports of an aggregation group, the one with the lowest port number serves as the master port for that group and the others are sub-ports.

In comparing system IDs, the system first compares system priority values; if they are equal, then it compares system MAC addresses. The smaller system ID is considered highest priority. Comparing port IDs works in the same way: the system first compares port priority values and then port numbers and the small port ID is considered highest priority. If the system ID changes from non-priority to priority, then the selected or standby state is determined by the port priority of the system. You can decide whether the port is selected or standby by setting system priority and port priority.

Load Sharing   Link aggregation may be load balancing and non-load balancing. In general, the system only provides limited load balancing aggregation resources, so the system need to rationally allocate these resources among manual aggregation groups, static LACP aggregation groups, dynamic LACP aggregation groups and the aggregation groups including special ports which require hardware aggregation resources. The system will always allocate hardware aggregation resources to the aggregation groups with higher priority levels. When the load sharing aggregation resources are used up for existing aggregation groups, newly-created aggregation groups will be non-load sharing ones. The priority levels (in descending order) for allocating load sharing aggregation resources are as follows:

- Aggregation groups including special ports which require hardware aggregation resources
- Manual and static LACP aggregation groups
- Aggregation groups that probably reach the maximum rate after the resources are allocated to them
- Aggregation groups with the minimum master port numbers if they reach the equal rate with other groups after the resources are allocated to them

When aggregation groups of higher priority levels appear, the aggregation groups of lower priority levels release their hardware resources. For single-port aggregation groups, if they can transceive packets normally without occupying hardware resources, they shall not occupy the resources.

A load sharing aggregation group may contain several selected ports, but a non-load sharing aggregation group can only have one selected port, while others as standby ports. Selection criteria of selected ports vary for different types of aggregation groups.

Configuring Link Aggregation

The Switch 7750 only supports LACP for ports on the same I/O module. A maximum number of 16 ports can be active in a link aggregation. For modules that have fewer than 16 ports, such as the 8-port 1000BASE-X-GE module, only eight ports can be active members of a link aggregation.

Link aggregation configuration includes tasks described in the following sections:

■ Enabling or Disabling LACP at a Port

■ Creating or Deleting an Aggregation Group

■ Adding or Deleting Ethernet Ports to or from an Aggregation Group

■ Setting or Deleting an Aggregation Group Descriptor

■ Configuring System Priority

■ Configuring Port Priority

■ Displaying and Debugging Link Aggregation

Enabling or Disabling LACP at a Port

You should first enable LACP at the ports before performing dynamic aggregation, so that both parties can agree on adding/deleting the ports into/from a dynamic LACP aggregation group.

Perform the following configuration in Ethernet port view.

Table 39   Enabling/Disabling LACP at a Port

Operation	Command
Enable LACP at the port	`lacp enable`
Disable LACP at the port	`undo lacp enable`

LACP is disabled at the port by default.

Note that:

■ You cannot enable LACP at a

  ■ Mirrored port

  ■ Port with a static MAC address configured

  ■ Port with static ARP configured

  ■ Port with 802.1x enabled.

■ You cannot enable LACP on a port in a manual aggregation group.

■ You can add a port with LACP enabled to a manual aggregation group, but the LACP will be disabled on it automatically. However, you can add a port with LACP disabled into a static LACP aggregation group, and the LACP will be enabled automatically.

Creating or Deleting an Aggregation Group

You can use the following command to create a manual aggregation group or static LACP aggregation group, but the dynamic LACP aggregation group is established by the system when LACP is enabled on the ports. You can also delete an existing aggregation group: when you delete a manual aggregation group, all its member ports are disaggregated; when you delete a static or dynamic LACP aggregation group, its member ports form one or several dynamic LACP aggregation groups.

Perform the following configuration in system view.

Table 40   Create or Delete an Aggregation Group

Operation	Command
Create an aggregation group	`link-aggregation group` agg-id `mode` { `manual` | `static` }
Delete an aggregation group	`undo link-aggregation group` agg-id

During creating an aggregation group, if it already exists in the system but contains no member port, it changes to the new type; if it already exists in the system and contains member ports, then you can only change a dynamic or static LACP aggregation group to a manual one, or a dynamic LACP aggregation group to a static one. In the former case, LACP shall be disabled at the member ports automatically, while in the latter case, LACP shall remain enabled.

Adding or Deleting Ethernet Ports to or from an Aggregation Group

You can add/delete ports into/from a manual or static LACP aggregation group, but the addition or deletion of member port for a dynamic LACP aggregation group is automatic.

Perform the following configuration in corresponding view.

Table 41   Add/Delete Ethernet Port to/from Aggregation Group

Operation	Command
Add an Ethernet port into the aggregation group (Ethernet port view)	`port link-aggregation group` *agg-id*
Delete an Ethernet port from the aggregation port (Ethernet port view)	`undo port link-aggregation group`
Aggregate Ethernet ports (System view)	`link-aggregation` interface_name1 `to` interface_name2 [`both`]

Note that:

- You cannot enable LACP at the mirrored port, port with static MAC address configured, port with static ARP configured, port with 802.1x enabled.

- You must delete the aggregation group, instead of the port, if the manual or static LACP aggregation group contains only one port.

Setting or Deleting an Aggregation Group Descriptor

Perform the following configuration in system view.

Table 42 Set/Delete an Aggregation Group Descriptor

Operation	Command
Set aggregation group descriptor	**link-aggregation group** agg-id **description** alname
Delete aggregation group descriptor	**undo link-aggregation group** agg-id **description**

By default, an aggregation group has no descriptor.

Note that if you have saved the current configuration with the **save** command, the configured manual aggregation groups, static LACP aggregation groups and corresponding descriptors will be retained when the system reboots. However, the dynamic LACP groups and descriptors are not retained when the system reboots.

Configuring System Priority

The LACP refers to system IDs in determining if the member ports are selected or standby one for a dynamic LACP aggregation group. The system ID consists of two-byte system priority and six-byte system MAC, that is, system ID = system priority + system MAC. In comparing system IDs, the system first compares system priority values; if they are equal, then it compares system MAC addresses. The smaller system ID is considered prior.

Changing system priority may affect the priority levels of member ports, and further their selected or standby state.

Perform the following configuration in system view.

Table 43 Configure System Priority

Operation	Command
Configure system priority	**lacp system-priority** system-priority-value
Restore the default system priority	**undo lacp system-priority**

By default, system priority is 32768.

Configuring Port Priority

The LACP compares system IDs first and then port IDs (if system IDs are the same) in determining if the member ports are selected or standby ones for a dynamic LACP aggregation group. If the ports in an aggregation group exceed the port quantity threshold for that group, the system sets some ports with smaller port IDs as selected ports and others as standby ports. The port ID consists of two-byte port priority and two-byte port number, that is, port ID = port priority + port number. The system first compares port priority values and then port numbers and the small port ID is considered prior.

Perform the following configuration in Ethernet port view.

Table 44   Configure Port Priority

Operation	Command
Configure port priority	**lacp port-priority** port-priority-value
Restore the default port priority	**undo lacp port-priority**

The default value for port priority is 32768.

Displaying and Debugging Link Aggregation

After you have completed your configuration, execute the **display** command in any view to display the link aggregation configuration, and to verify the effect of the configuration.

You can also use the **reset** command in user view to clear LACP statistics of the port. Use the debugging commands in user view to debug LACP.

Table 45   Display and Debug Link Aggregation

Operation	Command
Display summary information of all aggregation groups	**display link-aggregation summary**
Display detailed information of a specific aggregation group	**display link-aggregation verbose** agg-id
Display local system ID	**display lacp system-id**
Display detailed link aggregation information at the port	**display link-aggregation interface** { interface-type interface-number | interface-name } [**to** { interface-type interface-num | interface-name }]
Clear LACP statistics at the port	**reset lacp statistics** [**interface** { interface-type interface-number | interface-name } [**to** { interface-type interface-num | interface-name }]]
Disable/enable debugging LACP state machine	[**undo**] **debugging lacp state** [**interface** { interface-type interface-number | interface-name } [**to** { interface-type interface-num | interface-name }]] { { **actor-churn** | **mux** | **partner-churn** | **ptx** | **rx** }* | **all** }
Disable/enable debugging LACP packets	[**undo**] **debugging lacp packet** [**interface** { interface-type interface-number | interface-name } [**to** { interface-type interface-num | interface-name }]]
Disable/enable debugging link aggregation errors	[**undo**] **debugging link-aggregation error**
Disable/enable debugging link aggregation events	[**undo**] **debugging link-aggregation event**

Example: Link Aggregation Configuration

Switch A connects switch B with three aggregation ports, numbered as Ethernet1/0/1 to Ethernet1/0/3, so that the incoming and outgoing loads can be balanced among the member ports.

Figure 14   Networking For Link Aggregation
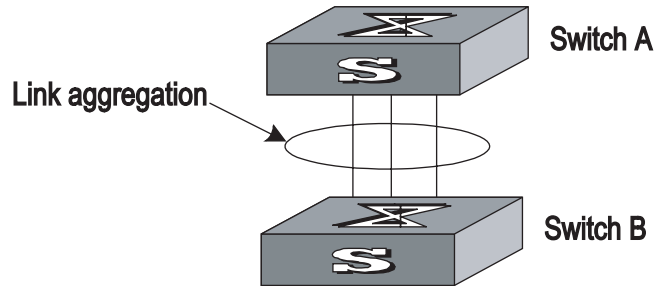
The following code example lists only the configuration for switch A. The configuration for switch B is similar.

1   Configure a manual link aggregation

- Create manual aggregation group 1.

```
[SW7750] link-aggregation group 1 mode manual
```

- Add Ethernet ports Ethernet1/0/1 to Ethernet1/0/3 into aggregation group 1.

```
[SW7750] interface ethernet1/0/1
[SW7750-Ethernet1/0/1] port link-aggregation group 1
[SW7750-Ethernet1/0/1] interface ethernet1/0/2
[SW7750-Ethernet1/0/2] port link-aggregation group 1
[SW7750-Ethernet1/0/2] interface ethernet1/0/3
[SW7750-Ethernet1/0/3] port link-aggregation group 1
```

2   Configure a static LACP aggregation

- Create static LACP aggregation group 1.

```
[SW7750] link-aggregation group 1 mode static
```

- Add Ethernet ports Ethernet1/0/1 to Ethernet1/0/3 into aggregation group 1.

```
[SW7750] interface ethernet1/0/1
[SW7750-Ethernet1/0/1] port link-aggregation group 1
[SW7750-Ethernet1/0/1] interface ethernet1/0/2
[SW7750-Ethernet1/0/2] port link-aggregation group 1
[SW7750-Ethernet1/0/2] interface ethernet1/0/3
[SW7750-Ethernet1/0/3] port link-aggregation group 1
```

3   Configure a dynamic LACP aggregation

- Enable LACP at Ethernet ports Ethernet1/0/1 to Ethernet1/0/3.

```
[SW7750] interface ethernet1/0/1
[SW7750-Ethernet1/0/1] lacp enable
[SW7750-Ethernet1/0/1] interface ethernet1/0/2
[SW7750-Ethernet1/0/2] lacp enable
[SW7750-Ethernet1/0/2] interface ethernet1/0/3
[SW7750-Ethernet1/0/3] lacp enable
```

Only when the three ports are configured with identical basic configuration, rate and duplex mode, can they be added into a same dynamic aggregation group after LACP is enabled on them, for load sharing.

3

VLAN CONFIGURATION

This chapter covers the following topics:

- VLAN Overview
- Configuring VLANs
- Configuring GARP/GVRP
-

VLAN Overview

A virtual local area network (VLAN) creates logical groups of LAN devices into segments to implement virtual workgroups.

Using VLAN technology, you can logically divide the physical LAN into different broadcast domains. Every VLAN contains a group of workstations with the same demands. However, the workstations of a VLAN do not have to belong to the same physical LAN segment.

Within a VLAN, broadcast and unicast traffic is not forwarded to other VLANs. Therefore, VLAN configurations are very helpful in controlling network traffic, saving device investment, simplifying network management and improving security.

VLANs are divided into four categories:

- Port-based VLAN
- Protocol-based VLAN
- MAC-based VLAN
- Policy-based VLAN

Port-based VLANs define VLAN members according to switch ports. This is the simplest and most efficient way to create VLANs.

The Switch 7750 supports port-based and network layer-based VLANs. The network layer-based VLANs are divided by protocols such as IP, so they are called *protocol-based VLANs*. Because this method is based on protocols, it is not related to routes and has nothing to do with routing at the network layer.

Configuring VLANs

The following sections describe how to configure VLANs:

- Common VLAN Configuration Tasks
- Configuring Port-Based VLANs
- Configuring Protocol-Based VLANs

Common VLAN Configuration Tasks   The following sections discuss the common tasks for configuring a VLAN:

- Creating or Deleting a VLAN
- Specifying the Broadcast Suppression Ratio for a VLAN
- Setting or Deleting the VLAN Description Character String
- Specifying or Removing VLAN Interfaces
- Shutting Down or Enabling a VLAN Interface
- Displaying and Debugging a VLAN

Creating or Deleting a VLAN

Use the following command to create or delete a VLAN.

Perform the following configurations in system view.

Table 46   Creating or Deleting a VLAN

Operation	Command
Create and enter a VLAN view	**vlan** *vlan_id*
Delete the specified VLAN	**undo vlan** *vlan_id*

The command creates the VLAN first then enters the VLAN view. If the VLAN already exists, the command enters the VLAN view directly.

Note that the default VLAN, VLAN 1, cannot be deleted.

Specifying the Broadcast Suppression Ratio for a VLAN

You can use the following command to specify the broadcast suppression ratio for the VLAN.

Perform the following configuration in VLAN view.

Table 47   Setting the Broadcast Suppression Ratio for VLAN

Operation	Command
Specify the broadcast suppression ratio for the VLAN.	`broadcast-suppression` max-ratio
Restore the default broadcast suppression ratio for the VLAN.	`undo broadcast-suppression`

Using this command, you can set the threshold for broadcast traffic that can pass through the VLAN. This value is represented by the following ratio format: *broadcast traffic/the entire traffic passed this VLAN*. The system discards the traffic that exceeds the threshold to limit broadcast traffic and maintain the normal operation of network services.

The lower the value of the *max-ratio* parameter, the lower the volume of broadcast traffic that is allowed to pass through. By default, *max-ratio* is set to 100 and broadcast suppression is not performed on the specified VLAN.

Note that you cannot use this command on a port on the 20-port 10/100/1000BASE-T or 20-port 1000BASE-X-SFP I/O modules

Setting or Deleting the VLAN Description Character String

You can use the following command to set or delete the VLAN description character string.

The description character strings, such as *workgroup_name* and *department_name*, are used to distinguish the different VLANs.

Perform the following configuration in VLAN view.

Table 48   Setting and Deleting VLAN Description Character String

Operation	Command
Set the description character string for the specified VLAN	**description** string
Delete the description character string of the specified VLAN	**undo description**

By default, the *string* parameter is null.

Specifying or Removing VLAN Interfaces

You can use the following command to specify or remove the VLAN interfaces. To implement the network layer function on a VLAN interface, the VLAN interface should be set the IP address and mask. For the corresponding configuration, refer to "Network Protocol Operation" on page 67.

Perform the following configurations in system view.

Table 49   Specifying and Removing VLAN interfaces

Operation	Command
Create a new VLAN interface and enter VLAN interface view	**interface vlan-interface** vlan_id
Remove the specified VLAN interface	**undo interface vlan-interface** vlan_id

Create a VLAN before creating an interface for it.

Shutting Down or Enabling a VLAN Interface

You can use the following command to shut down or enable VLAN interface.

Perform the following configuration in VLAN interface view.

Table 50   Shutting Down or Enabling a VLAN Interface

Operation	Command
Shut down the VLAN interface	**shutdown**
Enable the VLAN interface	**undo shutdown**

The operation of shutting down or enabling the VLAN interface has no effect on the UP/DOWN status of the Ethernet ports in the VLAN.

By default, when the status of all Ethernet ports in a VLAN is DOWN, the status of the VLAN interface is DOWN also so the VLAN interface is shut down. When the

status of one or more Ethernet ports is UP, the status of the VLAN interface is UP also, so the VLAN interface is enabled.

Displaying and Debugging a VLAN

After the configuring a VLAN, execute the `display` command in any view to display the VLAN configuration, and to verify the effect of the configuration.

Table 51   Displaying and Debugging a VLAN

Operation	Command
Display the information about a VLAN interface	`display interface vlan-interface` [vlan_id]
Display the information about a VLAN	`display vlan` [vlan_id | **all** | **static** | **dynamic**]
Display the protocol information and protocol index configured on the specified VLAN	`display protocol-vlan` vlan_list
Display the protocol information and protocol index configured on the specified port	`display protocol-vlan interface` interface_list

Example: VLAN Configuration

Create VLAN2 and VLAN3. Add Ethernet 1/0/1 and Ethernet 2/0/1 to VLAN2 and add Ethernet 1/0/2 and Ethernet 2/0/2 to VLAN3.

Figure 15   VLAN Configuration Example

1 Create VLAN 2 and enter its view.

```
[SW7750]vlan 2
```
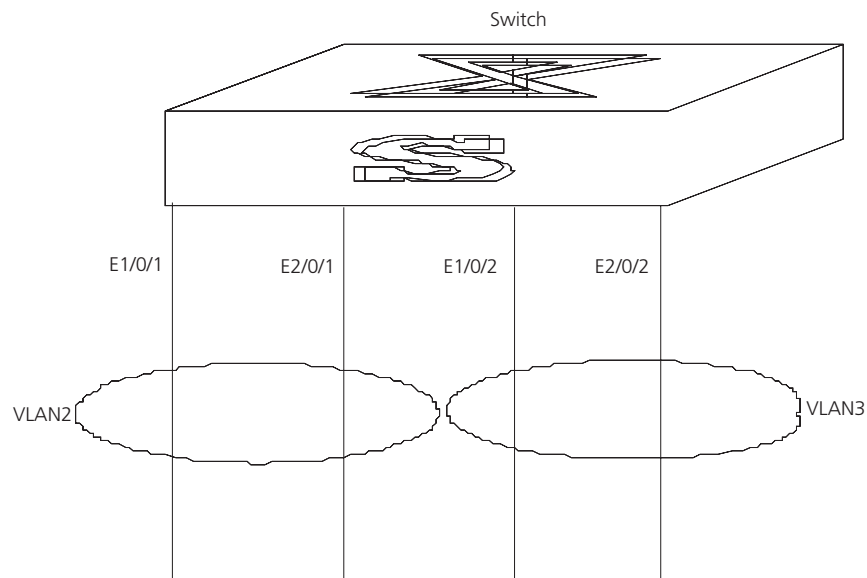
2 Add Ethernet 1/0/1 and Ethernet 2/0/1 to VLAN2.

```
[SW7750-vlan2]port Ethernet 1/0/1 Ethernet 2/0/1
```

3 Create VLAN 3 and enters its view.

```
[SW7750-vlan2]vlan 3
```

4 Add Ethernet 1/0/2 and Ethernet 2/0/2 to VLAN3.

```
[SW7750-vlan3]port Ethernet 1/0/2 Ethernet 2/0/2
```

Configuring Port-Based VLANs

Adding Ethernet Ports to a VLAN

Use the following command to add Ethernet ports to a VLAN.

Perform the following configuration in VLAN view.

Table 52   Adding Ethernet Ports to a VLAN

Operation	Command
Add Ethernet ports to a VLAN	**port** { interface_type interface_num | interface_name [**to** interface_type interface_num | interface_name] }& < 1-10 >
Remove Ethernet ports from a VLAN	**undo port** { interface_type interface_num | interface_name [**to** interface_type interface_num | interface_name] }& < 1-10 >

For the meanings of the parameters related to the Ethernet ports and the specific numbering rules of the ports, see "Port Configuration" on page 35.

The port number preceding the key word **to** must be smaller than the number following **to**. All ports within the specified range must be of the same type.

The **&<1-10>** of the command specifies the repetition times of the parameter, ranging from 1 to 10. In addition, you cannot specify any trunk ports.

By default, the system adds all ports to VLAN1.

Configuring Protocol-Based VLANs

Table 53 describes how incoming packets are treated when they pass through ports that are members of both tagged and protocol-based VLANs.

Table 53   Incoming Packets in Tagged and Protocol-Based VLANs

	Receiving Port on the VLAN		
Incoming Packet	Tagged	Untagged	Default VLAN PVID
Tagged	Perform VLAN check (802.1q)		
Tagged		Perform VLAN check	
Untagged	Perform protocol-VLAN match if a protocol-VLAN is configured		Add to PVID if no match or no protocol-VLAN is configured
Untagged		Perform protocol-VLAN match if a protocol-VLAN is configured	Add to PVID if no match or no protocol-VLAN is configured

Configuring protocol-based VLANs includes tasks described in the following sections:

- Creating and Deleting a VLAN Protocol Type

- Creating and Deleting the Association Between a Port and a Protocol-Based VLAN

Protocol-based VLANs are supported only in the 48-port 10/100BASE-T Auto-sensing FE, 24-port 100BASE-FX MMF FE, 8-port 1000BASE-X GE, and 8-port 10/100/1000BASE-T GE I/O modules.

Creating and Deleting a VLAN Protocol Type

You can use the following command to create or delete a VLAN protocol type.

Perform the following configuration in VLAN view.

Table 54   Creating and Deleting a VLAN Protocol Type

Operation	Command
Create a VLAN protocol type	**protocol-vlan** [**protocol-index**] { **ip** [ip_address [net_mask]] | { **ethernetii** | **llc** | **raw** | **snap** } | **at** | **mode** { **ethernetii** | **llc** | **snap** } }
Delete an existing VLAN protocol type	**undo protocol vlan protocol** { protocol_index [**to** protocol_end] | **all** }

Creating and Deleting the Association Between a Port and a Protocol-Based VLAN

Perform the following configuration in Ethernet port view.

Table 55   Creating and Deleting the Association Between a Port and a Protocol-Based VLAN

Operation	Command
Create the association between a port and a protocol-based VLAN	**port hybrid protocol-vlan** vlan-protocol_list
Delete the association between a port and a protocol-based VLAN	**undo port hybrid protocol-vlan** vlan-protocol_list

Note that the port must be a hybrid port and it must belong to that protocol-based VLAN.

Example: VLAN Configuration

Create VLAN2 and VLAN3. Add Ethernet1/0/1 and Ethernet1/0/2 to VLAN2. Add Ethernet1/0/3 and Ethernet1/0/4 to VLAN3.

Figure 16   VLAN Configuration Example

1 Create VLAN 2 and enter its view.

```
[SW7750]vlan 2
```
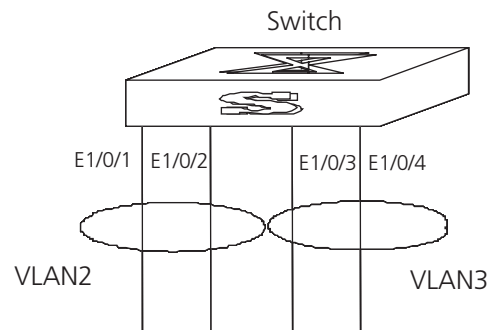
2 Add Ethernet1/0/1 and Ethernet1/0/2 to VLAN2.

```
[SW7750-vlan2]port ethernet1/0/1 to ethernet1/0/2
```

3 Create VLAN 3 and enters its view.

```
[SW7750-vlan2]vlan 3
```

4 Add Ethernet1/0/3 and Ethernet1/0/4 to VLAN3.

```
[SW7750-vlan3]port ethernet1/0/3 to ethernet1/0/4
```

Example: Protocol-Based VLAN Configuration

From port G1/0/1, all the traffic with source IP 10.0.0.1 will belong to VLAN 2 and any other IP traffic will belong to VLAN 3. If we configure port G1/0/2 in VLAN 2, the traffic with source IP 10.0.0.1 will be sent from port G1/0/2. If we configure port G1/0/3 in VLAN 3, any other IP traffic will be sent out from port G1/0/3.

Figure 17 Protocol-Based VLAN Configuration Example
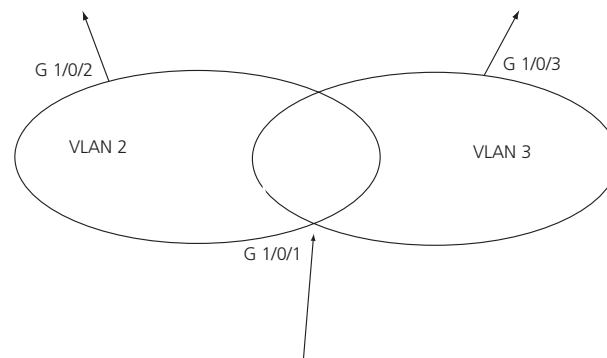
1 Configure port G1/0/1 as hybrid port and allow VLAN 2 and VLAN 3 to pass.

```
[SW7750-GigabitEthernet1/0/1]port link-type hybrid

[SW7750-GigabitEthernet1/0/1]display th

#

interface GigabitEthernet1/0/1

 port link-type hybrid

 port hybrid vlan 1 untagged

#

return


[SW7750-GigabitEthernet1/0/1]port hybrid vlan 2 to 3 t

[SW7750-GigabitEthernet1/0/1]display th

#

interface GigabitEthernet1/0/1

 port link-type hybrid

 port hybrid vlan 2 to 3 tagged
```

```
 port hybrid vlan 1 untagged
#
return
```

2   Configure VLAN 2 and VLAN 3 as protocol VLANs. Set VLAN 2 as IP 10.0.0.1 protocol and VLAN 3 as IP protocol

```
[SW7750-vlan2]protocol-vlan ?

  at    Specify AT(AppleTalk Protocol) configuration information

  ip    Specify IP(Internet Protocol) configuration information

  mode  Specify other protocol mode configuration information


[SW7750-vlan2]vlan

[SW7750-vlan2]protocol-vlan

[SW7750-vlan2]protocol-vlan ip 10.0.0.1

[SW7750-vlan2]vlan 3

[SW7750-vlan3]protocol-vlan ip

[SW7750-vlan3]dis protocol-vlan vlan all

[SW7750-vlan3]dis protocol-vlan vlan all

 VLAN ID: 2

 VLAN Type: Protocol-based VLAN

      Protocol-Index        Protocol-Type

            0                 ip 10.0.0.1 255.255.255.0


 VLAN ID: 3

 VLAN Type: Protocol-based VLAN

      Protocol-Index        Protocol-Type

            0                 ip
```

3   Configure the protocol VLAN on port G1/0/1

```
[SW7750]int g1/0/1

[SW7750-GigabitEthernet1/0/1]port hybrid

[SW7750-GigabitEthernet1/0/1]port hybrid ?

protocol-vlan  Specify current hybrid port's protocol-based VLAN
characteristics

pvid           Specify current hybrid port's PVID VLAN
characteristics
```

```
vlan            Specify current hybrid port's VLAN ID
[SW7750-GigabitEthernet1/0/1]port hybrid protocol

[SW7750-GigabitEthernet1/0/1]port hybrid protocol-vlan 2 0

[SW7750-GigabitEthernet1/0/1]port hybrid protocol-vlan 3 0

[SW7750-GigabitEthernet1/0/1]display th

#

interface GigabitEthernet1/0/1

 port link-type hybrid

 port hybrid vlan 2 to 3 tagged

 port hybrid vlan 1 untagged

 port hybrid protocol-vlan 2 0

 port hybrid protocol-vlan 3 0

#

return
```

4 Configure port G1/0/3 as VLAN 3 and port G1/0/2 as VLAN 2

```
[SW7750]vlan 3

[SW7750-vlan3]port g1/0/3

[SW7750-vlan3]vlan 2

[SW7750-vlan2]port g1/0/2
```

**Configuring
GARP/GVRP**

Generic Attribute Registration Protocol (GARP), allows members in the same switching network to distribute, propagate, and register information, such as VLAN and multicast addresses.

GARP does not exist in a switch as an entity. A GARP participant is called a GARP application. The main GARP applications are GVRP and GMRP. GVRP is described in Configuring GARP/GVRP and GMRP is described in "GMRP" on page 146. When a GARP participant is on a port of the switch, each port corresponds to a GARP participant.

Through GARP, configuration information on one GARP member is advertised rapidly to the entire switching network. A GARP member can be a terminal workstation or bridge. A GARP member can notify other members to register or remove its attribute information by sending declarations or withdrawal declarations. It can also register or remove the attribute information of other GARP members according to declarations or withdrawal declarations that it receives from them.

GARP members exchange information by sending GARP messages. There are three main types of GARP messages, including join, leave, and leaveall. When a GARP participant wants to register its attribute information on other switches, it sends a

join message. When the GARP participant wants to remove its attribute information from other switches, it sends a leave message. The leaveall timer is started at the same time that each GARP participant is enabled and a leaveall message is sent out when the leaveall timer times out. The join and leave messages cooperate to ensure the logout and the re-registration of a message. By exchanging messages, all the attribute information to be registered can be propagated to all the switches in the same switching network.

The destination MAC addresses of the packets of the GARP participants are specific multicast MAC addresses. A switch that supports GARP classifies the packets that it receives from GARP participants and processes them with the corresponding GARP applications (GVRP or GMRP).

GARP and GMRP are described in details in the IEEE 802.1p standard. The Switch 7750 fully supports GARP compliant with the IEEE standards.

> ■ *The value of the GARP timer is used in all GARP applications, including GVRP and GMRP, that are running in a switching network.*
>
> ■ *In one switching network, GARP timers on all the switching devices should be set to the same value.*

Setting the GARP Timers

GARP timers include the hold, join, and leaveall timers.

The GARP participant sends join message regularly when the join timer times out so that other GARP participants can register its attribute values.

When the GARP participant wants to remove attribute values, it sends a leave message. When the leave message arrives, the receiving GARP participant starts the leave timer. If the receiving participant does not receive a join message from the sender before the leave timer expires, the receiving participant removes the sender's GARP attribute values.

The leaveall timer is started as soon as a GARP participant is enabled. A leaveall message is sent at timeout so that other GARP participants remove all the attribute values of this participant. Then, the leaveall timer is restarted and a new cycle begins.

When a switch receives GARP registration information, it does not send a join message immediately. Instead, it enables a hold timer and sends the join message outward when the hold timer times out. In this way, all the VLAN registration information received within the time specified by the hold timer can be sent in one frame to save bandwidth.

Table 56   Setting the GARP Timers

Operation	Command
Configure the hold, join, and leave timers in Ethernet port view.	
Set the GARP hold, join, and leave timers	**garp timer** { **hold**	**join**	**leave** } timer_value
Restore the default GARP hold, join, and leave timer settings	**undo garp timer** { **hold**	**join**	**leave** }

Table 56 Setting the GARP Timers (continued)

Operation	Command
Configure the leaveall timer in system view.	
Set GARP leaveall timer	**garp timer leaveall** timer_value
Restore the default GARP leaveall timer settings.	**undo garp timer leaveall**

Note that the value of the join timer should be no less than twice the value of the hold timer, and the value of the leave timer should be greater than twice the value of the join timer and smaller than the leaveall timer value. Otherwise, the system displays an error message.

Join timer > 2 x hold timer

Leave timer > 2 x join timer AND < leavall timer

GARP timers have the following default values:

- Hold timer — 10 centiseconds
- Join timer — 20 centiseconds,
- Leave timer — 60 centiseconds
- Leaveall timer — 1000 centiseconds.

Displaying and Debugging GARP

After you configure the GARP timer, execute the **display** command in all views to display the GARP configuration, and to verify the effect of the configuration.

Execute the **reset** command in user view to reset the GARP configuration.

Execute the **debugging** command in user view to debug the GARP configuration.

Table 57 Display and Debug GARP

Operation	Command
Display GARP statistics information	**display garp statistics** [**interface** interface-list]
Display GARP timer	**display garp timer** [**interface** interface-list]
Reset GARP statistics information	**reset garp statistics** [**interface** interface-list]
Enable GARP event debugging	**debugging garp** event
Disable GARP event debugging	**undo debugging garp** event

Configuring GVRP

GARP VLAN Registration Protocol (GVRP) is a GARP application. GVRP is based on the GARP, and maintains the dynamic VLAN registration information in the switch and distributes the information to other switches. All the GVRP-supporting switches can receive VLAN registration information from other switches and can dynamically update local VLAN registration information, including the active members and the port through which each member can be reached.

All the switches that support GVRP can distribute their local VLAN registration information to other switches so that VLAN information is consistent on all GVRP devices in the same network. The VLAN registration information that is distributed by GVRP includes both the local static registration information that is configured manually and the dynamic registration information from other switches.

GVRP is described in the IEEE 802.1Q standard. The Switch 7750 fully supports GARP compliant with the IEEE standards.

GVRP configuration steps include tasks described in the following sections:

■ Enabling or Disabling Global GVRP

■ Enabling or Disabling Port GVRP

■ Setting the GVRP Registration Type

When you configure GVRP, you need to enable it globally and for each port participating in GVRP. Similarly, the GVRP registration type can take effect only after you configure port GVRP. In addition, you must configure GVRP on the trunk port.

Enabling or Disabling Global GVRP

Use the following commands to enable or disable global GVRP.

Perform the following configurations in system view.

Table 58   Enabling/Disabling Global GVRP

Operation	Command
Enable global GVRP	`gvrp`
Disable global GVRP	`undo gvrp`

By default, GVRP is disabled on a port.

Enabling or Disabling Port GVRP

Use the following commands to enable or disable GVRP on a port.

Perform the following configurations in Ethernet port view.

Table 59   Enabling/Disabling Port GVRP

Operation	Command
Enable port GVRP	`gvrp`
Disable port GVRP	`undo gvrp`

You should enable GVRP globally before you enable it on the port. GVRP can only be enabled or disabled on a trunk port.

By default, global GVRP is disabled.

Setting the GVRP Registration Type

The GVRP includes normal, fixed, and forbidden registration types (see IEEE 802.1Q).

- When an Ethernet port registration type is set to normal, the dynamic and manual creation, registration, and logout of VLAN are allowed on this port.

- When one trunk port registration type is set to fixed, the system adds the port to the VLAN if a static VLAN is created on the switch and the trunk port allows the VLAN passing. GVRP also adds this VLAN item to the local GVRP database, one link table for GVRP maintenance. However, GVRP cannot learn dynamic VLAN through this port. The learned dynamic VLAN from other ports of the local switch will not be able to send statements to the outside through this port.

- When an Ethernet port registration type is set to forbidden, all the VLANs except VLAN1 are logged out and no other VLANs can be created or registered on this port.

Perform the following configurations in Ethernet port view.

Table 60 Setting the GVRP Registration Type

Operation	Command
Set GVRP registration type	**gvrp registration** { **normal** | **fixed** | **forbidden** }
Set the GVRP registration type back to the default setting	**undo gvrp registration**

By default, the GVRP registration type is normal.

Displaying and Debugging GVRP

After you set the GVRP registration type, execute the **display** command in all views to display the GVRP configuration and to verify the effect of the configuration.

Execute the **debugging** command in user view to debug the configuration of GVRP.

Table 61 Displaying and Debugging GVRP

Operation	Command
Display GVRP statistics information	**display gvrp statistics** [**interface** interface-list]
Display GVRP global status information	**display gvrp status**
Enable GVRP packet or event debugging	**debugging gvrp** { **packet** | **event** }
Disable GVRP packet or event debugging	**undo debugging gvrp** { **packet** | **event** }

Example: GVRP Configuration Example

Set network requirements to dynamically register and update VLAN information among switches.

Figure 18 GVRP Configuration Example
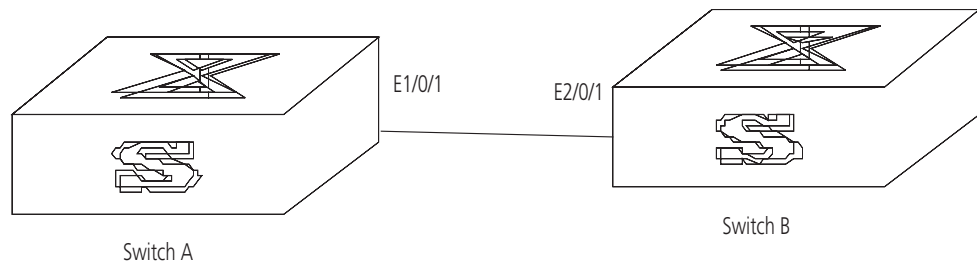
Switch A

Switch B

Configure Switch A:

1 Set Ethernet1/0/1 as a trunk port and allow all the VLANs to pass through.

```
[SW7750]interface Ethernet 1/0/1
[SW7750-Ethernet1/0/1]port link-type trunk
[SW7750-Ethernet1/0/1]port trunk permit vlan all
```

2 Create VLANs.

```
[SW7750-Ethernet1/0/1]vlan 3
[SW7750-vlan3]vlan 4
```

3 Enable GVRP globally.

```
[SW7750-vlan4]quit
[SW7750]gvrp
```

4 Enable GVRP on the trunk port.

```
[SW7750]interface Ethernet 1/0/1
[SW7750-Ethernet1/0/1]gvrp
```

Configure Switch B:

1 Set   Gigabit Ethernet2/1 as a trunk port and allow all the VLANs to pass through.

```
[SW7750]interface Ethernet 2/0/1
[SW7750-Ethernet2/0/1]port link-type trunk
[SW7750-Ethernet2/0/1]port trunk permit vlan all
```

2 Enable GVRP globally.

```
[SW7750-Ethernet2/0/1]quit
[SW7750]gvrp
```

3 Enable GVRP on the trunk port.

```
[SW7750]interface ethernet 2/0/1
[SW7750-Ethernet2/0/1]gvrp
```

4

NETWORK PROTOCOL OPERATION

This chapter covers the following topics:

- Configuring IP Address
- Configuring Address Resolution Protocol (ARP)
- DHCP Relay
- IP Performance

Configuring IP Address

IP address is a 32-bit address represented by four octets. IP addresses are divided into five classes, A, B, C, D and E. The octets are set according to the first few bits of the first octet.

The rule for IP address classification is described as follows:

- Class A addresses are identified with the first bit of the first octet being 0.
- Class B addresses are identified with the first bits of the first octet being 10.
- Class C addresses are identified with the first bits of the first octet being 110.
- Class D addresses are identified with the first bits of the first octet being 1110.
- Class E addresses are identified with the first bits of the first octet being 11110.

Addresses of Classes A, B and C are unicast addresses. The Class D addresses are multicast addresses and Class E addresses are reserved for future use.

At present, IP addresses are mostly Class A, Class B and Class C. IP addresses of Classes A, B and C are composed of two parts, network ID and host ID. Their network ID lengths are different.

- Class A IP addresses use only the first octet to indicate the network ID.
- Class B IP addresses use the first two octets to indicate the network ID.
- Class C IP addresses use the first three octets to indicate the network ID.

At most, there are: 28 =128 Class A addresses, 216=16384 Class B addresses and 224=2,097,152 Class C addresses.

The IP address is in dotted decimal format. Each IP address contains 4 integers in dotted decimal notation. Each integer corresponds to one byte, e.g.,10.110.50.101.

Configuring an IP Address is described in the following sections:

- Subnet and Mask
- Configuring an IP Address

■   Troubleshooting an IP Address Configuration

Subnet and Mask   IP protocol allocates one IP address for each network interface. Multiple IP addresses can only be allocated to a device which has multiple network interfaces. IP addresses on a device with multiple interfaces have no relationship among themselves.

With the rapid development of the Internet, IP addresses are depleting very fast. The traditional IP address allocation method uses up IP addresses with little efficiency. The concept of mask and subnet was proposed to make full use of the available IP addresses.

A mask is a 32-bit number corresponding to an IP address. The number consists of 1s and 0s. Principally, these 1s and 0s can be combined randomly. However, the first consecutive bits are set to 1s when designing the mask. The mask is divided into two parts, the subnet address and host address. The 1 bits and the mask indicate the subnet address, and the other bits indicate the host address.

If there is no subnet division, then the sub-net mask is the default value and the length of "1" indicates the net-id length. Therefore, for IP addresses of classes A, B and C, the default values of the corresponding sub-net mask is 255.0.0.0 for Class A, 255.255.0.0 for Class B, and 255.255.255.0 for Class C.

The mask can be used to divide a Class A network containing more than 16,000,000 hosts or a Class B network containing more than 60,000 hosts into multiple small networks. Each small network is called a subnet. For example, for the Class A network address 10.110.0.0, the mask 255.255.224.0 can be used to divide the network into 8 subnets: (10.110.0.0, 10.110.32.0, 10.110.64.0, and so on). Each subnet can contain more than 8000 hosts.

Configuring an IP Address   The following sections describe the tasks for configuring an IP address:

■   Configure IP Address and HostName for a Host

■   Configuring the IP Address of the VLAN Interface

■   Displaying and Debugging an IP Address

Configure IP Address and HostName for a Host

Perform the following configuration in System view.

Table 62   Configure the Host Name and the Corresponding IP Address

Operation	Command
Configure the host name and the corresponding IP address	**ip host** hostname ip-address
Delete the host name and the corresponding IP address	**undo ip host** hostname [ip-address]

By default, there is no host name associated to any host IP address.

Configuring the IP Address of the VLAN Interface

You can configure an IP address for every VLAN interface of the Ethernet Switch.

Perform the following configuration in VLAN interface view.

Table 63 Configure IP Address for a VLAN Interface

Operation	Command
Configure IP address for a VLAN interface	**ip address** ip-address net-mask [**sub**]
Delete the IP address of a VLAN interface	[**undo**] **ip address** [ip-address { net-mask | mask-length } [**sub**]]

The network ID of an IP address is identified by the mask. For example, the IP address of a VLAN interface is 129.9.30.42 and the mask is 255.255.0.0. After performing the AND operation for the IP address and the mask, you can assign that device to the network segment 129.9.0.0.

Generally, it is sufficient to configure one IP address for an interface. However, you can also configure more than one IP address for an interface so that it can be connected to several subnets. Among these IP addresses, one is the primary IP address and all others are secondary.

By default, the IP address of a VLAN interface is null.

**Displaying and Debugging an IP Address**

Use the **display** command in all views to display the IP address configuration on interfaces, and to verify configuration.

Table 64 Display and Debug IP Address

Operation	Command
Display all hosts on the network and the corresponding IP addresses	display ip hosts
Display the configurations of each interface	**display ip interface vlan-interface** *vlan-id*

Example: Configuring an IP Address

Configure the IP address as 129.2.2.1 and subnet mask as 255.255.255.0 for the VLAN interface 1 of the Ethernet Switch.

Figure 19 IP Address Configuration Networking
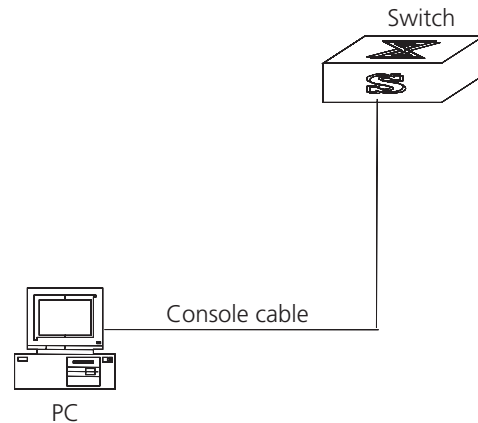
1 Enter VLAN interface 1.

```
[SW7750] interface vlan 1
```

2 Configure the IP address for VLAN interface 1.

```
[SW7750-vlan-interface1] ip address 129.2.2.1 255.255.255.0
```

Troubleshooting an IP Address Configuration

If the Ethernet Switch cannot ping a certain host on the LAN, proceed as follows:

1 Determine which VLAN includes the port connected to the host. Check whether the VLAN has been configured with the VLAN interface. Determine whether the IP address of the VLAN interface and the host are on the same network segment.

2 If the configuration is correct, enable ARP debugging on the switch from user level, and check whether or not the switch can correctly send and receive ARP packets. If it can only send but not receive the ARP packets, there are probably errors at the Ethernet physical layer.

Configuring Address Resolution Protocol (ARP)

An IP address cannot be directly used for communication between network devices, because devices can only identify MAC addresses. An IP address is the address of a host at the network layer. To send data packets through the network layer to the destination host, the physical address of the host is required. So the IP address must be resolved to a physical address.

When two hosts in Ethernet communicate, they must know each other's MAC address. Every host maintains an IP-MAC address translation table, which is known as the ARP mapping table. A series of maps between IP addresses and MAC addresses of other hosts are stored in the ARP mapping table. When a dynamic ARP mapping entry is not in use for a long time, the host will remove it from the mapping table to save memory space and shorten the search interval.

Example: IP Address Resolution

Host A and Host B are on the same network segment. The IP address of Host A is IP_A and the IP address of Host B is IP_B. Host A wants to transmit packets to Host B. Host A checks its own ARP mapping table first to make sure that there are corresponding ARP entries of IP_B in the table. If the corresponding MAC address is found, Host A will use the MAC address in the ARP mapping table to encapsulate the IP packet in an Ethernet frame and send it to Host B. If the

corresponding MAC address is not found, Host A will store the IP packet in the queue waiting for transmission, and broadcast an ARP request to attempt to resolve the MAX address of Host B.

The ARP request packet contains the IP address of Host B and the IP address and MAC address of Host A. Since the ARP request packet is broadcast, all hosts on the network segment receive the request. However, only the requested host (i.e., Host B) needs to process the request. Host B will first store the IP address and the MAC address of the request sender (Host A) from the ARP request packet in its own ARP mapping table. Host B will then generate an ARP reply packet and add the MAC address of Host B before sending it to Host A. The reply packet will be sent directly to Host A instead of being broadcast. Upon receiving the reply packet, Host A will extract the IP address and the corresponding MAC address of Host B and add them to its own ARP mapping table. Then Host A will send Host B all the packets standing in the queue.

Normally, dynamic ARP executes and automatically attempts to resolve the IP address to an Ethernet MAC address with no intervention from the administrator.

Configuring ARP   The ARP mapping table can be maintained dynamically or manually. Addresses that are mapped manually are referred to as static ARP. The user can display, add, or delete the entries in the ARP mapping table through manual commands.

ARP configuration includes tasks described in the following sections:

- Manually Adding/Deleting Static ARP Mapping Entries
- Learning Gratuitous ARPs
- Configuring the Dynamic ARP Aging Timer
- Displaying and Debugging ARP

Manually Adding/Deleting Static ARP Mapping Entries

Perform the following configuration in System view.

Table 65   Manually Adding/Deleting Static ARP Mapping Entries

Operation	Command
Manually add a static ARP mapping entry	**arp static** ip-address mac-address VLANID { interface_type interface_num | interface_name }
Manually delete a static ARP mapping entry	**undo arp static** ip-address

> **i** *Static ARP mapping entries will not time out, however dynamic ARP mapping entries time out after 20 minutes.*

The ARP mapping table is empty and the address mapping is obtained through dynamic ARP by default.

Learning Gratuitous ARPs

Perform the following configuration in System view.

Table 66   Learning Gratuitous ARPs

Operation	Command
Enable the switch to learn gratuitous ARPs	**gratuitous-arp-learning enable**

Table 66 Learning Gratuitous ARPs

Operation	Command
Prevent the switch from learning gratuitous ARPs	**undo gratuitous-arp-learning enable**

By default, the switch does not learn gratuitous ARPs.

Configuring the Dynamic ARP Aging Timer

The following commands assign a dynamic ARP aging period to enable flexible configurations. When the system learns a dynamic ARP entry, its aging period is based on the currently configured value.

Perform the following configuration in system view.

Table 67 Configure the Dynamic ARP Aging Timer

Operation	Command
Configure the dynamic ARP aging timer	**arp timer aging** aging-time
Restore the default dynamic ARP aging time	**undo arp timer aging**

By default, the aging time of the dynamic ARP aging timer is 20 minutes.

Displaying and Debugging ARP

After the previous configuration, execute **display** command in all views to display the operation of the ARP configuration, and to verify the effect of the configuration. Execute the **debugging** command in user view to debug the ARP configuration.

Table 68 Display and Debug ARP

| Operation	Command
Display ARP mapping table	**display arp** [ip-address	[**static**	**dynamic**] [{ **begin**	**include**|**exclude** } text]]
Display the current setting of the dynamic ARP map aging timer	**display arp timer aging**
Enable ARP information debugging	**debugging arp** { **packet**	**status** }
Disable ARP information debugging	**undo debugging arp** { **packet**	**status** }

By default, all ARP mapping entries of the Ethernet switch are displayed.

DHCP Relay

Dynamic Host Configuration Protocol (DHCP) offers dynamic IP address assignment. DHCP works in Client-Server mode. With this protocol, the DHCP Client can dynamically request configuration information and the DHCP server can configure the information for the Client.

The DHCP relay serves as conduit between the DHCP Client and the server located on different subnets. The DHCP packets can be relayed to the destination DHCP server (or Client) across network segments. The DHCP clients on different networks can use the same DHCP server. This is economical and convenient for centralized management.

Figure 20   DHCP Relay Schematic Diagram
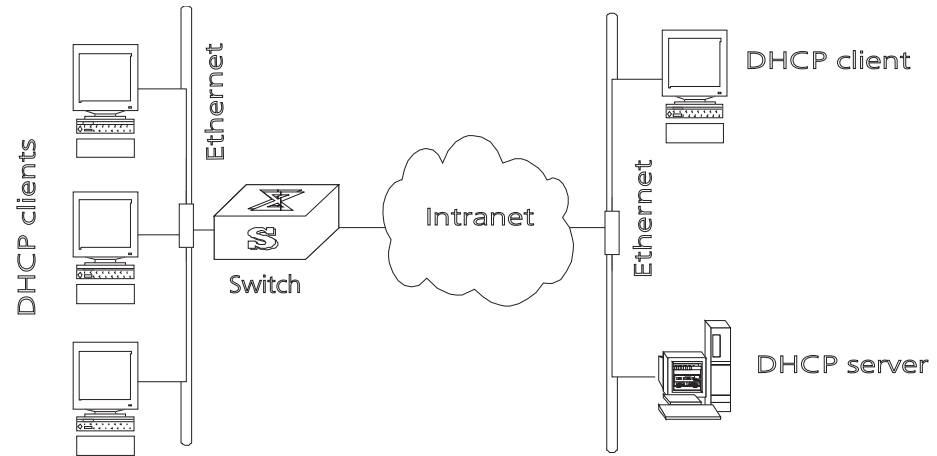
When the DHCP Client performs initialization, it broadcasts the request packet on the local network segment. If there is a DHCP server on the local network segment (e.g. the Ethernet on the right side of the figure), then the DHCP can be configured directly without the relay. If there is no DHCP server on the local network segment, DHCP relay will process the received broadcast packets and forward them to remote DHCP servers. The server configures the clients based on the information provided in the DHCP request packet and in the server setup. Then the server transmits the configuration information to the clients through the DHCP relay, thereby, completing the dynamic configuration of the client.

Configuring DHCP is described in the following sections:

■   Configuring DHCP Relay

■   Troubleshooting a DHCP Relay Configuration

Configuring DHCP Relay   DHCP relay configuration includes tasks described in the following sections:

■   Configuring a DHCP Server IP Address in a DHCP Server Group

■   Configuring the DHCP Server Group for the VLAN Interface

■   Configuring the Address Table Entry

■   Enabling/Disabling DHCP Security Features

■   Displaying and Debugging DHCP Relay

> *The server IP address is associated , through its DHCP server group, with a specific VLAN interface. This implementation differs from others in which the server IP is a global parameter.*

Configuring a DHCP Server IP Address in a DHCP Server Group

Perform the following configuration in System view.

Table 69   Configure/Delete the IP Address of the DHCP Server

Operation	Command
Configure the IP address for a DHCP Server	**dhcp-server** groupNo **ip** ipaddress1 [ipaddress2]

Table 69   Configure/Delete the IP Address of the DHCP Server

Operation	Command
Remove all the IP addresses of the DHCP Server (set the IP addresses of the primary and secondary servers to 0).	**undo dhcp-server** groupNo

i > *The backup server IP address cannot be configured independently, instead, it has to be configured together with the master server IP address.*

By default, the IP address of the DHCP Server is not configured. The DHCP Server address must be configured before DHCP relay can be used.

Configuring the DHCP Server Group for the VLAN Interface

Perform the following configuration in VLAN interface view.

Table 70   Configure/Delete the Corresponding DHCP Server Group of VLAN Interface

Operation	Command
Configure the DHCP server group for the VLAN interface	**dhcp-server** groupNo
Delete the DHCP server group for the VLAN interface	**undo dhcp-server**

When associating a VLAN interface to a new DHCP server group, you can configure the association without disassociating it from the previous group.

By default, VLAN interfaces have no associated DHCP server group.

Configuring the Address Table Entry

To check the address of users who have valid and fixed IP addresses in the VLAN (with DHCP enabled), it is necessary to add an entry in the static address table.

Perform the following configuration in system view.

Table 71   Configure/Delete the Address Table Entry

Operation	Command
Add an entry to the address table	**dhcp-security static** ip_address mac_address { **dynamic**|**static** }
Delete an entry from the address table	**undo dhcp-security** { ip_address | **all** | **dynamic** | **static** }

Enabling/Disabling DHCP Security Features

Enabling DHCP security features starts an address check on the VLAN interface, while disabling DHCP security features cancels an address check.

Perform the following configuration in VLAN interface view.

Table 72   Enable/Disable DHCP Security on VLAN Interfaces

Operation	Command
Enable DHCP security features	**address-check enable**
Disable DHCP security features on VLAN interface	**address-check disable**

By default, DHCP security features function are disabled.

Displaying and Debugging DHCP Relay

Execute **display** command in all views to display the current DHCP Relay configuration, and to verify the effect of the configuration. Execute the **debugging** command in user view to debug DHCP Relay configuration.

Table 73 Displaying and Debugging DHCP Relay

Operation	Command
Display the information about the DHCP server group	**display dhcp-server** groupNo
Display the information about the DHCP server group corresponding to the VLAN interface.	**display dhcp-server interface vlan-interface** vlan-id
Enable DHCP relay debugging	**debugging dhcp-relay**
Disable DHCP relay debugging	**undo debugging dhcp-relay**
Display address information for all the legal clients of the DHCP Server group.	**display dhcp-security** [ip_address | **dynamic** | **static**]

Example: Configuring DHCP Relay

Configure the VLAN interface corresponding to the user and the related DHCP server so as to use DHCP relay.

Figure 21 Networking Diagram of Configuring DHCP Relay
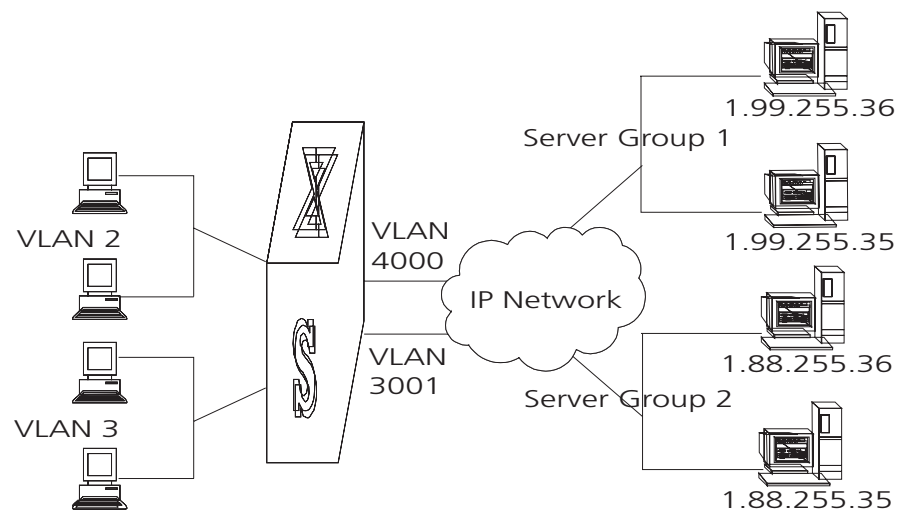
1 Configure the DHCP Server IP addresses into DHCP Server Group 1.

```
[SW7750]dhcp-server 1 ip 1.99.255.36 1.99.255.35
```

2 Associate DHCP Server Group 1 with VLAN interface 2.

```
[SW7750-VLAN-Interface2]dhcp-server 1
```

3 Configure the IP address corresponding to DHCP server group 2.

```
[SW7750]dhcp-server 2 ip 1.88.255.36 1.88.255.35
```

4 Associate the DHCP Server Group 2 with VLAN interface 3.

```
[SW7750-VLAN-Interface3]dhcp-server 2
```

5 Configure the corresponding interface and gateway address of VLAN2.

```
[SW7750]vlan 2
[SW7750-vlan2]port Ethernet 1/0/2
[SW7750]interface vlan 2
[SW7750-VLAN-Interface2]ip address 1.1.2.1 255.255.0.0
```

6 Configure the corresponding interface and gateway address of VLAN3.

```
[SW7750]vlan 3
[SW7750-vlan3]port Ethernet 1/0/3
[SW7750]interface vlan 3
[SW7750-VLAN-Interface3]ip address 21.2.2.1 255.255.0.0
```

7 It is necessary to configure a VLAN for the servers. The corresponding interface VLAN of the DHCP server group 1 is configured as 4000, and that of the group 2 is configured as 3001.

```
[SW7750]vlan 4000
[SW7750-vlan4000]port Ethernet 1/0/4
[SW7750]interface vlan 4000
[SW7750-VLAN-Interface4000]ip address 1.99.255.1 255.255.0.0
[SW7750]vlan 3001
[SW7750-vlan3001]port Ethernet 1/0/5
[SW7750]interface vlan 3001
[SW7750-VLAN-Interface3001]ip address 1.88.255.1 255.255.0.0
```

In this example, clients on VLAN2 will receive IP addresses from the servers in DHCP server group 1 (VLAN 4000). Clients on VLAN3 will receive IP addresses from the servers in DHCP server group 2 (VLAN 3001).

8 Show the configuration of DHCP server groups in User view.

```
<SW7750>display dhcp-server 1
```

9 Show the DHCP Server Group number corresponding to the VLAN interface in User view.

```
<SW7750>display dhcp-server interface vlan-interface 2
<SW7750>display dhcp-server interface vlan-interface 3
```

Troubleshooting a DHCP Relay Configuration

Perform the following procedure if a user cannot apply for an IP address dynamically:

1 Use the `display dhcp-server groupNo` command to check if the IP address of the corresponding DHCP server has been configured.

2 Use the `display VLAN` and `display IP` commands to check if the VLAN and the corresponding interface IP address have been configured.

3 Ping the configured DHCP Server to ensure that the link is connected.

4 Ping the IP address of the VLAN interface of the switch to where the DHCP user is connected from the DHCP server to make sure that the DHCP server can correctly find the route of the network segment the user is on. If the ping execution fails, check if the default gateway of the DHCP server has been configured as the address of the VLAN interface that it locates on.

5 If no problems are found in the last two steps, use the `display dhcp-server groupNo` command to view the packet that has been received. If you only see the Discover packet and there is no response packet, it means the DHCP Server has not sent the message to the Switch 7750. In this case, check if the DHCP Server has been configured properly. If the numbers of request and response packets are normal, enable the debugging dhcp-relay in User view and then use the `terminal`

`debugging` command to output the debugging information to the console. In this way, you can view the detailed information of all DHCP packets on the console while applying for the IP address, thereby, conveniently locating the problem.

IP Performance

IP performance configuration includes:

■ Configuring TCP Attributes

■ Configuring Special IP Packet Transmission to the CPU

■ Configuring L3 Broadcast Forwarding

■ Displaying and Debugging IP Performance

■ Troubleshooting IP Performance

Configuring TCP Attributes

The TCP attributes that can be configured include:

■ `synwait timer`: When sending the syn packets, TCP starts the synwait timer. If response packets are not received before synwait timeout, the TCP connection will be terminated. The timeout of synwait timer ranges 2 to 600 seconds and it is 75 seconds by default.

■ `finwait timer`: When the TCP connection state turns from FIN_WAIT_1 to FIN_WAIT_2, finwait timer will be started. If FIN packets are not received before finwait timer timeout, the TCP connection will be terminated. Finwait ranges 76 to 3600 seconds and it is 675 seconds by default.

■ The receiving/sending buffer size of connection-oriented Socket is in the range from 1 to 32K bytes and is 4K bytes by default.

Perform the following configuration in System view.

Table 74   Configure TCP Attributes

Operation	Command
Configure synwait timer time for TCP connection establishment	`tcp timer syn-timeout` time-value
Restore synwait timer time for TCP connection establishment to default value	`undo tcp timer syn-timeout`
Configure FIN_WAIT_2 timer time of TCP	`tcp timer fin-timeout` time-value
Restore FIN_WAIT_2 timer time of TCP to default value	`undo tcp timer fin-timeout`
Configure the Socket receiving/sending buffer size of TCP	`tcp window` window-size
Restore the socket receiving/sending buffer size of TCP to default value	`undo tcp window`

By default, the TCP finwait timer is 675 seconds, the synwait timer is 75 seconds, and the receiving/sending buffer size of connection-oriented Socket is 4K bytes.

Configuring Special IP Packet Transmission to the CPU

In IP packet forwarding, redirection packets, TTL timeout packets, and route unreachable packets are often sent to CPU, which will notify the peer end for further processing upon receiving them. Configuration errors and malicious assaults may cause CPU overload. In this case, to maintain normal system

operation, you may have to use the following commands to prevent the corresponding packets from being sent to the CPU.

Perform the following configuration in system view.

Table 75   Configure Whether to Send Special IP Packets to CPU

Operation	Command
Configure the system to send packets to the CPU	`ip { redirects	ttl-expires	unreachables }`
Configure the system not to send packets to the CPU	`undo ip { redirects	ttl-expires	unreachables }`

By default, redirection packets and route unreachable packets are not sent to CPU, while TTL timeout packets are sent to CPU.

Configuring L3 Broadcast Forwarding

Broadcast packets include full-net broadcast packets and direct-connected broadcast packets. The destination IP address of a full-net broadcast packet is all ones (255.255.255.255) or all zeros. A direct-connected broadcast packet is a packet whose destination IP address is the network broadcast address of a subnet, but the source IP address is not in the subnet segment. When a switch forwards a packet, it cannot tell whether the packet is a broadcast packet unless the switch is connected with the subnet.

If a broadcast packet reaches the destination network after being forwarded by the switch, the switch will receive the broadcast packet; the switch also belongs to the subnet. The VLAN of the switch isolates the broadcast domain, it will stop forwarding the packet to the network. Using the following configuration task, you can choose to forward the broadcast packet to the network for broadcasting.

Perform the following configuration in system view.

Table 76   Configure Whether to Forward L3 Broadcast Packets

Operation	Command
Configure forward L3 broadcast packets	`ip forward-broadcast`
Disable forward L3 broadcast packets	`undo ip forward-broadcast`

By default, L3 broadcast packets are forwarded.

Displaying and Debugging IP Performance

After the previous configuration, display the operation of the IP Performance configuration in all views, and verify the effect of the configuration. Execute the `debugging` command in user view to debug IP Performance configuration.

Table 77   Display and Debug IP Performance

Operation	Command
Display TCP connection state	`display tcp status`
Display TCP connection statistics data	`display tcp statistics`
Display IP statistics information	`display ip statistics`
Display ICMP statistics information	`display icmp statistics`
Reset IP statistics information	`reset ip statistics`
Reset TCP statistics information	`reset tcp statistics`

Troubleshooting IP Performance
If the IP layer protocol works normally, but TCP and UDP do not work normally, you can enable the corresponding debugging information output to view the debugging information.

- Use the **terminal debugging** command to output the debugging information to the console.

- Use the **debugging udp packet** command to enable the UDP debugging to trace the UDP packet. When the router sends or receives UDP packets, the content format of the packet can be displayed in real time. You can locate the problem from the contents of the packet.

  The following are the UDP packet formats:

```
UDP output packet:
Source IP address:202.38.160.1
Source port:1024
Destination IP Address 202.38.160.1
Destination port: 4296
```

- Use the **debugging tcp packet** or **debugging tcp transaction** command to enable the TCP debugging to trace the TCP packets. There are two available ways for debugging TCP.

- Debug and trace the packets of the TCP connection that take this device as one end.

  Operations include:

```
<SW7750>terminal debugging
<SW7750>debugging tcp packet
```

  The TCP packets, received or sent can be checked in real time. Specific packet formats include:

```
TCP output packet:
Source IP address:202.38.160.1
Source port:1024
Destination IP Address 202.38.160.1
Destination port: 4296
Sequence number :4185089
Ack number: 0
Flag  :SYN
Packet length :60
Data offset: 10
```

- Debug and trace the packets located in SYN, FIN or RST.

  Operations include:

```
<SW7750>terminal debugging
<SW7750>debugging tcp transact
```

  The TCP packets received or sent can be checked in real time, and the specific packet formats are the same as those mentioned above.

-

5

IP ROUTING PROTOCOL OPERATION

This chapter covers the following topics:

- IP Routing Protocol Overview
- Static Routes
- RIP
- IP Routing Policy
- Route Capacity

IP Routing Protocol Overview

Routers select an appropriate path through a network for an IP packet according to the destination address of the packet. Each router on the path receives the packet and forwards it to the next router. The last router in the path submits the packet to the destination host.

In a network, the router regards a path for sending a packet as a logical route unit, and calls it a hop. For example, in Figure 22, a packet sent from Host A to Host C goes through 3 networks and 2 routers and the packet is transmitted through two hops and router segments. Therefore, when a node is connected to another node through a network, there is a hop between these two nodes and these two nodes are considered adjacent in the Internet. Adjacent routers are two routers connected to the same network. The number of route segments between a router and hosts in the same network count as zero. In Figure 22, the bold arrows represent the hops. A router can be connected to any physical link that constitutes a route segment for routing packets through the network.

When an Ethernet switch runs a routing protocol, it can perform router functions. In this guide, a router and its icon represent a generic router or an Ethernet switch running routing protocols.

Figure 22   About Hops

Networks can have different sizes, so, the segment lengths connected between two different pairs of routers are also different.

If a router in a network is regarded as a node and a route segment in the Internet is regarded as a link, message routing in the Internet works in a similar way as the message routing in a conventional network. Routing a message through the shortest route may not always be the optimal route. For example, routing through three LAN route segments may be much faster than a route through two WAN route segments.

Configuring the IP Routing Protocol Overview is described in the following sections:

■   Selecting Routes Through the Routing Table

■   Routing Management Policy

Selecting Routes Through the Routing Table

For the router, a routing table is the key to forwarding packets. Each router saves a routing table in its memory, and each entry in this table specifies the physical port of the router through which a packet is sent to a subnet or a host. The packet can reach the next router over a particular path or reach a destination host through a directly connected network.

A routing table has the following key entries:

■   A destination address — Identifies the destination IP address or the destination network of the IP packet, which is 32 bits in length.

■   A network mask — Is made up of several consecutive 1s, which can be expressed either in the dotted decimal format, or by the number of the consecutive 1s in the mask. Combined with the destination address, the network mask identifies the network address of the destination host or router. With the destination address and the network mask, you have the address of the network segment where the destination host or router is located. For example, if the destination address is 129.102.8.10, the address of the network where the host or the router with the mask 255.255.0.0 is located is 129.102.0.0.

- The output interface — Indicates an interface through which an IP packet should be forwarded.

- The next hop address — Indicates the next router that an IP packet will pass through.

- The priority added to the IP routing table for a route — Indicates the type of route that is selected. There may be multiple routes with different next hops to the same destination. These routes can be discovered by different routing protocols, or they can be the static routes that are configured manually. The route with the highest priority (the smallest numerical value) is selected as the current optimal route.

Routes are divided into two types: subnet routes, in which the destination is a subnet, or host routes, in which the destination is a host.

In addition, depending on whether the network of the destination host is directly connected to the router, there are two types of routes:

- Direct route: The router is directly connected to the network where the destination is located.

- Indirect route: The router is not directly connected to the network where the destination is located.

To limit the size of the routing table, an option is available to set a default route. All the packets that fail to find a suitable table entry are forwarded through this default route.

In a complicated Internet, as shown in the following figure, the number in each network is the network address. The router R8 is connected to three networks, so it has three IP addresses and three physical ports. Its routing table is shown in Figure 23.

Figure 23   The Routing Table

Destination host location	Forwarding router	Port passed
10.0.0	Directly	2
11.0.0	Directly	1
12.0.0	11.0.0.2	1
13.0.0	Directly	3
14.0.0	13.0.0.2	3
15.0.0	10.0.0.2	2
16.0.0	10.0.0.2	2
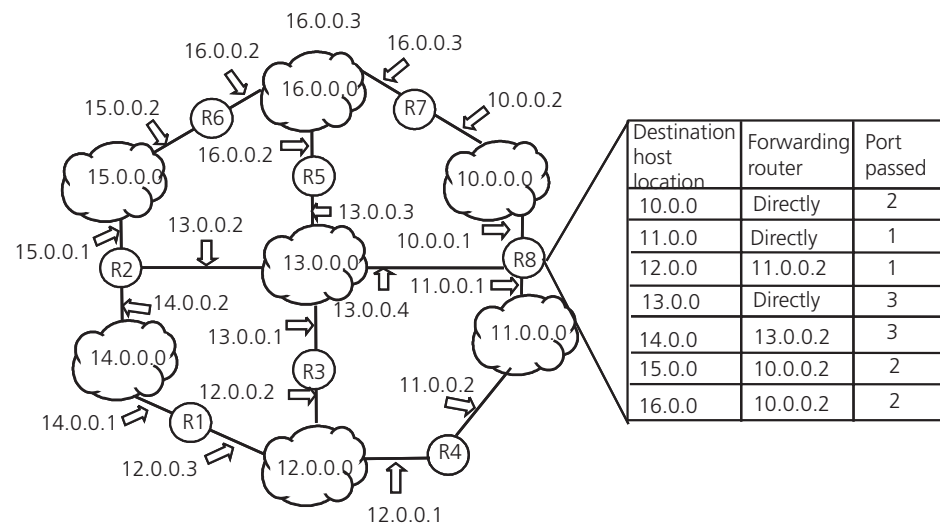
Routing Management Policy   The Switch 7750 supports the configuration of a series of dynamic routing protocols such as RIP, as well as static routes. The static routes configured by the

user are managed together with the dynamic routes as detected by the routing protocol. The static routes and the routes learned or configured by routing protocols can be shared with each other.

Routing protocols (as well as the static configuration) can generate different routes to the same destination, but not all these routes are optimal. In fact, at a certain moment, only one routing protocol can determine a current route to a single destination. Thus, each routing protocol (including the static configuration) has a set preference, and when there are multiple routing information sources, the route discovered by the routing protocol with the highest preference becomes the current route. Routing protocols and the default preferences (the smaller the value, the higher the preference) of the routes that they learn are shown in Table 78.

Table 78   Routing Protocols and the Default Preferences for Routes

Routing protocol or route type	The preference of the corresponding route
DIRECT	0
STATIC	60
RIP	100
UNKNOWN	255

In the table, 0 indicates a direct route, and 255 indicates any route from an unreliable source.

Except for direct routing, the preferences of various dynamic routing protocols can be manually configured to meet the user requirements. The preferences for individual static routes can be different.

Routes Shared Between Routing Protocols

As the algorithms of various routing protocols are different, different protocols can generate different routes. This situation creates the problem of how to resolve different routes being generated by different routing protocols. The Switch 7750 supports an operation to import the routes generated by one routing protocol into another routing protocol. Each protocol has its own route redistribution mechanism. For details, refer to "Enabling RIP to Import Routes of Other Protocols", or "Importing Routing Information Discovered by Other Routing Protocols".

Static Routes

A static route is a route that is manually configured by the network administrator. You can set up an interconnected network using static routes. However, if a fault occurs in the network, the static route cannot change automatically to steer packets away from the fault without the help of the administrator.

In a relatively simple network, you only need to configure static routes to make the router work normally. The proper configuration and usage of the static route can improve network performance and ensure bandwidth for important applications.

The following routes are static routes:

- Reachable route — The normal route in which the IP packet is sent to the next hop towards the destination. this is a common type of static route.

- Unreachable route — When a static route to a destination has the *reject* attribute, all the IP packets to this destination are discarded, and the originating host is informed that the destination is unreachable.

- Blackhole route — When a static route to a destination has the *blackhole* attribute, all the IP packets to this destination are discarded, and the originating host is not informed.

The attributes *reject* and *blackhole* are usually used to control the range of reachable destinations of this router, and to help troubleshoot the network.

Default Route

A default route is also a static route. A default route is used only when no suitable routing table entry is found. In a routing table, the default route is in the form of the route to the network 0.0.0.0 (with the mask 0.0.0.0). You can determine whether a default route has been set by viewing the output of the **display ip routing-table** command. If the destination address of a packet fails to match any entry of the routing table, the router selects the default route to forward this packet. If there is no default route and the destination address of the packet fails to match any entry in the routing table, the packet is discarded, and an Internet Control Message Protocol (ICMP) packet is sent to the originating host to indicate that the destination host or network is unreachable.

In a typical network that consists of hundreds of routers, if you used multiple dynamic routing protocols without configuring a default route then significant bandwidth would be consumed. Using the default route can provide appropriate bandwidth, but not high bandwidth, for communications between large numbers of users.

Configuring Static Routes is described in the following sections:

- Configuring Static Routes
- Troubleshooting Static Routes

Configuring Static Routes

Static route configuration tasks are described in the following sections:

- Configuring a Static Route
- Configuring a Default Route
- Deleting All Static Routes
- Displaying and Debugging Static Routes

Configuring a Static Route

Perform the following configurations in system view.

Table 79   Configuring a Static Route

Operation	Command
Add a static route	**ip route-static** ip-address {mask | mask-length } { interface-name | gateway-address } [**preference** value] [**reject**|**blackhole**]
Delete a static route	**undo ip route-static** ip-address {mask | mask-length } { interface-name | gateway-address} [**preference** value]

The parameters are explained as follows:

■   IP address and mask

   The IP address and mask use a decimal format. Because the 1s in the 32-bit mask must be consecutive, the dotted decimal mask can also be replaced by the mask-length which refers to the digits of the consecutive 1s in the mask.

■   Transmitting interface or next hop address

   When you configure a static route, you can specify either the interface-type port-number to designate a transmitting interface, or the gateway-address to decide the next hop address, depending on the actual conditions.

You can specify the transmitting interfaces in the cases below:

■   For the interface that supports resolution from the network address to the link layer address (such as the Ethernet interface that supports ARP), when ip-address and mask (or mask-length) specifies a host address, and this destination address is in the directly connected network, the transmitting interface can be specified.

■   For a P2P interface, the address of the next hop defines the transmitting interface because the address of the opposite interface is the address of the next hop of the route.

   In fact, for all routing items, the next hop address must be specified. When the IP layer transmits a packet, it first searches the matching route in the routing table, depending on the destination address of the packet. Only when the next hop address of the route is specified, can the link layer find the corresponding link layer address, and then forward the packet.

■   For different configurations of preference-value, you can flexibly apply the routing management policy.

■   The *reject* and *blackhole* attributes indicate the unreachable route and the blackhole route.

Configuring a Default Route

Perform the following configurations in system view.

Table 80   Configuring a Default Route

Operation	Command
Configure a default route	**ip route-static** 0.0.0.0 { 0.0.0.0 | 0 } { interface-name | gateway-address } [**preference value] [reject**|**blackhole**]
Delete a default route	**undo ip route-static** 0.0.0.0 { 0.0.0.0 | 0 } { interface-name | gateway-address }]

Parameters for default route are the same as for static route.

Deleting All Static Routes

You can use the **undo ip route-static** command to delete one static route. The Switch 7750 also provides the **delete static-route all** command for you to delete all static routes at one time, including the default routes.

Perform the following configuration in system view.

Table 81 Deleting All Static Routes

Operation	Command
Delete all static routes	`delete static-routes all`

Displaying and Debugging Static Routes

After you configure static and default routes, execute the `display` command in all views, to display the static route configuration, and to verify the effect of the configuration.

Table 82 Displaying and Debugging the Routing Table

Operation	Command
View routing table summary	`display ip routing-table`
View routing table details	`display ip routing-table verbose`
View the detailed information of a specific route	`display ip routing-table` `ip-address`
View the route filtered through specified basic access control list (ACL)	`display ip routing-table acl {` `acl-number` | `acl-name` `} [` `verbose` `]`
View the route information that through specified ip prefix list	`display ip routing-table` `ip-prefix` `ip-prefix-number` `[` `verbose` `]`
View the routing information found by the specified protocol	`display ip routing-table protocol` `protocol` `[` `inactive` | `verbose` `]`
View the tree routing table	`display ip routing-table radix`
View the integrated routing information	`display ip routing-table` `statistics`

Example: Typical Static Route Configuration

As shown in the Figure 24, the masks of all the IP addresses in the figure are 255.255.255.0. All the hosts or switches must be interconnected in pairs, by configuring static routes.

Figure 24   Static Route Configuration
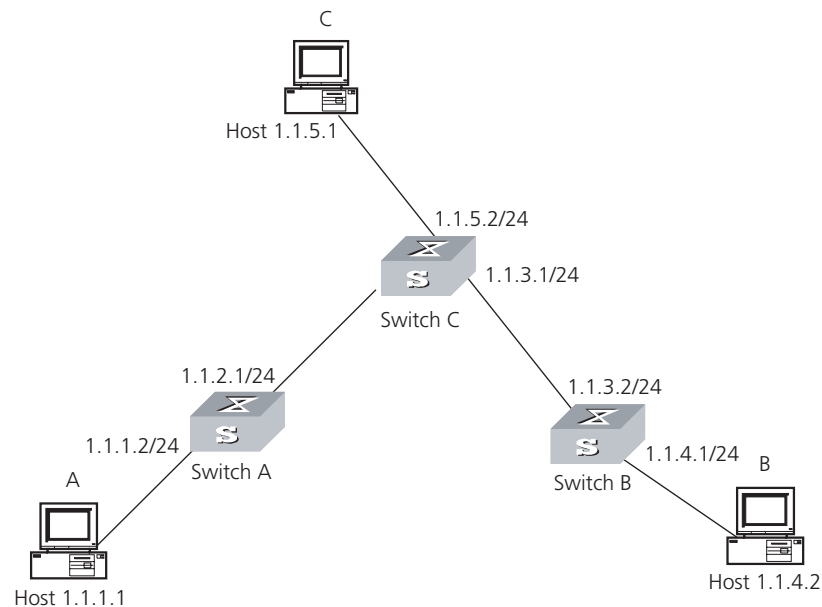
1 Configure the static route for Ethernet Switch A:

```
[Switch A]ip route-static 1.1.3.0 255.255.255.0 1.1.2.2
[Switch A]ip route-static 1.1.4.0 255.255.255.0 1.1.2.2
[Switch A]ip route-static 1.1.5.0 255.255.255.0 1.1.2.2
```

2 Configure the static route for Ethernet Switch B:

```
[Switch B]ip route-static 1.1.2.0 255.255.255.0 1.1.3.1
[Switch B]ip route-static 1.1.5.0 255.255.255.0 1.1.3.1
[Switch B]ip route-static 1.1.1.0 255.255.255.0 1.1.3.1
```

3 Configure the static route for Ethernet Switch C:

```
[Switch C]ip route-static 1.1.1.0 255.255.255.0 1.1.2.1
[Switch C]ip route-static 1.1.4.0 255.255.255.0 1.1.3.2
```

4 Configure the default gateway of the Host A to be 1.1.5.2

5 Configure the default gateway of the Host B to be 1.1.4.1

6 Configure the default gateway of the Host C to be 1.1.1.2

Using this procedure, all the hosts or switches in Figure 24 can be interconnected in pairs.

Troubleshooting Static Routes   The Switch 7750 is not configured with any dynamic routing protocols enabled. Both the physical status and the link layer protocol status of the interface are enabled, but the IP packets cannot be forwarded normally.

- Use the **display ip routing-table protocol static** command to view whether the corresponding static route is correctly configured.

- Use the **display ip routing-table** command to view whether the corresponding route is valid.

RIP   Routing Information Protocol (RIP) is a simple, dynamic routing protocol, that is Distance-Vector (D-V) algorithm-based. It uses hop counts to measure the distance to the destination host, which is called routing cost. In RIP, the hop count from a router to its directly connected network is 0. The hop count to a network which can be reached through another router is 1, and so on. To restrict the time to converge, RIP prescribes that the cost value is an integer that ranges from 0 to 15. The hop count equal to or exceeding 16 is defined as infinite, or the destination network or host is unreachable.

RIP exchanges routing information using UDP packets. RIP sends a routing refresh message every 30 seconds. If no routing refresh message is received from one network neighbor in 180 seconds, RIP tags all routes of the network neighbor as unreachable. If no routing refresh message is received from one network neighbor in 300 seconds, RIP removes the routes of the network neighbor from the routing table. RIP v2 has the MD5 cipher authentication function while RIP v1 does not.

To improve performance and avoid routing loops, RIP supports split horizon, poison reverse, and allows for importing routes discovered by other routing protocols.

Each router that is running RIP manages a route database, which contains routing entries to all the reachable destinations in the network. These routing entries contain the following information:

- Destination address — The IP address of a host or network.
- Next hop address — The address of the next router that an IP packet will pass through to reach the destination.
- Output interface — The interface through which the IP packet should be forwarded.
- Cost — The cost for the router to reach the destination, which should be an integer in the range of 0 to 15.
- Timer — The length of time from the last time that the routing entry was modified until now. The timer is reset to 0 whenever a routing entry is modified.
- Route tag — The indication whether the route is generated by an interior routing protocol, or by an exterior routing protocol.

The whole process of RIP startup and operation can be described as follows:

1 If RIP is enabled on a router for the first time, the router broadcasts a request packet to adjacent routers. When they receive the request packet, adjacent routers (on which RIP is also enabled) respond to the request by returning response packets containing information about their local routing tables.

2 After receiving the response packets, the router that sent the request modifies its own routing table.

3 RIP broadcasts its routing table to adjacent routers every 30 seconds. The adjacent routers maintain their own routing tables after receiving the packets and elect an optimal route, then advertise the modification information to their adjacent network to make the updated route globally available. Furthermore, RIP uses timeout mechanism to handle timed-out routes to ensure the timeliness and

validity of the routes. With these mechanisms, RIP, an interior routing protocol, enables the router to learn the routing information of the entire network.

RIP has become one of the most popular standards of transmitting router and host routes. It can be used in most campus networks and regional networks that are simple, yet extensive. RIP is not recommended for larger and more complicated networks.

Configuring RIP is described in the following sections:

- Configuring RIP
- Troubleshooting RIP

Configuring RIP   Only after RIP is enabled can other functional features be configured. But the configuration of the interface-related functional features is not dependent on whether RIP has been enabled.

> *After RIP is disabled, the interface-related features also become invalid.*

The RIP configuration tasks are described in the following sections:

- Enabling RIP and Entering the RIP View
- Enabling the RIP Interface
- Configuring Unicast RIP Messages
- Specifying the RIP Version
- Configuring RIP Timers
- Configuring RIP-1 Zero Field Check of the Interface Packet
- Specifying the Operating State of the Interface
- Disabling Host Route
- Enabling RIP-2 Route Aggregation
- Setting RIP-2 Packet Authentication
- Configuring Split Horizon
- Enabling RIP to Import Routes of Other Protocols
- Configuring the Default Cost for the Imported Route
- Setting the RIP Preference
- Setting Additional Routing Metrics
- Configuring Route Filtering
- Displaying and Debugging RIP

Enabling RIP and Entering the RIP View

Perform the following configurations in system view.

Table 83   Enabling RIP and Entering the RIP View

Operation	Command
Enable RIP and enter the RIP view	`rip`
Disable RIP	`undo rip`

By default, RIP is not enabled.

Enabling the RIP Interface

For flexible control of RIP operation, you can specify the interface and configure the network where it is located in the RIP network, so that these interfaces can send and receive RIP packets.

Perform the following configurations in RIP view.

Table 84 Enabling RIP Interface

Operation	Command
Enable RIP on the specified network interface	**network** *network-address*
Disable RIP on the specified network interface	**undo network** *network-address*

i *After the RIP interface is enabled, you should also specify its operating network segment, because RIP only operates on the interface when the network segment has been specified. RIP does not receive or send routes for an interface that is not on the specified network, and does not forward its interface route.*

The *network-address* parameter is the address of the enabled or disabled network, and it can also be configured as the IP network address of the appropriate interfaces.

When a **network** command is used for an address, the effect is to enable the interface of the network with the address. For example, for network *129.102.1.1*, you can see network *129.102.0.0* using either the **display current-configuration** command or the **display rip** command.

Configuring Unicast RIP Messages

RIP is a broadcast protocol. To exchange route information with the non-broadcast network, the unicast transmission mode must be adopted.

Perform the following configuration in the RIP view.

Table 85 Configuring Unicast RIP Messages

Operation	Command
Configure unicast RIP messages	**peer** ip-address
Cancel unicast RIP messages	**undo peer** ip-address

By default, RIP does not send messages to unicast addresses.

Usually, this command is not recommended because the opposite side does not need to receive two of the same messages at a time. It should be noted that the **peer** command should also be restricted by the **rip work**, **rip output**, **rip input** and **network** commands.

Specifying the RIP Version

RIP has two versions, RIP-1 and RIP-2. You can specify the version of the RIP packet processed by the interface.

RIP-1 broadcasts the packets. RIP-2 can transmit packets by both broadcast and multicast. By default, multicast is adopted for transmitting packets. In RIP-2, the

default multicast address is 224.0.0.9. The advantage of transmitting packets in the multicast mode is that the hosts in the same network that do not run RIP, do not receive RIP broadcast packets. In addition, this mode prevents the hosts that are running RIP-1 from incorrectly receiving and processing the routes with subnet mask in RIP-2. When an interface is running RIP-2, it can also receive RIP-1 packets.

Perform the following configuration in VLAN interface view.

Table 86   Specifying RIP Version of the Interface

Operation	Command
Specify the interface version as RIP-1	`rip version 1`
Specify the interface version as RIP-2	`rip version 2` [`broadcast` | `multicast`]
Restore the default RIP version running on the interface	`undo rip version` { `1` | `2` }

By default, the interface receives and sends RIP-1 packets. It transmits packets in multicast mode when the interface RIP version is set to RIP-2.

Configuring RIP Timers

As stipulated in RFC1058, RIP is controlled by three timers: period update, timeout, and garbage-collection:

- Period update is triggered periodically to send all RIP routes to all the neighbors.

- If a RIP route has not been updated when the timeout timer expires, the route will be considered unreachable.

- If the garbage-collection timer times out before the unreachable route is updated by the update packets from the neighbors, the route will be deleted completely from the routing table.

Modification of these timers can affect the convergence speed of RIP.

Perform the following configuration in RIP view.

Table 87   Configuring RIP Timers

Operation	Command
Configure RIP timers	`timers` { `update` update-timer-length | `timeout` timeout-timer-length }*
Restore the default settings of RIP	`undo timers` { `update` | `timeout` } *

The modification of RIP timers takes effect immediately.

By default, the values of period update and timeout timers are 30 seconds and 180 seconds. The value of garbage-collection timer is four times that of period update timer, 120 seconds.

In fact, you may find that the timeout time of garbage-collection timer is not fixed. If period update timer is set to 30 seconds, garbage-collection timer might range from 90 to 120 seconds.

Before RIP completely deletes an unreachable route from the routing table, it advertises the route by sending four update packets with route metric of 16, to let all the neighbors knows that the route is unreachable. Routes do not always become unreachable when a new period starts so the actual value of the garbage-collection timer is 3 to 4 times the value of the period update timer.

> *You must consider network performance when adjusting RIP timers, and configure all the routes that are running RIP, so as to avoid unnecessary traffic or network oscillation.*

Configuring RIP-1 Zero Field Check of the Interface Packet

According to the RFC1058, some fields in the RIP-1 packet must be 0. When an interface version is set to RIP-1, the zero field check must be performed on the packet. If the value in the zero field is not zero, processing is refused. There are no zero fields in RIP-2 packets so configuring a zero field check is invalid for RIP-2.

Perform the following configurations in RIP view.

Table 88   Configuring Zero Field Check of the Interface Packet

Operation	Command
Configure zero field check on the RIP-1 packet	`checkzero`
Disable zero field check on the RIP-1 packet	`undo checkzero`

By default, RIP-1 performs zero field check on the packet.

Specifying the Operating State of the Interface

In the VLAN interface view, you can specify whether RIP update packets are sent and received on the interface. In addition, you can specify whether an interface sends or receives RIP update packets.

Perform the following configuration in VLAN interface view.

Table 89   Specifying the Operating State of the Interface

Operation	Command
Enable the interface to run RIP	`rip work`
Disable RIP on the interface	`undo rip work`
Enable the interface to receive RIP update packets	`rip input`
Disable receipt of RIP update packets on the interface	`undo rip input`
Enable the interface to send RIP update packets	`rip output`
Disable transmission of RIP packets on the interface	`undo rip output`

The `rip work` command is functionally equivalent to both `rip input` and `rip output` commands.

By default, all interfaces except loopback interfaces both receive and transmit RIP update packets.

Disabling Host Route

In some cases, the router can receive many host routes from the same segment, and these routes are of little help in route addressing but consume a lot of network resources. Routers can be configured to reject host routes by using **undo host-route** command.

Perform the following configurations in RIP view.

Table 90   Disabling Host Routes

Operation	Command
Enable receiving host routes	`host-route`
Disable receiving host routes	`undo host-route`

By default, the router receives the host route.

Enabling RIP-2 Route Aggregation

Route aggregation means that different subnet routes in the same natural network can be aggregated into one natural mask route for transmission when they are sent to other outside networks. Route aggregation can be performed to reduce the routing traffic on the network, as well as to reduce the size of the routing table.

RIP-1 only sends the routes with natural mask, that is, it always sends routes in the route aggregation form.

RIP-2 supports subnet mask and classless inter-domain routing. To advertise all the subnet routes, the route aggregation function of RIP-2 can be disabled.

Perform the following configurations in RIP view.

Table 91   Enabling Route Aggregation

Operation	Command
Enable the automatic aggregation function of RIP-2	`summary`
Disable the automatic aggregation function of RIP-2	`undo summary`

By default, RIP-2 uses the route aggregation function.

Setting RIP-2 Packet Authentication

RIP-1 does not support packet authentication. However, you can configure packet authentication on RIP-2 interfaces.

RIP-2 supports two authentication modes:

■ Simple authentication — This mode does not ensure security. The key is not encrypted and can be seen in a network trace so simple authentication should not be applied when there are high security requirements

■ MD5 authentication — This mode uses two packet formats: One format follows RFC1723 (RIP Version 2 Carrying Additional Information); the other format follows RFC2082 (RIP-2 MD5 Authentication).

Perform the following configuration in VLAN interface view

Table 92   Setting RIP-2 Packet Authentication

Operation	Command
Configure RIP-2 simple authentication key	**rip authentication-mode simple** password-string
Configure RIP-2 MD5 authentication with packet type following RFC 1723	**rip authentication-mode** { **simple** password | **md5** { **usual** key-string | **nonstandard** key-string key-id } }
Configure RIP-2 MD5 authentication with packet type following RFC 2082	**rip authentication-mode** { **simple** password | **md5** { **usual** key-string | **nonstandard** key-string key-id } }
Set the packet format type of RIP-2 MD5 authentication	**rip authentication-mode** { **simple** password | **md5** { **usual** key-string | **nonstandard** key-string key-id } }
Cancel authentication of RIP-2 packet	**undo rip authentication-mode**

The **usual** packet format follows RFC1723 and **nonstandard** follows RFC2082.

Configuring Split Horizon

Split horizon means that the route received through an interface will not be sent through this interface again. The split horizon algorithm can reduce the generation of routing loops, but in some special cases, split horizon must be disabled to obtain correct advertising at the cost of efficiency. Disabling split horizon has no effect on the P2P connected links but is applicable on the Ethernet.

Perform the following configuration in VLAN interface view.

Table 93   Configuring Split Horizon

Operation	Command
Enable split horizon	**rip split-horizon**
Disable split horizon	**undo rip split-horizon**

By default, split horizon of the interface is enabled.

Enabling RIP to Import Routes of Other Protocols

RIP allows users to import the route information of other protocols into the routing table.

RIP can import direct and static routes.

Perform the following configurations in RIP view.

Table 94   Enabling RIP to Import Routes of Other Protocols

Operation	Command
Enable RIP to import routes of other protocols	**import-route** *protocol* [**cost** *value*] [**route-policy** *route-policy-name*]
Disable route imports from other protocols	**undo import-route** *protocol*

By default, RIP does not import the route information of other protocols.

Configuring the Default Cost for the Imported Route

When you use the **import-route** command to import the routes of other protocols, you can specify their cost. If you do not specify the cost of the imported route, RIP will set the cost to the default cost, specified by the default cost parameter.

Perform the following configurations in RIP view.

Table 95   Configuring the Default Cost for the Imported Route

Operation	Command
Configure default cost for the imported route	`default cost value`
Restore the default cost of the imported route.	`undo default cost`

By default, the cost value for the RIP imported route is 1.

Setting the RIP Preference

Each routing protocol has its own preference by which the routing policy selects the optimal one from the routes of different protocols. The greater the preference value, the lower the preference. The preference of RIP can be set manually.

Perform the following configurations in RIP view.

Table 96   Setting the RIP Preference

Operation	Command
Set the RIP Preference	`preference value`
Restore the default value of RIP preference	`undo preference`

By default, the preference of RIP is 100.

Setting Additional Routing Metrics

The additional routing metric, is the input or output routing metric added to a RIP route. It does not change the metric value of the route in the routing table, but adds a specified metric value when the interface receives or sends a route.

Perform the following configuration in VLAN interface view.

Table 97   Setting Additional Routing Metric

Operation	Command
Set the additional routing metric of the route when the interface receives an RIP packet	`rip metricin value`

Table 97   Setting Additional Routing Metric

Operation	Command
Disable the additional routing metric of the route when the interface receives an RIP packet	**undo rip metricin**
Set the additional routing metric of the route when the interface sends an RIP packet	**ip metricout** value
Disable the additional routing metric of the route when the interface sends an RIP packet	**undo rip metricout**

By default, the additional routing metric added to the route when RIP sends the packet is 1. The additional routing metric when RIP receives the packet is 0.

Configuring Route Filtering

The router provides the route filtering function. You can configure the filter policy rules by specifying the ACL and ip-prefix for route redistribution and distribution. To import a route, the RIP packet of a specific router can also be received by designating a neighbor router.

Perform the following configurations in RIP view.

Table 98   Configuring RIP to Filter Routes

Operation	Command
Configure filtering the received routing information distributed by the specified address	**filter-policy gateway** ip-prefix-name **import**
Cancel filtering the received routing information distributed by the specified address	**undo filter-policy gateway** ip-prefix-name **import**
Configure filtering the received global routing information	**filter-policy** { acl-number | **ip-prefix** ip-prefix-name } **import**
Cancel filtering the received global routing information	**undo filter-policy** { acl-number | **ip-prefix** ip-prefix-name } **import**

By default, RIP does not filter received and distributed routing information.

Displaying and Debugging RIP

After configuring RIP, execute the **display** command in all views to display the RIP configuration, and to verify the effect of the configuration. Execute the **debugging** command in user view to debug the RIP module. Execute the **reset** command in RIP view to reset the system configuration parameters of RIP.

Table 99   Displaying and Debugging RIP

Operation	Command
Display the current RIP state and configuration information.	**display rip**
Enable the RIP debugging information	**debugging rip packets**
Enable the debugging of RIP receiving packet.	**debugging rip receive**
Enable the debugging of RIP sending packet.	**debugging rip send**
Restore the default RIP settings	**reset**

Example: Typical RIP Configuration

As shown in Figure 25, the Switch C connects to the subnet 117.102.0.0 through the Ethernet port. The Ethernet ports of Switch A and Switch B are connected to the network 155.10.1.0 and 196.38.165.0. Switch C, Switch A, and Switch B are connected by Ethernet 110.11.2.0. Correctly configure RIP to ensure that Switch C, Switch A, and Switch B can interconnect.

Figure 25   RIP Configuration
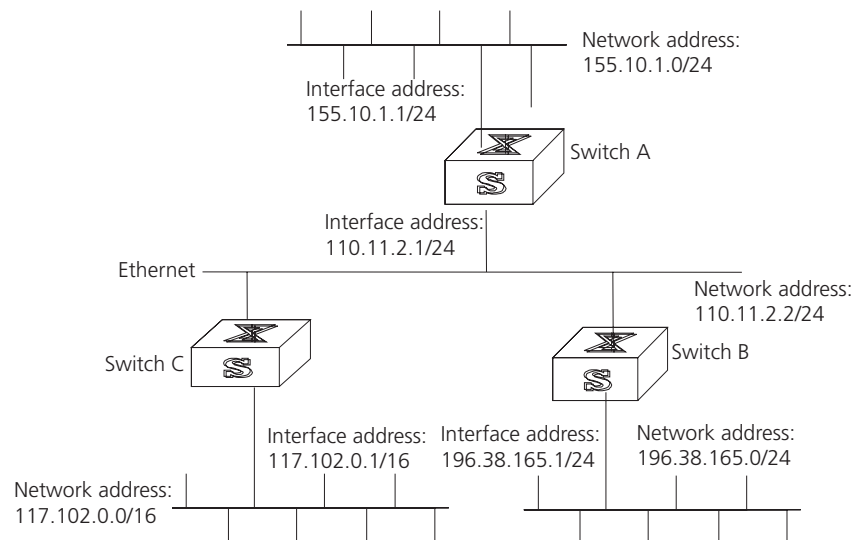
> *The following configuration only shows the operations related to RIP. Before performing the following configuration, verify that the Ethernet link layer works normally.*

1 Configure RIP on Switch A:

```
[Switch A]rip
[Switch A-rip]network 110.11.2.0
[Switch A-rip]network 155.10.1.0
```

2 Configure RIP on Switch B:

```
[Switch B]rip
[Switch B-rip]network 196.38.165.0
[Switch B-rip]network 110.11.2.0
```

3 Configure RIP on Switch C:

```
[Switch C]rip
[Switch C-rip]network 117.102.0.0
[Switch C-rip]network 110.11.2.0
```

Troubleshooting RIP   The Switch 7750 cannot receive update packets when the physical connection to the peer routing device is normal.

- RIP does not operate on the corresponding interface (for example, if the **undo rip work** command is executed) or this interface is not enabled through the **network** command.

- The peer routing device is configured for multicast mode (for example, the **rip version 2 multicast** command is executed) but the multicast mode has not been configured on the corresponding interface of the local Ethernet switch.

IP Routing Policy   When a router distributes or receives routing information, it needs to implement policies to filter the routing information so it can receive or distribute the routing information that meets only the specified condition. A routing protocol such as RIP may need to import routing information discovered by other protocols to enrich its routing knowledge. While importing the routing information, it must import only the information that meets its conditions.

To implement the routing policy, you must define a set of rules by specifying the characteristics of the routing information to be filtered. You can set the rules based on such attributes as destination address and source address of the information. The rules can be set in advance and then used in the routing policy to advertise, receive, and import the route information.

Configuring IP Routing Policy is described in the following sections:

- Routing Information Filters
- Configuring an IP Routing Policy
- Troubleshooting Routing Policies
- Configuring Route Capacity

Routing Information Filters   The Switch 7750 supports four kinds of filters, route-policy, acl, ip-prefix, and community-list. The following sections introduce these filters:

- Route Policy
- ACL
- IP Prefix

Route Policy

A route map is used for matching some attributes with given routing information and the attributes of the information will be set if the conditions are satisfied.

A route map can include multiple nodes. Each node is a unit for match testing, and the nodes are matched in a sequence-number-based order. Each node includes a set of if-match and apply clauses. The if-match clauses define the matching rules and the matching objects are attributes of routing information. The comparison of if-match clauses for a node uses a series of Boolean *and* statements. As a result, a match is found if all the matching conditions specified by the if-match clauses are satisfied. The apply clause specifies the actions that are performed after the node match test concerning the attribute settings of the route information.

The comparison of different nodes in a route policy uses a Boolean *or* statement. The system examines the nodes in the route policy in sequence. Once the route is permitted by a single node in the route policy, the route passes the matching test of the route policy without attempting the test of the next node.

ACL

The access control list (ACL) used by the route policy can be divided into three types: advanced ACL, basic ACL, and Layer-2 ACL.

A basic ACL is usually used for routing information filtering. When the user defines the ACL, the user defines the range of an IP address, subnet for the destination network segment address, or the next-hop address of the routing information. If an advanced ACL is used, perform the matching operation by the specified source address range. Layer-2 ACLs

IP Prefix

The function of the ip-prefix is similar to that of the acl, but it is more flexible and easier for users to understand. When the ip-prefix is applied to routing information filtering, its matching objects are the destination address information, and the domain of the routing information. In addition, in the ip-prefix, you can specify the gateway options and require it to receive only the routing information distributed by certain routers.

An ip-prefix is identified by the ip-prefix name. Each ip-prefix can include multiple list items, and each list item can specify the match range of the network prefix forms, and is identified with a index-number. The index-number designates the matching check sequence in the ip-prefix.

During the matching, the router checks list items identified by the sequence-number in ascending order. Once a single list item meets the condition, it means that it has passed the ip-prefix filtering and does not enter the testing of the next list item.

Configuring an IP Routing Policy

Configuring a routing policy includes tasks described in the following sections:

- Defining a Route Policy
- Defining If-match Clauses for a Route Policy
- Defining Apply Clauses for a Route Policy
- Importing Routing Information Discovered by Other Routing Protocols
- Defining IP Prefix
- Configuring for Filtering Received Routes
- Configuring for Filtering Distributed Routes
- Displaying and Debugging the Routing Policy

Defining a Route Policy

A route policy can include multiple nodes. Each node is a unit for the matching operation. The nodes are tested again by *sequence-number*.

Perform the following configurations in system view.

Table 100   Defining a Route Policy

Operation	Command
Enter Route policy view	**route-policy** route-policy-name { **permit** | **deny** } **node** { node-number }
Remove the specified route-policy	**undo route-policy** route-policy-name [**permit** | **deny** | **node** node-number]

The `permit` argument specifies that if a route satisfies all the if-match clauses of a node, the route passes the filtering of the node, and the apply clauses for the node are executed without taking the test of the next node. If a route does not satisfy all the if-match clauses of a node, however, the route takes the test of the next node.

The `deny` argument specifies that the apply clauses are not executed. If a route satisfies all the if-match clauses of the node, the node denies the route and the route does not take the test of the next node. If a route does not satisfy all the if-match clauses of the node, however, the route takes the test of the next node.

The router tests the route against the nodes in the route policy in sequence, once a node is matched, the route policy filtering is passed.

By default, the route policy is not defined.

If multiple nodes are defined in a route policy, at least one of them should be in permit mode. Apply the route policy to filter routing information. If the routing information does not match any node, the route policy denies the routing information. If all the nodes in the route policy are in deny mode, all routing information will be denied by the route policy.

Defining If-match Clauses for a Route Policy

The if-match clauses define the matching rules that the routing information must satisfy to pass the route policy. The matching objects are attributes of the routing information.

Perform the following configurations in route policy view.

Table 101   Defining If-match Conditions

Operation	Command
Match the destination address of the routing information	`if-match { acl	ip-prefix }`
Cancel the matched destination address of the routing information set by the ACL	`undo if-match [ acl` acl-number`| ip-prefix` ip-prefix-name `]`
Match the next-hop interface of the routing information	`if-match interface {` interface-type interface-number `}`
Cancel the matched next-hop interface of the routing information	`undo if-match interface`
Match the next-hop of the routing information	`if-match ip next-hop { acl` acl-number `| ip-prefix` ip-prefix-name `}`
Cancel the matched next-hop of the routing information set by the address prefix list	`undo if-match ip next-hop [ ip-prefix` ip-prefix-name `]`
Match the tag domain of the routing information	`if-match tag` value
Cancel the tag domain of the matched routing information	`undo if-match tag`

By default, no matching is performed.

> **i**> *The if-match clauses for a node in the route policy require that the route satisfy all the clauses to match the node before the actions specified by the apply clauses can be executed.*
>
> *If no if-match clauses are specified, all the routes pass the filtering on the node.*

Defining Apply Clauses for a Route Policy

The apply clauses specify actions, which are the configuration commands executed after a route satisfies the filtering conditions that are specified in the if-match clauses. In this way, some attributes of the route can be modified.

Perform the following configurations in Route policy view.

Table 102   Defining Apply Clauses

Operation	Command
Set the next-hop address of the routing information	**apply ip next-hop** { ip-address [ip-address]	**acl** acl-number }
Cancel the next-hop address of the routing information	**undo apply ip next-hop**
Set the tag domain of the routing information	**apply tag** value
Cancel the tag domain of the routing information	**undo apply tag**

By default, no apply clauses are defined.

If the routing information meets the match conditions specified in the route policy, then this value is regarded as the MED value of the IGP route.

Importing Routing Information Discovered by Other Routing Protocols

A routing protocol can import the routes that are discovered by other routing protocols to enrich its route information. The route policy can filter route information to implement the redistribution. If the destination routing protocol that imports the routes cannot directly reference the route costs of the source routing protocol, you should satisfy the requirement of the destination protocol by specifying a route cost for the imported route.

Perform the following configuration in routing protocol view.

Table 103   Configuring Importing Routes of Other Protocols

Operation	Command
Import routes of other protocols	**import-route** protocol [**med** med	**cost** cost] [**tag** value] [**type** **1**	**2**] [**route-policy** route-policy-name]
Do not import routes of other protocols	**undo import-route** protocol

By default, the routes discovered by other protocols are not imported.

> **i**> *In different routing protocol views, the parameter options are different. For details, refer to the description of the **import-route** command for each protocol .*

Defining IP Prefix

A prefix list is identified by the IP prefix name. Each IP prefix can include multiple items, and each item can specify the matching range of the network prefix forms. The index-number parameter specifies the matching sequence in the prefix list.

Perform the following configurations in system view.

Table 104 Defining Prefix-list

Operation	Command
Define a prefix list	**ip ip-prefix** ip-prefix-name [**index** index-number] { **permit** | **deny** } network len [**greater-equal** greater-equal] [**less-equal** less-equal]
Remove a prefix list	**undo ip ip-prefix** ip-prefix-name [**index** index-number | **permit** | **deny**]

During the matching, the router checks list items identified by the *index-number* in the ascending order. If only one list item meets the condition, it means that it has passed the ip-prefix filtering (and does not enter the testing of the next list item).

If more than one IP prefix item is defined, then the match mode of at least one list item should be the permit mode. The list items of the deny mode can be defined to rapidly filter the routing information not satisfying the requirement, but if all the items are in the deny mode, no route will pass the ip-prefix filtering. You can define an item of permit 0.0.0.0/0 greater-equal 0 less-equal 32 after the multiple list items in the deny mode to let all the other routes pass.

Configuring for Filtering Received Routes

Perform the following configuration in routing protocol view.

Define a policy that filters the routing information that does not satisfy the conditions and receives routes with the help of an ACL or address prefix-list. The **filter-policy gateway** command specifies that only the update packets from a specific neighboring router will be received.

Table 105 Configuring Filtering for Received Routes

Operation	Command
Configure to filter the received routing information distributed by the specified address	**filter-policy gateway** ip-prefix-name **import**
Cancel the filtering of the received routing information distributed by the specified address	**undo filter-policy gateway** ip-prefix-name **import**
Configure to filter the received global routing information	**filter-policy** { acl-number | **ip-prefix** ip-prefix-name } [**gateway**] **import**
Cancel the filtering of the received global routing information	**undo filter-policy** { acl-number | **ip-prefix** ip-prefix-name } [**gateway**] **import**

Configuring for Filtering Distributed Routes

Define a policy concerning route distribution that filters the routing information that does not satisfy the conditions, and distributes routes with the help of an ACL or address ip-prefix.

Perform the following configuration in routing protocol view.

Table 106   Configuring Filtering of Distributed Routes

Operation	Command
Configure to filter the routes distributed by the protocol	`filter-policy { acl-number |` **`ip-prefix`** `ip-prefix-name }` **`export`** `[ routing-process ]`
Cancel the filtering of the routes distributed by the protocol	**`undo filter-policy`** `{ acl-number |` **`ip-prefix`** `ip-prefix-name }` **`export`** `[ routing-process ]`

The route policy supports importing the routes discovered by the following protocols into the routing table:

■ Direct: The hop (or host) to which the local interface is directly connected.

■ Static: Static Route Configuration

■ RIP: Route discovered by RIP

By default, the filtering of the received and distributed routes will not be performed.

Displaying and Debugging the Routing Policy

Execute the **`display`** command in all views to display the operation of the routing policy configuration, and to verify the effect of the configuration.

Table 107   Displaying and Debugging the Route Policy

Operation	Command
Display the routing policy	**`display route-policy`** `[ route-policy-name ]`
Display the path information of the AS filter	**`display ip as-path-acl`** `[ acl-number ]`
Display the address prefix list information	**`display ip ip-prefix`** `[ ip-prefix-name ]`

Troubleshooting Routing Policies

Routing information filtering cannot be implemented in normal operation of the routing protocol

Check for the following faults:

■ The if-match mode of at least one node of the Route policy should be the permit mode. When a Route-policy is used for the routing information filtering, if a piece of routing information does not pass the filtering of any node, then it means that the route information does not pass the filtering of the Route-policy. When all the nodes of the Route-policy are in the deny mode, then all the routing information cannot pass the filtering of the Route-policy.

■ The if-match mode of at least one list item of the ip-prefix should be the permit mode. The list items of the deny mode can be defined to rapidly filter the

routing information not satisfying the requirement, but if all the items are in the deny mode, no routes will pass the ip-prefix filtering. You can define an item of permit 0.0.0.0/0 less-equal 32 after the multiple list items in the deny mode, so as to let all the other routes pass the filtering (If less-equal 32 is not specified, only the default route will be matched).

Route Capacity

In practical networking applications, there is always a large number of routes in the routing table. The routing information is usually stored in the memory of the Ethernet switch. When the size of the routing table increases, it can consume a significant amount of switch's memory.

The Switch 7750 provides a mechanism to control the size of the routing table. It monitors the free memory in the system to determine whether to add new routes to the routing table, and whether or not to keep connection with a routing protocol.

i▷ *The default value normally meets the network requirements. You should be careful when modifying the configuration to avoid reducing the stability of the network.*

Configuring Route Capacity

Route capacity configuration includes tasks described in the following sections:

- Setting the Lower Limit for Switch Memory
- Setting the Safety Value for Switch Memory
- Setting the Lower Limit and the Safety Value Simultaneously
- Preventing Automatic Recovery of Disconnected Routing Protocols
- Enabling Automatic Recovery of Disconnected Routing Protocols
- Displaying and Debugging Route Capacity

Setting the Lower Limit for Switch Memory

When the Ethernet switch memory is equal to or lower than the lower limit, routes will be disconnected.

Perform the following configurations in system view.

Table 108 Setting the Lower Limit of the Ethernet Switch Memory

Operation	Command
Set the lower limit of the Ethernet switch memory	**memory limit** value

By default, the lower limit of the Ethernet switch memory is 2Mbytes.

The lower limit value set for the memory must be smaller than the safety value.

Setting the Safety Value for Switch Memory

When the amount of free memory is reduced to the safety value but has not reached the lower limit, you can use the **display memory limit** command to see how much free memory remains.

If automatic memory restoration is enabled, when the free memory of the Ethernet switch exceeds the safety value, the disconnected routes will be restored.

Perform the following configurations in system view.

Table 109   Setting the Safety Value of the Ethernet Switch Memory

Operation	Command
Set the safety value of the Ethernet switch memory	`memory safety value`

By default, the safety value of the Ethernet switch memory is 4Mbytes.

The safety value of the memory must be larger than the lower limit value.

Setting the Lower Limit and the Safety Value Simultaneously

When you need to modify both the lower limit and the safety value of the Ethernet switch memory, 3Com recommends that you modify the two configurations simultaneously.

You can also restore the lower limit and the safety value of the Ethernet switch memory to the default value at the same time if it is necessary.

Perform the following configuration in the system view.

Table 110   Setting the Lower Limit and the Safety Value of the Ethernet Switch Memory Simultaneously

Operation	Command
Set the lower limit and the safety value of the Ethernet switch memory simultaneously	`memory safety` safety-value `limit` limit-value
Restore the lower limit and the safety value of the Ethernet switch memory to the default value	`undo memory` [`safety` | limit]

The default values of the lower limit and the safety value of the Ethernet switch memory are 2Mbytes and 4Mbytes, respectively.

Note that `safety-value` must have a higher value than `limit-value`.

Preventing Automatic Recovery of Disconnected Routing Protocols

> **i**   *If the automatic memory restoration function of a Ethernet switch is disabled, connection of routing protocols will not be restored even if the free memory returns to the safety value.*

Perform the following configurations in system view.

Table 111   Preventing Automatic Recovery of Disconnected Routing Protocols

Operation	Command
Prevent automatic recovery of disconnected routing protocols	`memory auto-establish disable`

By default, memory automatic restoration function of a Ethernet switch is enabled.

Enabling Automatic Recovery of Disconnected Routing Protocols

Perform the following configurations in system view.

Table 112   Enabling Automatic Recovery of Disconnected Routing Protocols

Operation	Command
Enable automatic recovery of disconnected routing protocols	`memory auto-establish enable`

By default, memory automatic restoration function is enabled.

Displaying and Debugging Route Capacity

Execute the **display** command in all views to display the route capacity configuration.

Table 113   Displaying and Debugging Route Capacity

Operation	Command
Display the route capacity related memory setting and state information	`display memory limit`

6

MULTICAST PROTOCOL

This chapter includes information on the following:

■ IP Multicast Overview

■ Configuring Common Multicast

■ Configuring IGMP

■ IGMP Snooping

■ Configuring PIM-DM

■ Configuring PIM-SM

■ GMRP

IP Multicast Overview   Many transmission methods can be used when the destination (including data, voice and video) is the secondary use of the network. If the multicast method is used you should establish an independent data transmission path for each user. The broadcast method can be used if you intend to send the information to all users on the network. In either case, the end users will receive the information. For example, if the same information is required by 200 users on the network, the traditional solution is to send the information 200 times in unicast mode. In the broadcast mode, the data is broadcast over the entire network. However, both of the methods waste bandwidth resources. In addition, the broadcast mode cannot ensure information security.

IP multicast technology solves this problem. The multicast source sends the information only once. Multicast routing protocols establish tree-type routing for multicast packets (see Figure 26) so that information can be correctly sent, with high efficiency, to each user.

Figure 26 Comparison Between the Unicast and Multicast Transmission
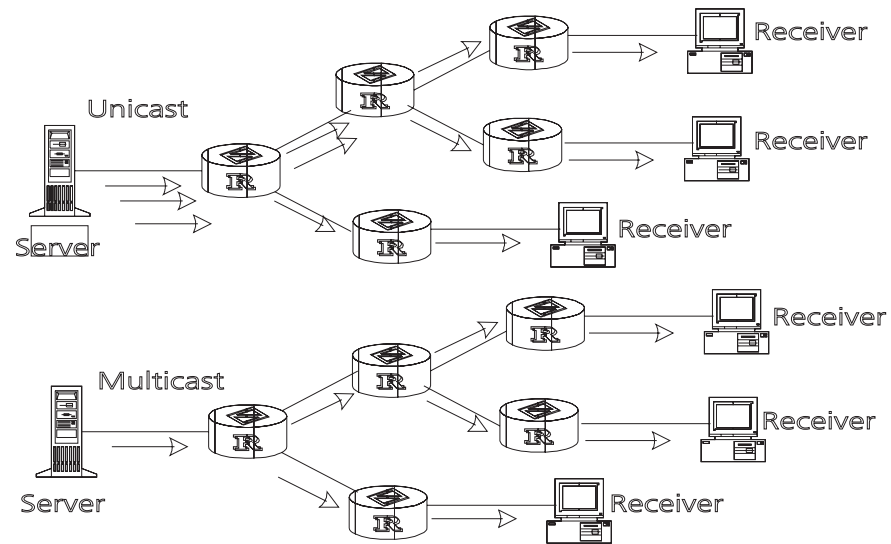
> ⓘ *A multicast source does not necessarily belong to a multicast group. It only sends data to the multicast group and it is not necessarily a receiver. Multiple sources can send packets to a multicast group simultaneously.*

A router that does not support multicast may exist on the network. A multicast router can encapsulate multicast packets in unicast IP packets by tunneling and sending them on to the neighboring multicast router. The neighboring multicast router removes the unicast IP header and continues the multicast transmission.

Multicast advantages:

- Enhanced efficiency by reducing network traffic and relieving server and CPU loads.
- Optimized performance decreases traffic redundancy.
- Distributed applications make multipoint applications possible.

Configuring an IP Multicast Overview is described in the following sections:

- Multicast Addresses
- IP Multicast Protocols
- Forwarding IP Multicast Packets
- Applying Multicast

Multicast Addresses   The destination addresses of multicast packets use Class D IP addresses ranging from 224.0.0.0 to 239.255.255.255. Class D addresses cannot appear in the source IP address fields of IP packets.

During unicast data transmission, a packet is transmitted from the source address to the destination address with the "hop-by-hop" principle of the IP network. A packet has more than one destination address in a multi-cast environment, i.e., a group of addresses. All the information receivers join a group. Once a receiver joins the group, data flowing to the group is sent to the receiver immediately. All members in the group can receive the packets. Membership of a multicast group is dynamic, that is, hosts can join and leave groups at any time.

A multicast group can be either permanent or temporary. Part of addresses in the multicast group are reserved by the IANA and are known as the permanent multicast group. IP addresses of a permanent group are unchanged, but the members in the group can change. The number of members in a permanent multicast group can be random or even 0. Those IP multicast addresses that are not reserved for permanent multicast groups can be used by temporary groups.

Ranges and meanings of Class D addresses are shown in Table 114.

Table 114   Ranges and Meanings of Class D Addresses

Class D address range	Meaning
224.0.0.0~224.0.0.255	Reserved multicast addresses (addresses of permanent groups). Address 224.0.0.0 is reserved. The other addresses can be used by routing protocols.
224.0.1.0~238.255.255.255	Multicast addresses available for users (addresses of temporary groups). They are valid in the entire network.
239.0.0.0~239.255.255.255	Multicast addresses for local management. They are valid only in the specified local range.

Reserved multicast addresses that are commonly used are shown Table 115:

Table 115   Reserved Multicast Address List

Class D address	Meaning
224.0.0.0	Base Address (Reserved)
224.0.0.1	Addresses of all hosts
224.0.0.2	Addresses of all multicast routers
224.0.0.3	Unassigned
224.0.0.4	DVMRP routers
224.0.0.7	ST routers
224.0.0.8	ST hosts
224.0.0.9	RIP-2 routers
224.0.0.10	IGRP routers
224.0.0.11	Mobile agents
224.0.0.12	DHCP server/Relay agent
224.0.0.13	All PIM routers
224.0.0.14	RSVP encapsulation
224.0.0.15	All CBT routers
224.0.0.16	Designated SBM
224.0.0.17	All SBMS
……	……

Ethernet Multicast MAC Addresses

When unicast IP packets are transmitted in Ethernet, the destination MAC address is the MAC address of the receiver. However, when multicast packets are transmitted, the destination is no longer a specific receiver but a group with unspecific members. Therefore, the multicast MAC address should be used. Multicast MAC addresses correspond to multicast IP addresses. IANA (Internet

Assigned Number Authority) stipulates that the higher 24 bits of the multicast MAC address is 0x01005e and the lower 23 bits of the MAC address is the lower 23 bits of the multicast IP address.

Figure 27   Mapping Between the Multicast IP Address and the Ethernet MAC Address
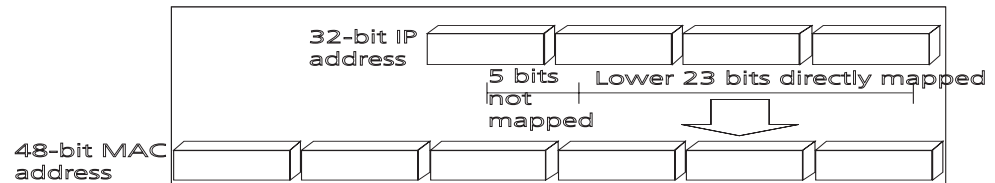
Only 23 bits of the last 28 bits in the IP multicast address is mapped to the MAC address. Therefore the 32 IP multicast addresses are mapped to the same MAC address.

IP Multicast Protocols

Multicast uses the multicast group management protocol, and the multicast routing protocol. The multicast group management protocol uses Internet Group Management Protocol (IGMP) as the IP multicast basic signaling protocol. It is used between hosts and routers and enables routers to determine if members of the multicast group are on the network segment. The multicast routing protocol is used between multicast routers and creates and maintains multicast routes, and allows high-efficient multicast packet forwarding. At present, multicast routing protocols mainly include PIM-SM, PIM-DM.

Tasks for configuring IP Multicast Protocols are described in the following sections:

- Internet Group Management Protocol (IGMP)
- Multicast Routing Protocol

Internet Group Management Protocol (IGMP)

Internet Group Management Protocol (IGMP) is the only protocol that hosts can use. It defines the membership establishment and maintenance mechanism between hosts and routers, and is the basis of the entire IP multicast. Hosts report the group membership to a router through IGMP and inform the router of the conditions of other members in the group through the directly connected host.

If a user on the network joins a multicast group through IGMP declaration, the multicast router on the network will transmit the information sent to the multicast group through the multicast routing protocol. Finally, the network will be added to the multicast tree as a branch. When the host, as a member of a multicast group, begins receiving the information, the router queries the group periodically to check whether members in the group are involved. As long as one host is involved, the router receives data. When all users on the network quit the multicast group, the related branches are removed from the multicast tree.

Multicast Routing Protocol

A multicast group address has a virtual address. Unicast allows packets to be routed from the data source to the specified destination address. This is not possible for multicast. The multicast application sends the packets to a group of receivers (as with multicast addresses) who are ready to receive the data but not only to one receiver (as with unicast address).

The multicast routing creates a loop-free data transmission path from one data source to multiple receivers. The task of the multicast routing protocol is to create a distribution tree architecture. A multicast router can use multiple methods to build up a path for data transmission, i.e., the distribution tree.

■ PIM-DM (Protocol-Independent Multicast Dense Mode)

PIM dense mode is suitable for small networks. It assumes that each subnet in the network contains at least one receiver who is interested in the multicast source. Multicast packets are flooded to all points of the network. Subsequent resources (such as bandwidth and CPU of routers) are consumed. In order to decrease the consumption of these precious network resources, branches that do not have members send Prune messages toward the source to reduce the unwanted/unnecessary traffic. To enable the receivers to receive multicast data streams, the pruned branches can be restored periodically to a forwarding state. To reduce latency time, the PIM dense mode uses the prune mechanism to actively restore multicast packet forwarding. The periodical flood and prune are characteristics of PIM dense mode. Generally, the forwarding path in dense mode is a "source tree" rooted at the source with multicast members as the branches. Since the source tree uses the shortest path from the multicast source and the receiver, it is also called the shortest path tree (SPT).

■ PIM-SM (Protocol-Independent Multicast Sparse Mode)

Dense mode uses the flood-prune technology, which is not applicable for WAN. In WAN, multicast receivers are sparse and therefore the sparse mode is used. In sparse mode, hosts need not receive multicast packets unless, by default, there is an explicit request for the packets. A multicast router must send a join message to the RP (Rendezvous Point, which needs to be built into the network and is a virtual place for data exchange) corresponding to the group for receiving the multicast data traffic from the specified group. The join message passes routers and finally reaches the root, i.e., the RP. The join message becomes a branch of the shared tree. In PIM sparse mode, multicast packets are sent to the RP first, and then are forwarded along the shared tree rooted at the RP and with members as the branches. To prevent the branches of the shared tree from being deleted, PIM sparse mode sends join messages to branches periodically to maintain the multicast distribution tree.

To send data to the specified address, senders register with the RP first before forwarding data to the RP. When the data reaches the RP, the multicast packets are replicated and sent to receivers along the path of the distribution tree. Replication only happens at the branches of the distribution tree. This process can be repeated automatically until the packets reach the destination.

Forwarding IP Multicast Packets

In the multicast model, the source host sends information to the host group represented by the multicast group address within the destination address fields of the IP packets. The multicast model must forward multicast packets to multiple external interfaces so that the packets can be forwarded to all receivers.

■ RPF (Reverse Path Forwarding)

To ensure that a multicast packet reaches the router along the shortest path, the multicast must depend on the unicast routing table or a unicast routing table independently provided for multicast. This check mechanism is the basis for most multicast routing protocols , which is known as a RPF (Reverse Path Forwarding) check. A multicast router uses the source address from the multicast packet to query the unicast routing table, or the independent

multicast routing table, to determine the incoming interface at which the packet arrives. If a source tree is used, the source address is the address of the source host sending the multicast packet. If a shared tree is used, the source address is the address of the root of the shared tree. When a multicast packet arrives at the router, if RPF check succeeds, the packet will be forwarded according to the multicast forwarding entry. Otherwise, the packet will be dropped.

Applying Multicast
IP multicast technology effectively solves the problem of packet forwarding from single-point to multi-point. It implements high-efficient data transmission from single-point to multi-point in IP networks and can save a large amount of network bandwidth and reduce network loads. New value-added services that use multicast can be delivered, including direct broadcasting, Web TV, distance learning, distance medicine, net broadcasting station and real-time audio/video conferencing.

- Multimedia and streaming media applications
- Communications of the training and corporate sites
- Data repository and finance (stock) applications
- Any "point-to-multi-point" data distribution

With the increase of multimedia services on IP networks, multicast has huge market potential.

Configuring Common Multicast

A common multicast configuration covers both the multicast group management protocol and the multicast routing protocol. The configuration includes enabling multicast, configuring multicast forwarding boundary, and displaying multicast routing table and multicast forwarding table.

Configuring Common Multicast
Common multicast configuration includes:

- Enabling Multicast
- Configuring the Multicast Route Limit
- Clearing MFC Forwarding Entries or Statistic Information
- Clearing Route Entries From the Core Multicast Routing Table
- Displaying and Debugging Common Multicast Configuration

Enabling Multicast

Enable multicast first before enabling the multicast routing protocol.

Perform the following configuration in system view.

Table 116   Enabling Multicast

Operation	Command
Enable multicast	`multicast routing-enable`
Disable multicast	`undo multicast routing-enable`

By default, multicast routing is disabled.

Only when multicast is enabled can another multicast configuration be used.

Configuring the Multicast Route Limit

If the existing route entries exceed the capacity value you configured when using this command, the system will not delete the existing entries, but displays the message, *"Existing route entries exceed the configured capacity value"*.

Perform the following configuration in system view.

Table 117 Configure the Multicast Route Limit

Operation	Command
Configure multicast route limit	**multicast route-limit** limit
Restore multicast route limit to the default value	**undo multicast route-limit**

By default, the multicast route-limit is 512.

Clearing MFC Forwarding Entries or Statistic Information

You can clear the multicast forwarding cache (MFC) forward entries or statistical information of FMC forward entries using the **reset multicast forwarding-table** command.

Perform the following configuration in user view.

Table 118 Clear MFC Forwarding Entries or Statistic Information

Operation	Command
Clear MFC forwarding entries or its statistic information	**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 } * }

Clearing Route Entries From the Core Multicast Routing Table

You can clear route entries from the core multicast routing table, as well as MFC forwarding entries using the reset **multicast routing-table** command.

Perform the following configuration in user view.

Table 119 Clear Routing Entries of Multicast Routing Table

Operation	Command
Clear routing entries of multicast routing table	**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-number } } * }

Displaying and Debugging Common Multicast Configuration

After the previous configurations, execute the **display** command to view the multicast configuration, and to verify the configuration.

Execute **debugging** command in user view for the debugging of multicast.

Table 120   Display and Debug Common Multicast Configuration

Operation	Command
Display the multicast routing table	**display multicast routing-table** [group-address [**mask** { mask | mask-length }] | source-address [**mask** { mask | mask-length }] | **incoming-interface** { interface-type interface-number | **register** }]*
Display the multicast forwarding table	**display multicast forwarding-table** [group-address [**mask** { mask | mask-length }] | source-address [**mask** { mask | mask-length }] | **incoming-interface register** }]*
Display the RPF routing information	**display multicast rpf-info** source-address
Enable multicast packet forwarding debugging	**debugging multicast forwarding**
Disable multicast packet forwarding debugging	**undo debugging multicast forwarding**
Enable multicast forwarding status debugging	**debugging multicast-status forwarding**
Disable multicast forwarding status debugging	**undo debugging multicast-status forwarding**
Enable multicast kernel routing debugging	**debugging multicast kernel-routing**
Disable multicast kernel routing debugging	**undo debugging multicast kernel-routing**

Configuring IGMP

IGMP (Internet Group Management Protocol) is a protocol, in the TCP/IP suite, responsible for management of IP multicast members. It is used to establish and maintain multicast membership among IP hosts and their connected neighboring routers. IGMP excludes transmitting and maintenance information among multicast routers, which are completed by multicast routing protocols. All hosts participating in multicast must implement IGMP.

Hosts participating in multicast can join or leave a multicast group at any time, in any place, and without limitation of member numbers. A multicast router does not need and cannot keep the membership of all hosts. It only uses IGMP to learn whether receivers (i.e., group members) of a multicast group are present on the subnet connected to each interface. A host only needs to keep the multicast groups it has joined.

IGMP is not symmetric on hosts and routers. Hosts need to respond to IGMP query messages from the multicast router, i.e., report the group membership to the router. The router needs to send membership query messages periodically to

discover whether hosts join the specified group on its subnets according to the received response messages. When the router receives the report that hosts leave the group, the router will send a group-specific query (IGMP Version 2) to discover whether there are no members in the group.

IGMP has three versions, IGMP Version 1 (defined by RFC1112), IGMP Version 2 (defined by RFC2236) and IGMP Version 3. IGMP Version 2 is the most widely used version.

IGMP Version 2 boasts the following improvements over IGMP Version 1:

■ Election mechanism of multicast routers on the shared network segment

  A shared network segment means that there are multiple multicast routers on a network segment. In this case, all routers running IGMP on the network segment can receive the membership report from hosts. Therefore, only one router is required to send membership query messages. In this case, the router election mechanism is required to specify a router as the querier.

  In IGMP Version 1, selection of the querier is determined by the multicast routing protocol. IGMP Version 2 specifies that the multicast router with the lowest IP address is elected as the querier when there are multiple multicast routers on the same network segment.

■ Leaving group mechanism

  In IGMP Version 1, hosts leave the multicast group quietly without informing the multicast router. The multicast router can only depend on the timeout of the response time to confirm when hosts leave the group. In Version 2, when a host leaves a multicast group, it will send a leave group message.

■ Specific group query

  In IGMP Version 1, a query of multicast routers is targeted at all the multicast groups on the network segment. This is known as General Query.

  In IGMP Version 2, besides general query, Group-Specific Query is added. The destination IP address of the query packet is the IP address of the multicast group. The group address domain in the packet is also the IP address of the multicast group. This prevents the hosts of members of other multicast groups from sending response messages.

■ Max response time

  The Max Response Time was added in IGMP Version 2. It is used to dynamically adjust the allowed maximum time for a host to respond to the membership query message.

Configuring IGMP   Once multicast is enabled, IGMP will automatically run on each interface. Generally, IGMP does not need to be configured. In the following configuration, only the first one is mandatory.

Basic IGMP configuration includes:

■ Enabling Multicast
■ Enabling IGMP on an Interface

Advanced IGMP configuration includes:

- Configuring the IGMP Version
- Configuring the Interval for Sending the IGMP Group-Specific Query Packet
- Configuring the Interval for Sending IGMP Group-Specific Query Packet
- Configuring the Limit of IGMP Groups on an Interface
- Configuring a Router to be a Member of a Group
- Limiting Access to IP Multicast Groups
- Configuring the IGMP Query Message Interval
- Configuring the IGMP Querier Present Timer
- Configuring the Maximum Query Response Time
- Deleting IGMP Groups Joined on an Interface
- Displaying and Debugging IGMP

Enabling Multicast

After multicast is enabled, IGMP will automatically run on all interfaces.

For details, see "Configuring Common Multicast " on page 114.

Enabling IGMP on an Interface

You must enable multicast before you can execute the **igmp enable** command. After this, you can initiate the IGMP feature configuration.

Perform the following configuration in VLAN interface view.

Table 121   Enable/Disable IGMP on an Interface

Operation	Command
Enable IGMP on an interface	`igmp enable`
Disable IGMP on an interface	`undo igmp enable`

By default, IGMP is not enabled.

Configuring the IGMP Version

Perform the following configuration in VLAN interface view.

Table 122   Select the IGMP Version

Operation	Command
Select the IGMP version that the router uses	`igmp version { 2	1 }`
Restore the default setting	`undo igmp version`

The default is IGMP Version 2.

i> *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.*

Configuring the Interval for Sending the IGMP Group-Specific Query Packet

In the shared network, where the same network segment includes 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 Group Leave message. When the IGMP query router receives the IGMP Leave message, it must send the IGMP group query message for the specified number of times (the r*obust-value* parameter in the **igmp robust-count** command, with a default value of 2) in a specified time interval (the *seconds* parameter in the **igmp lastmember-queryinterval** command, with a default value of 1 second).

If other hosts, which are interested in the specified group, receive the IGMP query message from the IGMP query router, they send back the IGMP Membership Report message within the specified maximum response time interval. If the IGMP query router receives the IGMP Membership Report message within the defined period (equal to *robust-value* seconds), it continues to maintain the membership of this group. When the IGMP query router receives no IGMP Membership Report messages from any host within the defined period, it perceives a timeout and stops membership maintenance for the group.

Perform the following configuration in VLAN interface view.

Table 123 Configure The Interval of Sending IGMP Group-Specific Query Packet

Operation	Command
Configure the interval of sending IGMP Group-Specific Query packet	**igmp lastmember-queryinterval seconds**
Restore the interval of sending IGMP Group-Specific Query packet to the default value	**undo igmp lastmember-queryinterval**

By default, the interval is 1 second.

> **i** *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 may not send the IGMP Leave message when it leaves a group.*

Configuring the Interval for Sending IGMP Group-Specific Query Packet

In a shared network where the 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 a IGMP Leave message. When receiving the IGMP Leave message, IGMP query router must send the IGMP group 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 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 the IGMP

query router receives the IGMP Membership Report message within the defined period (equal to robust-value seconds), it continues to maintain the membership of this group. When the IGMP query router receives no IGMP Membership Report messages from any hosts within the defined period, it perceives a timeout and stops membership maintenance for the group.

Perform the following configuration in VLAN interface view.

Table 124   Configure the Times of Sending IGMP Group-Specific Query Packet

Operation	Command
Configure the times of sending IGMP Group-Specific Query packet	`igmp robust-count robust-value`
Restore the times of sending IGMP Group-Specific Query packet to the default value	`undo igmp robust-count`

By default, the robust-value is 2.

This command is only available on an IGMP query router running IGMP v2. For a host running IGMP v1, this command cannot take effect, because the host may not send the IGMP Leave message when it leaves a group.

Configuring the Limit of IGMP Groups on an Interface

You limit the number of multicast groups, from 0 to 1024, on an interface using the following configuration.

Perform the following configuration in VLAN interface view.

Table 125   Configure the Limit of IGMP Groups on an Interface

Operation	Command
Configure the limit of IGMP groups on an interface	`igmp group-limit` limit
Restore the limit of IGMP groups on an interface to the default value	`undo igmp group-limit`

Configuring a Router to be a Member of a Group

Usually, the host operating IGMP will respond to IGMP query packet of the multicast router. In case of a response failure, the multicast router will consider that there is no multicast member on this network segment and will cancel the corresponding path. Configuring one interface of the router as a multicast member can avoid such a problem. When the interface receives an IGMP query packet, the router will respond, ensuring that the network segment is connected and can receive multicast packets.

Perform the following configuration in VLAN interface view.

Table 126   Configure a Router to Be a Member of a Group

Operation	Command
Configure a router to be a member of a multicast group (VLAN interface view)	`igmp host-join` *group-address* `port` { *interface_type interface_num* | *interface_name* } [`to` { *interface_type interface_num* | `interface_name` }]

Table 126   Configure a Router to Be a Member of a Group

Operation	Command
Cancel a router's membership of a multicast group (VLAN interface group)	**undo igmp host-join** *group-address* **port** { *interface_type interface_num* | *interface_name* } [**to** { *interface_type interface_num* | interface_name }]
Configure a router to be a member of a multicast group (Ethernet interface view)	**igmp host-join** *group-address* **vlan** *vlanid*
Cancel a router's membership of a multicast group (Ethernet interface group)	**undo igmp host-join** *group-address* **vlan** *vlanid*

By default, a router does not join a multicast group.

Limiting Access to IP Multicast Groups

A multicast router learns whether there are members of a multicast group on the network when it receives an IGMP membership message. A filter can be set on an interface to limit the range of allowed multicast groups.

Perform the following configuration in VLAN-interface view.

Table 127   Limit the Access to IP Multicast Groups

Operation	Command
Limit the range of allowed multicast groups on current interface	**igmp group-policy** acl-number [**1** | **2**]
Remove the filter set on the interface	**undo igmp group-policy**
Limit the range of allowed multicast groups on current interface (Ethernet port view)	**igmp group policy** *acl-number* **vlan** *vlanid*
Remove the filter set on the interface (Ethernet port view)	**undo igmp group policy vlan** *vlanid*

By default, no filters are configured. All multicast groups are allowed on the interface.

Configuring the IGMP Query Message Interval

Multicast routers send IGMP query messages to find present multicast groups on other networks. Multicast routers send query messages periodically to refresh their information of members present.

Perform the following configuration in VLAN interface view.

Table 128   Configure the IGMP Query Message Interval

Operation	Command
Configure the IGMP query message interval	**igmp timer query** seconds
Restore the IGMP query message interval to the default value	**undo igmp timer query**

When there are multiple multicast routers on a network segment, the querier is responsible for sending IGMP query messages to all hosts on the LAN.

The default interval is 60 seconds.

Configuring the IGMP Querier Present Timer

The IGMP querier present timer defines the period of time before the router takes over as the querier.

Perform the following configuration in VLAN interface view.

Table 129   Configure the IGMP Querier Present Timer

Operation	Command
Change the IGMP querier present timer	`igmp timer other-querier-present` seconds
Restore the IGMP querier present timer to the default value	`undo igmp timer other-querier-present`

By default, the value is 120 seconds. If the router has received no query message within twice the interval specified by the `igmp timer query` command, it will regard the previous querier invalid.

Configuring the Maximum Query Response Time

When a router receives a query message, the host will set a timer for each multicast group it belongs to. The value of the timer is randomly selected between 0 and the maximum response time. When any timer becomes 0, the host will send the membership report message of the multicast group.

Setting the maximum response time allows the host to respond to query messages quickly. In this case, the router can master the existing status of the members of the multicast group.

Perform the following configuration in VLAN interface view.

Table 130   Configure the Maximum Query Response Time

Operation	Command
Configure the maximum query response time for IGMP	`igmp max-response-time` seconds
Restore the maximum query response time to the default value	`undo igmp max-response-time`

The smaller the maximum query response time value, the faster the router prunes groups. The actual response time is a random value in the range from 1 to 25 seconds. The default value is 10 seconds.

Deleting IGMP Groups Joined on an Interface

You can delete an existing IGMP group from the interface via the following command.

Perform the following configuration in VLAN interface view.

Table 131   Delete IGMP Groups Joined on an Interface

Operation	Command
Delete IGMP groups joined on an interface	`reset igmp group { all	interface` interface-type interface-number `{ all |` group-address [ group-mask ] `} }`

Displaying and Debugging IGMP

After the previous configurations, execute the **display** command in all views to display the running of IGMP configuration, and to verify the effect of the configuration.

Execute the **debugging** command in user view to debug IGMP.

Table 132   Display and Debug IGMP

Operation	Command
Display the information about members of IGMP multicast groups	**display igmp group** [group-address | **interface** interface-type interface-number]
Display the IGMP configuration and running information about the interface	**display igmp interface** [interface-type interface-number]
Enable the IGMP information debugging	**debugging igmp** { **all** | **event** | **host** | **packet** | **timer** }
Disable the IGMP information debugging	**undo debugging igmp** { **all** | **event** | **host** | **packet** | **timer** }

IGMP Snooping

IGMP Snooping (Internet Group Management Protocol Snooping) is a multicast control mechanism running on layer 2. It is used for multicast group management and control.

IGMP Snooping runs on the link layer. When receiving the IGMP messages, the Switch 7750 uses IGMP Snooping to analyze the information. If the switch hears an IGMP host report message from an IGMP host, it adds the host to the corresponding multicast table. If the switch hears IGMP leave a message from an IGMP host, it will remove the host from the corresponding multicast table. The switch continuously listens to the IGMP messages to create and maintain a MAC multicast address table on Layer 2. It can then forward the multicast packets transmitted from the upstream router according to the MAC multicast address table.

When IGMP Snooping is disabled, the packets are multicast to all ports. See Figure 28.

Figure 28   Multicast Packet Transmission Without IGMP Snooping
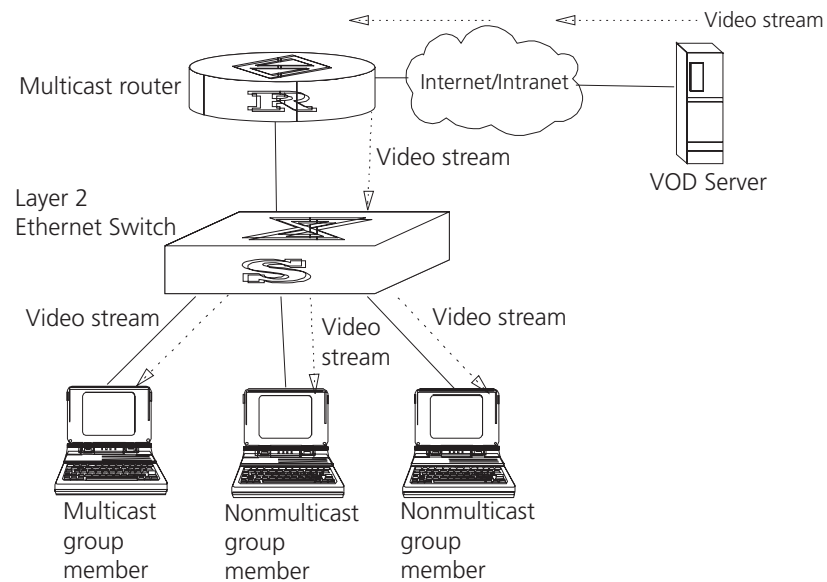
Packets are not forwarded to all ports when IGMP operates. See Figure 29.

Figure 29   Multicast Packet Transmission With IGMP Snooping
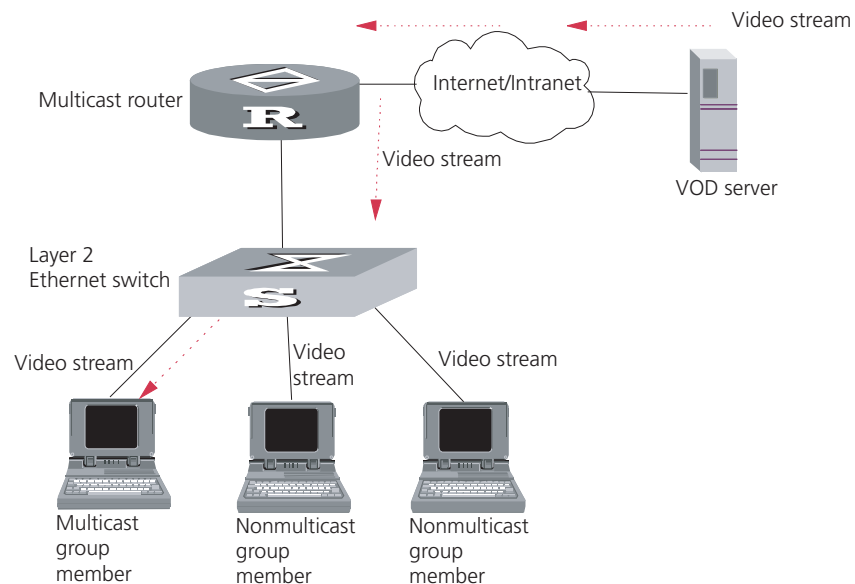
Implement IGMP Snooping

This section introduces related switch concepts of IGMP Snooping:

■   Router Port: The port directly connected to the multicast router.

■   Multicast member port: The port connected to the multicast member. The multicast member refers to a host that joined a multicast group.

■   MAC multicast group: The multicast group is identified with MAC multicast address and maintained by the Switch 7750.

■   Router port aging time: Time set on the router port aging timer. If the switch has not received any IGMP general query messages before the timer times out, it is no longer considered a router port.

■   Multicast group member port aging time: When a port joins an IP multicast group, the aging timer of the port begins timing. If the switch has not received any IGMP report messages before the timer times out, it transmits IGMP specific query message to the port.

■   Maximum response time: When the switch transmits IGMP specific query message to the multicast member port, the Switch 7750 starts a response timer, which times before the response to the query. If the switch has not received any IGMP report message before the timer times out, it will remove the port from the multicast member ports

The Switch 7750 runs IGMP Snooping to listen to the IGMP messages and map the host and its ports to the corresponding multicast group address. To implement IGMP Snooping, Switch 7750 processes different IGMP messages shown in the figure below:

Figure 30   Implementing IGMP Snooping
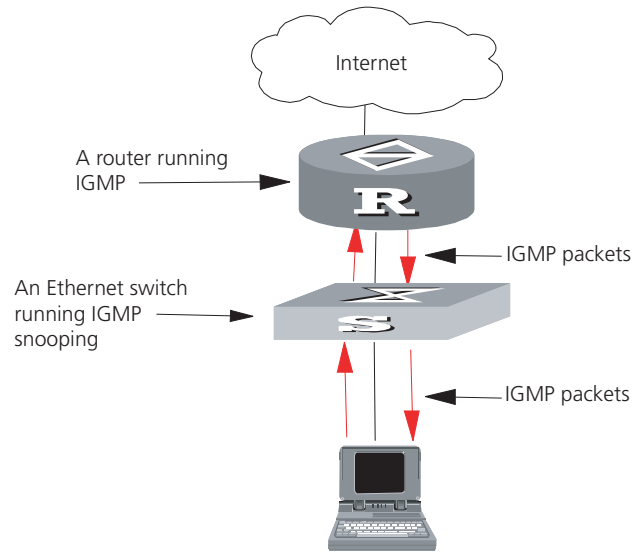
1   IGMP general query message: Transmitted by the multicast router to query which multicast group contains member. When a router port receives an IGMP general query message, the Switch 7750 will reset the aging timer of the port. When a port other than a router port receives the IGMP general query message, the Switch 7750 will notify the multicast router that a port is ready to join a multicast group and starts the aging timer for the port.

2   IGMP specific query message: Transmitted from the multicast router to the multicast members and used for querying if a specific group contains any member. When received IGMP specific query message, the switch only transmits the specific query message to the IP multicast group which is queried.

3   IGMP report message: Transmitted from the host to the multicast router and used for applying to a multicast group or responding to the IGMP query message. When received, the switch checks if the MAC multicast group is ready to join. If the corresponding MAC multicast group does not exist, the switch notifies the router that a member is ready to join a multicast group, creates a new MAC multicast group, adds the port that received the message to the group, starts the port aging timer, and then adds all the router ports in the native VLAN of the port into the MAC multicast forwarding table. Meanwhile, it creates an IP multicast group and adds the port received to it. If the corresponding MAC multicast group exists but does not contain the port that received the report message, the switch adds the port into the multicast group and starts the port aging timer. Then, the switch checks if the corresponding IP multicast group exists. If it does not exist, the switch creates a new IP multicast group and adds the port that received the report message to it. If it does exist, the switch adds the port. If the corresponding MAC multicast group exists and contains the port, the switch will only reset the aging timer of the port.

4   IGMP leave message: Transmitted from the multicast group member to the multicast router, to notify that a host has left the multicast group. The Switch 7750 transmits the specific query message, concerning the group, to the port that received the message in an effort to check if the host still has other members of this group, and then starts a maximum response timer. If the switch has not received any report message from the multicast group, the port will be removed from the corresponding MAC multicast group. If the MAC multicast group does

not have any member, the switch will notify the multicast router to remove it from the multicast tree.

Configuring IGMP Snooping is described in the following sections:

- Configuring IGMP Snooping
- Example: IGMP Snooping Configuration
- Troubleshooting IGMP Snooping

Configuring IGMP Snooping

The main IGMP Snooping configuration includes:

- Enabling/Disabling IGMP Snooping
- Configure Router Port Aging Time
- Configuring Maximum Response Time
- Configure Aging Time of Multicast Group Member
- Displaying and Debugging IGMP Snooping

Of the above configuration tasks, enabling IGMP Snooping is required, while others are optional.

Enabling/Disabling IGMP Snooping

You can use the following commands to enable/disable IGMP Snooping on Layer 2.

Perform the following configuration in system view. To enable IGMP snooping, you must also issue the **igmp-snooping enable** command in VLAN view.

Table 133   Enable/Disable IGMP Snooping

Operation	Command
Enable/disable IGMP Snooping	**igmp-snooping** { **enable**	**disable** }
Restore the default setting	**undo igmp-snooping**

IGMP Snooping and GMRP cannot run at the same time. You can check if GMRP is running, using the **display gmrp status** command, in all views, before enabling IGMP Snooping.

By default, IGMP Snooping is disabled.

Configure Router Port Aging Time

Use this to manually configure the router port aging time. If the switch has not received a general query message from the router prior to it aging, it will remove the port from all the MAC multicast groups.

Perform the following configuration in system view.

Table 134   Configure Router Port Aging Time

Operation	Command
Configure router port aging time	**igmp-snooping router-aging-time** seconds

Table 134 Configure Router Port Aging Time

Operation	Command
Restore the default aging time	`undo igmp-snooping router-aging-time`

By default, the port aging time is 260 seconds.

Configuring Maximum Response Time

This task sets the maximum response time. If the Switch 7750 receives no report message from a port in the maximum response time, it will remove the port from the multicast group.

Perform the following configuration in system view.

Table 135 Configuring the Maximum Response Time

Operation	Command
Configure the maximum response time	`igmp-snooping max-response-time seconds`
Restore the default setting	`undo IGMP-snooping max-response-time`

By default, the maximum response time is 10 seconds.

Configure Aging Time of Multicast Group Member

This task sets the aging time of the multicast group member port. If the switch receives no multicast group report message during the member port aging time, it will transmit the specific query message to that port and start a maximum response timer.

Perform the following configuration in system view.

Table 136 Configure Aging Time of the Multicast Member

Operation	Command
Configure aging time of the multicast member	`igmp-snooping host-aging-time seconds`
Restore the default setting	`undo igmp-snooping host-aging-time`

By default, the aging time of the multicast member is 260 seconds.

Displaying and Debugging IGMP Snooping

Execute the **display** command in all views to display the running of the IGMP Snooping configuration, and to verify the effect of the configuration. Execute the **debugging** command in user view to debug IGMP Snooping configuration.

Table 137 Display and Debug IGMP Snooping

Operation	Command
Display the information about current IGMP Snooping configuration	`display igmp-snooping configuration`
Display IGMP Snooping statistics of received and sent messages	`display igmp-snooping statistics`
Display IP/MAC multicast group information in the VLAN	`display igmp-snooping group [vlan vlanid ]`

Table 137   Display and Debug IGMP Snooping

Operation	Command
Enable/disable IGMP Snooping debugging (abnormal, group, packet, timer).	`debug igmp-snooping { all	abnormal	group	packet	timers }`
Disable IGMP Snooping debugging (abnormal, group, packet, timer).	`undo debug igmp-snooping { all	abnormal	group	packet	timers }`

Example: IGMP Snooping Configuration

To implement IGMP Snooping on the switch, first enable it. The switch is connected with the router through the router port, and with user PC through the non-router ports.

Figure 31   IGMP Snooping Configuration Network
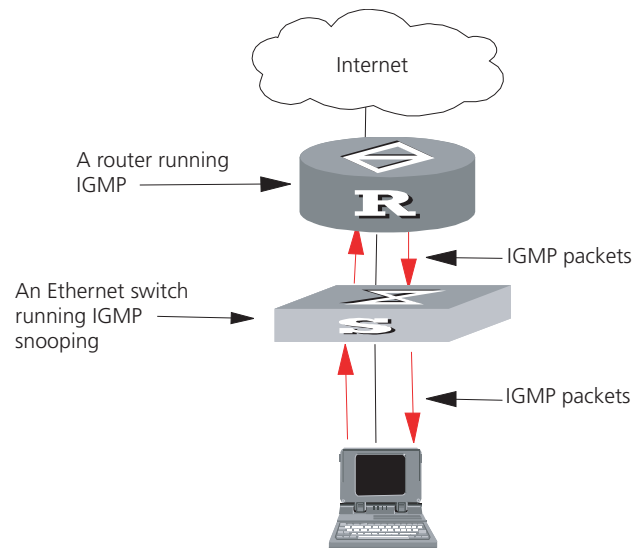
1 Display the status of GMRP.

`<SW7750>`**`display gmrp status`**

2 Display the current status of IGMP Snooping when GMRP is disabled.

`<SW7750>`**`display igmp-snooping configuration`**

3 Enable IGMP Snooping if it is disabled.

`[SW7750]`**`igmp-snooping enable`**

Troubleshooting IGMP Snooping

If the multicast function cannot be implemented on the switch, check for the following conditions and use the accompanying troubleshooting procedure:

1 IGMP Snooping is disabled.

■ Input the **`display current-configuration`** command to display the status of IGMP Snooping.

■ If the switch disabled IGMP Snooping, you can input **`igmp-snooping enable`** in the system view to enable IGMP Snooping.

2 Multicast forwarding table set up by IGMP Snooping is wrong.

■ Input the display `igmp-snooping group` command to see if the multicast group is the expected one.

■ Verify that the source IP address is correct for each multicast stream.

3 Multicast forwarding table set up on the bottom layer is wrong.

■ Enable IGMP Snooping group in user view and then input the `display igmp-snooping group` command to check if MAC multicast forwarding table in the bottom layer and that created by IGMP Snooping is consistent. You may also input the `display mac vlan` command in all views to check if MAC multicast forwarding table under vlanid in the bottom layer and that created by IGMP Snooping is consistent.

■ If they are not consistent, contact the maintenance personnel for help.

Configuring PIM-DM

PIM-DM (Protocol Independent Multicast, Dense Mode) belongs to dense mode multicast routing protocols. PIM-DM is suitable for small networks. Members of multicast groups are relatively dense in such network environments.

The working procedures of PIM-DM include neighbor discovery, flood and prune, and graft.

■ Neighbor discovery

The PIM-DM router needs to use Hello messages to perform neighbor discovery when it is started. All network nodes running PIM-DM keep in touch with one another with Hello messages, which are sent periodically.

■ Flood and Prune

PIM-DM assumes that all hosts on the network are ready to receive multicast data. When a multicast source "S" begins to send data to a multicast group "G", after the router receives the multicast packets, the router will perform RPF check according to the unicast routing table first. If an RPF check is passed, the router will create an (S, G) entry and then flood the data to all downstream PIM-DM nodes. If the RPF check is not passed, that is when multicast packets enter from an error interface, the packets will be discarded. After this process, an (S, G) entry will be created in the PIM-DM multicast domain.

If the downstream node has no multicast group members, it will send a Prune message to the upstream nodes to inform the upstream node not to forward data to the downstream node. Receiving the prune message, the upstream node will remove the corresponding interface from the outgoing interface list corresponding to the multicast forwarding entry (S, G). In this way, a SPT (Shortest Path Tree) rooted at Source S is built. Leaf routers initiate the pruning process.

This is called the "flood & prune" process. Nodes that are pruned provide timeout mechanism. Each router re-starts the "flood & prune" process upon pruning timeout. The consistent "flood & prune" process of PIM-DM is performed periodically.

During this process, PIM-DM uses the RPF check and the existing unicast routing table to build a multicast forwarding tree rooted at the data source. When a packet arrives, the router judges the validity of the path. If the interface is indicated by the unicast routing to the multicast source, the packet is regarded to be from the correct path, otherwise, the packet will be discarded

as a redundancy packet without the multicast forwarding. The unicast routing information as path judgment can come from any unicast routing protocol independent of any specified unicast routing protocol such as the routing information learned by RIP.

■ Assert mechanism

As shown in the following figure, both routers A and B on the LAN have their own receiving paths to multicast source S. In this case, when they receive a multicast packet sent from multicast source S, they will both forward the packet to the LAN. Multicast Router C at the downstream node will receive two copies of the same multicast packet.

Figure 32 Assert Mechanism Diagram
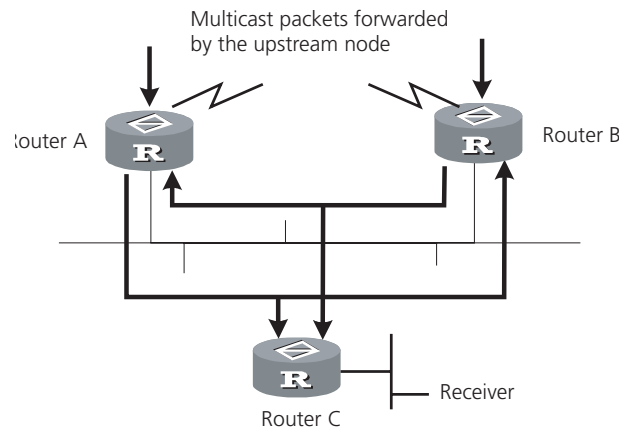
When they detect such a case, routers need to select a unique sender by using the assert mechanism. Routers send Assert packets to select the best path. If two or more have the same priority and metric, the path with a higher IP address will be the upstream neighbor of the (S, G) entry. This is responsible for forwarding the (S, G) multicast packet.

■ Graft

When the pruned downstream node needs to be restored to the forwarding state, the node will send a graft packet to inform the upstream node.

Configuring PIM-DM is described in the following sections:

■ Configuring PIM-DM
■ Example: PIM-DM Configuration

Configuring PIM-DM   Basic PIM-DM configuration includes:

■ Enabling Multicast
■ Enabling PIM-DM
■ Entering PIM View

Advanced PIM-DM configuration includes:

■ Configuring the Interface Hello Message Interval
■ Configuring the Filtering of Multicast Source/Group
■ Configuring the Filtering of PIM Neighbors

- Configuring the Maximum Number of PIM Neighbor on an Interface
- Displaying and Debugging PIM-DM

When the router is run in the PIM-DM domain, it is best to enable PIM-DM on all interfaces of the non-border router.

Enabling Multicast

See "Configuring Common Multicast " on page 114.

Enabling PIM-DM

PIM-DM needs to be enabled in the configuration of all interfaces.

After PIM-DM is enabled on an interface, it will send PIM Hello messages periodically, and process protocol packets sent by PIM neighbors.

Perform the following configuration in VLAN interface view.

Table 138   Enable PIM-DM

Operation	Command
Enable PIM-DM on an interface	`pim dm`
Disable PIM-DM on an interface	`undo pim dm`

3Com recommends that you configure PIM-DM on all interfaces. This configuration is effective only after the multicast routing is enabled in system view.

Once you enable PIM-DM on an interface, PIM-SM cannot be enabled on the same interface and vice versa.

Entering PIM View

Global parameters of PIM should be configured in PIM view.

Perform the following configuration in system view.

Table 139   Entering PIM View

Operation	Command
Enter PIM view	`pim`
Return to system view	`undo pim`

Use the `undo pim` command to clear the configuration in PIM view, and to return to system view.

Configuring the Interface Hello Message Interval

After PIM is enabled on an interface, it will send Hello messages periodically. The interval at which Hello messages are sent can be modified according to the bandwidth and type of the network connected to the interface.

Perform the following configuration in VLAN interface view.

Table 140   Configure Hello Message Interval on an Interface

Operation	Command
Configure the hello message interval on an interface	**pim timer hello** seconds
Restore the interval to the default value	**undo pim timer hello**

The default interval is 30 seconds. You can configure the value according to different network environments. Generally, this parameter does not need to be modified.

This configuration can be performed only after PIM (PIM-DM or PIM-SM) is enabled in VLAN interface view.

Configuring the Filtering of Multicast Source/Group

You can set to filter the source (and group) address of multicast data packets via this command. When this feature is configured, the router filters not only multicast data, but the multicast data encapsulated in the registration packets.

Perform the following configuration in the PIM view.

Table 141   Configuring the Filtering of Multicast Source/Group

Operation	Command
Configure the filtering of multicast source/group	**source-policy** acl-number
Remove the configuration of filtering	**undo source-policy**

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.

Configuring the Filtering of PIM Neighbors

You can set to filter the PIM neighbors on the current interface via the following configuration.

Perform the following configuration in the PIM view.

Table 142   Configuring the Filtering of PIM Neighbors

Operation	Command
Configure filtering of PIM neighbor	**pim neighbor-policy** acl-number
Remove the configuration of filtering	**undo pim neighbor-policy**

By default, no filtering rules are set.

Only the routers that match the filtering rule in the ACL can serve as a PIM neighbor of the current interface.

Configuring the Maximum Number of PIM Neighbor on an Interface

You can limit the PIM neighbors on an interface. No neighbor can be added any more when the limit is reached.

Perform the following configuration in the PIM view.

Table 143 Configure the Maximum Number of PIM Neighbor on an Interface

Operation	Command
Configure the maximum number of PIM neighbor on an interface	`pim neighbor-limit` limit
Restore the limit of PIN neighbor to the default value	`pim neighbor-limit`

By default, the PIM neighbors on the interface are limited to 128.

If the existing PIM neighbors exceed the configured value during configuration, they are not deleted.

Displaying and Debugging PIM-DM

Execute the **display** command in all views to display the running of PIM-DM configuration, and to verify the effect of the configuration.

Execute debugging command in user view for the debugging of PIM-DM.

Table 144 Displaying and Debugging PIM-DM

Operation	Command
Display the PIM multicast routing table	`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-num | interface-name | `null` } | { `dense-mode` | `sparse-mode` }] *
Display the PIM interface information	`display pim interface` [interface-type interface-number]
Display the information about PIM neighboring routers	`display pim neighbor` [`interface` interface-type interface-number]
Enable the PIM debugging	`debugging pim common` { `all` | `event` | `packet` | `timer` }
Disable the PIM debugging	`undo debugging pim common` { `all` | `event` | `packet` | `timer` }
Enable the PIM-DM debugging	`debugging pim dm` { `alert` | `all` | `mbr` | `mrt` | `timer` | `warning` | { `recv` | `send` } { `all` | `assert` | `graft` | `graft-ack` | `join` | `prune` } }

Table 144   Displaying and Debugging PIM-DM

Operation	Command
Disable the PIM-DM debugging	`undo debugging pim dm { alert	all	mbr	mrt	timer	warning	{ recv	send } { all	assert	graft	graft-ack	join	prune } }`

Example: PIM-DM Configuration

LS_A has a port carrying Vlan 10 to connect Multicast Source, a port carrying Vlan11 to connect LS_B and a port carrying Vlan12 to connect LS_C. Configure to implement multicast between Multicast Source and Receiver 1 and Receiver 2.

Figure 33   PIM-DM Configuration Networking
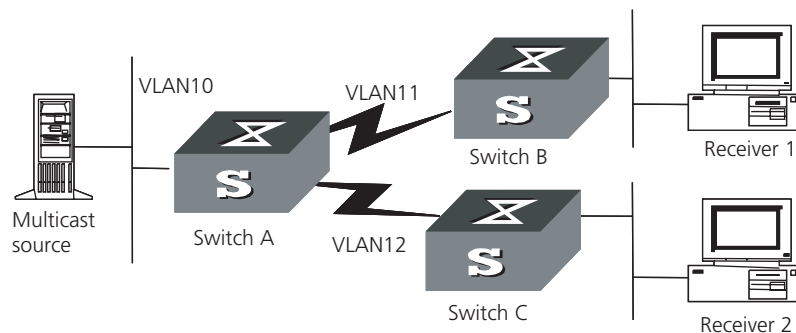
Configuration procedure

This section only provides the configuration for Switch A because the configuration procedures for Switch B and Switch C are similar.

1 Enable the multicast routing protocol.

```
[SW7750]multicast routing-enable
```

2 Enable PIM-DM.

```
[SW7750]vlan 10
[SW7750-vlan10]port Ethernet 1/0/2 to Ethernet 1/0/3
[SW7750-vlan10]quit
[SW7750]vlan 11
[SW7750-vlan11]port Ethernet 1/0/4 to Ethernet 1/0/5
[SW7750-vlan11]quit
[SW7750]vlan 12
[SW7750-vlan12]port Ethernet 1/0/6 to Ethernet 1/0/7
[SW7750-vlan12]quit
[SW7750]interface vlan-interface 10
[SW7750-vlan-interface10]ip address 1.1.1.1 255.255.0.0
[SW7750-vlan-interface10]igmp enable
[SW7750-vlan-interface10]pim dm
[SW7750-vlan-interface10]quit
[SW7750]interface vlan-interface 11
[SW7750-vlan-interface11]ip address 2.2.2.2 255.255.0.0
[SW7750-vlan-interface11]igmp enable
[SW7750-vlan-interface11]pim dm
[SW7750-vlan-interface11]quit
[SW7750]interface vlan-interface 12
[SW7750-vlan-interface12]ip address 3.3.3.3 255.255.0.0
[SW7750-vlan-interface12]igmp enable
```

```
[SW7750-vlan-interface12]pim dm
```

Configuring PIM-SM
PIM-SM (Protocol Independent Multicast, Sparse Mode) belongs to sparse mode multicast routing protocols. PIM-SM is mainly applicable to large-scale networks with broad scope and few group members.

Different from the flood & prune principle of the dense mode, PIM-SM assumes that all hosts do not need to receive multicast packets, unless clear request is put forward.

PIM-SM uses the RP (Rendezvous Point) and the BSR (Bootstrap Router) to advertise multicast information to all PIM-SM routers and uses the join/prune information of the router to build the RP-rooted shared tree (RPT). This helps to reduce the bandwidth occupied by data packets and control packets, and reduces the process overhead of the router. Multicast data flows along the shared tree to the network segments. When data traffic is sufficient, the multicast data flow switches over to the SPT (Shortest Path Tree) rooted on the source. This reduces network delay. To perform the RPF check, PIM-SM does not depend on the specified unicast routing protocol but uses the present unicast routing table.

Running PIM-SM, you would need to configure candidate RPs and BSRs. The BSR is responsible for collecting the information from the candidate RP and advertising the information.

Configuring PIM-SM is described in the following sections:

- PIM-SM Operating Principles
- Preparing to Configure PIM-SM
- Configuring PIM-SM

PIM-SM Operating Principles
The PIM-SM working process is as follows: neighbor discovery, building the RP-rooted shared tree (RPT), multicast source registration and SPT switchover etc. The neighbor discovery mechanism is the same as that of PIM-DM.

Build the RP shared tree (RPT)

When hosts join a multicast group G, the leaf routers send IGMP messages to learn the receivers of the multicast group G. The leaf routers calculate the corresponding rendezvous point (RP) for multicast group G, and then send join messages to the node of a higher level toward the rendezvous point (RP). Each router along the path, between the leaf routers and the RP, will generate (*, G) entries in the forwarding table, indicating that all packets sent to multicast group G are applicable. When the RP receives packets sent to multicast group G, the packets will be sent to leaf routers along the path built and then reach the hosts. In this way, an RP-rooted tree (RPT) is built as shown in Figure 34.

Figure 34 RPT Schematic Diagram

Multicast source S

RPT ┄┄┄►

join ───►

Multicast source ┄┄┄►
registration

Multicast Source Registration

When multicast source S sends a multicast packet to group G, the PIM-SM multicast router is responsible for encapsulating the packet into a registration packet upon receipt. It then sends the packet to the corresponding RP in unicast. If there are multiple PIM-SM multicast routers on a network segment, the Designated Router (DR) will be responsible for sending the multicast packet.

Preparing to Configure PIM-SM

Tasks for preparing to Configure PIM-SM are described in the following sections:

- Configure Candidate RPs
- Configure BSRs
- Configure Static RP

Configure Candidate RPs

In a PIM-SM network, multiple RPs (candidate-RPs) can be configured. Each Candidate-RP (C-RP) is responsible for forwarding multicast packets with the destination addresses in a certain range. Configuring multiple C-RPs is to implement load balancing of the RP. These C-RPs are equal. All multicast routers calculate the RPs corresponding to multicast groups according to the same algorithm, after receiving the C-RP messages that the BSR advertises.

> *One RP can serve multiple multicast groups or all multicast groups. Each multicast group can only be uniquely correspondent to one RP at a time rather than multiple RPs.*

Configure BSRs

The BSR is the management core in a PIM-SM network. Candidate-RPs send announcement to the BSR, which is responsible for collecting and advertising the information about all candidate-RPs.

It should be noted that there can be only one BSR in a network but you can configure multiple candidate-BSRs. In this case, once a BSR fails, you can switch over to another BSR. A BSR is elected among the C-BSRs automatically. The C-BSR with the highest priority is elected as the BSR. If the priority is the same, the C-BSR with the largest IP address is elected as the BSR.

Configure Static RP

The router that serves as the RP is the core router of multicast routes. If the dynamic RP elected by BSR mechanism is invalid for some reason, the static RP can

be configured to specify RP. As the backup of dynamic RP, static RP improves network robustness and enhances the operation and management capability of multicast network.

Configuring PIM-SM   Basic PIM-SM configuration includes:

- Enabling Multicast
- Enabling IGMP on an Interface
- Enabling PIM-SM
- Setting the PIM-SM Domain Border
- Entering PIM View
- Configuring Candidate-BSRs
- Configuring Candidate-RPs
- Configuring Static RP

Advanced PIM-SM configuration includes:

- Configuring the Interface Hello Message Interval
- Configuring the Filtering of Multicast Source/Group
- Configuring the Filtering of PIM Neighbor
- Configuring the Maximum Number of PIM Neighbor on an Interface
- Configuring RP to Filter the Register Messages Sent by DR
- Limiting the Range of Legal BSR
- Limiting the Range of Legal C-RP
- Clearing Multicast Route Entries from PIM Routing Table
- Clearing PIM Neighbors
- Displaying and Debugging PIM-SM

At least one router in an entire PIM-SM domain should be configured with Candidate-RPs and Candidate-BSRs.

Enabling Multicast

Refer to "Configuring Common Multicast " on page 114.

Enabling IGMP on an Interface

Refer to "Configuring IGMP" on page 116.

Enabling PIM-SM

This configuration can be effective only after multicast is enabled.

Perform the following configuration in VLAN interface view.

Table 145   Enabling PIM-SM

Operation	Command
Enable PIM-SM on an interface	`pim sm`
Disable PIM-SM on an interface	`undo pim sm`

Repeat this configuration to enable PIM-SM on other interfaces. Only one multicast routing protocol can be enabled on an interface at a time.

Once enabled, PIM-DM cannot be enabled on the same interface.

Setting the PIM-SM Domain Border

After the PIM-SM domain border is configured, bootstrap messages cannot cross the border in any direction. In this way, the PIM-SM domain can be split.

Perform the following configuration in VLAN interface view.

Table 146   Setting the PIM-SM Domain Border

Operation	Command
Set the PIM-SM domain border	`pim bsr-boundary`
Remove the PIM-SM domain border configured	`undo pim bsr-boundary`

By default, no domain border is set. After this configuration is performed, a bootstrap message cannot cross the border, but other PIM packets can. This configuration can effectively divide a network into domains using different BSRs.

> **i** *This command cannot create a multicast packet forwarding border but only a PIM bootstrap message border.*

Entering PIM View

Global parameters of PIM should be configured in PIM view.

Perform the following configuration in system view.

Table 147   Entering PIM View

Operation	Command
Enter PIM view	`pim`
Back to system view	`undo pim`

Using `undo pim` command, you can clear the configuration in PIM view and back to system view.

Configuring Candidate-BSRs

In a PIM domain, one or more candidate BSRs should be configured. A BSR (Bootstrap Router) is elected among candidate BSRs. The BSR takes charge of collecting and advertising RP information.

The automatic election among candidate BSRs is described as follows. One interface which has started PIM-SM must be specified when configuring the router as the candidate BSR. At first, each candidate BSR considers itself as the BSR of the PIM-SM domain, and sends a Bootstrap message by taking the IP address of the interface as the BSR address. When receiving Bootstrap messages from other routers, the candidate BSR will compare the BSR address of the newly received Bootstrap message with that of itself. Comparison standards include priority and IP address. The bigger IP address is considered better when the priority is the same. If the new BSR address is better, the candidate BSR will replace its BSR address.

Otherwise, the candidate BSR will keep its BSR address and continue to regard itself as the BSR.

Perform the following configuration in PIM view.

Table 148 Configuring Candidate-BSRs

Operation	Command
Configure a candidate-BSR	**c-bsr** interface-type interface-number hash-mask-len [priority]
Remove the candidate-BSR configured	**undo c-bsr**

Candidate-BSRs should be configured on the routers in the network backbone. By default, no BSR is set. The default priority is 0.

> *Only one router can be configured with one candidate-BSR. When a candidate-BSR is configured on another interface, it will replace the previous configuration.*

Configuring Candidate-RPs

In PIM-SM, the shared tree built by the multicast routing data is rooted at the RP. There is mapping from a multicast group to an RP. A multicast group can be mapped to an RP. Different groups can be mapped to one RP.

Perform the following configuration in PIM view.

Table 149 Configuring Candidate-RPs

Operation	Command
Configure a candidate-RP	**c-rp** interface-type interface-number [**group-policy** acl-number]
Remove the candidate-RP configured	**undo c-rp** interface-type interface-number

If the range of the served multicast group is not specified, the RP will serve all multicast groups. Otherwise, the range of the served multicast group is the multicast group in the specified range. It is suggested to configure Candidate RP on the backbone router.

Configuring Static RP

Static RP serves as the backup of dynamic RP to make the network more robust.

Perform the following configuration in PIM view.

Table 150 Configuring Static RP

Operation	Command
Configure static RP	**static-rp** rp-address [acl-number]
Configure static RP	**undo static-rp**

Basic ACLs can control the range of the multicast group served by static RP.

If static RP is in use, all routers in the PIM domain must adopt the same configuration. If the configured static RP address is the interface address of the local router whose state is UP, the router will function as the static RP. It is unnecessary to enable PIM on the interface that functions as static RP.

When the RP elected from BSR mechanism is valid, static RP does not work.

Configuring the Interface Hello Message Interval

Generally, PIM-SM advertises Hello messages periodically on the interface enabled with it to detect PIM neighbors and discover which router is the Designated Router (DR).

Perform the following configuration in VLAN interface view.

Table 151 Configuring the Interface Hello Message Interval

Operation	Command
Configure the interface hello message interval	`pim timer hello` seconds
Restore the interval to the default value	`undo pim timer hello`

By default, the hello message interval is 30 seconds. Users can configure the value according to different network environments.

This configuration can be performed only after the PIM (PIM-DM or PIM-SM) is enabled in VLAN interface view.

Configuring the Filtering of Multicast Source/Group

See "Configuring PIM-DM" on page 130.

Configuring the Filtering of PIM Neighbor

See "Configuring PIM-DM" on page 130.

Configuring the Maximum Number of PIM Neighbor on an Interface

See "Configuring PIM-DM" on page 130.

Configuring RP to Filter the Register Messages Sent by DR

In the PIM-SM network, the register message filtering mechanism can control which sources to send messages to, which groups on the RP, i.e., RP can filter the register messages sent by DR to accept specified messages only.

Perform the following configuration in PIM view.

Table 152 Configuring RP to Filter the Register Messages Sent by DR

Operation	Command
Configure RP to filter the register messages sent by DR	`register-policy` acl-number
Cancel the configured filter of messages	`undo register-policy`

If an entry of a source group is denied by the ACL, or the ACL does not define operation to it, or there is no ACL defined, the RP will send RegisterStop messages to the DR to prevent the register process of the multicast data stream.

> *Only the register messages matching the ACL permit clause can be accepted by the RP. Specifying an undefined ACL will make the RP deny all register messages.*

Limiting the Range of Legal BSR

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 these types 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 these types 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.

Perform the following configuration in PIM view.

Table 153 Limiting the Range of Legal BSR

Operation	Command
Limit the legal BSR range	`bsr-policy` acl-number
Restore to the default setting	`undo bsr-policy`

For detailed information of the `bsr-policy` command, see the *Switch 7750 Command Reference Guide*.

Limiting the Range of Legal C-RP

In the PIM SM network, using BSR mechanism, every router can set itself as the C-RP (candidate rendezvous point) servicing particular groups. If elected, a C-RP becomes the RP servicing the current group.

In the BSR mechanism, a C-RP router unicasts C-RP messages to the BSR, which then propagates the C-RP messages among the network by BSR message. To prevent C-RP spoofing, you need to configure `crp-policy` on the BSR to limit legal C-RP range and their service group range. Since each C-BSR has the chance to become BSR, you must configure the same filtering policy on each C-BSR router.

Perform the following configuration in PIM view.

Table 154 Limiting the Range of Legal C-RP

Operation	Command
Limit the legal C-RP range	`crp-policy` acl-number

Table 154   Limiting the Range of Legal C-RP

Operation	Command
Restore to the default setting	**undo crp-policy**

For detailed information of the **crp-policy** command, see the *Switch 7750 Command Reference Guide*.

Clearing Multicast Route Entries from PIM Routing Table

Perform the following configuration in user view.

Table 155   Clearing Multicast Route Entries from PIM Routing Table

Operation	Command
Clear multicast route entries from PIM routing table	**reset pim routing-table** { **all** | { group-address [**mask** group-mask | **mask-length** group-mask-length] | source-address [**mask** source-mask | **mask-length** source-mask-length] | { **incoming-interface** { interface-type interface-number | **null** } } } * }

If in this command, the *group-address* is 224.0.0.0/24 and *source-address* is the RP address (where group address can have a mask, but the resulting 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 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.

> **i** *This command clears multicast route entries from PIM routing table, as well as the corresponding route entries and forward entries in the multicast core routing table and MFC.*

Clearing PIM Neighbors

Perform the following configuration in user view.

Table 156   Clearing PIM Neighbors

Operation	Command
Clear PIM neighbors	**reset pim neighbor** { **all** | { neighbor-address | **interface** interface-type interface-number } * }

Displaying and Debugging PIM-SM

Execute the **display** command in all views to display the PIM-SM configuration, and to verify the configuration.

Execute the **debugging** command in user view to debug PIM-SM.

Table 157   Display and Debug PIM-SM

Operation	Command
Display the BSR information	**display pim bsr-info**
Display the RP information	**display pim rp-info** [group-address]
Enable the PIM-SM debugging	**debugging pim sm** { **all** │ **mbr** │ **register-proxy** │ **mrt** │ **timer** │ **warning** │ { **recv** │ **send** } { **assert** │ **graft** │ **graft-ack** │ **join** │ **prune** } }
Disable the PIM-SM debugging	**undo debugging pim sm** { **all** │ **mbr** │ **register-proxy** │ **mrt** │ **timer** │ **warning** │ { **recv** │ **send** } { **assert** │ **graft** │ **graft-ack** │ **join** │ **prune** } }

Example: Configuring PIM-SIM

Host A is the receiver of the multicast group at 225.0.0.1. Host B begins transmitting data destined to 225.0.0.1. Switch A receives the multicast data from Host B by Switch B.

Figure 35   PIM-SM Configuration Networking
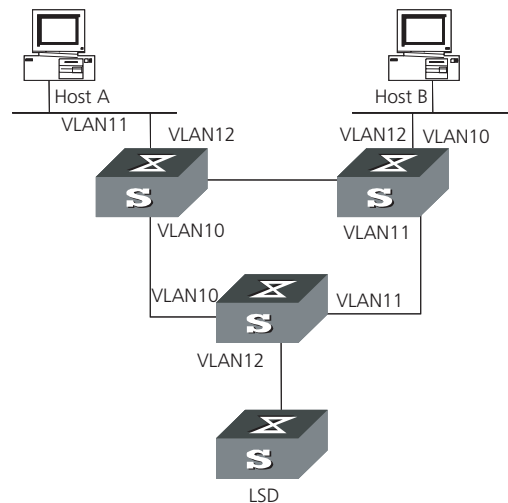
Configure Switch A

1 Enable PIM-SM.

```
[SW7750]multicast routing-enable
[SW7750]vlan 10
[SW7750-vlan10]port Ethernet 1/0/2 to Ethernet 1/0/3
[SW7750-vlan10]quit
[SW7750]interface vlan-interface 10
[SW7750-vlan-interface10]pim sm
[SW7750-vlan-interface10]quit
[SW7750]vlan 11
[SW7750-vlan11]port Ethernet 1/0/4 to Ethernet 1/0/5
[SW7750-vlan11]quit
[SW7750]pim
```

```
[SW7750-pim]interface vlan-interface 11
[SW7750-vlan-interface11]pim sm
[SW7750-vlan-interface11]quit
[SW7750]vlan 12
[SW7750-vlan12]port Ethernet 1/0/6 to Ethernet 1/0/7
[SW7750-vlan12]quit
[SW7750]pim
[SW7750-pim]interface vlan-interface 12
[SW7750-vlan-interface12]pim sm
[SW7750-vlan-interface12]quit
```

Configure Switch B

1 Enable PIM-SM.

```
[SW7750]multicast routing-enable
[SW7750]vlan 10
[SW7750-vlan10]port Ethernet 1/0/2 to Ethernet 1/0/3
[SW7750-vlan10]quit
[SW7750]pim
[SW7750-pim]interface vlan-interface 10
[SW7750-vlan-interface10]pim sm
[SW7750-vlan-interface10]quit
[SW7750]vlan 11
[SW7750-vlan11]port Ethernet 1/0/4 to Ethernet 1/0/5
[SW7750-vlan11]quit
[SW7750]pim
[SW7750-pim]interface vlan-interface 11
[SW7750-vlan-interface11]pim sm
[SW7750-vlan-interface11]quit
[SW7750]vlan 12
[SW7750-vlan12]port Ethernet 1/0/6 to Ethernet 1/0/7
[SW7750-vlan12]quit
[SW7750]pim
[SW7750-pim]interface vlan-interface 12
[SW7750-vlan-interface12]pim sm
[SW7750-vlan-interface12]quit
```

2 Configure the C-BSR.

```
[SW7750]pim
[SW7750-pim]c-bsr vlan-interface 10 30 2
```

3 Configure the C-RP.

```
[SW7750]acl number 2005
[SW7750-acl-basic-2005]rule permit source 225.0.0.0 0.255.255.255
[SW7750]pim
[SW7750-pim]c-rp vlan-interface 10 group-list 5
```

4 Configure PIM domain border.

```
[SW7750]interface vlan-interface 12
[SW7750-vlan-interface12]pim bsr-boundary
```

After VLAN-interface 12 is configured as BSR, the LS_D will be excluded from the local PIM domain and cannot receive the BSR information transmitted from LS_B anymore.

Configure Switch C:

1 Enable PIM-SM.

```
[SW7750]multicast routing-enable
[SW7750]vlan 10
[SW7750-vlan10]port Ethernet 1/0/2 to Ethernet 1/0/3
[SW7750-vlan10]quit
[SW7750]pim
[SW7750-pim]interface vlan-interface 10
[SW7750-vlan-interface10]pim sm
[SW7750-vlan-interface10]quit
[SW7750]vlan 11
[SW7750-vlan11]port Ethernet 1/0/4 to Ethernet 1/0/5
[SW7750-vlan11]quit
[SW7750]pim
[SW7750-pim]interface vlan-interface 11
[SW7750-vlan-interface11]pim sm
[SW7750-vlan-interface11]quit
[SW7750]vlan 12
[SW7750-vlan12]port Ethernet 1/0/6 to Ethernet 1/0/7
[SW7750-vlan12]quit
[SW7750]pim
[SW7750-pim]interface vlan-interface 12
[SW7750-vlan-interface12]pim sm
[SW7750-vlan-interface12]quit
```

GMRP

GMRP (GARP Multicast Registration Protocol), based on GARP, is used for maintaining dynamic multicast registration information. All the switches supporting GMRP can receive multicast registration information from other switches, and dynamically update local multicast registration information. Local multicast registration information can be transmitted to other switches. This information switching mechanism keeps consistency of multicast information maintained by every GMRP-supporting device in the same switching network.

A host transmits GMRP Join message. After receiving the message, the switch adds the port to the multicast group, and broadcasts the message throughout the VLAN; thereby the multicast source in the VLAN knows the multicast member. When the multicast source sends packets to its group, the switch only forwards the packets to the ports connected to members, thereby implementing the Layer 2 multicast in VLAN.

The multicast information transmitted by GMRP includes, local static multicast registration information configured manually, and the multicast registration information dynamically registered by other switches.

Configuring GMRP

The main tasks in a GMRP configuration are described in the following sections:

■ Enable/Disable GMRP Globally

■ Enabling/Disabling GMRP on the Port

■ Displaying and Debugging GMRP

In the configuration process, GMRP must be enabled globally before it is enabled on the port.

Enable/Disable GMRP Globally

Perform the following configuration in system view.

Table 158   Enabling/Disabling GMRP Globally

Operation	Command
Enable GMRP globally.	**gmrp**
Disable GMRP globally.	**undo gmrp**

By default, GMRP is disabled.

Enabling/Disabling GMRP on the Port

Perform the following configuration in Ethernet port view.

Table 159   Enabling/Disabling GMRP on the Port

Operation	Command
Enable GMRP on the port_	**gmrp**
Disable GMRP on the port_	**undo gmrp**

GMRP should be enabled globally before being enabled on a port.

By default, GMRP is disabled on the port.

Displaying and Debugging GMRP

After the previous configuration, execute the **display** command to display the GMRP configuration, and to verify the effect of the configuration. Execute the **debugging** command in user view to debug GMRP configuration.

Table 160   Display and Debug GMRP

Operation	Command
Display GMRP statistics.	**display gmrp statistics** [**interface** interface_list]
Display GMRP global status.	**display gmrp status**
Enable GMRP debugging	**debugging gmrp**
Disable GMRP debugging	**undo debugging gmrp event**

Example: Configuring GMRP

Implement dynamic registration and an update of multicast information between switches.

Figure 36   GMRP Networking

Configure LS_A:

1 Enable GMRP globally.

```
[SW7750]gmrp
```

2 Enable GMRP on the port.

```
[SW7750]interface Ethernet 1/0/1
[SW7750-Ethernet1/0/1]gmrp
```

Configure LS_B:

1 Enable GMRP globally.

```
[SW7750]gmrp
```

2 Enable GMRP on the port.

```
[SW7750]interface Ethernet 1/0/1
[SW7750-Ethernet1/0/1]gmrp
```

7

QoS/ OPERATION

- ACL Overview
- Configuring ACLs
- Displaying and Debugging an ACL
- Configuring QoS
- Configuring ACL Control

ACL Overview

The Access Control List (ACL) classifies the data packets with a series of matching rules, including source address, destination address and port number. The switch verifies the data packets with the rules in the ACL and decides to forward, prioritize, or discard them.

A series of matching rules are required for the network devices to identify the packets. After identifying the packets, the switch can permit or deny them to pass through according to the defined policy. The ACL is used to implement these functions.

The data packet matching rules, that are defined by ACL, can also be used in other cases requiring traffic classification, such as defining traffic classification for QoS.

An access control rule includes several statements. Different statements specify different ranges of packets. When matching a data packet with the access control rule, the issue of match-order arises.

Configuring ACL Overview is described in the following sections:

- Filtering or Classifying Data Transmitted by the Hardware
- Filtering or Classifying Data Transmitted by the Software
- ACL Support on the Switch 7750

Filtering or Classifying Data Transmitted by the Hardware

An ACL can be used to filter or classify the data transmitted by the hardware of the switch. In this case, the match order of the ACL's sub-rules is determined by the switch hardware and this match order takes precedence over the match order defined by the user.

An ACL is configured with multiple sub-rules. The sub-rule with the more accurate range is matched first. If some rules define the same range, the latest sub-rule will be matched first. For example, ACL 2000 has rule 0 and rule 1, the definition of rule 0 is "rule 0 permit ip source 1.1.1.1 0.0.255.255 destination 2.2.2.2 0.0.255.255", the definition of rule 1 is "rule 1 permit ip source 1.1.1.1 0.0.0.255 destination 2.2.2.20.0.0.255", rule 1 is more accurate, it will be matched first.

This type of filtering includes ACLs that are used with the QoS function, ACLs used to filter the packet transmitted by the hardware, and so on.

Filtering or Classifying Data Transmitted by the Software

An ACL can be used to filter or classify the data transmitted by the software of the switch. The user can determine the match order of ACL's sub-rules. There are two match-orders: configuration, which follows the user-defined configuration order when matching the rule, and automatic, which follows the depth-first principle.

The depth-first principle puts the statement specifying the smallest range of addresses on the top of the list. For example, 129.102.1.1 0.0.0.0 specifies a host, while 129.102.1.1 0.0.255.255 specifies the network segment 129.102.0.1 through 129.102.255.255. The host is listed first in the access control list. The specific standard is:

■ For basic ACL statements, source address wildcards are compared directly. If the wildcards are the same, the configuration sequence is used.

■ For the ACL based on the interface filter, the rule that is configured is listed at the end, while others follow the configuration sequence.

■ For the advanced ACL, source address wildcards are compared first. If they are the same, then destination address wildcards are compared. For the same destination address wildcards, ranges of port numbers are compared and the smaller range is listed first. If the port numbers are in the same range, the configuration sequence is used.

After you specify the match-order of an access control rule, you cannot modify it later unless you delete all the contents and specify the match-order again.

This type of filtering includes ACLs cited by route policy function, ACLs used for controlling user logons, and so on.

ACL Support on the Switch 7750

Table 161 lists the categories of ACLs, their value ranges and the maximum number of each ACL on a Switch 7750.

Table 161   Quantitative Limitation to the ACL

Item	Value range	Maximum
Numbered basic ACL	2000 to 2999	99
Numbered advanced ACL	3000 to 3999	100
Numbered Layer-2 ACL	4000 to 4999	100
User-defined ACL	5000 to 5999	100
Named basic ACL	-	1000
Named advanced ACL	-	1000
Named Layer-2 AC	-	1000
The sub items of an ACL	0 to 127	128
Maximum sub items for all ACLs (for a 7-slot chassis)	-	1536 (with 6 48-port I/O modules installed)
Maximum sub items for all ACLs (for 4-slot chassis)	-	768 (with 3 48-port I/O modules installed)
Maximum sub items for all ACLs (for an 8-slot chassis)	-	1536 (with 6 48-port I/O modules installed)

Configuring ACLs	ACL configuration includes the tasks described in the following sections:

- Configuring the Time Range
- Selecting the ACL Mode
- Defining an ACL
- Activating an ACL

Configure the time range first, then define the ACL (using the defined time range in the definition), followed by activating the ACL to validate it. These steps must be done in sequence.

Configuring the Time Range	The process of configuring a time-range includes configuring the hour-minute range, date range, and period range. The hour-minute range is expressed in the units of minutes and hour. The date range is expressed in the units of date, month, and year. The periodic time range is expressed by the day of the week.

Use the following command to set the time range in system view.

Table 162   Set the Absolute Time Range

Operation	Command
Set the absolute time range	**time-range** *time-name* { *start-time* **to** *end-time days-of-the-week*	**from** *start-time start- date*	**to** *end-time end-date*]
Delete the absolute time range	**undo time-range** *time-name* [*start-time* **to** *end-time days-of-the-week*] [**from** *start-time start- date*] [**to** *end time end-date*]

When the *start-time* and *end-time* are not configured, they are set to define one day. The end time must be later than the start time.

When the *end-time end-date* is not configured, it will be all the time from now to the latest date that can be displayed by the system. The end time must be later than the start time.

Selecting the ACL Mode	The Switch 7750 can only have one of two modes, **ip-based** or **link-based**. In either mode, only L2 ACLs can be defined, activated, and cited by other applications.

You can use the following command to configure a traffic classification rule in **ip-based** or **link-based** mode.

Perform the following configuration in system view.

Table 163   Select ACL Mode

Operation	Command
Select ACL mode	**acl mode** { **ip-based	link-based** }

By default, the Switch 7750 uses **ip-based** mode and the L3 traffic classification rule.

Defining an ACL	The Switch 7750 supports several kinds of ACLs.

To define the ACL:

1 Enter the corresponding ACL view

2 Add a rule to the ACL

You can add multiple rules to one ACL.

i *If a specific time range is not defined, the ACL functions after it is activated.*

During the process of defining the ACL, you can use the **rule** command several times to define multiple rules for an ACL.

If ACL is used to filter or classify the data transmitted by the hardware of the switch, the match order defined in the **acl** command is ignored. If ACL is used to filter or classify the data treated by the software of the switch, you can determine the match order for the ACL sub-rules. After you specify the match-order of an ACL rule, you cannot modify it later.

The default matching-order of ACL follows the order that is configured by the user.

Tasks for defining an ACL are described in the following sections:

■ Defining a Basic ACL

■ Define an Advanced ACL

■ Defining a Layer-2 ACL

Defining a Basic ACL

The rules of the basic ACL are defined on the basis of the Layer 3 source IP address to analyze the data packets.

Perform the following configuration in the designated view.

Table 164 Define Basic ACL

Operation	Command
Enter basic ACL view (from system view)	**acl** { **number** *acl-number* | **name** *acl-name* **basic** } [**match-order** { **config** | **auto** }]
Add a sub-item to the ACL (from basic ACL view)	**rule** [*rule-id*] { **permit** | **deny** } [**source** *source-addr wildcard* | **any**] [**fragment**] [**time-range** *name*]
Delete a sub-item from the ACL (from basic ACL view)	**undo rule** *rule-id* [**source**] [**fragment**] [**time-range**]
Delete one ACL or all the ACL (from system view)	**undo acl** { **number** *acl-number* | **name** *acl-name* | **all** }

A basic ACL is defined by numbers from 2000 to 2999.

Define an Advanced ACL

The classification rules for advanced ACL are defined on the basis of attributes, such as, source and destination IP address, the TCP or UDP port number in use, and the packet priority to process the data packets. The advanced ACL supports the analyses of three kinds of packet priorities, ToS (Type of Service), IP, and DSCP priorities.

Perform the following configuration in designated view.

Table 165   Define Advanced ACL

Operation	Command
Enter advanced ACL view (from system view)	**acl** { **number** *acl-number*	**name** *acl-name* **advanced** } [**match-order** { **config**	**auto** }]
Add a sub-item to the ACL (from advanced ACL view)	**rule** [*rule-id*] { **permit**	**deny** } *protocol* [**source** *source-addr source-wildcard*	**any**] [**destination** *dest-addr wildcard*	**any**] [**source-port** *operator port1* [*port2*]] [**destination-port** *operator port1* [*port2*]] [**icmp-type** *type-code*] [**established**] [[**precedence** *precedence*	**tos** *tos*]*	**dscp** *dscp*] [**fragment**] [**time-range** *name*]
Delete a sub-item from the ACL (from advanced ACL view)	**undo rule** *rule-id* [**source**] [**destination**] [**source-port**] [**destination-port**] [**icmp-type**] [**precedence**] [**tos**] [**dscp**] [**fragment**] [**time-range**]
Delete one ACL or all the ACL (from system view)	**undo acl** { **number** *acl-number*	**name** *acl-name*	**all** }

An advanced ACL is identified with numbers ranging from 3000 to 3999.

Note that port1 and port2 in this command specify the TCP or UDP ports used by various high-layer applications. For some common port numbers, you can use the mnemonic symbols as a shortcut.

i> *When you configure the rule, the following parameters are not supported by the switch:* icmp-type type code, tos tos, fragment.

When you configure the TCP/UDP port parameter, the following restrictions apply:

- If you use the operator **gt**, the value of parameter port1 can only be 32767.

- If you use the **lt** operator, the value of parameter port1 should be a power value of 2, i.e. 2^n

- The switch doesn't support the operator **neq**.

- If you use the operator **range**, these rules for the parameters port1 and port2 (support port_range = port2 - port1 + 1) should be followed:

- *port_range* is a power value of 2.

- *port1* is a multiple value of port_range.

Defining a Layer-2 ACL

The rules of Layer-2 ACL are defined on the basis of the Layer-2 information, such as, source MAC address, source VLAN ID, Layer-2 protocol type, Layer-2 packet fomat, and destination MAC address.

Perform the following configuration in the designated view.

Table 166   Define Layer-2 ACL

Operation	Command
Enter Layer-2 ACL view (from system view)	**acl** { **number** *acl-number*	**name** *acl-name* **link** } [**match-order** { **config**	**auto** }]

Table 166 Define Layer-2 ACL

Operation	Command
Add a sub-item to the ACL (from Layer-2 ACL view)	**rule** [*rule-id*] { **permit**	**deny** } [*protocol-type*] [*format-type*] **ingress** { { *source-vlan-id*	*source-mac-addr* }| **any** } **egress** { [*dest-mac-addr*	**any**] } [**time-range** *name*]
Delete a sub-item from the ACL (from Layer-2 ACL view)	**undo rule** *rule-id*
Delete one ACL or all the ACL (from system view)	**undo acl** { **number** *acl-number*	**name** *acl-name*	**all** }

A Layer-2 ACL can be identified with numbers ranging from 4000 to 4999.

If you assign an ACL to an interface and then make changes to the ACL, you must reassign the ACL to the interface before the changes to the ACL will apply on the interface.

Activating an ACL
A defined ACL can be active after being enabled globally on the switch. This function is used to activate ACL filtering or to classify the data transmitted by the hardware of the switch.

Perform the following configuration in Qos view.

Table 167 Activate ACL

Operation	Command
Activate an ACL	**packet-filter inbound** { **ip-group** { *acl-number*	*acl-name* } [**rule** *rule*]	**link-group** { *acl-number*	*acl-name* } [**rule** *rule*] } [**not-care-for-interface**]
Deactivate an ACL	**undo packet-filter inbound** { **ip-group** { *acl-number*	*acl-name* } [**rule** *rule*]	**link-group** { *acl-number*	*acl-name* } [**rule** *rule*] } [**not-care-for-interface**]

> **i** > *ARP packets are always permitted to pass through the switch. You can't use the* ***packet-filter*** *command to filter ARP packets.*

See the *Switch 7750 Command Reference Guide* for additional details.

Displaying and Debugging an ACL

After you configure an ACL, execute the **display** command in all views to display the ACL configuration, and to verify the effect of the configuration. Execute the **reset** command in user view to clear the statistics of the ACL module.

Table 168 Display and Debug ACL

Operation	Command
Display the status of the time range	**display time-range** [**all**	*name*]
Display the detail information about the ACL	**display acl config** { **all**	*acl-number*	*acl-name* }
Display the ACL mode chosen by the switch	**display acl mode**

Table 168 Display and Debug ACL

Operation	Command
Display the information about the ACL running state	**display acl running-packet-filter** { **all** | **interface** { *interface-name* | *interface-type interface-num* } }
Clear ACL counters	**reset acl counter** { **all** | *acl-number* | *acl-name* }

The matched information of the **display acl config** command specifies the rules treated by the switch's CPU. The matched information of the transmitted data by the switch can be displayed with the **display qos-info traffic-statistic** command.

For a description of the syntax of these commands, see the *Switch 7750 Command Reference Guide*.

ACL Configuration Examples

This section provides examples for the following configurations:

■ Access Control

■ Basic ACL

■ Link ACL

Access Control

The interconnection between different departments on a company network is implemented through the 100M ports of the Switch 7750. The payment query server of the Financial Dept. is accessed through Ethernet1/0/1 (at 129.110.1.2). The ACL must be properly configured to prevent departments other than the Office of President from having access to the payment query server between 8:00 AM and 6:00 PM. The Office of President (at 129.111.1.2) can access the server without limitation.

Figure 37 Access Control Configuration Example

Office of President
129.111.1.2

Pay query server
129.110.1.2

#3 #4
#1 #2
Switch

Financial Department
subnet address
10.110.0.0

Connected to
a router

Administration Department
subnet address
10.120.0.0
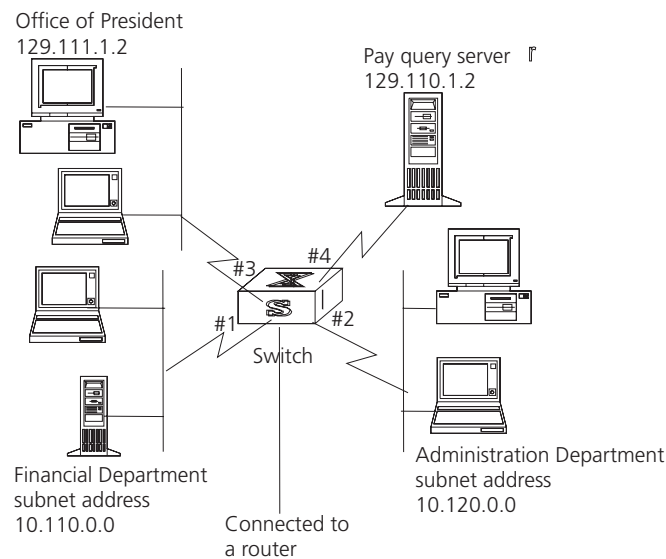
In the following configuration steps, only the commands related to ACL configurations are listed.

Define the work time range:

1 Set the time range 8:00 to 18:00.

```
[SW7750] time-range 3com 8:00 to 18:00 working day
```

Define the ACL to access the payment server:

1 Enter the name of the advanced ACL, named traffic-of-payserver.

```
[SW7750]acl name traffic-of-payserver advanced match-order config
```

2 Set the rules for other department to access the payment server.

```
[SW7750-acl-adv-traffic-of-payserver]rule 1 deny ip source any
destination 129.110.1.2 0.0.0.0 time-range 3com
```

3 Set the rules for the Office of President to access the payment server.

```
[SW7750-acl-adv-traffic-of-payserver]rule 2 permit ip source
129.111.1.2 0.0.0.0 destination 129.110.1.2 0.0.0.0
```

Activate ACL:

1 Activate the traffic-of-payserver ACL .

```
[SW7750-Ethernet2/0/1]qos
[SW7750-qoss-Ethernet2/0/1]packet-filter inbound ip-group
traffic-of-payserver
```

Basic ACL   Using basic ACL, filter the packet with source IP address 10.1.1.1 between 8:00 and 18:00 every day. The host connects to port Ethernet2/0/1 of the switch.

Figure 38   Access Control Configuration Example
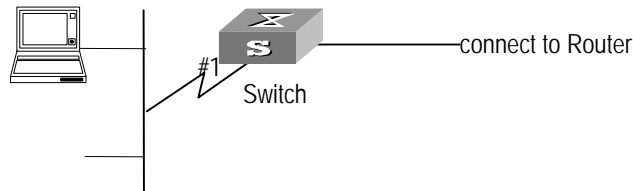
> **i** *In the following configurations, only the commands related to ACL configurations are listed.*

1 Define the time range

Define time range 8:00 to 18:00.

```
[SW7750]time-range 3com 8:00 to 18:00 daily
```

2 Select ACL mode

Select ip-based ACL mode.

```
[SW7750]acl mode ip-based
```

3 Define the ACL for packet with source IP address 10.1.1.1.

Enter the named basic ACL, named as traffic-of-host.

```
[SW7750]acl name traffic-of-host basic
```

Define the rules for packet with source IP address 10.1.1.1.

```
[SW7750-acl-basic-traffic-of-host]rule 1 deny ip source 10.1.1.1 0
time-range 3com
```

4 Activate ACL.

Activate the ACL traffic-of-host .

```
[SW7750-Ethernet2/0/1]qos
[QSW7750-qoss-Ethernet2/0/1]packet-filter inbound ip-group
traffic-of-host
```

Link ACL Using Link ACL, filter the packet whose source MAC address is 00e0-fc01-0101 and destination MAC address is 00e0-fc01-0303 during time range 8:00 to 18:00 every day. The ACL is activated on Ethernet2/0/1.

i *In the following configurations, only the commands related to ACL configurations are listed.*

To configure a link ACL:

1 Define the time range

Define time range 8:00 to 18:00.

```
[SW7750]time-range 3com 8:00 to 18:00 daily
```

2 Select ACL mode

Select link-based ACL mode.

```
[SW7750]acl mode link-based
```

3 Define the ACL for packet whose source MAC address is 00e0-fc01-0101 and destination MAC address is 00e0-fc01-0303.

Enter the named link ACL, named as traffic-of-link.

```
[SW7750]acl name traffic-of-link link
```

Define the rules for a packet whose source MAC address is 00e0-fc01-0101 and destination MAC address is 00e0-fc01-0303.

```
[SW7750-acl-link-traffic-of-link]rule 1 deny ip ingress
00e0-fc01-0101 egress 00e0-fc01-0303 time-range 3com
```

4 Activate ACL.

Activate the ACL traffic-of-link .

```
[SW7750-Ethernet2/0/1]qos
[SW7750-qoss-Ethernet2/0/1]packet-filter inbound link-group
traffic-of-link
```

Configuring QoS In a traditional IP network, all packets are treated equally without priority difference. Every switch or router handles the packets following the first-in first-out (FIFO) policy. Switches and routers make their best effort to transmit the

packets to the destination, not making any commitment or guarantee of the transmission reliability, delay, or to satisfy other performance requirements.

Ethernet technology is currently the most widely used network technology. Ethernet has been the dominant technology of various independent Local Area Networks (LANs), and many Ethernet LANs have been part of the Internet. To implement the end-to-end QoS solution on the whole network, one must consider how to guarantee Ethernet QoS service. This requires the Ethernet switching devices to apply Ethernet QoS technology and deliver the QoS guarantee at different levels to different types of signal transmissions over the networks, especially those having requirements of shorter time delay and lower jitter.

Configuring Qos is described in the following sections:

- Qos Concepts
- Configuring QoS
- QoS Configuration Examples

Qos Concepts   Tasks for configuring Qos Concepts are as follows:

- Traffic
- Traffic Classification
- Packet Filter
- Traffic Policing
- Bandwidth Assurance
- Port Traffic Limit
- Redirection
- Traffic Priority
- Queue Scheduling
- Traffic Mirroring
- Traffic Counting
- RED

Traffic

Traffic refers to all packets passing through a switch.

Traffic Classification

Traffic classification means identifying the packets with certain characteristics. This is done by using a matching rule called the classification rule that is set by the configuration administrator, based on the actual requirements. The rule can be very simple. For example, traffic with different priorities can be identified according to the ToS field in the IP packet header.

There are also some complex rules. For example, the information over the integrated link layer (Layer-2), network layer (Layer-3) and transport layer (Layer-4), such as MAC address, IP protocol, source IP address, destination IP address, and the port number of an application, can be used for traffic classification. Generally,

the classification standards are encapsulated in the header of the packets. The packet content is seldom used as the classification standard.

Packet Filter

Packet filters filter network traffic. For example, the **deny** operation discards the traffic that is matched with a traffic classification rule, while allowing other traffic to pass through. With the complex traffic classification rules, Ethernet switches enable the filtering of information carried in Layer 2 traffic to discard useless, unreliable, or doubtful traffic, and to enhance network security.

To filter packets:

1 Classify the incoming traffic according to the classification rule.

2 Filter the classified traffic.

Traffic Policing

To deliver better service with limited network resources, QoS monitors the traffic of the specific user on the incoming traffic, so it can make better use of the assigned resources.

Bandwidth Assurance

Through the traffic reservation, a minimum bandwidth is reserved for specified traffic flow. Even when network congestion occurs, QoS requirements such as packet dropping ratio, delay, and jitter can also be satisfied.

Port Traffic Limit

The port traffic limit is the port-based traffic limit used for limiting the general speed of packet output on the port.

Redirection

You can specify a new port to forward the packets according to your requirements on the QoS policy.

Traffic Priority

The Switch 7750 can deliver priority tag service for special packets. The tags include TOS, DSCP and 802.1p, etc., which can be used and defined in different QoS modules.

Queue Scheduling

When congestion occurs, packets compete for resources. Strict-Priority Queue (SP) algorithms overcome the problem.

Figure 39 SP
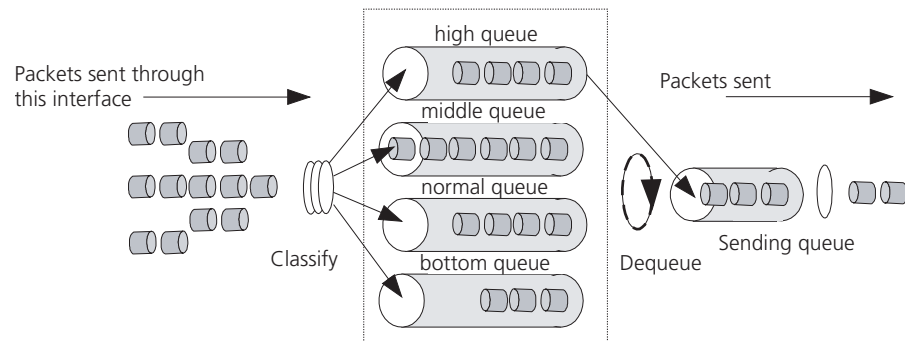
SP is designed for the key service application. A significant feature of the key service is required, for priority to enjoy the service, to reduce the response delay when congestion occurs. Take 4 egress queues for each port as example, SP divides the queue of a port into 4 kinds at most, high-priority, medium-priority, normal-priority and low-priority queues (which are shown as the Queue 3, 2, 1 and 0 in turn) with sequentially reduced priority.

During the progress of queue dispatching, SP strictly follows the priority order from high to low and gives preference, and sends the packets in the higher-priority queue first. When the higher-priority queue is empty, SP sends the packets in the lower-priority groups. In this way, SP can guarantee that key service packets of higher priority are transmitted first, while the packets of lower service priority are transmitted during the idling gap between higher priority

When congestion occurs and many packets are queued in the higher-priority queue, messages in the lower-priority queue are set aside without service until all high-priority messages are transmitted.

Traffic Mirroring

The traffic mirroring function copies the specified data packets to the monitoring port for network diagnosis and troubleshooting.

Traffic Counting

With flow-based traffic counting, you can request a traffic count to count and analyze the packets.

RED

When the congestion reaches a certain degree, the Switch 7750 selects some frames to drop using the RED algorithm. The RED algorithm can alleviate the excessive congestion. Also, the global TCP synchronization caused by the Tail-Drop algorithm can be avoided.

In the RED algorithm, every queue has a pair of high and low limits. This algorithm also regulates that:

■ If the queue length is smaller than the low limit, no packets are discarded.

■ If the queue length is greater than the high limit, all the packets that arrive after the limit is reached are discarded.

■ If the queue length is between the high and low limits, the packets are discarded randomly as they arrive. Every new packet is given a random number.

This random number is compared with the discarding probability for the current queue. Any packet whose random number is greater than the probability is discarded. The longer the queue, the higher the discarding probability . However, there is a maximum discarding probability.

Through randomly discarding packets, RED avoids global TCP synchronism. When some packets of a TCP connection are discarded and the transmission speed is lowered, other TCP connections can still keep the higher transmission speed. In this way, there are always some TCP connections with higher transmission speeds, that make a better use of the line bandwidth.

Configuring QoS   Before you create a QoS configuration, you must define an ACL. Packet filtering is enabled when you create an ACL so packet filtering configuration is not described here.

The following sections describe QoS configuration tasks:

- Setting Port Priority
- Setting Port Mirroring
- Setting Queue Scheduling
- Entering QoS View
- Configuring the Traffic Limit
- Setting Line Limit
- Setting Traffic Bandwidth
- Setting Traffic Redirection
- Relabeling the Priority Level
- Configuring the RED Operation
- Configuring Traffic Statistics
- Displaying and Debugging QoS

The 20-Port 10/100/1000BASE-T and 20-Port 1000BASE-X-SFP I/O modules only support QoS configuration for the inbound packets.

Setting Port Priority

If the received packets contain no VLAN labels, the switch adds the default VLAN and modifies their 802.1p priority levels with port priority levels.

Perform the following configurations in Ethernet interface view.

Table 169   Setting Port Priority

Operation	Command
Set port priority	**priority** *priority-level*
Restore the default priority	**undo priority**

The switch supports eight priority levels, numbered 0~7, according to your needs.

By default, the port priority level is 0.

Perform the following two configuration tasks in system view.

Setting Port Mirroring

Port mirroring means duplicating data on the monitored port to the designated monitor port, for purpose of data analysis and supervision. The switch supports many-to-one mirroring, that is, you can duplicate packets from multiple ports to a monitoring port.

You can also specify the monitoring direction for only inbound or outbound packets.

Perform the following configurations in system view.

Table 170 Setting Port Mirroring

Operation	Command
Set port mirroring	**mirroring-group** *groupid* { **inbound** | **outbound** } *mirroring-port-list* &<1-8> **mirrored-to** *monitor-port*
Remove port mirroring	**undo mirroring-group** *groupid*

You can configure up to 20 mirroring groups, Each group includes one monitoring port and multiple monitored ports.

The monitoring port and the monitored ports must be on the same interface unit.

For a non-48-port interface unit, only one mirroring group can be configured in one direction. For example, you can only configure one mirroring group for the inbound packets on one interface unit. Failure will be prompted if you configure a second. The same restriction applies to outbound packets.

For a 48-port interface unit, the monitoring port and the monitored port must all be at the ports 1~24 or the ports 25~48, at which only one mirroring group can be configured in one direction.

Setting Queue Scheduling

Queue scheduling is often used in solving the problem of resource contention during network congestion.

Each port supports eight outbound queues. The switch only supports SP algorithm, but you can distribute packets into the target queues according to several types of priority. The following tables show the mapping between outbound queues and priority schemes.

Table 171 Mapping Between 802.1p Priority Levels and Outbound Queues

802.1p priority level	Queues
2	0
0	1
1	2
3	3
4	4
5	5
6	6

Table 171   Mapping Between 802.1p Priority Levels and Outbound Queues

802.1p priority level	Queues
7	7

Table 172   Mapping Between Local or IP Priority Levels and Outbound Queues

Local or IP Priority Level	Queue
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

Table 173   Mapping Between DSCP Priority Levels and Outbound Queues

DSCP Value	Name (DSCP value)	Queue
0-7	be(0)	0
8-15	cs1(8), af1(10)	1
16-23	cs2(16), af2(18)	2
24-31	cs3(24), af3(26)	3
32-39	cs4(32), af4(34)	4
40-47	cs5, ef(46)	5
47-55	cs6(48)	6
56-63	cs7(56)	7

Configuring the Mapping List for 802.1p Priority

You cannot modify the mapping between local priority levels and outbound queues, but you can change the mapping between 802.1p and local priority levels. Then the mapping between 802.1p priority levels and outbound queues change.

Perform the following configurations in system view.

Table 174   Setting Mapping Table

Operation	Command
Configure the COS local-precedence mapping table	**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*
Restore the default mapping	**undo qos cos-local-precedence-map**

By default, the switch selects the default mapping.

Configuring the Priority for Queue Scheduling

You can use the following command to configure which priority is used for queue scheduling.

Perform the following configuration in system view.

Table 175   Configuring the Priority for Queue Scheduling

Operation	Command
Configure the priority for queue scheduling	**priority-trust** { **dscp**	**ip-precedence**	**cos**	**local-precedence** }

By default, the switch chooses the local preference as the basic priority.

Entering QoS View

You should run most QoS configurations in QoS view.

Perform the following configuration in Ethernet interface view.

Table 176   Entering QoS View

Operation	Command
Enter QoS view	**qos**

$\boxed{\mathbf{i}}$ *Different I/O modules may support different QoS functions and you can view the QoS configuration items available for the current interface unit by keying in "?" in QoS view.*

$\boxed{\mathbf{i}}$ Only the *20-Port 10/100/1000BASE-T and 20-Port 1000BASE-X-SFP I/O modules* support setting of line rate and packet redirection.

Configuring the Traffic Limit

Traffic limiting establishes actions to deal with the traffic flow that exceeds the threshold. These actions can include discarding packets or lowering priority.

You must define the corresponding ACL before performing this configuration task.

Perform the following configuration in QoS view.

Table 177   Configuring the Traffic Limit

Operation	Command
Configure the flow-based rate limit	**traffic-limit** { **inbound**	**outbound** } { **ip-group** { *acl-number*	*acl-name* } [**rule** *rule*]	**link-group** { *acl-number*	*acl-name* } [**rule** *rule*] } *target-rate* [**exceed** *action*]
Cancel the configuration of the flow-based rate limit	**undo traffic-limit** { **inbound**	**outbound** } { **ip-group** { *acl-number*	*acl-name* } [**rule** *rule*]	**link-group** { *acl-number*	*acl-name* } [**rule** *rule*] }

For details about the command, see the *Switch 7750 Command Reference Guide*.

Setting Line Limit

Line limit refers to limiting the total rate at the port. The adjustment step for the line rate of the Switch 7750 is 1Mbps.

Perform the following configurations in QoS view.

Table 178 Setting the Line Rate

Operation	Command
Set the line limit	**line-rate** *target-rate*
Remove the line limit	**undo line-rate**

You can set line limit at a single port.

Setting Traffic Bandwidth

You can set desired traffic bandwidth to ensure target services.

Perform the following configurations in QoS view.

Table 179 Setting Traffic Bandwidth

Operation	Command
Set traffic bandwidth	**traffic-bandwidth outbound** { **ip-group** { *acl-number* | *acl-name* } [**rule** *rule*] | **link-group** { *acl-number* | *acl-name* } [**rule** *rule*] } *min-guaranteed-bandwidth max-guaranteed-bandwidth weight*
Remove traffic bandwidth setting	**undo traffic-bandwidth outbound** { **ip-group** { *acl-number* | *acl-name* } [**rule** *rule*] | **link-group** { *acl-number* | *acl-name* } [**rule** *rule*] }

Setting Traffic Redirection

Traffic redirection refers to changing packet forwarding direction, that is, forwarding packets to CPU or other ports.

Perform the following configurations in QoS view.

Table 180 Setting Traffic Redirection

Operation	Command
Set traffic redirection	**traffic-redirect inbound** { **ip-group** { *acl-number* | *acl-name* } [**rule** *rule*] | **link-group** { *acl-number* | *acl-name* } [**rule** *rule*] } { **cpu** | **interface** { *interface-name* | *interface-type interface-num* } }
Remove traffic redirection	**undo traffic-redirect inbound** { **ip-group** { *acl-number* | *acl-name* } [**rule** *rule*] | **link-group** { *acl-number* | *acl-name* } [**rule** *rule*] }

Note that the packets cannot be forwarded normally when they are redirected to the CPU.

Traffic redirection is only available to the permitted rules in ACL.

> **i** *Only the 20-Port 10/100/1000BASE-T and 20-Port 1000BASE-X-SFP I/O modules support this configuration.*

Relabeling the Priority Level

Relabeling the priority level creates a policy to tag the priority of the packets so they match the ACL. The new priority can be filled in the priority field of the packet header.

Perform the following configuration in QoS view.

Table 181   Relabeling the Priority Level

Operation	Command
Relabel traffic priority	**traffic-priority** { **inbound**	**outbound** } { **ip-group** { *acl-number*	*acl-name* } [**rule** *rule*]	**link-group** { *acl-number*	*acl-name* } [**rule** *rule*] } { { **dscp** *dscp-value*	**ip-precedence** *pre-value*] [**local-precedence** *pre-value* }* }
Cancel the traffic priority marking	**undo traffic-priority** { **inbound**	**outbound** } { **ip-group** { *acl-number*	*acl-name* } [**rule** *rule*]	**link-group** { *acl-number*	*acl-name* } [**rule** *rule*] }

The Switch 7750 tags the packets with IP precedence (specified by *ip-precedence* in the **traffic-priority** command), or DSCP (specified by *dscp* in the **traffic-priority** command). You can tag the packets with different priorities as required on QoS policy.

For details about the command, see the *Switch 7750 Command Reference Guide*.

Configuring the RED Operation

The RED operation monitors and processes, packet forwarding to prevent network congestion.

> **i** *The 20-Port 10/100/1000BASE-T and 20-Port 1000BASE-X-SFP I/O modules do not support this configuration.*

Perform the following configuration in QoS view.

Table 182   Configure RED Operation

Operation	Command
Configure RED Operation	**traffic-red outbound** { **ip-group** { *acl-number*	*acl-name* } [**rule** *rule*]	**link-group** { *acl-number*	*acl-name* } [**rule** *rule*] } *qstart qstop probability*
Cancel the configuration of RED Operation	**undo traffic-red outbound** { **ip-group** { *acl-number*	*acl-name* } [**rule** *rule*]	**link-group** { *acl-number*	*acl-name* } [**rule** *rule*] }

For details about the command, see the *Switch 7750 Command Reference Guide*.

Configuring Traffic Statistics

The traffic statistics function counts the transmitted data that matches the ACL rules. After the traffic statistics function is configured, you can use the **display qos-info traffic-statistic** command to display the statistics information.

Perform the following configuration in QoS view.

Table 183 Configuring Traffic Statistics

Operation	Command
Configure traffic statistics	**traffic-statistic** { **inbound**	**outbound** } { **ip-group** { *acl-number*	*acl-name* } [**rule** *rule*]	**link-group** { *acl-number*	*acl-name* } [**rule** *rule*] }
Cancel the traffic statistics configuration	**undo traffic-statistic** { **inbound**	**outbound** } { **ip-group** { *acl-number*	*acl-name* } [**rule** *rule*]	**link-group** { *acl-number*	*acl-name* } [**rule** *rule*] }
Display the statistics information	**display qos-info traffic-statistic** [interface-name	interface-type	interface-num] **traffic-statistic**

For details about the command, see the *Switch 7750 Command Reference Guide*.

Displaying and Debugging QoS

After you configure QoS, execute the **display** command in all views to display the QoS configuration, and to verify the effect of the configuration. Execute the **reset** command in user view to clear the statistics of the QoS module.

Table 184 Display and Debug QoS

Operation	Command
Display port mirroring configuration	**display mirroring-group** [*groupid*]
Display the mapping relationship between cos and local precedence	**display qos cos-local-precedence-map**
Display line rate for outbound packets	**display qos-interface** [*interface-name*	*interface-type interface-num*] **line-rate**
Display traffic redirection	**display qos-interface** [*interface-name*	*interface-type interface-num*] **traffic-redirect**
Display the parameter settings of all the QoS actions	**display qos-interface** [*interface-name*	*interface-type interface-num*] **all**
Display the queue scheduling mode and parameter	**display qos-interface** [*interface-name*	*interface-type interface-num*] **queue-scheduler**
Display the parameter settings of rate limit	**display qos-interface** [*interface-name*	*interface-type interface-num*] **traffic-limit**
Display the settings of priority tag	**display qos-interface** [*interface-name*	*interface-type interface-num*] **traffic-priority**
Display information about the traffic	**display qos-interface** [*interface-name*	*interface-type interface-num*] **traffic-statistic**
Display the information about traffic bandwidth	**display qos-interface** [*interface-name*	*interface-type interface-num*] **traffic-bandwidth**
Display the information about the RED operation	**display qos-interface** [*interface-name*	*interface-type interface-num*] **traffic-red**

Table 184   Display and Debug QoS

Operation	Command
Display the settings of priority used for putting the packet to the sending queue	**display priority-trust**
Clear the statistics information	**reset traffic-statistic** { inbound	outbound } { **all**	**ip-group** { *acl-number*	*acl-name* } [**rule** *rule*]	**link-group** { *acl-number*	*acl-name* } [**rule** *rule*] }

For output and description of the related commands, see the *Switch 7750 Command Reference Guide*.

QoS Configuration Examples

This section provides the following configuration examples:

- Traffic Limit and Line Rate
- Port Mirroring
- Priority Relabeling Configuration Example
- Packet Redirection
- Queue Scheduling
- RED
- Traffic Bandwidth
- Traffic Statistics

Traffic Limit and Line Rate

In this example, the intranet is connected through 100M ports between departments, and the wage server is connected through the port GigabitEthernet7/0/1 (subnet address 129.110.1.2). For the wage server, the inbound traffic is limited to 20M and the outbound traffic to 20M, on average. Those packets exceeding the threshold are labeled with priority level 4.

> **i** *Only the 20-Port 10/100/1000BASE-T and 20-Port 1000BASE-X-SFP I/O modules support further processing for excessive traffic.*
>
> *Only the 20-Port 10/100/1000BASE-T and 20-Port 1000BASE-X-SFP I/O modules support line rate setting.*
>
> *For the 20-Port 10/100/1000BASE-T and 20-Port 1000BASE-X-SFP I/O modules, the adjustment step for both traffic limit and line rate is 1 Mbps, but for other interface units, the adjustment step for traffic limit is 64 Kbps.*

Figure 40 Traffic Limit and Line Rate Configuration
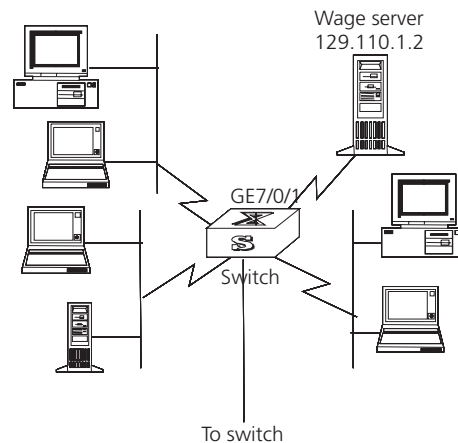
i *Only the commands concerning QoS/ACL configuration are listed here.*

To create this configuration:

1 Define outbound traffic for the wage server.

Enter name-based advanced ACL view using the traffic-of-payserver.

```
[SW7750]aclname traffic-of-payserver advanced
```

Define the traffic-of-payserver rule in the advanced ACL.

```
[SW7750-acl-adv-traffic-of-payserver]rule 1 permit ip source
129.110.1.2 0.0.0.0 destination any
```

2 Set traffic limit for the wage server.

Enter QoS view.

```
[SW7750-GigabitEthernet7/0/1]qos
[SW7750-qosb-GigabitEthernet7/0/1]
```

Limit average outbound traffic of the wage server to 20 Mbps and label over-threshold packets with priority level 4.

```
[SW7750-qosb-GigabitEthernet7/0/1]traffic-limit inbound ip-group
traffic-of-payserver 20 exceed remark-dscp 4
```

Limit inbound traffic of the wage server from the port GigabitEthernet7/0/1 to 20 Mbps.

```
[SW7750-qosb-GigabitEthernet7/0/1]line-rate 20
```

Port Mirroring

This configuration uses one server to monitor the packets of two PCs. One PC is accessed from the port E3/0/1 and the other from the port E3/0/2. The server is connected to the port Ethernet3/0/8.

i *The monitoring port and the monitored ports must be on the same I/O module.*

For a non-48-port module, only one mirroring group can be configured in one direction. For example, you can only configure one mirroring group for the inbound packets on one module. The configuration will fail if you configure a second mirroring group. The same restriction applies to outbound packets.

For a 48-port module, the monitoring port and the monitored port must all be at the ports 1-24 or ports 25-48, on which only one mirroring group can be configured in one direction.

Figure 41 Port Mirroring Configuration
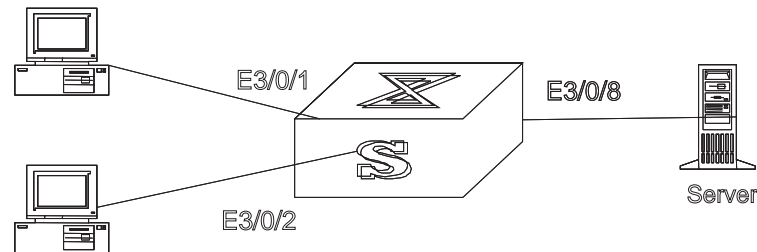
To create this configuration:

Define a mirroring group, with monitoring port being Ethernet0/8:

```
[SW7750]mirroring-group 1 inbound ethernet3/0/1 ethernet3/0/2
mirrored-to ethernet3/0/8
[SW7750]mirroring-group 2 outbound ethernet3/0/1 ethernet3/0/2
mirrored-to ethernet3/0/8
```

Priority Relabeling Configuration Example

In this example, **ef** labels are appended on packets sent between 8:00 and 18:00 each day from PC1 (IP 1.0.0.2), as priority labeling reference for the upper-layer device.

Figure 42 Priority Relabeling Configuration
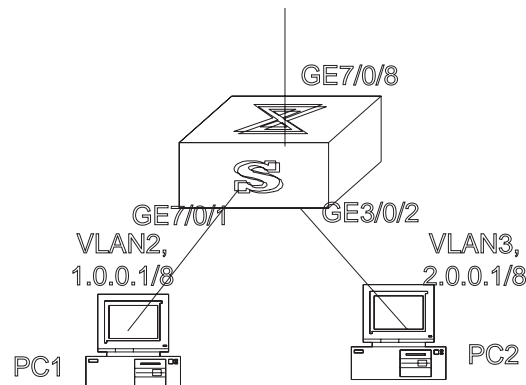
To create this configuration:

1 Define the time range.

Define the time range between 8:00 and 18:00.

```
[SW7750]time-range 3com 8:00 to 18:00 daily
```

2 Define traffic rules for PC packets.

Enter the number-based basic ACL and select the ACL 2000.

```
[SW7750]acl number 2000
```

Define traffic classification rules for PC1 packets.

```
[SW7750-acl-basic-2000]rule 0 permit ip source 1.0.0.2 0 time-range
3com
```

3 Relabel ef priority for PC1 packets.

Enter QoS view.

```
[SW7750-GigabitEthernet7/0/1]qos
[SW7750-qosb-GigabitEthernet7/0/1]
```

Relabel ef priority for PC1 packets.

```
[SW7750-qosb-GigabitEthernet7/0/1]traffic-priority inbound ip-group
1 dscp ef
```

Packet Redirection

In this example, packets sent 8:00~18:00 each day are forwarded from PC1 (IP 1.0.0.2) to the port GE7/0/8.

Only the 20-Port 10/100/1000BASE-T and 20-Port 1000BASE-X-SFP I/O modules support packet redirection.

Figure 43   Packet Redirection
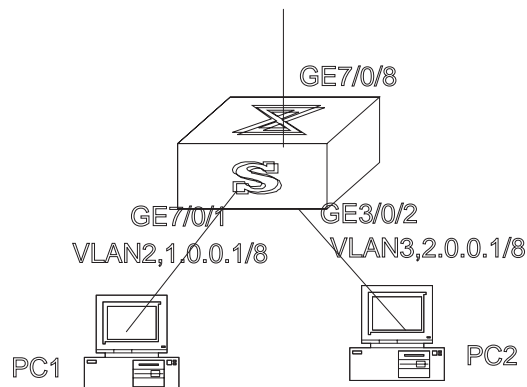
To create this configuration:

1 Define the time range 8:00 to 18:00.

```
[SW7750]time-range 3com 8:00 to 18:00 daily
```

2 Define traffic rules for PC1 packets.

Enter the number-based basic ACL and select ACL 2000.

```
[SW7750]acl number 2000
```

Define traffic classification rules for PC1 packets.

```
[SW7750-acl-basic-2000]rule 0 permit ip source 1.0.0.2 0 time-range
3com
```

3 Forward PC1 packets to the port GE7/0/8.

Enter QoS view.

```
[SW7750-GigabitEthernet7/0/1]qos
[SW7750-qosb-GigabitEthernet7/0/1]
```

Forward PC1 packets to the port GE7/0/8.

```
[SW7750-qosb-GigabitEthernet7/0/1]traffic-redirect inbound ip-group
1 rule 0 interface gigabitetherent7/0/8
```

Queue Scheduling

Modify the correspondence between 802.1p priority levels and local priority levels
to change the mapping between 802.1p priority levels and queues. That is, put
packets into outbound queues according to the new mapping. Use WRR
algorithm, and the weight for different queues is respectively 5, 5, 10, 10, 15, 15,
9 and 9. The mapping between the modified 802.1p priority levels and the local
priority levels is listed in the following figure (See Queue Scheduling for the default
mapping).

Table 185 Modifying Mapping Between 802.1p and Local Priority Levels

802.1p Priority Level	Local Priority Level
0	7
1	6
2	5
3	4
4	3
5	2
6	1
7	0

i *The 20-Port 10/100/1000BASE-T and 20-Port 1000BASE-X-SFP I/O modules
support SP, WRR and RR algorithm.*

Other interface units support only SP algorithm.

Figure 44 Queue Scheduling
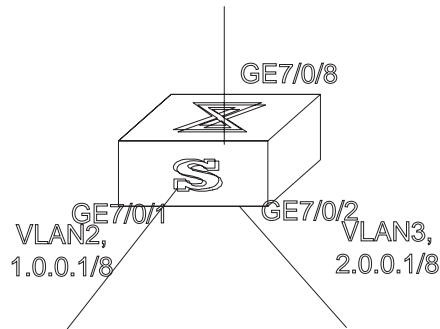
To create this configuration:

1 Respecify mapping between 802.1p priority levels and local priority levels.

```
[SW7750]qos cos-local-precedence-map 7 6 5 4 3 2 1 0
```

2 Define WRR algorithm for the switch and specify the weight of outbound queues
as 5, 5, 10, 10, 15, 15, 9 and 9.

```
[SW7750]queue-scheduler wrr 5 5 10 10 15 15 9 9
```

3 View the configuration with the display command.

```
[SW7750]display queue-scheduler
```

RED

Run the RED operation for the packets sent between 8:00 and 18:00 every day from IP address 1.0.0.1 to the port E3/0/8. RED operation is set so that the queue length that triggers random discarding ranges from 64 Kbytes to 128 Kbytes. The probability for random discarding is 20%.

> **i** *The 20-Port 10/100/1000BASE-T and 20-Port 1000BASE-X-SFP I/O modules do not support this configuration.*

Figure 45   RED
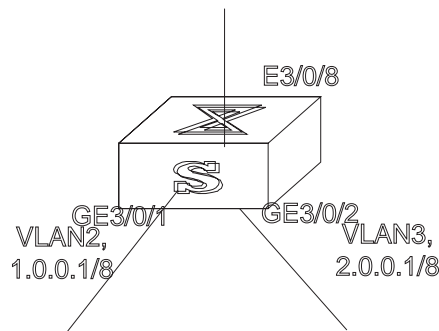
To create this configuration:

1 Define the time range 8:00 to 18:00.

Define the time range.

```
[SW7750]time-range 3com 8:00 to 18:00 daily
```

2 Define traffic rules for the packets of IP address 1.0.0.1.

```
[SW7750]acl number 2000
[SW7750-acl-basic-2000]rule 0 permit ip source 1.0.0.1 0.0.0.0
time-range 3com
```

3 Run the RED operation for the packets of IP address 1.0.0.1 and view the configuration with the **display** command.

Enter QoS view.

```
[SW7750-Ethernet3/0/8]qos
[SW7750-qoss-Ethernet3/0/8]
```

Run RED operation for the packets of IP address 1.0.0.1 and view the configuration with the **display** command.

```
[SW7750-qoss-Ethernet3/0/8]traffic-red outbound ip-group 1 rule 0
[SW7750]display qos-interface Ethernet3/0/8 traffic-red
```

Traffic Bandwidth

For the packets sent between 8:00 and 18:00 each day to the port E3/0/8, the minimum bandwidth for those of source IP address 1.0.0.1 is 20M, the maximum bandwidth is 60M, with bandwidth weight of 40. The minimum bandwidth for those of source IP address 2.0.0.1 is 20M; maximum bandwidth is 60M, with bandwidth weight of 60.

i⟩ *The 20-Port 10/100/1000BASE-T and 20-Port 1000BASE-X-SFP I/O modules do not support this configuration.*

Figure 46 Traffic Bandwidth
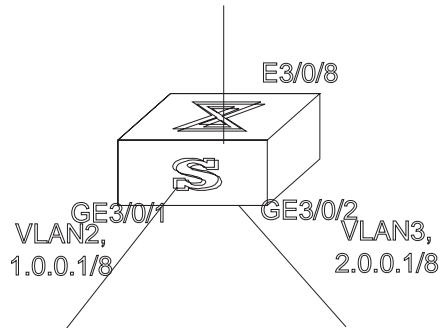
To create this configuration:

1 Define the time range 8:00 to 18:00.

```
[SW7750]time-range 3com 8:00 to 18:00 daily
```

2 Define traffic rules for the packets of IP addresses 1.0.0.1 and 2.0.0.1.

```
[SW7750]acl number 2000
[SW7750-acl-basic-2000]rule 0 permit ip source 1.0.0.1 0.0.0.0
time-range 3com
[SW7750-acl-basic-2000]rule 1 permit ip source 2.0.0.1 0.0.0.0
time-range 3com
```

3 Configure traffic bandwidth for the packets of IP addresses 1.0.0.1 and 2.0.0.1, view the configuration with the **display** command.

Enter QoS view.

```
[SW7750-Ethernet3/0/8]qos
[SW7750-qoss-Ethernet3/0/8]
```

Configure traffic bandwidth for the packets of IP addresses 1.0.0.1 and 2.0.0.1, view the configuration with the **display** command.

```
[SW7750-qoss-Ethernet3/0/8]traffic-bandwidth outbound ip-group 1
rule 0 20 60 40
[SW7750-qoss-Ethernet3/0/8]traffic-bandwidth outbound ip-group 1
rule 1 40 60 60
[SW7750]display qos-interface Ethernet3/0/8 traffic-bandwidth
```

Traffic Statistics

In this example, the IP address of the PC1 is 1.0.0.1 and the address of PC2 is 2.0.0.2. The switch is uplinked through the port GE7/0/8. Count the packets sent between 8:00 and 18:00 each day from the switch to PC1.

Figure 47 Traffic Statistics
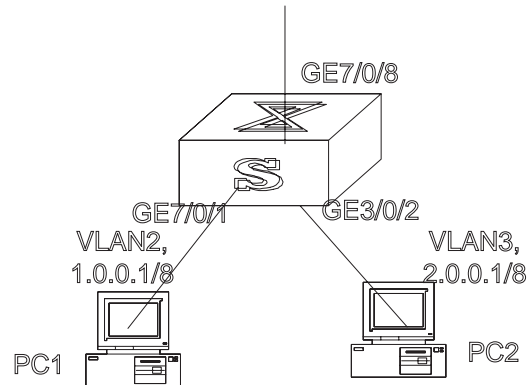
To create this configuration:

1 Define the time range 8:00 to 18:00.

```
[SW7750]time-range 3com 8:00 to 18:00 daily
```

2 Define traffic rules for PC1 packets.

```
[SW7750]acl number 2000
[SW7750-acl-basic-2000]rule 0 permit ip source 1.0.0.1 0.0.0.0
time-range 3com
```

3 Count PC1 packets, view the statistics with the **display** command.

Enter QoS view.

```
[SW7750-GigabitEthernet7/0/1]qos
[SW7750-qosb-GigabitEthernet7/0/1]
```

Count PC1 packets, view the statistics with the **display** command.

```
[SW7750-qosb-GigabitEthernet7/0/1]traffic-statistic inbound ip-group
1 rule 0
[SW7750]display qos-interface GigabitEthernet7/0/1 traffic-statistic
```

Configuring ACL Control

The Switch 7750 provides several logon and device access measures, including TELNET access, SNMP access, and HTTP access. The security control, over the access measures, is provided with the switches to prevent illegal users from logging onto and accessing the devices. There are two levels of security controls. At the first level, the user connection is controlled with an ACL filter and only legal users can be connected to the switch. At the second level, a connected user can log on to the device only if the user can pass the password authentication.

This chapter introduces how to configure the first level security control to filter the logon users with ACL. For the information about how to configure the first level security, see "System Access".

Configuring ACL Control is described in the following sections:

■ Configuring ACL Control for TELNET Users

■ Configuring ACL Control for SNMP Users

Configuring ACL Control for TELNET Users

By configuring ACL control over TELNET, users can filter the malicious and illegal connection requests before password authentication, and ensure device security.

The steps to control TELNET users with ACL are described in the following sections:

■ Defining an ACL

■ Importing an ACL

Defining an ACL

To implement the ACL control function, you can only call the numbered basic ACL, ranging from 2000 to 2999.

Perform the following configuration in system view.

Table 186 Defining a Basic ACL

Operation	Command
Enter basic ACL view (from system view)	**acl** { **number** *acl-number* | **name** *acl-name* **basic ip** } [**match-order** { **config** | **auto** }]
Add a sub-item to the ACL (from basic ACL view)	**rule** [*rule-id*] { **permit** | **deny** } [**source** *source-addr source-wildcard* | **any**] [**fragment**] [**time-range** *name*]
Delete a sub-item from the ACL (from basic ACL view)	**undo rule** *rule-id* [**source**] [**fragment**] [**time-range**]
Delete one ACL or all the ACL (from system view)	**undo acl** { **number** *acl-number* | **name** *acl-name* | **all** }

In the definition process, you can configure multiple rules for an ACL, using the **rule** command repeatedly.

Importing an ACL

To implement ACL control, you can import the defined ACL in user interface view.

Perform the following configuration in the designated view.

Table 187 Importing an ACL

Operation	Command
Enter user-interface view (from system view)	**user-interface** [*type*] *first-number* [*last-number*]
Call an ACL (from user-interface view)	**acl** *acl-number* { **inbound** | **outbound** }

For more information about the command, see the *Switch 7750 Command Reference Guide*.

Only a numbered basic ACL can be imported for TELNET user control.

Example: Controlling TELNET Users with ACL

Figure 48 illustrates a configuration that controls TELNET users with an ACL.

Figure 48 Control TELNET User With ACL

Switch
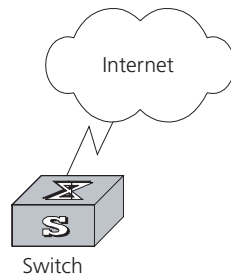
Use the following commands to control TELNET users with ACL.

1 Define the basic ACLs.

```
[SW7750]acl number 2000 match-order config
[SW7750-acl-basic-2000]rule 1 permit source 10.110.100.52 0
[SW7750-acl-basic-2000]rule 2 permit source 10.110.100.46 0
[SW7750-acl-basic-2000]quit
```

2 Call an ACL.

```
[SW7750]user-interface vty 0 4
[SW7750-user-interface-vty0-4]acl 2000 inbound
```

Configuring ACL Control for SNMP Users

The Switch 7750 supports remote management with the network management software. The network management users can access the switch with SNMP. Controlling such users with an ACL can filter the illegal network management users, and prevent them from accessing the local switch.

The steps to control SNMP users with ACL are described in the following sections:

- Defining an ACL
- Importing an ACL to Control SNMP Users

Defining an ACL

To implement the ACL control function, you can only call the numbered basic ACL, ranging from 2000 to 2999. Use the configuration commands introduced in "Configuring ACL Control for TELNET Users".

Importing an ACL to Control SNMP Users

To control network management users with an ACL, import the defined ACL when configuring the SNMP community name, username, and group name.

Perform the following configuration in system view.

Table 188 Define a Numbered Basic ACL

Operation	Command
Import an ACL when configuring the SNMP community name	**snmp-agent community** { **read**	**write** } *community-name* [[**mib-view** *view-name*]	[**acl** *acl-number*]]*

Table 188 Define a Numbered Basic ACL

Operation	Command
Import an ACL when configuring SNMP group name.	**snmp-agent group** { **v1** | **v2c** } *group-name* [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*] [**acl** *acl-number*] **snmp-agent group v3** *group-name* [**authentication** | **privacy**] [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*] [**acl** *acl-number*]
Import an ACL when configuring SNMP username.	**snmp-agent usm-user** { **v1** | **v2c** } *user-name group-name* [**acl** *acl-number*] **snmp-agent usm-user v3** *user-name group-name* [**authentication-mode** { **md5** | **sha** } *auth-password*] [**privacy des56** *priv-password*] [**acl** *acl-number*]

> *The **privacy-mod** priv-password parameters are supported only in the extended version of the software.*

SNMP community is one of the features of SNMP v1 and SNMP v2, so with these versions of SNMP, you can import the ACL into the commands with SNMP community already configured.

SNMP username or group name is one of the features of SNMP V2 and above, so with these versions of SNMP, you import the ACL into the commands with SNMP username or group name already configured. If you import the ACL into both features, the switch will filter both features for the users.

> *You can call different ACLs for these commands. Only the numbered basic ACL can be called for network management user control.*

For more about the commands, see the *Switch 7750 Command Reference Guide*.

Example: Controlling SNMP Users with an ACL

Figure 49 illustrates a configuration that controls SNMP users with ACL.

Figure 49 Control SNMP User With ACL
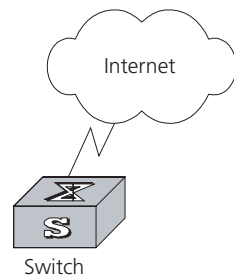
Use the following commands to control SNMP users with ACL.

1 Define the basic ACLs.

```
[SW7750]acl number 2000 match-order config
[SW7750-acl-basic-2000]rule 1 permit source 10.110.100.52 0
[SW7750-acl-basic-2000]rule 2 permit source 10.110.100.46 0
[SW7750-acl-basic-2000]quit
```

2 Import the basic ACLs.

```
[SW7750]snmp-agent community read 3com acl 2000
[SW7750]snmp-agent group v2c 3comgroup acl 2001
[SW7750]snmp-agent usm-user v2c 3comuser 3comgroup acl 2002
```

8
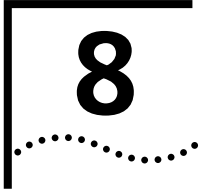
STP OPERATION

This chapter covers the following topics:

- STP Overview
- Configuring STP
- MSTP Overview
- Configuring MSTP

STP Overview

Spanning Tree Protocol (STP) is applied in a loop network to block undesirable redundant paths. Using STP avoids the proliferation and infinite cycling of a packet in a loop network.

The fundamental feature of STP is that the switches exchange packets called configuration Bridge Protocol Data Units, or BPDU, to decide the topology of the network. The configuration BPDU contains the information that ensures that switches can compute the spanning tree.

The configuration BPDU contains the following information:

- The root ID consisting of root priority and MAC address
- The cost of the shortest path to the root
- A designated switch ID consisting of designated switch priority and MAC address
- A designated port ID consisting of port priority and port number
- The age of the configuration BPDU (MessageAge)
- The maximum age of the configuration BPDU (MaxAge)
- A configuration BPDU interval (HelloTime)
- A forward delay of the port (ForwardDelay)

Configuring STP

STP configuration is described in the following sections:

- Designating Switches and Ports
- Calculating the STP Algorithm
- Generating the Configuration BPDU
- Selecting the Optimum Configuration BPDU
- Designating the Root Port
- Configuring the BPDU Forwarding Mechanism

Designating Switches and Ports

A designated switch is a switch in charge of forwarding packets to the local switch by a port called the designated port. For a LAN, the designated switch is a switch that forwards packets to the network segment by the designated port.

As illustrated in Figure 50, Switch A forwards data to Switch B through Ethernet port 1/0/1. So to Switch B, the designated switch is Switch A and the designated port is Ethernet 1/0/1 of Switch A. Also, Switch B and Switch C are connected to the LAN and Switch B forwards packets to the LAN. So the designated switch of the LAN is Switch B and the designated port is Ethernet 1/0/4 of Switch B.

Figure 50   Designated Switch and Designated Port
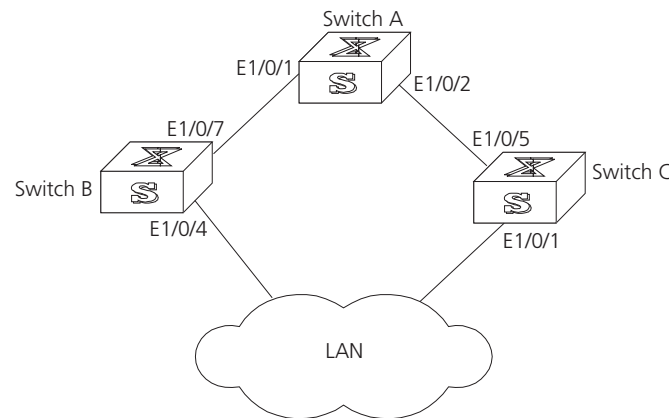
Calculating the STP Algorithm

The following example illustrates the calculation process of STP.

The Figure 51 illustrates the network.

Figure 51   Switch 7750 Networking
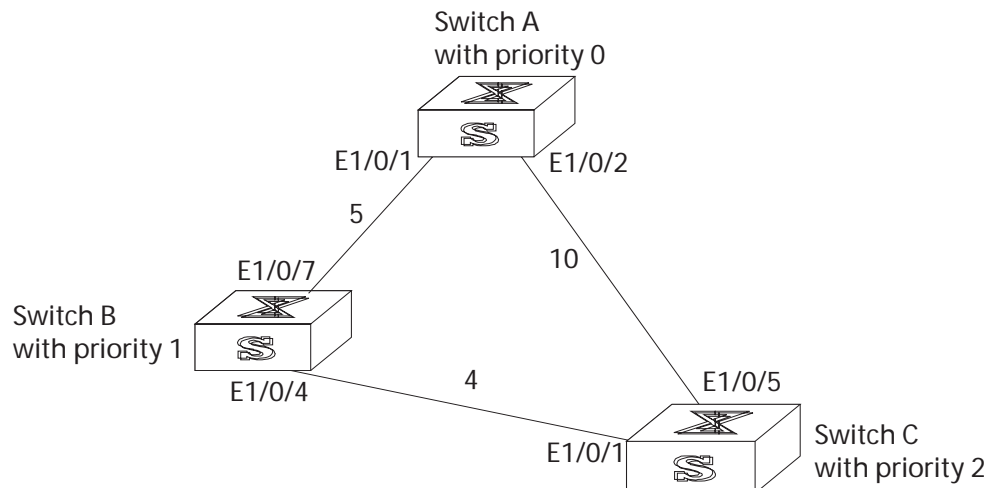
Only the first four parts of the configuration BPDU are given in the example. They are root ID (expressed as Ethernet switch priority), path cost to the root, designated switch ID (expressed as Ethernet switch priority) and the designated port ID (expressed as the port number). As illustrated in the figure above, the priorities of Switch A, B and C are 0, 1, and 2 and the path costs of their links are 5, 10, and 4.

| **Generating the Configuration BPDU** | When initialized, each port of the switches will generate the configuration BPDU taking itself as the root, root path cost as 0, designated switch IDs as their own switch IDs, and the designated ports as their ports. |

- Switch A

  Configuration BPDU of Ethernet 1/0/1: {0, 0, 0, e1/0/1}

  Configuration BPDU of Ethernet 1/0/2: {0, 0, 0, e1/0/2}

- Switch B

  Configuration BPDU of Ethernet 1/0/7: {1, 0, 1, e1/0/7}

  Configuration BPDU of Ethernet 1/0/4: {1, 0, 1, e1/0/4}

- Switch C

  Configuration BPDU of Ethernet 1/0/1: {2, 0, 2, e1/0/1}

  Configuration BPDU of Ethernet 1/0/5: {2, 0, 2, e1/0/5}

Selecting the Optimum Configuration BPDU

Every switch transmits its configuration BPDU to others. When a port receives a configuration BPDU with a lower priority than that of its own, it will discard the message and keep the local BPDU unchanged. When a higher-priority configuration BPDU is received, the local configuration BPDU will be updated.

The optimum configuration BPDU will be elected through comparing the configuration BPDUs of all the ports.

The comparison rules are:

- The configuration BPDU with a smaller root ID has a higher priority

- If the root IDs are the same, perform the comparison based on root path costs. The cost comparison is as follows: the path cost to the root recorded in the configuration BPDU plus the corresponding path cost of the local port is set as X, the configuration BPDU with a smaller X has a higher priority.

- If the costs of a path to the root are the same, compare, in sequence, the designated switch ID, designated port ID, and the ID of the port through which the configuration BPDU was received.

Designating the Root Port

On a bridge, the port receiving the optimum configuration BPDU is considered the root port whose configuration BPDU remains the same. Any other port, whose configuration BPDU has been updated, as explained in "Selecting the Optimum Configuration BPDU", will be blocked and will not forward any data. In addition, any other port only receives, but does not retransmit, a BPDU and its BPDU remains the same.

On other bridges, a port whose BPDU has not been updated is called the designated port. Its configuration BPDU is modified by substituting:

- The root ID with the root ID in the configuration BPDU of the root port

- The cost of path to root with the value made by the root path cost, plus the path cost corresponding to the root port

- The designated switch ID with the local switch ID

- The designated port ID with the local port ID

The comparison process of each switch is:

- Switch A

    Ethernet 1/0/1 receives the configuration BPDU from Switch B and finds out that the local configuration BPDU priority is higher than that of the received one, so it discards the received configuration BPDU.

    The configuration BPDU is processed on the Ethernet 1/0/2 in a similar way. Thus, Switch A finds itself the root and designated switch in the configuration BPDU of every port; it regards itself as the root, retains the configuration BPDU of each port and transmits configuration BPDU to others regularly thereafter. By now, the configuration BPDUs of the two ports are as follows:

    Configuration BPDU of Ethernet 1/0/1: {0, 0, 0, e1/0/1}

    Configuration BPDU of Ethernet 1/0/2: {0, 0, 0, e1/0/2}

- Switch B

    Ethernet 1/0/7 receives the configuration BPDU from Switch A and finds that the received BPDU has a higher priority than the local one, so it updates its configuration BPDU.

    Ethernet 1/0/4 receives the configuration BPDU from Switch C and finds that the local BPDU priority is higher than that of the received one, so it discards the received BPDU.

    By now the configuration BPDUs of each port are as follows:

    Configuration BPDU of Ethernet 1/0/7: {0, 0, 0, e1/0/1}

    Configuration BPDU of Ethernet 1/0/4: {1, 0, 1, e1/0/4}

    Switch B compares the configuration BPDUs of the ports and selects the Ethernet 1/0/7 BPDU as the optimum one. Thus, Ethernet 1/0/7 is elected as the root port and the configuration BPDUs of Switch B ports are updated as follows.

    The configuration BPDU of the root port Ethernet 1/0/7 remains {0, 0, 0, e1/0/1}. Ethernet 1/0/4 updates the root ID with the root ID in the optimum configuration BPDU, updates the path cost to root with 5, sets the designated switch as the local switch ID and the designated port ID as the local port ID. Thus, the configuration BPDU becomes {0, 5, 1, e1/0/4}.

    All the designated ports of Switch B then transmit the configuration BPDUs regularly.

- Switch C

    Ethernet 1/0/1 receives from the Ethernet 1/0/4 of Switch B, the configuration BPDU {1, 0, 1, e1/0/4} that has not been updated, then the updating process is launched. {1, 0, 1, e1/0/4}.

    Ethernet 1/0/5 receives the configuration BPDU {0, 0, 0, e1/0/2} from Switch A, and Switch C launches the updating. The configuration BPDU is updated as {0, 0, 0, e1/0/2}.

    By comparison, the Ethernet 1/0/5 configuration BPDU is elected as the optimum one. The Ethernet 1/0/5 is thus specified as the root port with no modifications made on its configuration BPDU. However, Ethernet 1/0/1 is blocked and its BPDU also remains the same, but it will not receive the data (excluding the STP packet) forwarded from Switch B until spanning tree

calculation is launched again by new events, for example, the link from Switch B to C is down or the port receives a better configuration BPDU.

Ethernet 1/0/1 receives the updated configuration BPDU, {0, 5, 1, e1/0/4}, from Switch B. Since this configuration BPDU is better then the old one, the old BPDU will be updated to {0, 5, 1, e1/0/4}.

Meanwhile, Ethernet 1/0/5 receives the configuration BPDU from Switch A but its configuration BPDU is not updated and remains {0, 0, 0, e1/0/2}.

By comparison, the configuration BPDU of Ethernet 1/0/1 is elected as the optimum one. Ethernet 1/0/1 is elected as the root port, whose BPDU does not change, while Ethernet 1/0/5 is blocked and retains its BPDU, but it does not receive the data forwarded from Switch A until spanning tree calculation is triggered again by changes, for example, the link from Switch B to C is down.

Thus the spanning tree is stabilized. The tree with the root Switch A is illustrated in Figure 52.

Figure 52   The Final Stabilized Spanning Tree
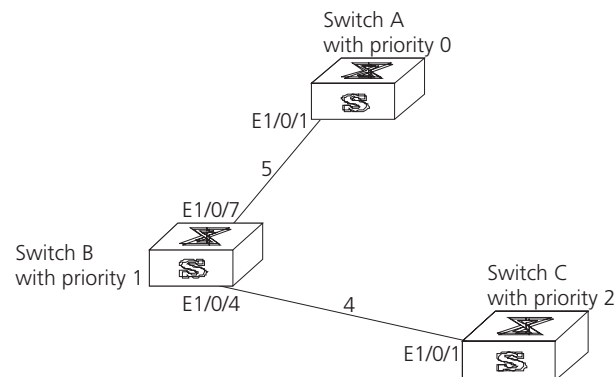
The root ID and the designated switch ID, in actual calculation, should include both switch priority and switch MAC address. The designated port ID should include port priority and port MAC address. In the updating process of a configuration BPDU, other configuration BPDUs besides the first four items make modifications according to certain rules. The basic calculation process is described below.

Configuring the BPDU Forwarding Mechanism

Upon the initiation of the network, all the switches regard themselves as the roots. The designated ports send the configuration BPDUs of local ports at a regular interval of HelloTime. If it is the root port that receives the configuration BPDU, the switch will enable a timer to time the configuration BPDU, as well as increase MessageAge carried in the configuration BPDU by certain rules. If a path goes wrong, the root port on this path will not receive configuration BPDUs anymore, and the old configuration BPDUs will be discarded due to timeout. Recalculation of the spanning tree will be initiated to generate a new path to replace the failed one, and thus restore the network connectivity.

The new configuration BPDU as now recalculated will not be propagated throughout the network right away, so the old root ports and designated ports, that have not detected the topology change, will continue to forward the data through the old path. If the new root port and designated port begin to forward data immediately after they are elected, a occasional loop may still occur. In RSTP,

a transitional state mechanism is then adopted to ensure the new configuration BPDU has been propagated throughout the network before the root port and designated port begin to send data again. That is, the root port and designated port should undergo a transitional state for a period of Forward Delay before they enter the forwarding state.

MSTP Overview

The Switch 7750 implements the Multiple Spanning Tree Protocol (MSTP), which is an enhancement to STP, and is compatible with both STP and RSTP. An MSTP switch can recognize both STP and RSTP packets and can calculate the spanning tree with them. Beside the basic MSTP functions, the Switch 7750 provides additional MSTP features which include root bridge hold, secondary root bridge, root protection, and BPDU protection.

STP cannot stabilize a network rapidly. Even on the point-to-point link or the edge port, it takes an interval as long as twice the forward delay before the network converges.

MSTP makes the network converge rapidly, and distributes the traffic of different VLANs along their respective paths. This provides a better load-balance mechanism for the redundant links.

MSTP associates VLAN with a spanning tree domain, and divides a switching network into several regions, each of which has a spanning tree independent of one another. MSTP prunes the network into a loopfree tree to avoid proliferation, it also provides multiple redundant paths for data forwarding to implement the VLAN data forwarding load-balance.

Configuring MSTP is described in the following sections:

- MSTP Concepts
- MSTP Principles

MSTP Concepts

MSTP Concepts are described in the following sections

- MST Region
- VLAN Mapping Table
- Internal Spanning Tree (IST)
- Common Spanning Tree (CST)
- Common and Internal Spanning Tree (CIST)
- Multiple Spanning Tree Instance (MSTI)
- MSTI Region root
- Common Root Bridge
- Boundary port
- Port role

There are 4 MST regions in Figure 53.

Figure 53   MSTP Concepts

Region A0
vlan 1 mapped to Instance 1
vlan 2 mapped to Instance 2
Other vlans mapped to CIST

CIST: Common and Internal Spanning Tree
MSTI: Multiple SpanningTree Instance

Region A0
vlan 1 mapped to Instance 1,
    region root B
vlan 2 and 3 mapped to
    Instance 2, region root C
Other vlans mapped to CIST

CST: Common
Spanning Tree

Region B0
vlan 1 mapped to Instance 1
vlan 2 mapped to Instance 2
Other vlans mapped to CIST

Region C0
vlan 1 mapped to Instance 1
vlan 2 and 3 mapped to Instance 2
Other vlans mapped to CIST

MST Region

A multiple spanning tree region contains several physically and directly connected MSTP-capable switches sharing the same region name, VLAN-spanning tree mapping configuration and MSTP revision level configuration, and the network segments between them. There can be several MST regions on a switching network. You can group several switches into a MST region, using MSTP configuration commands. For example, in Figure 53, in MST region A0, the 4 switches are configured with the same region name, vlan mapping table (VLAN1 map to instance 1, VLAN 2 map to instance 2, other VLAN map to instance 0), and revision level (not indicated in Figure 53).

VLAN Mapping Table

A VLAN mapping table is an attribute of an MST region and is used for describing the mapping relationship of VLAN and STI. For example, the VLAN mapping table of MST region A0 in Figure 53 is VLAN1 map to instance 1, VLAN 2 map to instance 2, other VLAN map to instance 0.

Internal Spanning Tree (IST)

The entire switching network has a Common and Internal Spanning Tree (CIST). An MSTP region has an Internal Spanning Tree (IST), which is a fragment of CIST. For example, every MST region in Figure 53 has an IST.

Common Spanning Tree (CST)

CST connects the spanning trees of the MST region. Taking every MST region as a "switch", the CST can be regarded as their spanning tree generated with STP/RSTP. For example, the red line indicates the CST in Figure 53.

Common and Internal Spanning Tree (CIST)

A single spanning tree made of IST and CST. The CIST in Figure 53 is composed of each IST in every MST region and the CST.

Multiple Spanning Tree Instance (MSTI)

Multiple spanning trees can be generated in an MST region and are independent of one another. Each of these spanning trees is called an MSTI.

MSTI Region root

The MSTI region root refers to the root of the MSTI in an MST region. Each spanning tree in an MST region can have a different topology with a different region root.

Common Root Bridge

The common root bridge refers to the root bridge of the CIST. There is only one common root bridge in the network.

Boundary port

The boundary port refers to the port located at the edge of the MST region. The boundary port connects different MST regions, an MST region and an STP region, or an MST region and an RSTP region. For MSTP calculation, the boundary port has the same role on MSTI and CIST instance. For example, the boundary port as a master port on a CIST instance should serve as a master port on every MSTI in the region.

Port role

In the process of MSTP calculation, a port can serve as a designated port, root port, master port, alternate port, or BACKUP.

- The root port is the port through which the data is forwarded to the root.

- The designated port is the one through which the data is forwarded to the downstream network segment or switch.

- Master port is the port connecting the entire region to the common root bridge and located on the shortest path between them.

- An alternate port is the backup of the master port. When the master port is blocked, the alternate port takes its place.

- If two ports of a switch are connected, there must be a loop. In this case, the switch will block one of them. The blocked port is called BACKUP port.

A port can play different roles in different spanning tree instances.

Figure 54 illustrates the these concepts.

Figure 54   Port Roles
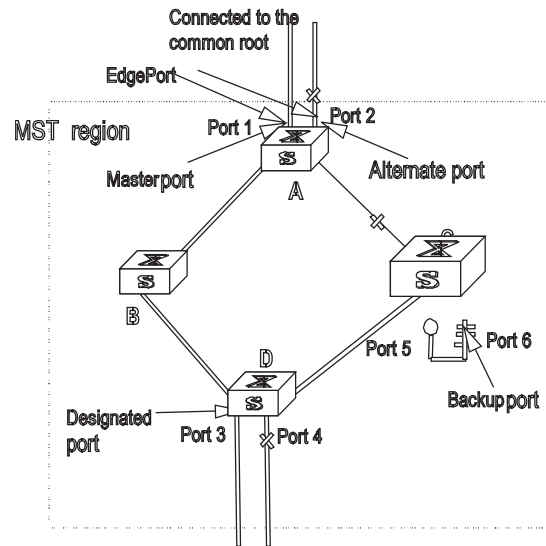
MSTP Principles   MSTP divides the entire Layer 2 network into several MST regions, and calculates and generates CST for them. Multiple spanning trees are generated in a region and each of them is called an MSTI. The instance 0 is called IST, and others are called MSTI.

CIST calculation

The CIST root is the highest-priority switch, elected from the switches on the entire network by comparing their configuration BPDUs. MSTP calculates and generates an IST in an MST region and also the CST connecting the regions. CIST is the unique single spanning tree of the entire switching network.

MSTI calculation

Inside an MST region, MSTP generates different MSTIs for different VLANs according to the association between the VLAN and the spanning tree.

In this way, the packets of a VLAN travel along the corresponding MSTI; inside the MST region and the CST between different regions.

Configuring MSTP   Configuring MSTP includes tasks that are described in the following sections:

- Configuring the MST Region for a Switch
- Specifying the Switch as Primary or Secondary Root Switch
- Configuring the MSTP Running Mode
- Configuring the Bridge Priority for a Switch
- Configuring the Max Hops in an MST Region
- Configuring the Switching Network Diameter
- Configuring the Time Parameters of a Switch
- Configuring the Max Transmission Speed on a Port
- Configuring a Port as an Edge Port

- Configuring the Path Cost of a Port
- Configuring the Priority of a Port
- Configuring the Port Connection with the Point-to-Point Link
- Configuring the mCheck Variable of a Port
- Configuring the Switch Security Function
- Enabling MSTP on the Device
- Enabling or Disabling MSTP on a Port
- Displaying and Debugging MSTP

Only after MSTP is enabled on the device will other configurations take effect. Before enabling MSTP, you can configure the related parameters of the device and Ethernet ports. The configuration of the related parameters and Ethernet ports will take effect upon enabling MSTP, and stay effective even after resetting MSTP.

The **display stp-region-configuration** command shows the parameters that are configured before MSTP is enabled. To display parameters configured after MSTP is enabled, you can use the related **display** commands. For detailed information, see "Displaying and Debugging MSTP" on page 205.

You do not have to perform all these tasks to configure MSTP. Many of them are designed to adjust the MSTP parameters provided with default values. You can configure these parameters depending on your actual conditions or simply take the defaults. For more detailed information, refer to the task description or to the command descriptions in the *Switch 7750 Command Reference Guide*.

i *When GVRP and MSTP start up on the switch simultaneously, GVRP packets will propagate along CIST, which is a spanning tree instance. In this case, if you want to issue a certain VLAN through GVRP on the network, you should make sure that the VLAN is mapped to CIST when configuring the VLAN mapping table of MSTP. CIST is spanning tree instance 0.*

Configuring the MST Region for a Switch The MST region that a switch belongs to is determined with the configurations of the region name, VLAN mapping table, and MSTP revision level. You can perform the following configurations to put a switch into an MST region.

Tasks for configuring the MST Region for a Switch is described in the following sections:

- Entering MST region view
- Configuring the MST Region
- Activating the MST Region Configuration and Exiting the MST Region View

Entering MST region view

Perform the following configuration in system view.

Table 189 Enter MST Region View

Operation	Command
Enter MST region view (from system view)	**stp region-configuration**
Restore the default settings of MST region	**undo stp region-configuration**

Configuring the MST Region

Perform the following configuration in MST region view.

Table 190   Configure the MST Region for a Switch

Operation	Command
Configure MST region name	**region-name** name
Restore the default MST region name	**undo region-name**
Configure VLAN mapping table	**instance** instance-id **vlan** vlan-list
Restore the default VLAN mapping table	**undo instance**
Configure the MSTP revision level of MST region	**revision-level** level
Restore the MSTP revision level of MST region	**undo revision-level**

An MST region can contain up to 16 spanning tree instances, among which Instance 0 is an IST and instances 1 through 16 are MSTIs. Upon the completion of these configurations, the current switch is put into a specified MST region.

> **i** *Two switches belong to the same MST region only if they have been configured with the same MST region name, STI-VLAN mapping tables of an MST region, and the MST region revision level.*

Configuring the related parameters, especially the VLAN mapping table, of the MST region will lead to the recalculation of spanning tree and network topology flapping. To reduce such flapping, MSTP triggers to recalculate the spanning tree according to the configurations only if one of the following conditions are met:

■ The user manually activates the configured parameters related to the MST region, using the **active region-configuration** command.

■ The user enables MSTP, using the **stp enable** command.

By default, the MST region name is the first switch MAC address, all the VLANs in the MST region are mapped to the STI 0, and the MSTP region revision level is 0. You can restore the default settings of MST region, using the **undo stp region-configuration** command in system view.

Activating the MST Region Configuration and Exiting the MST Region View

Perform the following configuration in MST region view.

Table 191   Activate the MST Region Configuration and Exit the MST Region View

Operation	Command
Show the configuration information of the MST region under revision (from MST region view)	**check region-configuration**
Manually activate the MST region configuration (from MST region view)	**active region-configuration**
Exit MST region view (from MST region view)	**quit**

Specifying the Switch as Primary or Secondary Root Switch

MSTP can determine the spanning tree root through calculation. You can also specify the current switch as the root, using the command provided by the switch.

You can use the following commands to specify the current switch as the primary or secondary root of the spanning tree.

Perform the following configuration in system view.

Table 192 Specify the Switch as Primary or Secondary Root Switch

Operation	Command
Specify current switch as the primary root switch of the specified spanning tree.	`stp instance` instance-id `root primary` [`bridge-diameter` bridgenum [`hello-time` centi-senconds]]
Specify current switch as the secondary root switch of the specified spanning tree.	`stp instance` instance-id `root secondary` [`bridge-diameter` bridgenum [`hello-time` centi-senconds]]
Specify current switch not to be the primary or secondary root.	`undo stp instance` instance-id `root`

After a switch is configured as primary root switch or secondary root switch, you cannot modify the bridge priority of the switch.

You can configure the current switch as the primary or secondary root switch of the STI (specified by the `instance` instance-id parameter). If the instance-id takes 0, the current switch is specified as the primary or secondary root switch of the CIST.

The root types of a switch in different STIs are independent of one another. A switch can be a primary or secondary root of any STI. However, a switch cannot serve as both the primary and secondary roots of one STI.

If the primary root is down or powered off, unless you configure a new primary root, the secondary root will take its place. If there are two or more configured secondary root switches, MSTP selects the one with the smallest MAC address to take the place of the failed primary root.

When configuring the primary and secondary switches, you can also configure the network diameter and hello time of the specified switching network. For detailed information, refer to the configuration tasks "Configuring the Switching Network Diameter" and "Configuring the Time Parameters of a Switch".

> 🛈 *You can configure the current switch as the root of several STIs, however, it is not necessary to specify two or more roots for an STI. In other words, please do not specify the root for an STI on two or more switches.*
>
> *You can configure more than one secondary root for a spanning tree by specifying the secondary STI root on two or more switches.*
>
> *Generally, you are recommended to designate one primary root and more than one secondary root for a spanning tree.*

By default, a switch is neither the primary root or the secondary root of the spanning tree.

Configuring the MSTP Running Mode

MSTP and RSTP are compatible and can recognize each other's packets. However, STP cannot recognize MSTP packets. To implement the compatibility, MSTP

provides two operation modes, STP-compatible mode and MSTP mode. In STP-compatible mode, the switch sends STP packets by every port and serves as a region itself. In MSTP mode, the switch ports send MSTP or STP packets (when connected to the STP switch) and the switch provides the multiple spanning tree function.

You can use the following command to configure MSTP running mode. MSTP can intercommunicate with STP. If there is a STP switch in the switching network, you can use the command to configure the current MSTP to run in STP-compatible mode, otherwise, configure it to run in MSTP mode.

Perform the following configuration in system view.

Table 193   Configure the MSTP Running Mode

Operation	Command
Configure MSTP to run in STP-compatible mode	`stp mode stp`
Configure MSTP to run in RSTP mode	`stp mode rstp`
Configure MSTP to run in MSTP mode.	`stp mode mstp`
Restore the default MSTP running mode	`undo stp mode`

Generally, if there is a STP switch on the switching network, the port connected to it will automatically transit from MSTP mode to STP-compatible mode. The port cannot automatically transition itself back to MSTP mode after the STP switch is removed. In this case, you can perform the mcheck operation to transit the port to MSTP mode by force.

By default, MSTP runs in MSTP mode.

Configuring the Bridge Priority for a Switch

Whether a switch can be elected as the spanning tree root depends on its bridge priority. The switch configured with a lower bridge priority is more likely to become the root. An MSTP switch can have different priorities in different STIs.

You can use the following command to configure the bridge priorities of the designated switch in different STIs.

Perform the following configuration in system view.

Table 194   Configure the Priority for a Switch

Operation	Command
Configure the priority of the designated switch.	`stp instance` instance-id `priority` priority
Restore the default priority of the designated switch.	`undo stp instance` instance-id `priority`

When configuring the switch priority with the **instance** instance-id parameter, with a value of 0, you are configuring the CIST priority of the switch.

In the process of spanning tree root election of two or more switches, with the lowest priorities, the one has a smaller MAC address will be elected as the root.

By default, the switch priority is 32768.

Configuring the Max Hops in an MST Region

The scale of an MST region is limited by the max hops in the MST region; which is configured on the region root. As the BPDU travels from the spanning tree root, each time it is forwarded by a switch, the max hop is reduced by 1. The switch discards the configuration BPDU with 0 hops left. This makes it impossible for the switch beyond the max hops to take part in the spanning tree calculation, thereby limiting the scale of the MST region.

You can use the following command to configure the max hops in an MST region.

Perform the following configuration in system view.

Table 195   Configure the Max Hops in an MST Region

Operation	Command
Configure the max hops in an MST region.	`stp max-hops` hop
Restore the default max hops in an MST region	`undo stp max-hops`

The more the hops in an MST region, the larger the scale of the region. Only the max hops configured on the region root can limit the scale of MST region. Other switches in the MST region also apply the configurations on the region root, even if they have been configured with max hops.

By default, the max hops of an MST is 20.

Configuring the Switching Network Diameter

Any two hosts on the switching network are connected with a specific path carried by a series of switches. Among these paths, the one passing more switches than all others is the network diameter, expressed as the number of passed switches.

You can use the following command to configure the diameter of the switching network.

Perform the following configuration in system view.

Table 196   Configure the Switching Network Diameter

Operation	Command
Configure the switching network diameter.	`stp bridge-diameter` bridgenum
Restore the default switching network diameter.	`undo stp bridge-diameter`

The network diameter is the parameter specifying the network scale. The larger the diameter, the larger the scale.

When a user configures the network diameter on a switch, MSTP automatically calculates and sets the hello time, forward-delay time, and maximum-age time, of the switch, to the desirable values.

The setting of the network diameter takes effect on CIST only, but has no effect on MSTI.

By default, the network diameter is 7 and the three corresponding timers take the default values.

Configuring the Time Parameters of a Switch	The switch has three time parameters:

- Forward delay

- Hello time

- Max age

Forward delay is the switch state transition mechanism. The spanning tree will be recalculated upon link faults and its structure will change accordingly. The configuration BPDU recalculated cannot be immediately propagated throughout the network. Temporary loops can occur if the new root port and designated port forward data, right after being elected. Therefore, the protocol adopts a state transition mechanism. It takes a forward delay interval for the root port and designated port to transit from the learning state to forwarding state. The forward delay guarantees a period of time during which the new configuration BPDU can be propagated throughout the network.

The switch sends a hello packet periodically to check if there is any link fault. The interval in which the hello packet is sent is specified by the hello timer.

Max age specifies when the configuration BPDU expires. The switch will discard the expired configuration BPDU.

You can use the following command to configure the time parameters for the switch.

Perform the following configuration in system view.

Table 197 Configure the Time Parameters of a Switch

Operation	Command
Configure Forward Delay on the switch.	`stp timer forward-delay centiseconds`
Restore the default Forward Delay of the switch.	`undo stp timer forward-delay`
Configure Hello Time on the switch.	`stp timer hello centiseconds`
Restore the default Hello Time on the switch.	`undo stp timer hello`
Configure Max Age on the switch.	`stp timer max-age centiseconds`
Restore the default Max Age on the switch.	`undo stp timer max-age`

Every switch on the switching network adopts the values of the time parameters configured on the root switch of the CIST.

The forward delay configured on a switch depends on the switching network diameter. Generally, the forward delay is supposed to be longer when the network diameter is longer. Note that a forward delay that is too short can redistribute some redundant routes temporarily, while a forward delay that is too long can prolong the network connection resuming. The default value is recommended.

A suitable hello time ensures that the switch can detect the link fault on the network, but also occupy moderate network resources. The default value is recommended. If you set a hello time that is too long, when there is packet dropped over a link, the switch may consider it as link fault and the network device will recalculate the spanning tree accordingly. However, for a hello time

that is too short, the switch frequently sends configuration BPDU, which adds burden and wastes the network resources.

A max age that is too short, can cause the network device to calculate the spanning tree frequently and mistake the congestion as a link fault. If the max age is too long, the network device may not be able to discover the link fault and recalculate the spanning tree in time, which weakens the auto-adaptation capacity of the network. The default value is recommended.

To avoid frequent network flapping, the values of hello time, forward delay and maximum age should guarantee the following formulas equal.

2 * (forward-delay - 1seconds) >= maximum-age

maximum-age >= 2 * (hello + 1.0 seconds)

You should use the **stp root primary** command to specify the network diameter and hello time of the switching network so MSTP will calculate automatically and give better values.

By default, forward delay is 15 seconds, hello time is 2 seconds, and max age is 20 seconds.

Configuring the Max Transmission Speed on a Port

The max transmission speed on a port specifies how many MSTP packets will be transmitted, every hello time, through the port.

The max transmission speed on a port is limited by the physical state of the port and the network structure. You can configure it according to the network conditions.

You can configure the max transmission speed on a port in the following ways.

Configuring in system view

Perform the following configuration in system view.

Table 198   Configure the Max Transmission Speed on a Port

Operation	Command
Configure the max transmission speed on a port.	**stp interface** interface-list **transit-limit** packetnum
Restore the max transmission speed on a port.	**undo stp interface** interface-list **transit-limit**

Configuring in Ethernet port view

Perform the following configuration in Ethernet port view.

Table 199   Configure the Max Transmission Speed on a Port

Operation	Command
Configure the max transmission speed on a port.	**stp transit-limit** packetnum
Restore the max transmission speed on a port.	**undo stp transit-limit**

For more about the commands, see the *Switch 7750 Command Reference Guide*.

This parameter only takes a relative value without units. If it is set too large, too many packets will be transmitted during every hello time and too many network resources will be occupied. The default value is recommended.

By default, the max transmission speed on every Ethernet port of the switch is 3.

Configuring a Port as an Edge Port

An edge port refers to the port not directly connected to any switch, or indirectly connected to a switch over the connected network.

You can configure a port as an edge port or non-edge port in the following ways.

Configuring in System View

Perform the following configuration in system view.

Table 200   Configure a Port as an Edge Port or a Non-edge Port

Operation	Command
Configure a port as an edge port.	**stp interface** interface-list **edged-port enable**
Configure a port as a non-edge port.	**stp interface** interface-list **edged-port disable**
Restore the default setting, non-edge port, of the port.	**undo stp interface** interface-list **edged-port**

Configuring in Ethernet Port View

Perform the following configuration in Ethernet port view.

Table 201   Configure a Port as an Edge Port or a Non-edge Port

Operation	Command
Configure a port as an edge port.	**stp edged-port enable**
Configure a port as a non-edge port.	**stp edged-port disable**
Restore the default setting, non-edge port, of the port.	**undo stp edged-port**

For more about the commands, see the *Switch 7750 Command Reference Guide*.

After it is configured as an edge port, the port can transit rapidly from a blocking state to a forwarding state without any delay. In the case that BPDU protection has not been enabled on the switch, the configured edge port will turn into non-edge port again when it receives BPDU from the other port. In case BPDU protection is enabled, the port will be disabled. This parameter is configured the same, and takes effect on all the STIs.

i *To reenable a port that was disabled by the* **stp edged-port disable** *command, use the* **undo shutdown** *command in port view.*

It is better to configure the BPDU protection on the edge port to prevent the switch from being attacked.

Before BPDU protection is enabled on the switch, the port runs as a non-edge port when it receives BPDU, even if the user has set it as an edge port.

By default, all the Ethernet ports of the switch have been configured as non-edge ports.

Configuring the Path Cost of a Port

Path cost is related to the speed of the link connected to the port. On the MSTP switch, a port can be configured with different path costs for different STIs. Thus the traffic from different VLANs can run over different physical links, thereby implementing the VLAN-based load-balancing.

You can configure the path cost of a port in the following ways.

Configuring in System View

Perform the following configuration in system view.

Table 202   Configure the Path Cost of a Port

Operation	Command
Configure the Path Cost of a port.	**stp interface** interface-list **instance** instance-id **cost** cost
Restore the default path cost of a port.	**undo stp interface** interface-list **instance** instance-id **cost**

Configuring in Ethernet Port View

Perform the following configuration in Ethernet port view.

Table 203   Configure the Path Cost of a Port

Operation	Command
Configure the Path Cost of a port	**stp instance** instance-id **cost** cost
Restore the default path cost of a port.	**undo stp instance** instance-id **cost**

For more about the commands, see the *Switch 7750 Command Reference Guide*.

Upon the change of path cost of a port, MSTP will recalculate the port role and transit the state. When *instance-id* takes 0, it indicates to set the path cost on the CIST.

By default, MSTP is responsible for calculating the port path cost.

Specify the Standard To BeFollowed in Path Cost Calculation

The following two standards are currently available on the switch:

- **dot1d-1998**: The switch calculates the default Path Cost of a port by the IEEE 802.1D-1998 standard.
- **dot1t**: The switch calculates the default Path Cost of a port by the IEEE 802.1t standard.
- **legacy**: The switch calculates the default Path Cost of a port by the Huawei-3Com standard.

You can specify the intended standard by using the following commands.

Perform the following configuration in system view.

Table 204 Specifying the Standard To Be Followed in Path Cost Calculation

Operation	Command
Specify the standard to be adopted when the switch calculates the default Path Cost for the connected link	`stp pathcost-standard{ dot1d-1998| dot1t|legacy}`
Restore the default standard to be used	`undo stp pathcost-standard`

By default, the switch calculates the default Path Cost of a port by the IEEE 802.1t standard.

Table 205 Cost Corresponding to the Port Speed of Different Standard

Link speed	Duplex state	dot1d-1998 value range	dot1t value range	Huawei-3Com cost value
0	-	65535	200,000,000	200,000
10Mb/s	Half-Duplex	100	2,000,000	2,000
	Full-Duplex	99	1,999,999	2,000
	Aggregated Link 2 Aggregated Link 3 Ports	95	1,000,000	1,800
		95	666,666	1,600
	Aggregated Link 4 Ports	95	500,000	1,400
100Mb/s	Half-Duplex	19	200,000	200
	Full-Duplex	18	199,999	200
	Aggregated Link 2 Ports	15	100,000	180
		15	66,666	160
	Aggregated Link 3 Ports	15	50,000	140
	Aggregated Link 4 Ports			
1000Mb/s	Full-Duplex	4	20,000	20
	Aggregated Link 2 Ports	3	10,000	18
		3	6,666	16
	Aggregated Link 3 Ports	3	5,000	14
	Aggregated Link 4 Ports			
10G/s	Full-Duplex	2	2,000	2
	Aggregated Link 2 Ports	1	1,000	1
		1	666	1
	Aggregated Link 3 Ports	1	500	1
	Aggregated Link 4 Ports			

Generally the path cost of the links in full duplex status is lower than those in half duplex status.

In calculating the path cost of aggregation links, the 802.1D-1998 does not take into account the number of aggregation links, but the 802.1T does. The formula involved is:

Path Cost = 200,000,000/link speed in 100Kbps

Where the link speed is the sum of the speed of the ports in unblocked status within the aggregation links.

Configuring the Priority of a Port

For spanning tree calculation, the port priority is an important factor when determining if a port can be elected as the root port. With other attributes being equal, the port with the highest priority is elected as the root port. On the MSTP switch, a port can have different priorities in different STIs, and play different roles. The traffic from different VLANs can run over different physical links, thereby implementing the VLAN-based load-balancing.

You can configure the port priority in the following ways.

Configuring in System View

Perform the following configuration in system view.

Table 206   Configure the Port Priority

Operation	Command
Configure the port priority.	**stp interface** interface-list **instance** instance-id **port priority** priority
Restore the default port priority.	**undo stp interface** interface-list **instance** instance-id **port priority**

Configuring in Ethernet Port View

Perform the following configuration in Ethernet port view.

Table 207   Configure the Port Priority

Operation	Command
Configure the port priority.	**stp instance** instance-id **port priority** priority
Restore the default port priority.	**undo stp instance** instance-id **port priority**

For more about the commands, see the *Switch 7750 Command Reference Guide*.

After the change of port priority, MSTP will recalculate the port role and transit the state. A smaller value represents a higher priority. If all the Ethernet ports of a switch are configured with the same priority value, the priorities of the ports will be differentiated by the index number. The change of Ethernet port priority will lead to spanning tree recalculation. You can configure the port priority with actual networking requirements.

By default, the priority of all the Ethernet ports is 128.

Configuring the Port Connection with the Point-to-Point Link	The point-to-point link directly connects two switches.

You can configure the port to connect or not connect with the point-to-point link in the following ways.

Configuring in System View

Perform the following configuration in system view.

Table 208   Configure the Port Connection With the Point-to-point Link

Operation	Command
Configure the port to connect with the point-to-point link.	**stp interface** interface-list **point-to-point force-true**
Configure the port not to connect with the point-to-point link.	**stp interface** interface-list **point-to-point force-false**
Configure MSTP to automatically detect if the port is directly connected with the point-to-point link.	**stp interface** interface-list **point-to-point auto**
Configure MSTP to automatically detect if the port is directly connected with the point-to-point link, as defaulted.	**undo stp interface** interface-list **point-to-point**

Configuring in Ethernet Port View

Perform the following configuration in Ethernet port view.

Table 209   Configure the Port Connection With the Point-to-point Link

Operation	Command
Configure the port to connect with the point-to-point link.	**stp point-to-point force-true**
Configure the port not to connect with the point-to-point link.	**stp point-to-point force-false**
Configure MSTP to automatically detect if the port is directly connected with the point-to-point link.	**stp point-to-point auto**
Configure MSTP to automatically detect if the port is directly connected with the point-to-point link, as defaulted.	**undo stp point-to-point**

For more about the commands, see the *Switch 7750 Command Reference Guide*.

The ports connected with the point-to-point link, upon some port role conditions being met, can transit to forwarding state rapidly through transmitting synchronization packet, thus reducing the unnecessary forwarding delay. If the parameter is configured in auto mode, MSTP will automatically detect if the current Ethernet port is connected with the point-to-point link.

i⊳ *For a link aggregation, only the master port can be configured to connect with the point-to-point link. If a port in auto-negotiation mode operates in full-duplex mode upon negotiation, it can be configured to connect with the point-to-point link.*

This configuration takes effect on the CIST and all the MSTIs. The settings of a port determine whether or not the point-to-point link will be applied to all the STIs to which the port belongs. Note that a temporary loop may be redistributed if you

configure a port not physically connected with the point-to-point link, rather, connected to such a link by force.

By default, the parameter is configured as **`auto`**.

Configuring the mCheck Variable of a Port

The port of an MSTP switch operates in either STP-compatible or MSTP mode.

If a port of an MSTP switch on a switching network is connected to an STP switch, the port will automatically transition to operate in STP-compatible mode. The port stays in STP-compatible mode and cannot automatically transition back to MSTP mode when the STP switch is removed. In this case, you can perform an mCheck operation to transit the port to MSTP mode by force.

You can use the following measures to perform mCheck operation on a port.

Configuring in system view

Perform the following configuration in system view.

Table 210   Configure the mCheck Variable of a Port

Operation	Command
Perform mCheck operation on a port.	**`stp interface`** `interface-list` **`mcheck`**

Configuring in Ethernet port view

Perform the following configuration in Ethernet port view.

Table 211   Configure the mCheck Variable of a Port

Operation	Command
Perform mCheck operation on a port.	**`stp mcheck`**

For more about the commands, see the *Switch 7750 Command Reference Guide*.

The command can be used only if the switch runs MSTP. The command does not make any sense when the switch runs in STP-compatible mode.

Configuring the Switch Security Function

An MSTP switch provides BPDU protection, Root protection, and loop-protection functions.

For an access device, the access port is, mainly, directly connected to the user terminal or a file server, and the access port is set to edge port to implement fast transition. When such a port receives a BPDU packet, the system will automatically set it as a non-edge port and recalculate the spanning tree, which causes the network topology flapping. Normally, these ports will not receive STP BPDU. If someone forges BPDU to attack the switch, the network will flap. BPDU protection function is used against such network attacks.

The primary and secondary root switches of the spanning tree, especially those of ICST, must be located in the same region. This is because the primary and secondary roots of CIST are generally placed in the core region with a high bandwidth in network design. In case of configuration error or malicious attack, the legal primary root may receive the BPDU with a higher priority and then lose its place, which causes network topology change errors. Due to the illegal change, the traffic that is supposed to travel over the high-speed link may be pulled to the

low-speed link and congestion will occur on the network. The root protection function is used against such problem.

The root port and other blocked ports maintain their state according to the BPDUs sent by an uplink switch. Once the link is blocked or has trouble, the ports cannot receive BPDUs and the switch will select a root port again. In this case, the former root port will turn into a specified port and the former blocked ports will enter the forwarding state and a link loop will be created.

The security functions can control the generation of loop. After it is enabled, the root port cannot be changed, the blocked port will remain in the discarding state and will not forward packets.

You can use the following command to configure the security functions of the switch.

Perform the following configuration in corresponding configuration modes.

Table 212   Configure the Switch Security Function

Operation	Command
Configure switch BPDU protection (from system view)	**stp bpdu-protection**
Restore the disabled BPDU protection state as defaulted (from system view)	**undo stp bpdu-protection**
Configure switch Root protection (from system view)	**stp interface** interface-list **root-protection**
Restore the disabled Root protection state as defaulted (from system view)	**undo stp interface** interface-list **root-protection**
Configure switch Root protection (from Ethernet port view)	**stp root-protection**
Restore the disabled Root protection state as defaulted (from Ethernet port view)	**undo stp root-protection**
Configure switch loop protection function (from Ethernet port view)	**stp loop-protection**
Restore the disabled loop protection state, as defaulted (from Ethernet port view)	**stp loop-protection**

After configured with BPDU protection, the switch will disable the edge port through MSTP, which receives a BPDU, and notifies the network manager at the same time. These ports can be resumed by the network manager only.

The port configured with root protection only plays the role of designated port on every instance. Whenever such a port receives a higher-priority BPDU, that is, it is about to turn into non-designated port, it will be set to listening state and will not forward packets any more (as if the link to the port is disconnected). If the port has not received any higher-priority BPDU for a certain period of time thereafter, it will resume the normal state.

When you configure a port, only one configuration at a time can be effective among loop protection, root protection, and edge port configuration.

By default, the switch does not enable BPDU protection, root protection, or edge port protection.

For more about the configuration commands, see the *Switch 7750 Command Reference Guide*.

Enabling MSTP on the Device

You can use the following command to enable MSTP on the device.

Perform the following configuration in system view.

Table 213 Enable/Disable MSTP on a Device

Operation	Command
Enable MSTP on a device.	**stp enable**
Disable MSTP on a device.	**stp disable**
Restore the disable state of MSTP, as defaulted.	**undo stp**

Only if MSTP has been enabled on the device will other MSTP configurations take effect.

By default, MSTP is disabled.

Enabling or Disabling MSTP on a Port

You can use the following command to enable or disable MSTP on a port. You may disable MSTP on some Ethernet ports of a switch to spare them from spanning tree calculation. This measure flexibly controls MSTP operation and saves the CPU resources of the switch.

MSTP can be enabled/disabled on a port the following ways.

Configuring in System View

Perform the following configuration in system view.

Table 214 Enable/Disable MSTP on a Port

Operation	Command
Enable MSTP on a port.	**stp interface** interface-list **enable**
Disable MSTP on a port.	**stp interface** interface-list **disable**
Restore the default MSTP state on the port.	**undo stp** interface-list

Configuring in Ethernet Port View

Perform the following configuration in Ethernet port view.

Table 215 Enable/Disable MSTP on a Port

Operation	Command
Enable MSTP on a port.	**stp enable**
Disable MSTP on a port.	**stp disable**
Restore the default MSTP state on the port.	**undo stp**

For more information about the commands, see the *Switch 7750 Command Reference Guide*.

A redundant route may be generated after MSTP is disabled.

By default, MSTP is enabled on all the ports after it is enabled on the device.

Displaying and Debugging MSTP

After you configure MSTP, execute the **display** command in all views to display the running of the MSTP configuration, and to verify the effect of the configuration. Execute the **reset** command in user view to clear the statistics of MSTP module. Use the **debugging** command in user view to debug the MSTP module

Table 216   Display and Debug MSTP

Operation	Command
Show the configuration information about the current port and the switch.	**display stp instance** instance-id [**interface** interface-list] [**brief**]
Show the configuration information about the region.	**display stp region-configuration**
Clear the MSTP statistics information.	**reset stp** [**interface** interface-list]
Enable/Disable MSTP (packet receiving/transmitting, event, error) debugging on the port.	[**undo**] **debugging stp** [**interface** interface-list] { **packet**	**event** }
Enable/Disable the global MSTP debugging.	[**undo**] **debugging stp** { **global-event**	**global-error**	**all** }
Enable/Disable specified STI debugging	[**undo**] **debugging stp instance** instance-id

Digest Snooping

According to IEEE 802.1s, two connected switches can communicate through MSTIs (multiple spanning tree instances) in a MSTP (multiple spanning tree protocol) domain only when they are configured with the same domain settings. With MSTP employed, interconnected switches determine whether or not they are in the same domain by checking the configuration IDs of the BPDUs between them. (Configuration ID comprises information such as domain ID and configuration digest.)

As some switches come with some proprietary protocols concerning STP employed, they cannot communicate with other switches in MSTP domains even both of these two types of switches are configured with the same domain configuration settings.

This can be overcome by implementing digest snooping. Digest snooping enables a switch to track and maintain configuration digests of other switches that are in the same domain by examining their BPDUs and insert corresponding configuration digests in its BPDUs destined for these switches, through which switches of different type are capable of communicating with each other in a MSTP domain.

Configuring Digest Snooping

Configure digest snooping on a switch to enable it to communicate in MSTP domains with other switches that are configured with some proprietary protocols to calculate configuration digest through MSTI.

Prerequisites

Switches of different manufacturers are interconnected in a network and have MSTP properly employed. The network operates properly.

Configuration Procedure

Table 217　Configure digest snooping

Operation	Command	Remark
Enter system view	system-view	-
Enter Ethernet interface view	**interface** *interface_type* *interface_num*	*interface_type*: Interface type *interface_num*: Interface number
Enable digest snooping on the interface	**stp config-digest-snooping**	Required. Digest snooping is disabled by default
Quit Ethernet interface view	**quit**	-
Enable digest snooping globally	**stp config-digest-snooping**	Required. Digest snooping is disabled by default
Display current configuration information	**display current-configuration**	This command can be executed in any view

Note the following:

- You must enable digest snooping on an interface first before enabling it globally.

- Digest snooping is unnecessay if the interconnected switches are from the same vendor.

- To enable digest snooping, the interconneted switches must be configured with the same settings.

- To enable digest snooping, all interfaces in a MSTP domain used to connect other switches must have digest snooping enabled.

- Do not enable digest snooping on border interfaces of an MSTP domain.

- To change domain configuration, be sure to disable digest snooping first to prevent broadcast storm.

9

AAA AND RADIUS OPERATION

This chapter covers the following topics:

- IEEE 802.1x
- Implementing the AAA and RADIUS Protocols
- Configuring AAA
- Configuring the RADIUS Protocol
- Configuring HWTACACS
- Displaying and Debugging the AAA, RADIUS, and HWTACACS Protocols
- AAA, RADIUS, and HWTACACS Protocol Configuration Examples
- Troubleshooting AAA, RADIUS, and HWTACACS Configurations

IEEE 802.1x

IEEE 802.1x (referred to as 802.1x) is a port-based network access control protocol that is used as the standard for LAN user access authentication.

In LANs that comply with IEEE 802 standards, the user can access devices and share resources in the LAN by connecting a device such as a LAN Switch. In telecom access, commercial LAN (a typical example is the LAN in the office building) and mobile office, etc., the LAN providers generally aim to control the user's access. The requirement on the above-mentioned "port-based network access control" is the most applicable.

As the name implies, "port-based network access control" means to authenticate and control all accessed devices on the port of the device. If the user's device can pass authentication, the user can access resources in the LAN.

802.1x defines port based network access control protocol, and the point-to-point connection between the access device and the access port, only. The port can be either physical or logical. A typical application environment is as follows: Each physical port of the LAN Switch only connects to one user workstation (based on the physical port) and the wireless LAN access environment (based on the logical port), etc.

Configuring IEEE 802.1x is described in the following sections:

- 802.1x System Architecture
- Configuring 802.1x

802.1x System Architecture

The system using 802.1x is a typical C/S (Client/Server) system architecture. It contains three entities: Supplicant System, Authenticator System and Authentication Server System.

The LAN access control device needs to provide the Authenticator System of 802.1x. The computers need to be installed with the 802.1x client Supplicant software, for example, the 802.1x client provided by Microsoft Windows XP. The 802.1x Authentication Server system normally stays in the carrier's AAA center.

Authenticator and Authentication Server exchange information through EAP (Extensible Authentication Protocol) frames. The Supplicant and the Authenticator exchange information through the EAPoL (Extensible Authentication Protocol over LANs) frame defined by IEEE 802.1x. Authentication data are encapsulated in the EAP frame, which is encapsulated in packets of other AAA upper layer protocols (e.g. RADIUS). This provides a channel through the complicated network to the Authentication Server. Such procedure is called EAP Relay.

There are two types of ports for the Authenticator. One is the Uncontrolled Port, and the other is the Controlled Port. The Uncontrolled Port is always in a bi-directional connection state. The user can access and share the network resources any time through the ports. The Controlled Port will be in a connecting state only after the user passes the authentication. Then the user is allowed to access the network resources.

Figure 55   802.1x System Architecture
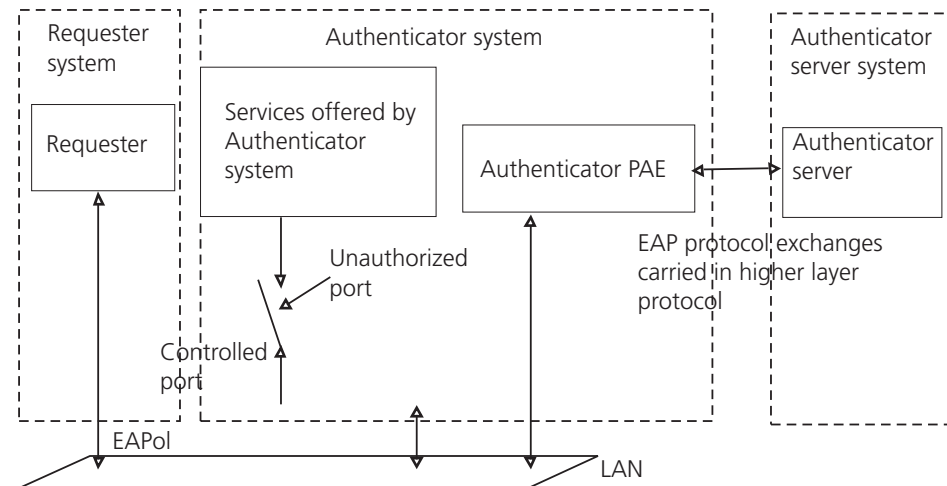
Tasks for configuring 802.1x System Architecture is described in the following sections:

- 802.1x Authentication Process
- Implement 802.1x on Ethernet Switch

802.1x Authentication Process

802.1x configures EAP frame to carry the authentication information. The Standard defines the following types of EAP frames:

- EAP-Packet: Authentication information frame, used to carry the authentication information.
- EAPoL-Start: Authentication originating frame, actively originated by the Supplicant.
- EAPoL-Logoff: Logoff request frame, actively terminating the authenticated state.

- EAPoL-Key: Key information frame, supporting to encrypt the EAP packets.
- EAPoL-Encapsulated-ASF-Alert: Supports the Alerting message of Alert Standard Forum (ASF).

The EAPoL-Start, EAPoL-Logoff, and EAPoL-Key only exist between the Supplicant and the Authenticator. The EAP-Packet information is re-encapsulated by the Authenticator System and then transmitted to the Authentication Server System. The EAPoL-Encapsulated-ASF-Alert is related to the network management information and terminated by the Authenticator.

802.1x provides an implementation solution of user ID authentication. However, 802.1x itself is not enough to implement the scheme. The administrator of the access device should configure the AAA scheme by selecting RADIUS or local authentication to assist 802.1x in implementing the user ID authentication. For a detailed description, refer to the corresponding AAA configuration.

Implement 802.1x on Ethernet Switch

The Switch 7750 not only supports the port access authentication method regulated by 802.1x, but also extends and optimizes it in the following way:

- Support to connect several End Stations in the downstream by a physical port.
- The access control (or the user authentication method) can be based on port or MAC address.

In this way, the system becomes more secure, and easier to manage.

Configuring 802.1x   The configuration tasks of 802.1x itself, can be fulfilled in system view of the Ethernet switch. When the global 802.1x is not enabled, the user can configure the 802.1x state of the port. The configured items will take effect after the global 802.1x is enabled.

> *Do not enable 802.1x and RSTP at the same time or the switch may not work normally.*

The 802.1x configuration tasks are described in the following sections:

- Enabling/Disabling 802.1x
- Setting the Port Access Control Mode
- Setting Port Access Control Method
- Checking the Users that Log on the Switch by Proxy
- Setting Number of Users on a Port
- Enabling DHCP to Launch Authentication
- Configuring the Authentication Method for 802.1x Users
- Setting the Maximum Retransmission Times
- Configuring Timers
- Enabling/Disabling Quiet-Period Timer
- Displaying and Debugging 802.1x

Enabling/Disabling 802.1x

The following commands can be used to enable/disable the 802.1x on the specified port. When no port is specified in system view, the 802.1x is enabled/disabled globally.

Perform the following configurations in system view or Ethernet port view.

Table 218 Enable/Disable 802.1x

Operation	Command
Enable the 802.1x	**dot1x** [**interface** interface-list]
Disable the 802.1x	**undo dot1x** [**interface** interface-list]

User can configure 802.1x on an individual port. The configuration will take effect right after 802.1x is enabled globally.

By default, 802.1x authentication has not been enabled globally, or on any port.

Setting the Port Access Control Mode

The following commands can be used for setting 802.1x access control mode on the specified port. When no port is specified, the access control mode of all ports is configured.

Perform the following configurations in system view or Ethernet port view. .

Table 219 Set the Port Access Control Mode

Operation	Command
Set the port access control mode.	**dot1x port-control** { **authorized-force** | **unauthorized-force** | **auto** } [**interface** interface-list]
Restore the default access control mode of the port.	**undo dot1x port-control** [**interface** interface-list]

By default, access control on the port is auto (automatic identification mode, which is also called protocol control mode). That is, the initial state of the port is unauthorized. It only permits EAPoL packets receiving/transmitting, and does not permit the user to access the network resources. If the authentication flow is passed, the port will be switched to the authorized state and permit the user to access the network resources; this is most common.

Setting Port Access Control Method

The following commands are used for setting 802.1x access control method on the specified port. When no port is specified in system view, the access control method of the port is configured globally.

Perform the following configurations in system view or Ethernet port view.

Table 220 Set Port Access Control Method

Operation	Command
Set port access control method	**dot1x port-method** { **macbased** | **portbased** } [**interface** interface-list]

Table 220   Set Port Access Control Method

Operation	Command
Restore the default port access control method	**undo dot1x port-method** [**interface** interface-list]

By default, 802.1x authentication method on the port is MAC-based. That is, authentication is performed based on MAC addresses.

Checking the Users that Log on the Switch by Proxy

The following commands are used for checking the users that log on by proxy.

Perform the following configurations in system view or Ethernet port view.

Table 221   Check the Users that Log on the Switch by Proxy

Operation	Command
Enable the check for access users by proxy	**dot1x supp-proxy-check** { **logoff** | **trap** } [**interface** interface-list]
Cancel the check for access users by proxy	**undo dot1x supp-proxy-check** { **logoff** | **trap** } [**interface** interface-list]

Setting Number of Users on a Port

The following commands are used for setting the number of users allowed by 802.1x on a specified port. When no port is specified, all the ports accept the same number of users.

Perform the following configurations in system view or Ethernet port view.

Table 222   Set Maximum Number of Users by Specified Port

Operation	Command
Set maximum number of users by specified port	**dot1x max-user** user-number [**interface** interface-list]
Restore the maximum number of users on the port to the default value	**undo dot1x max-user** [**interface** interface-list]

By default, 802.1x allows up to 1024 supplicants on each port for Switch 7750

Enabling DHCP to Launch Authentication

When the user runs DHCP and applies for dynamic IP addresses, use the following commands to set whether or not 802.1x will enable the Ethernet switch to launch the user ID authentication.

Perform the following configurations in system view.

Table 223   Set to Enable DHCP to Launch Authentication

Operation	Command
Enable DHCP to launch authentication	**dot1x dhcp-launch**
Disable DHCP to launch authentication	**undo dot1x dhcp-launch**

By default, authentication will not be launched when the user runs DHCP and applies for dynamic IP addresses.

Configuring the Authentication Method for 802.1x Users

The following commands can be used to configure the authentication method for 802.1x users. Three kinds methods of authentication are available:

- PAP — the RADIUS server must support this method

- CHAP — the RADIUS server must support this method

- EAP relay — the switch sends authentication information to the RADIUS server in the form of EAP packets, directly, so that the RADIUS server never supports EAP authentication

Perform the following configurations in system view.

Table 224   Configure the Authentication Method for 802.1x Users

Operation	Command
Configure the authentication method for 802.1x users	**dot1x authentication-method** { **chap** | **pap** | **eap md5-challenge** }
Restore the default authentication method for 802.1x users	**undo dot1x authentication-method**

Setting the Maximum Retransmission Times

The following commands are used for setting the maximum authenticator-to-supplicant frame-retransmission times.

Perform the following configurations in system view.

Table 225   Set the Maximum Retransmission Times

Operation	Command
Set the maximum retransmission times	**dot1x retry** max-retry-value
Restore the default maximum retransmission times	**undo dot1x retry**

By default, the max-retry-value is 3. That is, the switch can retransmit the authentication request frame to a supplicant 3 times at most.

Configuring Timers

The following commands are used for configuring the 802.1x timers.

Perform the following configurations in system view.

Table 226   Configure Timers

Operation	Command
Configure timers	**dot1x timer {quiet-period** quiet-period-value | **tx-period** tx-period-value | **supp-time-out** supp-timeout-value | **server-timeout** server-timeout-value }

Table 226 Configure Timers

Operation	Command
Restore default settings of the timers	**undo dot1x timer** { **quiet-period** | **tx-period** | **supp-timeout** | **server-timeout** }

By default, the quiet-period-value is 60 seconds, the tx-period-value is 30 seconds, the supp-timeout-value is 30 seconds, the server-timeout-value is 100 seconds. For more detailed information on the **dot1x timer** command, see the *Switch 7750 Command Reference Guide*.

Enabling/Disabling Quiet-Period Timer

You can use the following commands to enable/disable a quiet-period timer of the Switch 7750. If an 802.1x user has not passed authentication, the Authenticator will keep quiet (specified by **quiet-period**) before launching the authentication again. During the quiet period, the Authenticator does not do anything related to 802.1x authentication.

Perform the following configuration in system view.

Table 227 Enable/Disable a Quiet-Period Timer

Operation	Command
Enable a quiet-period timer.	**dot1x quiet-period**
Disable a quiet-period timer	**undo dot1x quiet-period**

Displaying and Debugging 802.1x

Execute the **display** command in all views to display the VLAN configuration, and to verify the configuration. Execute the **reset** command in user view to reset 802.1x statistics information. Execute the **debugging** command in user view to debug the 802.1x module.

Table 228 Display and Debug 802.1x

Operation	Command
Display the configuration, running and statistics information of 802.1x	**display dot1x** [**sessions** | **statistics**] [**interface** interface-list]
Reset the 802.1x statistics information	**reset dot1x statistics** [**interface** interface-list]
Enable the error/event/packet/all debugging of 802.1x	**debugging dot1x** { **error** | **event** | **packet** | **all** }
Disable the error/event/packet/all debugging of 802.1x.	**undo debugging dot1x** { **error** | **event** | **packet** | **all** }

Example: 802.1x Configuration

As shown in the following figure, the workstation is connected to port 1/0/2 of the Switch 7750.

The switch administrator will enable 802.1x on all the ports to authenticate the supplicants in order to control their access to the Internet. The access control mode is based on the MAC address.

All the supplicants belong to the default domain 3com163.net, which can contain up to 30 users. RADIUS authentication is performed first. If there is no response from the RADIUS server, local authentication will be performed. For accounting, if the RADIUS server fails to account, the user will be disconnected. In addition, when the user is connected, the domain name does not follow the user name. Normally, if the user's traffic is less than 2kbps, consistently, over a period of 20 minutes, they will be disconnected.

A server group, consisting of two RADIUS servers at 10.11.1.1 and 10.11.1.2, is connected to the switch. The former one acts as the primary-authentication/second-accounting server. The latter one acts as the secondary-authentication/primary-accounting server. Set the encryption key as "name" when the system exchanges packets with the authentication RADIUS server, and "money" when the system exchanges packets with the accounting RADIUS server. Configure the system to retransmit packets to the RADIUS server if no response is received in 5 seconds. Retransmit the packet no more than 5 times in all. Configure the system to transmit a real-time accounting packet to the RADIUS server every 15 minutes. The system is instructed to transmit the user name to the RADIUS server after removing the user domain name.

The user name of the local 802.1x access user is localuser and the password is localpass (input in plain text). The idle cut function is enabled.

Figure 56   Enabling 802.1x and RADIUS to Perform AAA on the Requester
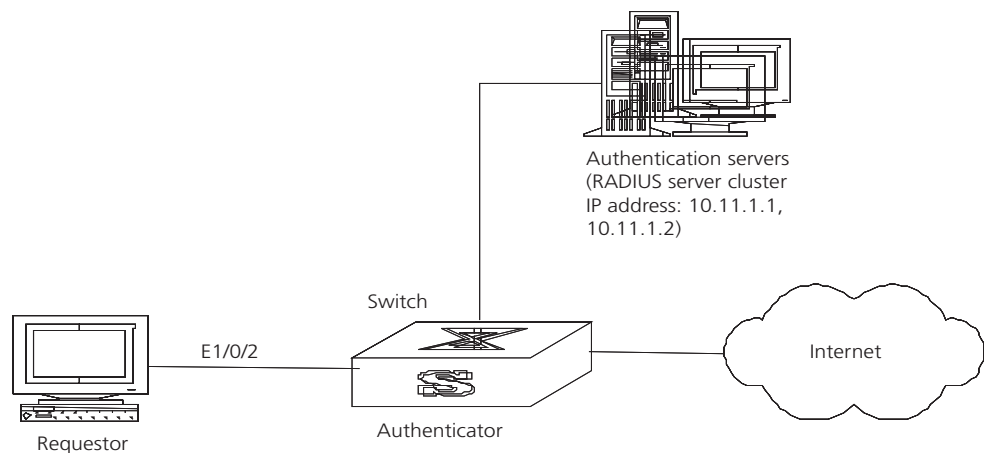
The following examples concern most of the AAA/RADIUS configuration commands. The configurations for accessing user workstation and the RADIUS server are omitted.

1 Enable the 802.1x performance on the specified port Ethernet 1/0/2.

```
[SW7750]dot1x interface ethernet 1/0/2
```

2 Set the access control mode. (This command could not be configured, when it is configured as MAC-based by default.)

```
[SW7750]dot1x port-method macbased interface ethernet 1/0/2
```

3 Create the RADIUS group radius1 and enter its configuration mode.

```
[SW7750]radius scheme radius1
```

4 Set the IP address of the primary authentication/accounting RADIUS servers.

```
[SW7750-radius-radius1]primary authentication 10.11.1.1
[SW7750-radius-radius1]primary accounting 10.11.1.2
```

5 Set the IP address of the second authentication/accounting RADIUS servers.

```
[SW7750-radius-radius1]secondary authentication 10.11.1.2
[SW7750-radius-radius1]secondary accounting 10.11.1.1
```

6 Set the encryption key when the system exchanges packets with the authentication RADIUS server.

```
[SW7750-radius-radius1]key authentication name
```

7 Set the encryption key when the system exchanges packets with the accounting RADIUS server.

```
[SW7750-radius-radius1]key accounting money
```

8 Set the timeouts and times for the system to retransmit packets to the RADIUS server.

```
[SW7750-radius-radius1]timer 5
[SW7750-radius-radius1]retry 5
```

9 Set the interval for the system to transmit real-time accounting packets to the RADIUS server.

```
[SW7750-radius-radius1]timer realtime-accounting 15
```

10 Configure the system to transmit the user name to the RADIUS server after removing the domain name.

```
[SW7750-radius-radius1]user-name-format without-domain
[SW7750-radius-radius1]quit
```

11 Create the user domain 3com163.net and enters isp configuration mode.

```
[SW7750]domain 3com163.net
```

12 Specify radius1 as the RADIUS server group for the users in the domain 3com163.net.

```
[SW7750-isp-3com163.net]radius-scheme radius1
```

13 Set a limit of 30 users to the domain 3com163.net.

```
[SW7750-isp-3com163.net]access-limit enable 30
```

14 Enable idle cut function for the user and set the idle cut parameter in the domain 3com163.net.

```
[SW7750-isp-3com163.net]idle-cut enable 50 5000
```

15 Add a local supplicant and set its parameter.

```
[SW7750]local-user localuser
[SW7750-luser-localuser]attribute service-type lan-access
[SW7750-luser-localuser]password simple localpass
```

16 Enable the 802.1x globally.

```
[SW7750]dot1x
```

Implementing the AAA and RADIUS Protocols

The Authentication, Authorization, and Accounting (AAA) protocol provides a uniform framework for configuring these three security functions and implements network security management.

The network security mentioned here refers to access control, including:

- Which user can access the network server
- Which service can the authorized user enjoy
- How to keep accounts for the user who is using network resource

AAA provides the following services:

- Authenticates whether the user can access the network server.
- Authorizes the user with specified services.
- Accounts for network resources that are consumed by the user.

Generally, by applying client/server architecture, AAA framework boasts the following advantages:

- Good scalability.
- Ability to use standard authentication schemes.
- Easy control, and convenient for centralized management of user information.
- Ability to use multiple-level backup systems to enhance the security of the whole framework.

As mentioned above, AAA is a management framework, so it can be implemented by some protocols. RADIUS is frequently used.

Remote Authentication Dial-In User Service (RADIUS) is distributed information switching protocol in Client/Server architecture. RADIUS can prevent the network from an interruption by unauthorized access, and it is often used in the network environments requiring both high security and remote user access. For example, it is often used for managing a large number of scattering dial-in users who use serial ports and modems. RADIUS system is the important auxiliary part of Network Access Server (NAS).

After the RADIUS system is started, if the user wants to access other networks or use network resources through connection to NAS (dial-in access server in PSTN environment or Ethernet switch with access function in Ethernet environment), the RADIUS client transmits the user's AAA request to the RADIUS server. The RADIUS server has a user database recording all user authentication and network services information. On receiving the user's request from NAS, the RADIUS server performs AAA through user database query and update, and returns the configuration information and accounting data to NAS. NAS then controls supplicant and corresponding connections, while the RADIUS protocol regulates how to transmit configuration and accounting information between NAS and RADIUS.

NAS and RADIUS exchange the information with UDP packets. During the interaction, both sides encrypt the packets with keys before uploading user configuration information (like password etc.) to avoid being intercepted or stolen.

RADIUS server generally uses a proxy function of the devices, like access server, to perform user authentication. The operation process is as follows:

1 Send client username and encrypted password to RADIUS server.

2 User receives one of the following response messages:

■ ACCEPT: Indicates that the user has passed the authentication

■ REJECT: Indicates that the user has not passed the authentication and needs to input username and password again, otherwise he will be rejected from access.

Implementing AAA/RADIUS on Ethernet Switch

As described above, the Switch 7750, serving as the user access device, or NAS, is the RADIUS client. Figure 57 illustrates the RADIUS authentication network.

Figure 57   Networking with Switch 7750 Applying RADIUS Authentication
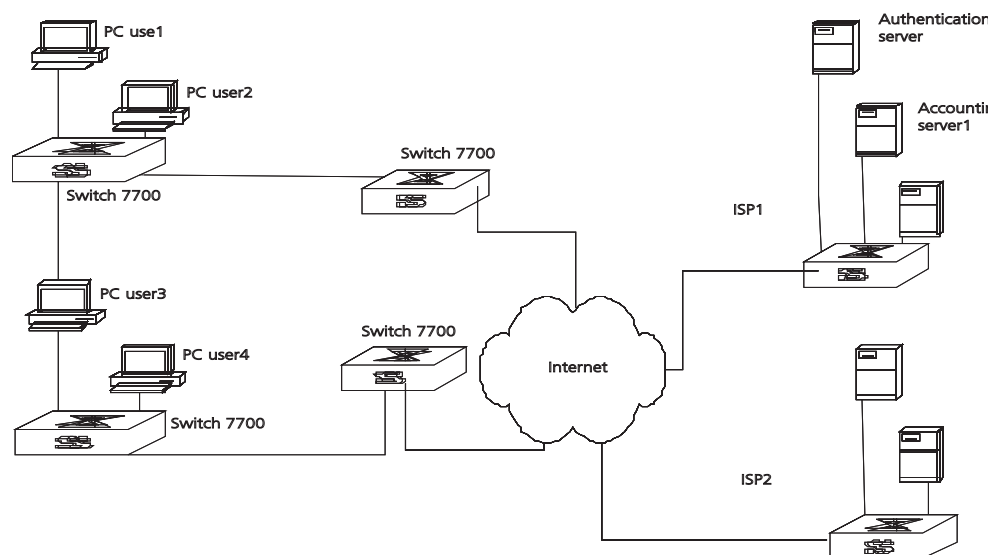
Configuring AAA

AAA configuration includes tasks that are described in the following sections:

■ Creating/Deleting an ISP Domain

■ Configuring Relevant Attributes of an ISP Domain

■ Creating a Local User

■ Setting Attributes of a Local User

■ Disconnecting a User by Force

Among the above configuration tasks, creating an ISP domain is required, otherwise the supplicant attributes cannot be distinguished. The other tasks are optional. You can configure them as required.

Creating/Deleting an ISP Domain

An ISP domain is a group of users belonging to the same ISP. Taking gw20010608@3com163.net as an example in the userid@isp-name format, the isp-name (i.e. 3com163.net) following the @ is the ISP domain name. When the Switch 7750 controls user access, as for an ISP user whose username is in

userid@isp-name format, the system will take userid part as username for identification and take isp-name part as domain name.

The purpose of introducing ISP domain settings is to support the multi-ISP application environment. In such an environment, one access device might access users of different ISPs. Because the attributes of ISP users, such as username support and password formats, etc., are usually different, it is necessary to group them by setting ISP domain. In the Switch 7750 ISP domain view, you can configure a complete set of exclusive ISP domain attributes on a per-ISP domain basis, which includes AAA policy (RADIUS server group applied etc.)

For the Switch 7750, each supplicant belongs to an ISP domain. Up to 16 domains can be configured in the system. If a user has not reported its ISP domain name, the system will put it into the default domain.

Perform the following configurations in system view.

Table 229   Create/Delete ISP Domain

Operation	Command
Create ISP domain or enter the view of a specified domain.	**domain** [isp-name | **default** { **disable** | **enable** isp-name }]
Remove a specified ISP domain	**undo domain** isp-name

By default, the domain name system is already created. The attributes of *system* are all default values.

Configuring Relevant Attributes of an ISP Domain

The relevant attributes of an ISP domain include the adopted RADIUS server group, state, and maximum number of supplicants. Note the following:

- The adopted RADIUS server group is the one used by all the users in the ISP domain. The RADIUS server group can be used for RADIUS authentication or accounting. By default, the default RADIUS server group is used. For details, refer to "Configuring the RADIUS Protocol ".

- Every ISP has active/block states. If an ISP domain is in active state, the users can request for network service, while in block state, users cannot request any network service. An ISP is in the block state when it is created.

- Maximum number of supplicants specifies how many supplicants can be contained in the ISP. By default, for any ISP domain, there is no limit to the number of supplicants.

- The idle cut function means that if the traffic from a certain connection is lower than the defined traffic, cut off the connection.

Perform the following configurations in ISP domain view.

Table 230   Configure Relevant Attributes of ISP Domain

Operation	Command
Specify the adopted RADIUS server group	**radius-scheme** radius-scheme-name
Specify the ISP domain state to be used	**state** { **active** | **block** }
Set a limit to the amount of supplicants	**access-limit** { **disable** | **enable** max-user-number }

Table 230   Configure Relevant Attributes of ISP Domain

Operation	Command
Set the idle	**idle-cut** { **disable**	**enable** minute flow }

By default, after an ISP domain is created, the used RADIUS server group is the default *system* (for relevant parameter configuration, refer to "Configuring the RADIUS Protocol "), the state of domain is **active**, there is no limit to the amount of supplicants, and the idle-cut is **disabled**.

Creating a Local User

A local user is a group of users set on NAS. The username is the unique identifier of a user. A supplicant requesting network service may use local authentication only if its corresponding local user has been added onto NAS.

Perform the following configurations in system view.

Table 231   Create/Delete a Local User and Relevant Properties

Operation	Command
Add local users	**local-user** user-name
Delete all the local users	**undo local-user all**
Delete a local user by specifying its type	**undo local-user** { user-name	**all** [**service-type** { **lan-access**	**ftp**	**telnet**	}] }

By default, there is no local user in the system.

Setting Attributes of a Local User

The attributes of a local user include its password, state, service type and other settings.

Perform the following configurations in system view.

Table 232   Set the Method that a Local User Uses to Set Password

Operation	Command
Set the method that a local user uses to set password	**local-user password-display-mode** { **cipher-force**	**auto** }
Cancel the method that the local user uses to set password	**undo local-user password-display-mode**

The **auto** parameter means that the password display mode will be the one specified by the user at the time of configuring a password (see the **password** command in the following table for reference), and **cipher-force** means that the password display mode of all the accessing users must be in cipher text.

Perform the following configurations in local user view.

Table 233   Set/Remove the Attributes Concerned with a Specified User

Operation	Command
Set a password for a specified user	**password** { **simple**	**cipher** } password

Table 233 Set/Remove the Attributes Concerned with a Specified User

Operation	Command
Remove the password set for the specified user	`undo password`
Set the state of the specified user	`state { active	block }`
Disable the state of the specified user	`undo state { active	block }`
Set a service type for the specified user	`service-type { ftp [ftp-directory directory]	lan-access	[level level	telnet [level level]]	telnet [level level	[level level]] }`
Cancel the service type of the specified user	`undo service-type { telnet [level	[level]]	ftp [ftp-directory]	lan-access	[level	telnet [level]] }`
Configure the attributes of lan-access users	`attribute { ip ip-address	mac mac-address	idle-cut second	access-limit max-user-number	vlan vlanid	location { nas-ip ip-address port portnum	port portnum }*`
Remove the attributes defined for the lan-access users	`undo attribute { ip	mac	idle-cut	access-limit	vlan	location }`

Disconnecting a User by Force

Sometimes it is necessary to disconnect a user or a category of users by force. The system provides the following command to serve this purpose.

Perform the following configurations in system view.

Table 234 Disconnect a User by Force

Operation	Command
Disconnect a user by force	`cut connection { all	access-type { dot1x	gcm }	domain domain-name	interface portnum	ip ip-address	mac mac-address	radius-scheme radius-scheme-name	vlan vlanid	ucibindex ucib-index	user-name user-name }`

By default, no online user will be disconnected by force.

Configuring the RADIUS Protocol

On the Switch 7750, the RADIUS protocol is configured per RADIUS server group basis. In a real networking environment, a RADIUS server group can be an independent RADIUS server or a set of primary/secondary RADIUS servers with the same configuration but two different IP addresses. Attributes of every RADIUS server group include IP addresses of primary and secondary servers, shared key and RADIUS server type, etc.

RADIUS protocol configuration only defines some necessary parameters using information for interaction between NAS and RADIUS Server. To make these parameters effective, it is necessary to configure, in the view, an ISP domain to use

the RADIUS server group, and specify it to use RADIUS AAA schemes. For more about the configuration commands, refer to "Configuring AAA ".

Tasks for configuring RADIUS are described in the following sections:

- Creating/Deleting a RADIUS Server Group
- Setting the IP Address and Port Number of RADIUS Server
- Setting the RADIUS Packet Encryption Key
- Setting the Response Timeout Timer of RADIUS Server
- Setting Retransmission Times of the RADIUS Request Packet
- Enabling the Selection of the RADIUS Accounting Option
- Setting a Real-time Accounting Interval
- Setting Maximum Times of Real-time Accounting Request
- Enabling/Disabling Stop Accounting Request Buffer
- Setting the Maximum Retransmitting Times of the Stop Accounting Request
- Setting the Supported Type of RADIUS Server
- Setting RADIUS Server State
- Setting Username Format Transmitted to RADIUS Server
- Setting the Unit of Data Flow that Transmitted to RADIUS Server
- Configuring a Local RADIUS Server Group
- Configuring Source Address for RADIUS Packets Sent by NAS
- Displaying and Debugging the AAA, RADIUS, and HWTACACS Protocols
- Configuring FTP/Telnet User Authentication at Remote RADIUS Server
- Configuring FTP/Telnet User Authentication at the Local RADIUS Server

Among these tasks, creating RADIUS server group, and setting IP address of the RADIUS server are required, while other takes are optional and can be performed per your requirements.

Creating/Deleting a RADIUS Server Group

As mentioned above, RADIUS protocol configurations are performed on the per RADIUS server group basis. Therefore, before performing other RADIUS protocol configurations, it is compulsory to create the RADIUS server group and enter its view to set its IP address.

You can use the following commands to create/delete a RADIUS server group.

Perform the following configurations in system view.

Table 235   Create/Delete a RADIUS Server Group

Operation	Command
Create a RADIUS server group and enter its view	**radius scheme** radius-server-name
Delete a RADIUS server group	**undo radius scheme** radius-server-name

Several ISP domains can use a RADIUS server group at the same time.

By default, the system has a RADIUS server group named *system* whose attributes are all default values. The default attribute values are introduced in the following section.

Setting the IP Address and Port Number of RADIUS Server

After creating a RADIUS server group, you set IP addresses and UDP port numbers for the RADIUS servers, including primary/second authentication/authorization servers and accounting servers. You can configure up to 4 groups of IP addresses and UDP port numbers. However, you have to set one group of IP address' and UDP port numbers for each pair of primary/second servers to ensure normal AAA operation.

Perform the following configurations in RADIUS server group view.

Table 236   Set IP Address and Port Number of RADIUS Server

Operation	Command
Set IP address and port number of primary RADIUS authentication/authorization server.	**primary authentication** ip-address [port-number]
Restore IP address and port number of primary RADIUS authentication/authorization or server to the default values.	**undo primary authentication**
Set IP address and port number of primary RADIUS accounting server.	**primary accounting** ip-address [port-number]
Restore IP address and port number of primary RADIUS accounting server or server to the default values.	**undo primary accounting**
Set IP address and port number of secondary RADIUS authentication/authorization server.	**secondary authentication** ip-address [port-number]
Restore IP address and port number of second RADIUS authentication/authorization or server to the default values.	**undo secondary authentication**
Set IP address and port number of second RADIUS accounting server.	**secondary accounting** ip-address [port-number]
Restore IP address and port number of second RADIUS accounting server or server to the default values.	**undo secondary accounting**

In real networking environments, the above parameters should be set according to the specific requirements. For example, you may specify 4 groups of different data to map 4 RADIUS servers, or specify one of the two servers as primary authentication/authorization server and second accounting server and the other one as second authentication/authorization server and primary accounting server. You may also set 4 groups of exactly the same data so that every server serves as a primary and secondary AAA server.

To guarantee normal interaction between the NAS and RADIUS servers, you must to guarantee a default route between RADIUS server and NAS before setting IP address and UDP port of the RADIUS server. Because RADIUS protocol uses different UDP ports to receive/transmit authentication/authorization and accounting packets, you should set two different ports accordingly. Suggested by RFC2138/2139, the authentication/authorization port number is 1812 and the accounting port number is 1813. However, you may use values other than the

ones suggested. (Especially for some earlier RADIUS Servers, authentication/authorization port number is often set to 1645 and accounting port number is 1646.)

The RADIUS service port settings on the Switch 7750 need to be consistent with the port settings on the RADIUS server. Normally, RADIUS accounting service port is 1813 and the authentication/authorization service port is 1812.

By default, all the IP addresses of primary/second authentication/authorization and accounting servers are 0.0.0.0, authentication/authorization service port is 1812 and accounting service UDP port is 1813.

Setting the RADIUS Packet Encryption Key

RADIUS client (switch system) and RADIUS server use MD5 algorithm to encrypt the exchanged packets. The two ends verify the packet by setting the encryption key. Only when the keys are identical can both ends accept the packets from each other and give a response.

Perform the following configurations in RADIUS server group view.

Table 237   Set RADIUS Packet Encryption Key

Operation	Command
Set RADIUS authentication/authorization packet encryption key	**key authentication** string
Restore the default RADIUS authentication/authorization packet encryption key.	**undo key authentication**
Set RADIUS accounting packet key	**key accounting** string
Restore the default RADIUS accounting packet key	**undo key accounting**

Setting the Response Timeout Timer of RADIUS Server

RADIUS (authentication/authorization or accounting) request packet is transmitted for a specific period of time. If NAS has not received the response from RADIUS server, it has to retransmit the request to guarantee RADIUS service for the user.

Perform the following configurations in RADIUS server group view.

Table 238   Set Response Timeout Timer of RADIUS Server

Operation	Command
Set response timeout timer of RADIUS server	**timer** second
Restore the response timeout timer of RADIUS server to default value	**undo timer**

By default, timeout timer of RADIUS server is 3 seconds.

Setting Retransmission Times of the RADIUS Request Packet

Since RADIUS protocol uses UDP packets to carry the data, the communication process is not reliable. If the RADIUS server has not responded to NAS before timeout, NAS has to retransmit the RADIUS request packet. If it transmits the packet for more than retry-time, and RADIUS server still has not given any

response, NAS considers the communication with the current RADIUS server disconnected and will transmit the request packet to other RADIUS servers.

Perform the following configurations in RADIUS server group view.

Table 239 Set Retransmission Times of RADIUS Request Packet

Operation	Command
Set retransmission times of RADIUS request packet	`retry` retry-time
Restore the default value of retransmission times	`undo retry`

By default, RADIUS request packet will be retransmitted up to three times.

Enabling the Selection of the RADIUS Accounting Option

If no RADIUS server is available or if RADIUS accounting server fails when the accounting optional is configured, the user can still use the network resource, otherwise, the user will be disconnected.

Perform the following configurations in RADIUS server group view.

Table 240 Enable the Selection of the RADIUS Accounting Option

Operation	Command
Enable the selection of the RADIUS accounting option	`accounting optional`
Disable the selection of the RADIUS accounting option	`undo accounting optional`

The user configured with accounting optional command in RADIUS scheme longer sends a real-time accounting update packet or offline accounting packet.

The `accounting optional` command in a RADIUS server group view is only effective on the accounting that uses this RADIUS server group.

By default, selection of RADIUS accounting option is disabled.

Setting a Real-time Accounting Interval

To implement this feature, it is necessary to set a real-time accounting interval. After the attribute is set, NAS will transmit the accounting information of online users to the RADIUS server regularly.

Perform the following configurations in RADIUS server group view.

Table 241 Set a Real-Time Accounting Interval

Operation	Command
Set a real-time accounting interval	`timer realtime-accounting` minute
Restore the default value of the interval	`undo timer realtime-accounting`

The *minute* variable specifies the real-time accounting interval in minutes. The value must be a multiple of 3.

The value of *minute* is related to the performance of NAS and RADIUS server. The smaller the value is, the higher the performances of NAS and RADIUS have to be. When there are a large amount of users (more than 1000, inclusive), we suggest a

larger value. The following table recommends the ratio of *minute* value to the number of users.

Table 242   Recommended Ratio of Minute to Number of Users

Number of users	Real-time accounting interval (minute)
1 to 99	3
100 to 499	6
500 to 999	12
1000	15

By default, `minute` is set to 12 minutes.

Setting Maximum Times of Real-time Accounting Request

The RADIUS server usually verifies that a user is online with timeout timer. If the RADIUS server has not received the real-time accounting packet from NAS for a specified period, it stops accounting. Therefore, it may be necessary to disconnect the user at the NAS end and on the RADIUS server when some unpredictable failure exists. The Switch 7750 allows you to configure the maximum number of retries for real-time accounting requests. NAS disconnects the user if it has not received a real-time accounting response from the RADIUS server for the specified number of times.

Perform the following configurations in RADIUS server group view.

Table 243   Set Maximum Times of Real-Time Accounting Request Failing to be Responded

Operation	Command
Configure the maximum number of retries for real-time accounting requests.	`retry realtime-accounting` `retry-times`
Restore the maximum number of retries for real-time accounting requests to the default value.	`undo retry realtime-accounting`

The value of `retry-times` is the ceiling value of T/t, where *T* is the period of time in which the RADIUS server connection will timeout, and *t* is the real-time accounting interval of NAS.

By default, the value for `retry-times` is 5.

Enabling/Disabling Stop Accounting Request Buffer

Because the stop accounting request concerns the account balance, and affects the amount to charge a customer, NAS makes its best effort to send the message to the RADIUS accounting server. If the message from the Switch 7750 to RADIUS accounting server has not been responded to, the switch saves it in the local buffer and retransmits until the server responds or discards the messages. The following command can be used to enable the storage of the stop accounting message. If the stop-accounting buffer is enabled, make sure you set the maximum retransmission time.

Perform the following configurations in RADIUS server group view.

Table 244   Enable/Disable Stopping Accounting Request Buffer

Operation	Command
Enable the stop accounting request buffer	`stop-accounting-buffer enable`
Disable the stop accounting request buffer	`undo stop-accounting-buffer enable`

By default, the stop accounting request will be saved in the buffer.

Setting the Maximum Retransmitting Times of the Stop Accounting Request

Because the stop accounting request concerns account balance, and will affect the amount to charge a customer, which is very important for both the subscribers and the ISP, NAS will make its best effort to send the message to the RADIUS accounting server. If the message from the Switch 7750 to RADIUS accounting server has not replied, the switch saves it in the local buffer and retransmits it until the server responds or discards the messages. Use this command to set the maximum retransmission times.

Perform the following configurations in RADIUS server group view.

Table 245   Set the Maximum Retransmitting Times of Stopping Accounting Request

Operation	Command
Set the maximum retransmitting times of stop accounting request	`retry stop-accounting` retry-times
Restore the maximum retransmitting times of stop accounting request to the default value	`undo retry stop-accounting`

By default, the stop accounting request can be retransmitted for up to 500 times.

Setting the Supported Type of RADIUS Server

The Switch 7750 supports the standard RADIUS protocol and the extended RADIUS service platforms, such as IP Hotel, and Portal.

Perform the following configurations in RADIUS server group view.

Table 246   Setting the Supported Type of RADIUS Server

Operation	Command
Setting the supported type of RADIUS Server	`server-type { 3ComType	iphotel	portal	standard }`
Restore the supported type of RADIUS Server to the default setting	`undo server-type`

By default, the RADIUS server type is `standard`.

Setting RADIUS Server State

For the primary and secondary servers, if the primary server is disconnected from NAS because of a fault, NAS will automatically turn to exchange packets with the secondary server. However, after the primary server recovers, NAS does not resume communication with the primary server immediately. Instead, it continues communicating with the secondary server. When the secondary server fails to

communicate, NAS returns to the primary server. The following commands can be used to set the primary server to be active manually, so that NAS can communicate with it immediately after troubleshooting.

When the primary and second servers are both active or block, NAS sends the packets to the primary server only.

Perform the following configurations in RADIUS server group view.

Table 247   Set RADIUS Server State

Operation	Command
Set the state of primary RADIUS server	**state primary** { **accounting** | **authentication** } { **block** | **active** }
Set the state of second RADIUS server	**state secondary** { **accounting** | **authentication** } { **block** | **active** }

By default, the state of each server in RADIUS server group is active.

Setting Username Format Transmitted to RADIUS Server

As mentioned before, clients are generally named in userid@isp-name format. The part following "@" is the ISP domain name. The Switch 7750 will put users into different ISP domains according to their domain name. However, some earlier RADIUS servers rejected the username including ISP domain name. In this case, you have to remove the domain name before sending the username to the RADIUS server. The following command decides whether the username to be sent to RADIUS server carries ISP domain name or not.

Table 248   Set Username Format Transmitted to RADIUS Server

Operation	Command
Set username format transmitted to the RADIUS Server	**user-name-format** { **with-domain** | **without-domain** }

i   *If a RADIUS server group is configured not to allow usernames including ISP domain names, the RADIUS server group cannot be simultaneously used in more than one ISP domain. Otherwise, the RADIUS server will regard two users in different ISP domains as the same user by mistake, if they have the same username (excluding their respective domain names.)*

By default, the RADIUS server group acknowledges that the username sent to it includes ISP domain name.

Setting the Unit of Data Flow that Transmitted to RADIUS Server

The following command defines the unit of the data flow sent to RADIUS server.

Table 249   Set the Unit of Data Flow Transmitted to RADIUS Server

Operation	Command
Set the unit of data flow transmitted to RADIUS server	**data-flow-format data** { **byte** | **giga-byte** | **kilo-byte** | **mega-byte** } **packet** { **giga-byte** | **kilo-byte** | **mega-byte** | **one-packet** }

By default, the default data unit is a byte and the default data packet unit is one packet.

Configuring a Local RADIUS Server Group

RADIUS service adopts authentication/authorization/accounting servers to manage users. Local authentication/authorization/accounting service is also used in these products and it is called local RADIUS function.

Perform the following commands in system view to create/delete local RADIUS server group.

Table 250 Create/Delete a Local RADIUS Server Group

Operation	Command
Create a local RADIUS server group and enter its view	**local-radius nas-ip** ip-address **key** password
Delete a local RADIUS server group	**undo local-radius nas-ip** ip-address

By default, the IP address of local RADIUS server group is 127.0.0.1 and the password is 3com.

When using the local RADIUS server function of the Switch 7750, remember the number of the UDP port used for authentication is 1812 and the number for accounting is 1813.

Configuring Source Address for RADIUS Packets Sent by NAS

Perform the following configurations in the corresponding view.

Table 251 Configuring source address for the RADIUS packets sent by the NAS

Operation	Command
Configure the source address to be carried in the RADIUS packets sent by the NAS (RADIUS scheme view).	**nas-ip** *ip-address*
Cancel the configured source address to be carried in the RADIUS packets sent by the NAS (RADIUS scheme view).	**undo nas-ip**
Configure the source address to be carried in the RADIUS packets sent by the NAS (System view).	**radius nas-ip** *ip-address*
Cancel the configured source address to be carried in the RADIUS packets sent by the NAS (System view).	**undo radius nas-ip**

You can use either command to bind a source address with the NAS.

By default, no source address is specified and the source address of a packet is the address of the interface where it is sent.

Setting the Timers of the RADIUS Server

I. Setting the Response Timeout Timer of the RADIUS Server

After RADIUS (authentication/authorization or accounting) request packet has been transmitted for a period of time, if NAS has not received the response from

RADIUS server, it has to retransmit the request to guarantee RADIUS service for the user.

You can use the following command to set response timeout timer of RADIUS server.

Perform the following configurations in RADIUS scheme view.

Table 2-32 Setting the response timeout timer of the RADIUS server

Operation	Command
Set response timeout timer of RADIUS server	timer seconds
Restore the response timeout timer of RADIUS server to default value	undo timer

By default, timeout timer of RADIUS server is 3 seconds.

II. Setting a Real-time Accounting Interval

To implement real-time accounting, it is necessary to set a real-time accounting interval. After the attribute is set, NAS will transmit the accounting information of online users to the RADIUS server regularly.

You can use the following command to set a real-time accounting interval.

Perform the following configurations in RADIUS scheme view.

Table 2-33 Setting a real-time accounting interval

Operation	Command
Set a real-time accounting interval	timer realtime-accounting minutes
Restore the default value of the interval	undo timer realtime-accounting

minute specifies the real-time accounting interval in minutes. The value shall be a multiple of 3.

The value of minute is related to the performance of NAS and RADIUS server. The smaller the value is, the higher the performances of NAS and RADIUS are required. When there are a large amount of users (more than 1000, inclusive), we suggest a larger value. The following table recommends the ratio of minute value to the number of users.

Table 2-34 Recommended ratio of minute to number of users

Number of users	Real-time accounting interval (minute)
1 to 99	3
100 to 499	6

500 to 99912

=1000=15

By default, minute is set to 12 minutes.

III. Configure the RADIUS Server Response Timer

If the NAS receives no response from the RADIUS server after sending a RADIUS request (authentication/authorization or accounting request) for a period of time, the NAS resends the request, thus ensuring the user can obtain the RADIUS service. You can specify this period by setting the RADIUS server response timeout timer, taking into consideration the network condition and the desired system performance.

Perform the following configurations in RADIUS scheme view.

Table 2-35 Configure the RADIUS server response timer

OperationCommand

Configure the RADIUS server response timertimer response-timeout seconds

Restore the default value of the intervalundo timer response-timeout

By default, the response timeout timer for the RADIUS server is set to three seconds.

Configuring HWTACACS

HWTACACS configuration tasks include:

Table 2-36 HWTACACS configuration

SubsectionTaskCommandViewDescription

1   Creating a HWTACACS schemehwtacacs schemeSystem viewCreating a scheme

2   Configuring the TACACS authentication serverprimary authentication HWTACACS viewConfiguring the primary authentication server

    secondary authenticationHWTACACS viewConfiguring the secondary authentication server

3   Configuring the TACACS authorization serverprimary authorization HWTACACS viewConfiguring the primary authorization server

    secondary authorizationHWTACACS viewConfiguring the secondary authorization server

4   Configuring the TACACS accounting server and related featuresprimary accountingHWTACACS viewConfiguring the primary accounting server

    secondary accountingHWTACACS viewConfiguring the secondary accounting server

    retry stop-accountingHWTACACS viewEnabling stop-accounting packet retransmission and setting the allowed maximum number of transmission attempts

    reset stop-accounting-buffer hwtacacs-schemeHWTACACS viewClearing the stop-accounting request packets that have no response

5   Configuring the source address for HWTACACS packets sent from NASnas-ip HWTACACS viewOptional

    hwtacacs nas-ipSystem viewRequired

6   Setting the key of the TACACS serverkeyHWTACACS viewConfiguring keys

7   Setting the username format for the TACACS serveruser-name-format HWTACACS viewConfiguring the format of user name

8   Setting the data flow unit for the TACACS serverdata-flow-formatHWTACACS viewConfiguring flow traffic unit

9   Setting the timers of the TACACS servertimer response-timeoutHWTACACS viewSetting the TACACS server response timeout time

    timer quietHWTACACS viewSetting the waiting time before the primary TACACS server resumes the active state

    timer realtime-accountingHWTACACS viewSetting the real-time accounting interval

    Note:

Pay attention to the following when configuring a TACACS server:

    HWTACACS server does not check whether a scheme is being used by users when changing most of HWTACS attributes, unless you delete the scheme.

    By default, the TACACS server has no key.

In the above configuration tasks, creating HWTACACS scheme and configuring TACACS authentication/authorization server are required; all other tasks are optional and you can determine whether to perform these configurations as needed.

2.4.2 Creating a HWTACAS Scheme

As aforementioned, HWTACACS protocol is configured scheme by scheme. Therefore, you must create a HWTACACS scheme and enter HWTACACS view before you perform other configuration tasks.

Perform the following configuration in system view.

Table 2-37 Creating a HWTACACS scheme

OperationCommand

Create a HWTACACS scheme and enter HWTACACS view.hwtacacs scheme hwtacacs-scheme-name

Delete a HWTACACS scheme.undo hwtacacs scheme hwtacacs-scheme-name

By default, no HWTACACS scheme exists.

If the HWTACACS scheme you specify does not exist, the system creates it and enters HWTACACS view.

The system supports up to 16 HWTACACS schemes. You can only delete the schemes that are not being used.

2.4.3 Configuring HWTACACS Authentication Servers

Perform the following configuration in HWTACACS view.

Table 2-38 Configuring HWTACACS authentication servers

OperationCommand

Configure the HWTACACS primary authentication server.primary authentication ip-address [port]

Delete the HWTACACS primary authentication server.undo primary authentication

Configure the HWTACACS secondary authentication server.secondary authentication ip-address [port]

Delete the HWTACACS secondary authentication server.undo secondary authentication

The primary and secondary authentication servers cannot use the same IP address. The default port number is 49.

If you execute this command repeatedly, the new settings will replace the old settings.

The authentication server can be deleted only when there is no active TCP connection used for sending authentication packets.

2.4.4 Configuring HWTACACS Authorization Servers

Perform the following configuration in HWTACACS view.

Table 2-39 Configuring HWTACACS authorization servers

OperationCommand

Configure the primary HWTACACS authorization server.primary authorization ip-address [port]

Delete the primary HWTACACS authorization server.undo primary authorization

Configure the secondary HWTACACS authorization server.secondary authorization ip-address [port]

Delete the secondary HWTACACS authorization server.undo secondary authorization

The primary and secondary authorization servers cannot use the same IP address. The default port number is 49.

If you execute this command repeatedly, the new settings will replace the old settings.

2.4.5 Configuring HWTACACS Accounting Servers and the Related Attributes

I. Configuring HWTACACS accounting servers

Perform the following configuration in HWTACACS view.

Table 2-40 Configuring HWTACACS accounting servers

OperationCommand

Configure the primary TACACS accounting server.primary accounting ip-address [port]

Delete the primary TACACS accounting server.undo primary accounting

Configure the secondary TACACS accounting server.secondary accounting ip-address [port]

Delete the secondary TACACS accounting server.undo secondary accounting

The primary and secondary accounting servers cannot use the same IP address. The default port number is 49.

If you execute this command repeatedly, the new settings will replace the old settings.

II. Enabling stop-accounting packet retransmission

Perform the following configuration in HWTACACS view.

Table 2-41 Configuring stop-accounting packet retransmission

OperationCommand

Enable stop-accounting packet retransmission and set the allowed maximum number of transmission attemptsretry stop-accounting retry-times

Disable stop-accounting packet retransmissionundo retry stop-accounting

Clear the stop-accounting request packets that have no responsereset stop-accounting-buffer hwtacacs-scheme hwtacacs-scheme-name

By default, stop-accounting packet retransmission is enabled, and the maximum number of transmission attempts is 300.

2.4.6 Configuring Source Address for HWTACACS Packets Sent by NAS

Perform the following configuration in the corresponding view.

Table 2-42 Configuring source address for HWTACACS packets sent by the NAS

OperationCommand

Configure the source address for HWTACACS packets sent from the NAS (HWTACACS view).nas-ip ip-address

Delete the configured source address for HWTACACS packets sent from the NAS (HWTACACS view).undo nas-ip

Configure the source address for HWTACACS packets sent from the NAS (System view).hwtacacs nas-ip ip-address

Cancel the configured source address for HWTACACS packets sent from the NAS (System view).undo hwtacacs nas-ip

The HWTACACS view takes precedence over the system view when configuring the source address for HWTACACS packets sent from the NAS.

By default, the source address is not specified, and the interface address for packet sending is used as the source address.

2.4.7 Setting a Key for Securing the Communication with TACACS Server

When using a TACACS server as an AAA server, you can set a key to improve the communication security between the switch and the TACACS server.

Perform the following configuration in HWTACACS view.

Table 2-43 Setting a key for securing the communication with the HWTACACS server

OperationCommand

Configure a key for securing the communication with the accounting, authorization or authentication serverkey { accounting | authorization | authentication } string

Delete the configurationundo key { accounting | authorization | authentication }

No key is configured by default.

2.4.8 Setting the Username Format Acceptable to the TACACS Server

Username is usually in the "userid@isp-name" format, with the domain name following "@".

If a TACACS server does not accept the username with domain name, you can remove the domain name and resend it to the TACACS server.

Perform the following configuration in HWTACACS view.

Table 2-44 Setting the username format acceptable to the TACACS server

OperationCommand

Send username with domain name.user-name-format with-domain

Send username without domain name.user-name-format without-domain

By default, each username sent to a TACACS server contains a domain name.

2.4.9 Setting the Unit of Data Flows Destined for the TACACS Server

Perform the following configuration in HWTACACS view.

Table 2-45 Setting the unit of data flows destined for the TACACS server

OperationCommand

Set the unit of data flows destined for the TACACS serverdata-flow-format data { byte | giga-byte | kilo-byte | mega-byte }

data-flow-format packet { giga-packet | kilo-packet | mega-packet | one-packet }

Restore the default unit of data flows destined for the TACACS serverundo data-flow-format { data | packet }

The default data flow unit is byte.

Setting TACACS Server Timers

Setting the response timeout timer   After HWTACACS is implemented on the basis of TCP, server response timeout or TCP timeout may terminate the connection to the TACACS server.

Perform the following configuration in HWTACACS view.

Table 252   Setting the response timeout timer

Operation	Command
Set the response timeout time	**timer response-timeout** *seconds*
Restore the default setting	**undo timer response-timeout**

The default response timeout timer is set to 5 seconds.

Setting the quiet timer for the primary TACACS server   Perform the following configuration in HWTACACS view.

Table 253   Setting the quiet timer for the primary TACACS server

Operation	Command
Set the quiet timer for the primary TACACS server.	**timer quiet** *minutes*
Restore the default setting.	**undo timer quiet**

By default, the primary TACACS server must wait five minutes before it can resume the active state.

Setting a realtime accounting interval   The setting of real-time accounting interval is necessary to real-time accounting. After an interval value is set, the NAS transmits the accounting information of online users to the TACACS accounting server periodically.

Perform the following configuration in HWTACACS view.

Table 254   Setting a real-time accounting interval

Operation	Command
Set a real-time accounting interval	**timer realtime-accounting** *minutes*
Restore the default real-time accounting interval	**undo timer realtime-accounting**

The interval is in minutes and must be a multiple of 3.

The setting of real-time accounting interval somewhat depends on the performance of the NAS and the TACACS server: a shorter interval requires higher device performance. You are therefore recommended to adopt a longer interval when there are a large number of users (more than 1000, inclusive). The following table lists the numbers of users and the recommended intervals.

Table 255   Numbers of users and the recommended intervals

Number of users	Real-time accounting interval (minutes)
1 - 99	3
100 - 499	6

Table 255   Numbers of users and the recommended intervals

Number of users	Real-time accounting interval (minutes)
500 - 999	12
¦1000	¦15

The real-time accounting interval defaults to 12 minutes.

Displaying and Debugging the AAA, RADIUS, and HWTACACS Protocols

After you configure RADIUS, execute the **display** command in all views to display the running of the AAA, RADIUS, and HWTACACS configuration, and to verify the effect of the configuration. Execute the **reset** command in user view to reset the configuration. Execute the **debugging** command in user view to debug the configuration.

Table 256   Displaying and Debugging AAA and RADIUS/HWTACACS Protocol

Operation	Command
Display the configuration information of the specified or all the ISP domains.	**display domain** [isp-name]
Display related information of user's connection	**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** vlanid | **ucibindex** ucib-index | **user-name** user-name]
Display related information of the local user	**display local-user** [**domain** isp-name | **idle-cut** { **disable** | **enable** } | **service-type** { **telnet** | **ftp** | **lan-access** | **terminal** } | **state** { **active** | **block** } | **user-name** user-name | **vlan** vlan-id]
Display the statistics of local RADIUS authentication server	**display local-server statistics**
Display the configuration information of RADIUS schemes	**display radius** [radius-scheme-name]
Display the statistics of RADIUS packets	**display radius statistics**
Display the stopping accounting requests saved in buffer without response	**display stop-accounting-buffer** { **radius-scheme** radius-scheme-name | **session-id** session-id | **time-range** start-time stop-time | **user-name** user-name }
Display the specified or all the HWTACACS schemes	**display hwtacacs** [hwtacacs-scheme-name]
Display information on the stop-accounting packets in the buffer	**display stop-accounting-buffer hwtacacs-scheme** hwtacacs-scheme-name
Delete the stopping accounting requests saved in buffer without response	**reset stop-accounting-buffer** { **radius-scheme** radius-scheme-name | **session-id** session-id | **time-range** start-time stop-time | **user-name** user-name }

Table 256   Displaying and Debugging AAA and RADIUS/HWTACACS Protocol

Operation	Command
Clear stop-accounting packets from the buffer	`reset stop-accounting-buffer { radius-scheme` radius-scheme-name `| session-id` session-id `| time-range` start-time stop-time `| user-name` user-name `}`
Reset the statistics of RADIUS server	`reset radius statistics`
Clear stop-accounting packets from the buffer	`reset stop-accounting-buffer hwtacacs-scheme` hwtacacs-scheme-name
Reset the statistics of HWTACACS server	`reset hwtacacs statistics { accounting	authentication	authorization	all }`
Enable RADIUS packet debugging	`debugging radius packet`
Disable RADIUS packet debugging	`undo debugging radius packet`
Enable debugging of local RADIUS authentication server	`debugging local-server { all	error	event	packet }`
Disable debugging of local RADIUS authentication server	`undo debugging local-server { all	error	event	packet }`
Enable HWTACACS debugging	`debugging hwtacacs { all	error	event	message	receive-packet	send-packet }`
Disable HWTACACS debugging	`undo debugging hwtacacs { all	error	event	message	receive-packet	send-packet }`

AAA, RADIUS, and HWTACACS Protocol Configuration Examples

AAA/RADIUS protocol configuration commands are generally used together with 802.1x configuration commands. Refer to the typical configuration examples provided in "Configuring 802.1x" on page 209.

Configuring FTP/Telnet User Authentication at Remote RADIUS Server

Configuring Telnet user authentication at the remote server is similar to configuring FTP users. The following description is based on Telnet users.

In the environment illustrated in the following figure, the the RADIUS server must be configured to authenticate the Telnet users to be registered.

One RADIUS server (the authentication server) is connected to the switch and the server IP address is 10.110.91.146. The password for exchanging messages between the switch and the authentication server is "expert". The switch cuts off domain name from username and sends the left part to the RADIUS server.

Figure 58 Configuring Remote RADIUS Authentication for Telnet Users

Authentication Servers
(IP address: 10.110.91.164)

Internet

Telnet user

Switch
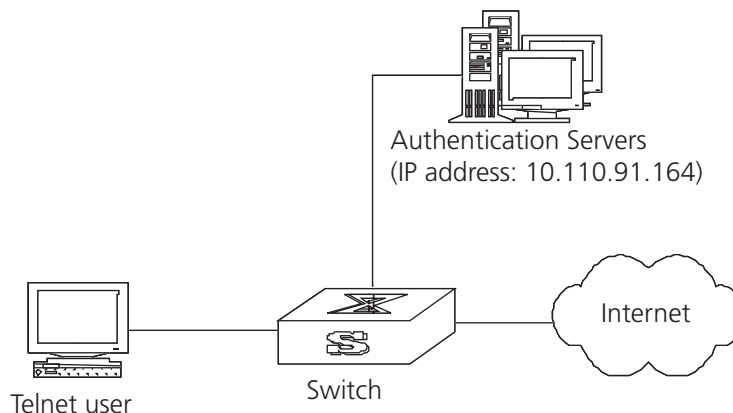
1 Add a Telnet user.

For details about configuring FTP and Telnet users, see "Configuring the User Interface" on page 20.

2 Configure the remote authentication mode for the Telnet user, in this example, the scheme mode.

```
[SW7750-ui-vty0-4]authentication-mode scheme
```

3 Configure the domain.

```
[SW7750]domain cams
[SW7750-isp-cams]quit
```

4 Configure RADIUS scheme.

```
[SW7750]radius scheme cams
[SW7750-radius-cams]primary authentication 10.110.91.146 1812
[SW7750-radius-cams]key authentication expert
[SW7750-radius-cams]server-type 3com
[SW7750-radius-cams]user-name-format without-domain
```

5 Configure the association between domain and RADIUS.

```
[SW7750-radius-cams]quit
[SW7750]domain cams
[SW7750-isp-cams]radius-scheme cams
```

Configuring FTP/Telnet User Authentication at the Local RADIUS Server

Local RADIUS authentication of Telnet/FTP users is similar to remote RADIUS authentication. But you should modify the server IP address to 127.0.0.1, authentication password to 3Com, the UDP port number of the authentication server to 1645.

For details about local RADIUS authentication of Telnet/FTP users, see "Configuring a Local RADIUS Server Group"on page 228.

Configuring the FTP/Telnet User Authentication at a Remote TACACS Server

Configure the switch to use a TACACS server to provide AAA services to login users (see the following figure).

Connect the switch to one TACACS server (providing the services of authentication and authorization) with the IP address 10.110.91.164. On the

switch, set the shared key for AAA packet encryption to *expert*. Configure the switch to send usernames to the TACACS server with isp-name removed.

On the TACACS server, set the shared key for encrypting the packets exchanged with the switch to **expert**; add the usernames and passwords of users:

1 Configure a HWTACACS scheme.

```
[Quidway]hwtacacs scheme hwtac
[Quidway-hwtacacs-hwtac]primary authentication 10.110.91.164 1812
[Quidway-hwtacacs-hwtac]primary authorization 10.110.91.164 1813
[Quidway-hwtacacs-hwtac]key authentication expert
[Quidway-hwtacacs-hwtac]key authorization expert
[Quidway-hwtacacs-hwtac]undo user-name-format with-domain
[Quidway-hwtacacs-hwtac]quit
```

2 Associate the domain with the HWTACACS.

```
[Quidway]domain hwtacacs
[Quidway-isp-hwtacacs]scheme hwtacacs-scheme hwtac
```

Dynamic VLAN with RADIUS Server Configuration Example

The RADIUS server (taking Windows IAS as example) delivers sting VLAN ID *test*, which corresponds to the name of VLAN 100 on the switch. The switch can add the port to VLAN 100 when the server delivers **test**.

1 Specify RADIUS scheme

```
[Quidway]radius scheme ias
[Quidway-radius-ias]primary authentication 10.11.1.1
[Quidway-radius-ias]primary accounting 10.11.1.2
[Quidway-radius-ias]key authentication hello
[Quidway-radius-ias]key accounting hello
[Quidway-radius-ias]quit
```

2 Create ISP domain

```
[Quidway]domain ias
[Quidway-isp-ias]scheme radius-scheme ias
```

3 Configure VLAN delivery mode as string

```
[Quidway-isp-ias]vlan-assignment-mode string
[Quidway-isp-ias]quit
```

4 Create a VLAN and specify its name.

Create a VLAN.

```
[Quidway]vlan 100
```

Configure name of the delivered VLAN.

```
[Quidway-vlan100]name test
```

5 Configure on the Windows IAS server the VLAN delivery mode to string and the name of the delivered VLAN to *test*.

i *For the string delivery mode, the VLAN to be delivered must be an existing one on the switch. That is, you must have created the VLAN and configured a name for it on the switch. There is no such a restriction for the integer mode.*

Troubleshooting AAA, RADIUS, and HWTACACS Configurations

The RADIUS protocol of the TCP/IP protocol suite is located on the application layer. It specifies how to exchange user information between the NAS and RADIUS servers of an ISP.

Tasks for Troubleshooting AAA and Radius are described in the following sections:

■ User authentication/authorization always fails

■ RADIUS packet cannot be transmitted to RADIUS server.

■ After being authenticated and authorized, the user cannot send charging bill to the RADIUS server.

User authentication/authorization always fails

■ The username may not be in the userid@isp-name format or NAS has not been configured with a default ISP domain. Please use the username in proper format and configure the default ISP domain on NAS.

■ The user may not have been configured in the RADIUS server database. Check the database and make sure that the configuration information of the user does exist in the database.

■ The user may have input a wrong password. Make sure that the supplicant inputs the correct password.

■ The encryption keys of the RADIUS server and NAS server may be different. Check carefully and make sure that they are identical.

■ There might be some communication fault between NAS and RADIUS server, which can be discovered through pinging RADIUS from NAS. Ensure the normal communication between NAS and RADIUS.

RADIUS packet cannot be transmitted to RADIUS server.

■ The communication lines (on physical layer or link layer) connecting NAS and RADIUS server may not work well.

■ The IP address of the corresponding RADIUS server may not have been set on NAS. Set a proper IP address for RADIUS server.

■ UDP ports of authentication/authorization and accounting services may not be set properly. Make sure they are consistent with the ports provided by RADIUS server.

After being authenticated and authorized, the user cannot send charging bill to the RADIUS server.

1 The accounting port number may be set improperly. Set a proper number.

2 The accounting service and authentication/authorization service are provided on different servers, but NAS requires the services to be provided on one server (by specifying the same IP address). Make sure the settings of servers are consistent with the actual conditions.

11

SYSTEM MANAGEMENT

This chapter covers the following topics:

- File System
- Managing the MAC Address Table
- Managing Devices
- Maintaining and Debugging the System
- SNMP
- RMON
- NTP

File System

The Switch 7750 provides a file system module for efficient management with storage devices such as flash memory. The file system offers file access and directory management, including creating the file system; creating, deleting, modifying, and renaming a file or a directory; and opening files.

By default, the file system requires that the user confirm before executing commands. This prevents unwanted data loss.

Managing the file system is described in the following sections:

- Using a Directory
- Managing Files
- Formatting Storage Devices
- Setting the Prompt Mode of the File System
- Configuring File Management
- FTP
- TFTP

Using a Directory

You can use the file system to create or delete a directory, display the current working directory, and display the information about the files or directories under a specified directory. Use the commands in Table 257 to perform directory operations.

Perform the following operations in user view.

Table 257   Directory Operation

Operation	Command
Create a directory	**mkdir** directory

Table 257 Directory Operation

Operation	Command
Delete a directory	**rmdir** directory
Display the current working directory	**pwd**
Display the information about directories or files	**dir** [/ **all**] [file-url]
Change the current directory	**cd** directory

Managing Files You can use the file system to delete, undelete, or permanently delete a file. It can also be used to display file contents; rename, copy, and move a file; and display the information about a specified file. Use the commands in Table 258 to perform file operations.

Perform the following operations in user view.

Table 258 File Operation

Operation	Command
Delete a file from the file system and move it to the recycle bin	**delete** file-url
Restore a file from the recycle bin	**undelete** file-url
Delete a file from the recycle bin permanently	**reset recycle-bin** file-url
View contents of a file	**more** file-url
Rename a file	**rename** fileurl-source fileurl-dest
Copy a file	**copy** fileurl-source fileurl-dest
Move a file	**move** fileurl-source fileurl-dest
Display the information about directories or files	**dir** [/ **all**] [file-url]
Execute the specified batch file (System view)	**execute** *filename*

Formatting Storage Devices The file system can be used to format the flash memory on the Switch 7750 fabric module.

Perform the following operation in user view.

Table 259 Formatting Storage Devices

Operation	Command
Format the storage device	**format** filesystem

Setting the Prompt Mode of the File System Use the command in Table 260 to confirm prompts for file system commands.

Perform the following operation in system view.

Table 260 File System Operation

Operation	Command
Set the file system prompt mode.	**file prompt** { **alert**	**quiet** }

Example: File System Operation

1 Format the flash.

```
<SW7750>format flash:
All sectors will be erased, proceed? [confirm] y
Format flash: completed
```

2 Display the working directory in the flash.

```
<SW7750>cd flash:/
<SW7750>pwd
flash:/
```

3 Create a directory named test.

```
<SW7750>mkdir test
```

4 Display the flash directory information after creating the test directory.

```
<SW7750>dir
Directory of *
0   drw-        0  Mar 09 2002 12:01:44   test
523776 bytes total (476160 bytes free)
```

Configuring File Management

The management module configuration file provides a user-friendly operation interface. It saves the configuration of the switch in a text file, in command line format, as a record of the whole configuration process. You can view the configuration information.

The configuration file includes:

■ Configuration commands — Commands are based on command views. The commands are sorted in one section. The sections are separated with a blank line or a comment line (A comment line begins with a pound sign "# "). Default constants are not saved.

■ Generally, the sections in the file are arranged in the following order: system configuration, ethernet port configuration, vlan interface configuration, routing protocol configuration, and so on.

Management of the configuration files includes tasks described in the following sections:

■ Displaying the Current and Saved Configuration of the Switch

■ Saving the Current Configuration

■ Erasing the Configuration Files from Flash Memory

Displaying the Current and Saved Configuration of the Switch

After being powered on, the system reads the configuration file from flash memory. The default configuration file is sw7750cfg.txt. If there is no configuration file in flash, the system begins the initialization with the default parameters. You can use the commands in Table 261 to display the current and saved configuration of the switch.

Perform the following configuration in all views.

Table 261   Display the Configurations of the Ethernet Switch

Operation	Command
Display the saved configuration of the Ethernet switch	**display saved-configuration**
Display the current configuration of the Ethernet switch	**display current-configuration** [**controller** | **interface** interface-type [interface-number] | **configuration** [configuration] [| { begin | exclude | **include** } regular-expression]

> *The configuration files are displayed in their corresponding saving formats.*

Saving the Current Configuration

Use the **save** command to retain the current-configuration in the flash memory. The configurations are saved and used when the system is next powered on.

Perform the following configuration in user view.

Table 262   Save the Current-Configuration

Operation	Command
Save the current-configuration	**save**

Erasing the Configuration Files from Flash Memory

The **reset saved-configuration** command can be used to erase the configuration files from flash memory. The system will use the default configuration parameters for initialization when the switch is powered on the next time.

Perform the following configuration in user view.

Table 263   Erase the Configuration Files from Flash Memory

Operation	Command
Erase the configuration files from the Flash Memory	**reset saved-configuration**

You can erase the configuration files from flash memory in the following cases:

■ If the software does not match the configuration files after the software is upgraded.

■ If the configuration files in flash are damaged, for example, if the wrong configuration file has been downloaded.)

FTP   FTP is a common way to transmit files on the Internet and IP network. FTP is a TCP/IP protocol on the application layer and is used for transmitting files between a remote server and a local host.

The Ethernet switch provides the following FTP services:

■ FTP server — You can run the FTP client program to log in to the server and access the files on it.

■ FTP client — After connecting to the server by running the terminal emulator or Telnet on a PC, you can access the files on it, using the FTP command.

FTP Server configuration includes tasks described in the following sections:

■ Enabling and Disabling the FTP Server
■ Configuring the FTP Server Authentication and Authorization
■ Configuring FTP Server Parameters
■ Displaying and Debugging the FTP Server
■ Introduction to FTP Client

Enabling and Disabling the FTP Server

You can use the following commands to enable or disable the FTP server. Perform the following configuration in system view.

Table 264   Enable/Disable FTP Server

Operation	Command
Enable the FTP server	`ftp server enable`
Disable the FTP server	`undo ftp server`

The FTP server supports multiple user access. A remote FTP client sends a request to the FTP server. Then, the FTP server carries out the corresponding operation and returns the result to the client.

By default, the FTP server is disabled.

Configuring the FTP Server Authentication and Authorization

You can use the following commands to configure FTP server authentication and authorization. The authorization information of the FTP server includes the top working directory provided for FTP clients.

Perform the following configuration in system view.

Table 265   Configure the FTP Server Authentication and Authorization

Operation	Command
Create new local user and enter local user view (system view)	`local-user` username
Delete local user (system view)	`undo local-user` [username | **all** [**service-type ftp**]]
Configure password for local user (local user view)	`password` [**cipher** | **simple**] password
Configure service type for local user (local user view)	`service-type ftp ftp-directory` directory
Cancel password for local user (local user view)	`undo password`
Cancel service type for local user (local user view)	`undo service-type ftp` [`ftp-directory`]

Only clients who have passed the authentication and authorization successfully can access the FTP server.

Configuring FTP Server Parameters

You can use the following commands to configure the connection timeout of the FTP server. If the FTP server does not receive a service request from the FTP client for a period of time, it will cut the connection to it, thereby avoiding illegal access by unauthorized users.

Perform the following configuration in system view.

Table 266   Configure FTP Server Connection Timeout

Operation	Command
Configure FTP server connection timeouts	`ftp timeout minute`
Restoring the default FTP server connection timeouts	`undo ftp timeout`

By default, the FTP server connection timeout is 30 minutes.

Displaying and Debugging the FTP Server

Execute the `display` command in all views to display the FTP Server configuration, and to verify the effect of the configuration.

Table 267   Display and Debug the FTP Server

Operation	Command
Display FTP server	`display ftp-server`
Display the connected FTP users.	`display ftp-user`

The `display ftp-server` command can be used for displaying configuration information about the current FTP server, including, the maximum amount of users supported by FTP server and the FTP connection timeout. The `display ftp-user` command can be used for displaying the detail information about connected FTP users.

Introduction to FTP Client

As an additional function provided by the Switch 7750, the FTP client is an application module and has no configuration functions. The switch connects the FTP clients and the remote server and inputs the command from the clients for corresponding operations (such as creating or deleting a directory).

TFTP   Trivial File Transfer Protocol (TFTP) is a simple protocol for file transmission that has no complicated interactive access interface or authentication control, and therefore it can be used when there is no complicated interaction between the clients and server. TFTP is implemented on the basis of UDP.

TFTP transmission originates with the client. To download a file, the client sends a request to the TFTP server and receives the data, then sends an acknowledgement to it. To upload a file, the client sends a request to the TFTP server and transmits data to it, then receives the acknowledgement from it.

TFTP configuration tasks include:

■ Configuring the File Transmission Mode

■ Downloading Files with TFTP

■   Downloading Files with TFTP

Configuring the File Transmission Mode

TFTP transmits files in two modes; binary mode for program files and ASCII mode for text files. Use the following commands to configure the file transmission mode.

Perform the following configuration in system view.

Table 268   Configuring the File Transmission Mode

Operation	Command
Configure the file transmission mode	**tftp** { **ascii**	**binary** }

By default, TFTP transmits files in binary mode.

Downloading Files with TFTP

To download a file, the client sends a request to the TFTP server and receives data from it, then sends acknowledgement to it. Use the following commands to download files with TFTP.

Perform the following configuration in system view.

Table 269   Downloading Files with TFTP

Operation	Command
Download files with TFTP	**tftp** tftp-server **get** source-file [dest-file]

Uploading Files with TFTP

To upload a file, the client sends a request to the TFTP server and transmits data to it, then receives the acknowledgement from it. Use the following commands to upload files.

Perform the following configuration in system view.

Table 270   Uploading Files with TFTP

Operation	Command
Upload files with TFTP	**tftp** tftp-server **put** source-file [dest-file]

Managing the MAC Address Table

The Switch 7750 maintains a MAC address table for fast forwarding of packets. A table entry includes the MAC address of a device and the port ID of the switch connected to it. The switch learns dynamic entries when it receives a data frame from a port (assumed as port A). The switch analyzes the source MAC address and considers that the packets destined for the source MAC address can be forwarded through port A. If the MAC address table contains the MAC_SOURCE, the switch updates the corresponding entry, otherwise, it adds the new MAC address (and the corresponding forwarding port) as a new entry to the table.

The system forwards the packets whose destination addresses can be found in the MAC address table. The network device responds after receiving a broadcast packet and the response contains the MAC address of the device, which the

switch learns and adds in the MAC address table. After this, subsequent packets destined for the same MAC address can be forwarded directly. If the MAC address cannot be found after broadcasting the packet, the switch will drop it and notify the transmitter that the packet did not arrive at the destination.

Figure 59   The Switch 7750 Forwards Packets According to the MAC Address Table
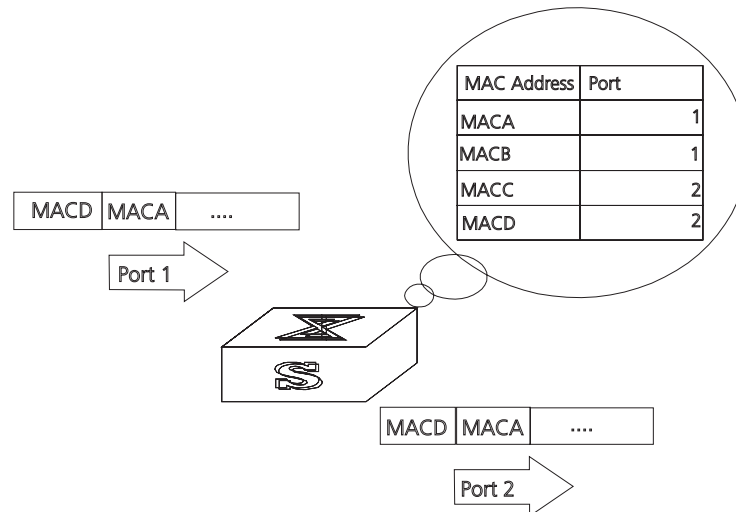
The Switch 7750 also provides the function of MAC address aging. If the switch does not receive a packet from a MAC address for a set period of time, it will delete the related entry from the MAC address table.

You can add or modify MAC address entries manually according to the actual networking environment. The entries can be static or dynamic.

Configuring the MAC Address Table

MAC address table management includes:

- Setting MAC Address Table Entries
- Disabling or Enabling Global MAC Address Learning
- Disabling or Enabling MAC Address Learning on a Port
- Setting MAC Address Aging Time
- Displaying and Debugging the MAC Address Table

Setting MAC Address Table Entries

You can manually add, modify, or delete entries in a MAC address table according to actual needs. you can also delete all (unicast) MAC address table entries related to a specified port or delete a specified type of entries, such as dynamic or static entries.

Use the following commands to add, modify, or delete the entries in MAC address table.

Perform the following configuration in system view.

Table 271   Setting MAC Address Table Entries

Operation	Command
Add or modify an address entry	**mac-address** { **static** | **dynamic** } hw-addr **interface** { interface-name | interface-type interface-num }
Delete an address entry	**undo mac-address** [{ **static** | **dynamic** } mac-address **interface** { interface-name | interface-type interface-num } vlan-id]

Disabling or Enabling Global MAC Address Learning

With the address learning function, an Ethernet switch can learn new MAC addresses. When it receives a packet destined for a MAC address it has already learned, the switch forwards the packet directly, instead of flooding all ports.

Sometimes, for the sake of security, it is necessary to disable the address learning function. A common threat is from hackers who attack the switch with packets from different source MAC addresses, thereby exhausting the address table resources and making it impossible for the switch to update the MAC address table to reflect network changes. Such an attack can be avoided by disabling the MAC address learning function.

You can use the following commands to disable or enable the MAC address learning globally.

Perform the following configuration in system view.

Table 272   Disabling or Enabling the MAC Address Learning

Operation	Command
Disable the MAC address learning	**mac-address mac-learning disable**
Enable the MAC address learning	**undo mac-address mac-learning disable**

By default, the MAC address learning function is enabled.

Disabling or Enabling MAC Address Learning on a Port

After the MAC address learning has been enabled globally, you can disable it on individual ports.

Use the following commands to disable the MAC address learning on a specified port.

Perform the following configurations in the Ethernet port view.

Table 273   Disable/Enable the MAC Address Learning

Operation	Command
Disable the MAC address learning	**mac-address mac-learning disable**
Enable the MAC address learning	**undo mac-address mac-learning disable**

By default, the MAC address learning function is enabled.

Setting MAC Address Aging Time

Setting an appropriate aging time implements MAC address aging. Too long or too short an aging time set by subscribers will cause the Ethernet switch to flood a large amount of data packets. This affects the switch operation performance.

If aging time is set too long, the Ethernet switch stores a great number of out-of-date MAC address tables. This consumes MAC address table resources and the switch will not be able to update the MAC address table according to the network change.

If aging time is set too short, the Ethernet switch may delete valid MAC address table entries.

You can use the following commands to set the MAC address aging time for the system.

Perform the following configuration in system view.

Table 274   Setting the MAC Address Aging Time for the System

Operation	Command
Set the dynamic MAC address aging time	`mac-address timer { aging age | no-aging }`
Restore the default MAC address aging time	`undo mac-address timer aging-time`

In addition, this command takes effect on all the ports. However, the address aging only functions on the dynamic addresses (the learned or configured as age entries by the user).

By default, the aging-time is 300 seconds. With the no-aging parameter, the command performs no aging on the MAC address entries.

Displaying and Debugging the MAC Address Table

Execute the `display` command in all views to display the MAC address table configuration, and to verify the effect of the configuration.

Execute the `debugging` command in user view to debug MAC address table configuration.

Table 275   Displaying and Debugging MAC Address Table

Operation	Command
Display the information in the address table	`display mac-address [ static | dynamic ] [ [ interface { interface-name | interface-type interface-num } ] [ vlan vlan-id ] ]`
Display the aging time of dynamic address table entries	`display mac-address aging-time`
Display the dynamic MAC address learning capability of the system and ports	`display mac-address learning [ interface-type interface-num | interface-name ]`

Table 275   Displaying and Debugging MAC Address Table

Operation	Command
Enable the address table management debugging	**debugging mac-address**
Disable the address table management debugging	**undo debugging mac-address**

Example: Configuring MAC Address Table Management

The user logs in to the switch through the console port to configure the address table management. Set the address aging time to 500s and add a static address 00e0-fc35-dc71 to Ethernet 1/0/2 in vlan1.

Figure 60   Typical Configuration of Address Table Management
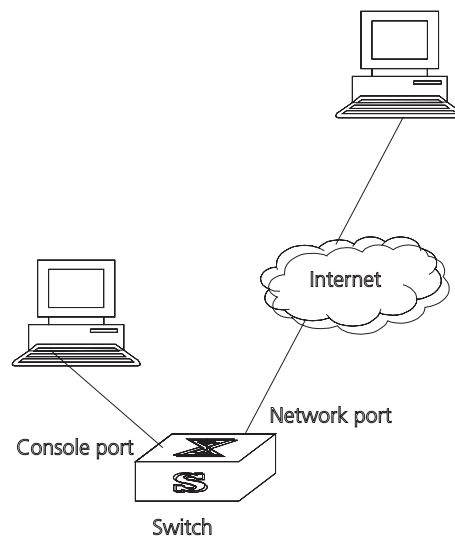
1 Enter the system view of the switch.

```
<SW7750>system-view
```

2 Add a MAC address (specify the native VLAN, port and state).

```
[SW7750]mac-address static 00e0-fc35-dc71 interface Ethernet 1/0/2
vlan 1
```

3 Set the address aging time to 500s.

```
[SW7750]mac-address timer 500
```

4 Display the MAC address configurations in all views.

```
[SW7750]display mac-address interface Ethernet 1/0/2
MAC ADDR            VLAN ID   STATE   PORT INDEX  AGING TIME(s)
00-e0-fc-35-dc-71  1         Static Ethernet1/0/2  NOAGED
00-e0-fc-17-a7-d6  1         LearnedEthernet1/0/2  300
00-e0-fc-5e-b1-fb  1         Learned Ethernet1/0/2  300
00-e0-fc-55-f1-16  1         Learned Ethernet1/0/2  300
```

Managing Devices   With device management, the Switch 7750 displays the current state and event debugging information about the slots and physical devices. In addition, there is a command for rebooting the system when a function failure occurs.

Configuring the Managing Devices is described in the following sections:

■ Designating the APP for the Next Boot

■ Displaying Devices

Designating the APP for the Next Boot

In the case that there are several operational images in the flash memory, you can use this command to designate the operational file (*.app) to use when the Switch 7750 is booted.

Perform the following configuration in user view.

Table 276 Designating the APP for the next boot

Operation	Command
Designate the APP for the next boot	**boot bootloader** file-url

Tasks for designating the APP for the next boot are described in the following sections:

■ Upgrading BootROM

■ Resetting a Slot

■ Setting the Slot Temperature Limit

■ Setting the Backboard View

Upgrading BootROM

You can use this command to upgrade the BootROM with the BootROM program in the flash memory. This configuration task facilitates the remote upgrade. You can upload the BootROM program file, from a remote end to the switch, by FTP and then use this command to upgrade the BootROM on the modules.

Perform the following configuration in user view.

Table 277 Upgrading BootROM

Operation	Command
Upgrade BootROM	**boot BootROM** file-url

Resetting a Slot

The Switch 7750 allows the administrator to reset a slot in the system.

Perform the following configuration in user view.

Table 278 Resetting a Slot

Operation	Command
Reset a slot	**reboot** [**slot** slot-num]

The parameter *slot-num* ranges from 0 to 6. Setting the parameter to 0 resets the fabric module, taking the same effect as resetting the entire system. Setting the parameter from 1 through 6 resets the I/O modules in the corresponding slots.

If you input **reboot** only, the whole system will be reset.

Setting the Slot Temperature Limit

The Switch 7750 sounds an alarm when the temperature on a slot exceeds the preset limit.

Perform the following configuration in user view.

Table 279   Setting the Slot Temperature Limit

Operation	Command
Set slot temperature limit	**temperature-limit slot** down-value up-value

Setting the Backboard View

The **backboard view** command determines the backplane bandwidth allocated to each slot in the Switch 7750. The Switch 7750 Fabric 64 is capable of 64 Gbps full duplex on the backplane, but the chassis has a maximum capability of 240 Gbps full duplex. The Switch 7750 Fabric 32 is capable of 32 Gbps full duplex on the backplane, but the chassis has a maximum capability of 128 Gbps full duplex. This command sets the bandwidth available to each slot in the system.

Perform the following configuration in system view.

Table 280   Set Backboard View

Operation	Command
Set back board view	**set backboard view** value

The default setting is 1.

Displaying Devices   Execute the **display** command in all views to display the device management configuration, and to verify the configuration.

Table 281   Displaying Devices

Operation	Command
Display the CPU	**display cpu** [**slot** slotnum]
Display the set back board view	**display backboard view**
Display the module types and states of each card	**display device** [**detail** | { **shelf** shelf-no | **frame** frame-no | **slot** slot-no } *]
Display the state of the built-in fans	**display fan** [fan-id]
Display the information about the environment	**display environment**
Display the used status of switch memory	**display memory** [**slot** slot-number]
Display the state of the power	**display power** [power-ID]

Maintaining and Debugging the System

This section includes descriptions of the following types of system maintenance and debugging:

- Configuring System Basics
- Displaying System Information and State

- Debugging the System
- Testing Tools for Network Connection
- Logging Function

Configuring System Basics

This section describes the following basic system configuration tasks:

- Setting the System Name
- Setting the System Clock
- Setting the Time Zone
- Setting Daylight Saving Time

Setting the System Name

Perform the following commands in system view.

Table 282   Setting the System Name

Operation	Command
Set the switch name	**sysname** sysname
Restore the switch name to the default name	**undo sysname**

Setting the System Clock

Perform the following command in user view.

Table 283   Setting the System Clock

Operation	Command
Set the system clock	**clock datetime** HH:MM:SS YYYY/MM/DD

Setting the Time Zone

You can configure the name of the local time zone, and the time difference between the local time and the standard Universal Time Coordinated (UTC).

Perform the following commands in user view.

Table 284   Setting the Time Zone

Operation	Command
Set the local time	**clock timezone** zone_name { **add** | **minus** } HH:MM:SS
Restore to the default UTC time zone	**undo clock timezone**

By default, the UTC time zone is set.

Setting Daylight Saving Time

Use these commands to configure the start and end time of daylight saving time.

Perform this command in user view.

Table 285   Setting Daylight Saving Time

Operation	Command
Set the name and range of daylight saving time	`clock summer-time` zone_name { `one-off` | `repeating` } start-time start-date end-time end-date offset-time
Remove the setting of the summer time	`undo clock summer-time`

By default, daylight saving time is not set.

Displaying System Information and State

The following display commands are used for displaying the system state and the statistics information. For the display commands related to each protocol and different ports, refer to the appropriate chapters.

Perform the following operations in all views.

Table 286   The Display Commands of the System

Operation	Command
Display the system clock	`display clock`
Display the system version	`display version`
Display the terminal user	`display users` [`all`]
Display the state of the debugging	`display debugging` [`interface` { interface-name | interface-type interface-number }] [module-name]

Debugging the System

Tasks for debugging the system are described in the following sections:

- Enabling and Disabling Terminal Debugging
- Displaying Diagnostic Information

Enabling and Disabling Terminal Debugging

The Switch 7750 provides various ways for debugging most of the supported protocols and functions.

The following switches control the outputs of debugging information:

- The protocol debugging switch controls debugging output of a protocol.
- The terminal debugging switch controls debugging output on a specified user screen.

Figure 61 illustrates the relationship between two switches.

Figure 61 Debugging Output
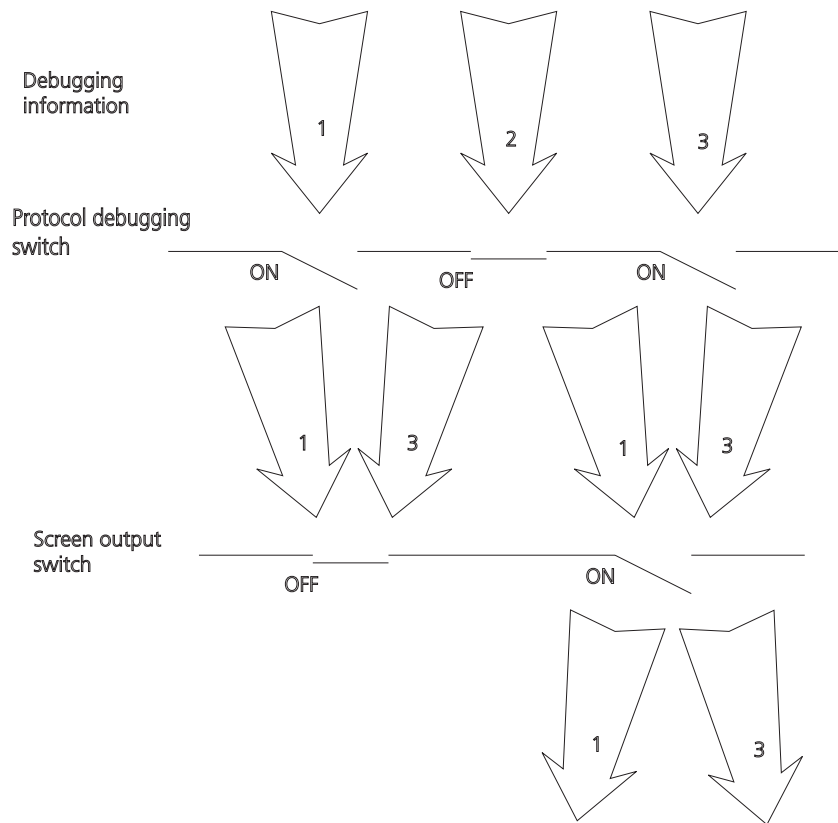
You can use the following commands to control debugging.

Perform the following operations in user view.

Table 287 Enabling and Disabling Debugging

Operation	Command
Enable the protocol debugging	**debugging** { **all** [**timeout** interval] | module-name [debugging-option] }
Disable the protocol debugging	**undo debugging** { **all** | { protocol-name | function-name } [debugging-option] }
Enable the terminal debugging	**terminal debugging**
Disable the terminal debugging	**undo terminal debugging**

For more about the usage and format of the debugging commands, refer to the appropriate chapters.

ⓘ *Since the debugging output will affect the system operating efficiency, do not enable the debugging command unnecessarily. Use the* **debugging all** *command, especially, with caution. When the debugging is over, disable all debugging.*

Displaying Diagnostic Information

You can collect information about the switch to locate the source of faults. Each module has a corresponding display command, which makes it difficult to collect

all the information needed. In this case, use **display diagnostic-information** command.

You can perform the following operations in all views.

Table 288   Displaying Diagnostic Information

Operation	Command
Display diagnostic information	**display diagnostic-information**

To view the data later, enable saving a screen capture to a file.

Testing Tools for Network Connection

The descriptions of testing tools for a network connection are found in the following sections:

- Ping
- Tracert Command

Ping

The **ping** command can be used to check the network connection and to verify whether the host can be reached.

Perform the following operation in user view.

Table 289   The Ping Command

Operation	Command
Support IP ping	**ping** [**-a** ip-address] [**-c** count] [**-d**] [**-i** {interface-type interface-num | interface-name }] [**ip**] [**-n**] [**-p** pattern] [**-q**] [**-r**] [**-s** packetsize] [**-t** timeout] [**-v**] host

The output of the **ping** command includes:

- The response to each ping message. If no response packet is received when time is out, "Request time out" information appears. Otherwise, the data bytes, the packet sequence number, TTL, and the round-trip time of the response packet will be displayed.
- The final statistics, which include the:
    - number of the packets the switch sent out and received
    - packet loss ratio
    - round-trip time in its minimum value, mean value and maximum value

Tracert Command

Tracert is used for testing the gateways from the source host to the destination. It is used for checking if the network is connected and analyzing where faults occur in the network.

The following list provides the tracert execution process:

1 Tracert sends a packet with TTL value of 1.

2 The first hop sends back an ICMP error message indicating that the packet cannot be sent, for the TTL is timeout.

3 Re-send the packet with TTL value of 2.

4 The second hop returns the TTL timeout message.

The process is repeated until the packet reaches the destination. The process is to record the source address of each ICMP TTL timeout message to provide the route of an IP packet to the destination.

Perform the following operation in user view.

Table 290   The Tracert Command

Operation	Command
Trace a route	**tracert** [**-f** first-TTL] [**-m** max-TTL] [**-p** port] [**-q** nqueries] [**-w** timeout] host

Logging Function   The Syslog is an indispensable part of the Switch 7750. It serves as an information center of the system software modules. The logging system is responsible for most of the information output, and also to make detailed classification to filter the information efficiently. Coupled with the debugging program, the syslog provides powerful support for the network administrators to monitor the operational state of networks and to diagnose network failures.

The syslog of the Switch 7750 has the following features:

- Support for six different output destinations: console, monitor to Telnet terminal, log buffer, loghost, trap buffer, and SNMP.

- The log is divided into 8 levels according to the significance of the event, and it can be filtered based on the levels.

- The information can be classified in terms of the source modules, and the information can be filtered by module.

- The output language can be selected between English and Chinese.

SYSLOG configuration includes tasks described in the following sections:

- Enabling and Disabling the Logging Function

- Setting the Output Channel of the Log

- Defining the Log Filtering Rules

- Configuring the SNMP Timestamp Output Format

- Configuring the Info-center Loghost

- Displaying and Debugging the Syslog Function

For the above configuration, the log host is not configured on the switch. All other configurations will take effect after enabling the logging function.

Enabling and Disabling the Logging Function

You can use the following commands to enable or disable the logging function.

Perform the following operation in system view.

Table 291 Enable/Disable the Logging Function

Operation	Command
Enable the logging function.	**info-center enable**
Disable the logging function.	**undo info-center enable**

By default, syslog is disabled. When syslog is enabled, system performance is affected by the information classification and the output, especially when there is a large amount of information to be processed.

Setting the Output Channel of the Log

The syslog of the Ethernet switch has six possible output destinations. Use the configuration commands to specify the required channels for syslog output. All the information will be filtered by the specified channel and then transmitted to the configured destination. You can configure the channel and filtering information for every destination to implement the filtering and redirection of different information.

Use the following commands to configure the output channel of the log.

Perform the following configuration in system view.

Table 292 Log Output

Operation	Command
Configure to output the information to the Console	**info-center console channel** { channel-number | channel-name }
Disable the output of the information to the Console	**undo info-center console channel**
Configure to output the information to the Telnet terminal or monitor	**info-center monitor channel** { channel-number | channel-name }
Disable the output of the information to the Telnet terminal or monitor	**undo info-center monitor channel**
Configure to output the information to the logging buffer.	**info-center logbuffer** [**size** buffersize] [**channel** { channel-number | channel-name }]
Disable the output of the information to the logging buffer.	**undo info-center logbuffer** [**channel** | **size**]
Configure to output the information to the info-center loghost.	**info-center loghost** host-ip-addr [**channel** { channel-number | channel-name }] [**facility** local-number] [**language** { **chinese** | **english** }]
Disable the output of the information to the info-center loghost.	**undo info-center loghost** host-ip-addr

Table 292   Log Output (continued)

Operation	Command
Set the address of the interface specified by *interface-name as* the source address for packets sent to loghost	**info-center loghost source** interface-name
Cancel the source address setting for the packets sent to loghost	**undo info-center loghost source**
Configure to output the information to the trap buffer.	**info-center trapbuffer** [**size** buffersize] [**channel** { channel-number | channel-name }]
Disable the output of the information to the trap buffer.	**undo info-center trapbuffer** [**channel** | size]
Configure to output the information to SNMP.	**info-center snmp channel** { channel-number | channel-name }
Disable the output of the information to SNMP.	**undo info-center snmp channel**
Rename a channel specified by *channel-number* as *channel-name*	**info-center channel** channel-number **name** channel-name

The system assigns a channel in each output direction by default. See Table 293.

Table 293   Numbers and Names of the Channels for Log Output

Name	Channel number	Default channel name
Console	0	console
Monitor	1	monitor
Info-center loghost	2	loghost
Trap buffer	3	trapbuf
Logging buffer	4	logbuf
SNMP	5	snmpagent

i *The six settings are independent from each other. The settings will take effect only after enabling the information center.*

Defining the Log Filtering Rules

The SYSLOG classifies the information into eight levels of severity. The log filtering prevents the system from outputting information whose severity level is greater than the set threshold. The more urgent the logging packet is, the lower its severity level. The level for emergencies is 1, and the level for debugging is 8. Therefore, when the threshold of the severity level is 8, the system will output all information.

Table 294   Syslog-Defined Severity

Severity	Description
1 Emergencies	The extremely urgent errors that endanger data.
2 Alerts	The errors that need to be corrected immediately.
3 Critical	Critical errors
4 Errors	The errors that need to be addressed but are not critical

Table 294   Syslog-Defined Severity

Severity	Description
5 Warnings	Warning, there might be an error
6 Notifications	The information should be read
7 Informational	Common prompting information
8 Debugging	Helpful information for debugging

Use the following commands to define the filtering rules of the channels.

Perform the following operation in system view.

Table 295   Define the Filtering Rules of the Channels

Operation	Command
Add the filtering record about a certain type of information in a module to the information channel	**info-center source** { modu-name | **default** } **channel** { channel-number | channel-name } [{ **log** | **trap** | **debug** } * { **level** severity | **state** state] } *
Delete the filtering record about a certain type of information in a module or all the modules from the channel	**undo info-center source** { modu-name | **default** } **channel** { channel-number | channel-name }

- modu-name: specifies the module name.

- **level** : refers to the severity levels.

- severity: specifies the severity level of information. The information with the level below it will not be output.

- channel-number: specifies the channel number.

- channel-name: specifies the channel name.

Every channel has been set with a default record, whose module name is *default* and the module number is 0xffff0000. However, for different channels, the default record may have different default settings of log, trap and debugging. When there is no specific configuration record for a module in the channel, use the default one.

> *When there is more than one Telnet user or monitor user at the same time, some configuration parameters are shared among the users, such as module-based filtering settings and the severity threshold. When you modify these settings, the changes affect all users.*

Configuring the SNMP Timestamp Output Format

Perform the following operation in system view.

Table 296   Configuring the SNMP Timestamp Output Format

Operation	Command
Configure the SNMP Timestamp Output Format	**info-center timestamp** { **log** | **trap** | **debugging** } { **boot** | **date** | **none** }
Disable the output of the timestamp field	**undo info-center timestamp** { **log** | **trap** | **debugging** }

Configuring the Info-center Loghost

This configuration is performed on the info-center loghost. The following configuration example is implemented on SunOS 4.0. The configurations on the Unix operating systems of other vendors are similar.

1 Perform the following commands with the identity of root

```
mkdir /var/log/SW7750
touch /var/log/SW7750/config
touch /var/log/SW7750/security
```

2 Edit the file "/etc/syslog.conf" with the identity of root and add the following selector/action pairs.

SW7750 configuration messages:

```
Local4.crit    /var/log/SW7750/config
```

SW7750 security messages:

```
local5.notice /var/log/SW7750/security
```

Pay attention to the following points when editing the file "/etc/syslog.conf":

- The description must start from a fresh line and begin with a pound key #.
- Use tab character to separate the selectors/action pairs instead of space.
- No redundant spaces should be left behind the name of the file.

3 When the log files "config" and "security" are created, and the file "/etc/syslog.conf" is modified, perform the following commands to send a HUP signal to the system demon syslogd, so that the syslogd can read the configuration file "/etc/syslog.conf" again.

```
ps -ae | grep syslogd 147
kill -HUP 147
```

After the operations are performed, the system can record information in the corresponding logging files

> *Configuring the facility, severity, filter and the file "syslog.conf" integrally makes it possible to perform the detailed classification for the purpose of information filtering.*

If you are using a UNIX workstation as a syslog server, consult your UNIX system manager manual for syslog configuration information.

Example: Log Configuration

Configure to output log on the console, as follows:

1 Enable the logging system.

```
[SW7750]info-center enable
```

2 Configure the logging output of the console and allows the log output of RSTP module with the severity ranged from "emergencies" to "debugging".

```
[SW7750]info-center console channel console
[SW7750]info-center source rstp channel 6 log level debugging
```

3 Enable RSTP module debugging.

```
<SW7750>debugging rstp all
```

Configure the info-center loghost as follows:

1 Enable the logging system.

```
[SW7750]info-center enable
```

2 Set the host at 202.38.1.10 as info-center loghost, sets the severity threshold to informational, the output language to English and allows the RSTP and IP modules to output information.

```
[SW7750]info-center loghost 202.38.1.10 language english
[SW7750]info-center source rstp channel 5 log level informational
[SW7750]info-center source ip channel 4 log level informational
```

For the configurations at the host side, see "Configuring the Info-center Loghost" on page 264.

Displaying and Debugging the Syslog Function

After performing the syslog configuration, execute the **display** command in all views to display the configuration and to verify the effect of the configuration. Execute the **reset** command in user view to clear the statistics of the syslog module. Execute the **debugging** command in user view to debug the syslog module.

Perform the following configuration in system view.

Table 297   Displaying and Debugging the Syslog Function

Operation	Command
View details about the information channel	**display channel** [channel-number | channel-name]
View the configuration of the system log and the information recorded in the memory buffer	**display info-center**
Reset the information in the log buffer	**reset logbuffer**
Reset the information in the trap buffer	**reset trapbuffer**
Enable terminal log information display	**terminal logging**
Disable terminal log information display	**undo terminal logging**
Enable the log debugging/log/trap on the terminal monitor	**terminal monitor**
Disable the log debugging/log/trap on the terminal monitor	**undo terminal monitor**
Enable terminal trap information display	**terminal trapping**
Disable terminal trap information display	**undo terminal trapping**

SNMP

The Simple Network Management Protocol (SNMP) is used for transmitting management information between any two nodes. In this way, network administrators can easily search and modify the information on any node on the network. They can also locate faults promptly and implement the fault diagnosis, capacity planning, and report generating. SNMP adopts the polling mechanism and provides the most basic function set. It is most applicable to the small-sized, fast-speed, and low-cost environment. It only requires the unverified transport layer protocol UDP, and is widely supported by many other products.

In terms of structure, SNMP can be divided into two parts, NMS and Agent. NMS (Network Management Station) is the workstation for running the client program. At present, the commonly used NM platforms include Sun NetManager and IBM NetView. The agent is the server software operated on network devices. NMS can send GetRequest, GetNextRequest, and SetRequest messages to the agent. Upon receiving the requests from the NMS, the agent will perform a read or write operation according to the message types, and generate and return the response message to NMS. On the other hand, the agent will send a trap message on its own initiative to NMS to report events whenever the device encounters any abnormalities.

Configuring SNMP is described in the following sections:

■ SNMP Versions and Supported MIB

■ Configuring SNMP

SNMP Versions and Supported MIB

To uniquely identify the management variables of a device in SNMP messages, SNMP adopts the hierarchical naming scheme to identify the managed objects. It is like a tree. A tree node represents a managed object, as shown in the figure below. Thus the object can be identified with the unique path starting from the root.

Figure 62   Architecture of the MIB Tree
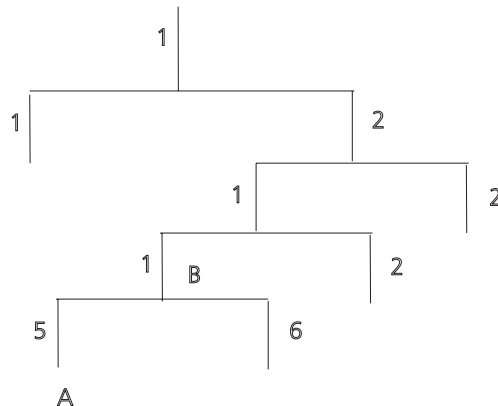
The MIB (Management Information Base) is used to describe the hierarchical architecture of the tree, and is the set defined by the standard variables of the monitored network device. In the above figure, the managed object B can be uniquely specified by a string of numbers {1.2.1.1}. The number string is the Object Identifier of the managed object.

The current SNMP Agent of Ethernet switch supports SNMP V1, V2C and V3. The MIBs supported are listed in the following table.

Table 298 MIBs Supported by the Ethernet Switch

MIB Attribute	MIB Content	References
Public MIB	MIB II based on TCP/IP network device	RFC1213
	BRIDGE MIB	RFC1493
		RFC2675
	RIP MIB	RFC1724
	RMON MIB	RFC2819
	Ethernet MIB	RFC2665
	IF MIB	RFC1573
Private MIB	DHCP MIB	
	QACL MIB	
	ADBM MIB	
	RSTP MIB	
	VLAN MIB	
	Device management	
	Interface management	

Configuring SNMP   Configuring SNMP includes tasks that are described in the following sections:

- Setting the Community Name
- Enabling and Disabling the SNMP Agent to Send a Trap
- Setting the Destination Address of a Trap
- Setting the Lifetime of the Trap Message
- Setting SNMP Information
- Setting the Engine ID of a Local or Remote Device
- Setting and Deleting an SNMP Group
- Setting the Source Address of the Trap
- Adding and Deleting a User to or from an SNMP Group
- Creating and Updating View Information or Deleting a View
- Setting the Size of an SNMP Packet Sent or Received by an Agent
- Enabling and Disabling Transmission of Trap Information
- Disabling the SNMP Agent
- Displaying and Debugging SNMP

Setting the Community Name

Both SNMP V1 and SNMPV2C use the community name authentication scheme. An SNMP message that does not comply with the community name that is accepted by the device is discarded. An SNMP community is named with a character string, which is called the community name. Communities can have read-only or read-write access modes. A community with read-only authority can

only query the device information, whereas the community with read-write authority can also configure the device.

Use the following commands to set the community name.

Perform the following configuration in system view.

Table 299   Setting the Community Name

Operation	Command
Set the community name and the access authority	`snmp-agent community { read | write } community-name [ [ mib-view view-name ] [ acl acl-list ] ]`
Remove the community name and the access authority	`undo snmp-agent community community-name`

Enabling and Disabling the SNMP Agent to Send a Trap

The managed device transmits a trap without a request to the NMS to report critical and urgent events, such as a restart.

You can use the following commands to enable or disable the managed device to transmit a trap message.

Perform the following configuration in system view.

Table 300   Enabling and Disabling an SNMP Agent to Send a Trap

Operation	Command
Enable to send a trap	`snmp-agent trap enable [ standard [ authentication ] [ coldstart ] [ linkdown ] [ linkup ] [ warmstart ] ]`
Disable to send a trap	`undo snmp-agent trap enable [ standard [ authentication ] [ linkdown ] [ linkup ] [ coldstart ] [ warmstart ] ]`

Setting the Destination Address of a Trap

You can use the following commands to set or delete the destination address of the trap.

Perform the following configuration in system view.

Table 301   Setting the Destination Address of a Trap

Operation	Command
Set the destination address of trap	`snmp-agent target-host trap address udp-domain host-addr [ udp-port udp-port-number ] params securityname community-string [ v1 | v2c | v3 { authentication | privacy } ]`
Delete the destination address of trap	`undo snmp-agent target-host host-addr securityname community-string`

The `authentication` parameter specifies that the packet is authenticated *without* encryption. This parameter is supported only in SNMP V3.

The `privacy` parameter specifies that the packet is authenticated and encrypted. This parameter is supported only in SNMP V3.

Setting the Lifetime of the Trap Message

You can use the following command to set lifetime of a trap message. A trap message that exists longer than the set lifetime will be dropped.

Perform the following configuration in system view.

Table 302   Setting the Lifetime of the Trap Message

Operation	Command
Set lifetime of Trap message	**snmp-agent trap life** seconds
Restore lifetime of Trap message	**undo snmp-agent trap life**

By default, the lifetime of a trap message is 120 seconds.

Setting SNMP Information

The SNMP system information includes the character string sysContact (system contact), the character string describing the system location, and the version information for SNMP in the system.

Use the following commands to set the system information.

Perform the following configuration in system view.

Table 303   Setting SNMP System Information

Operation	Command
Set SNMP system information	**snmp-agent sys-info** { **contact** sysContact	**location** syslocation	**version** { { **v1**	**v2c**	**v3**] *	**all** } }
Restore the default SNMP system information of the Ethernet switch	**undo snmp-agent sys-info** [{ **contact**	**location** }*	**version** { { **v1**	**v2c**	**v3**] *	**all** }]

By default, *syslocation* is specified as "Marlborough MA".

Setting the Engine ID of a Local or Remote Device

Use the following commands to set the engine ID of a local or remote device.

Perform the following configuration in system view.

Table 304   Setting the Engine ID of a Local or Remote Device

Operation	Command
Set the engine ID of the device	**snmp-agent local-engineid** engineid
Restore the default engine ID of the device.	**undo snmp-agent local-engineid** engineid

By default, the engine ID is expressed as enterprise No. + device information. The device information can be IP address, MAC address, or user-defined text.

Setting and Deleting an SNMP Group

Use the following commands to set or delete an SNMP group.

Perform the following configuration in system view.

Table 305 Setting and Deleting an SNMP Group

Operation	Command
Setting an SNMP group	**snmp-agent group** group-name { **v1** | **v2c** } [**read-view** *read-view*] [**write-view** write-view] [**notify-view** notify-view] [**acl** acl-list]
	snmp-agent group group-name **v3** [**authentication** | **privacy**] [**read-view** read-view] [**write-view** write-view] [**notify-view** notify-view] [**acl** acl-list]
Deleting an SNMP group	**undo snmp-agent group** group-name { **v1** | **v2c** }
	undo snmp-agent group group-name **v3** [**authentication** | **privacy**]

The authentication parameter specifies that the packet is authenticated *without* encryption. This parameter is supported only in SNMP V3.

The privacy parameter specifies that the packet is authenticated *and* encrypted. This parameter is supported only in SNMP V3.

Setting the Source Address of the Trap

Use the following commands to set or remove the source address of the trap.

Perform the following configuration in system view.

Table 306 Setting the Source Address of the Trap

Operation	Command
Set the Source Address of Trap	**snmp-agent trap source** interface-name interface-num
Remove the source address of trap	**undo snmp-agent trap source**

Adding and Deleting a User to or from an SNMP Group

Use the following commands to add or delete a user to or from an SNMP group.

Perform the following configuration in system view.

Table 307 Adding and Deleting a User to or from an SNMP Group

Operation	Command
Add a user to an SNMP group	**snmp-agent usm-user** { **v1** | **v2c** } username groupname [**acl** acl-list]
	snmp-agent usm-user v3 username groupname [**authentication-mod** { **md5** | **sha** } auth_password [**privacy-mod** { **des56** priv_password }]] **acl** acl-list
Delete a user from an SNMP group	**undo snmp-agent usm-user** { **v1** | **v2c** } username groupname
	undo snmp-agent usm-user v3 username groupname { **local** | **engineid** engine-id }

The `authentication-mode` parameter specifies the use of authentication. The `privacy-mode` parameter specifies the use of authentication and encryption. This parameter is supported only in SNMP V3.

For details, see the *Switch 7750 Command Reference Guide*.

Creating and Updating View Information or Deleting a View

Use the following commands to create, update the information of views, or delete a view.

Perform the following configuration in system view.

Table 308 Creating and Updating View Information or Deleting a View

Operation	Command
Create or update view information	**snmp-agent mib-view** { **included** | **excluded** } view-name oid-tree
Delete a view	**undo snmp-agent mib-view** view-name

Setting the Size of an SNMP Packet Sent or Received by an Agent

Use the following commands to set the size of SNMP packet sent or received by an agent.

The agent can receive or send the SNMP packets ranging from 484 bytes to 17940 bytes. By default, the size of an SNMP packet is 1500 bytes.

Perform the following configuration in system view.

Table 309 Setting the Size of an SNMP Packet Sent or Received by an Agent

Operation	Command
Set the size of an SNMP packet set or received by an agent	**snmp-agent packet max-size** byte-count
Restore the default size of an SNMP packet sent or received by an agent	**undo snmp-agent packet max-size**

Enabling and Disabling Transmission of Trap Information

To enable or disable transmission of trap information, perform the following configuration in Ethernet port view.

Table 310 Enable/Disable Transmission of Trap Information

Operation	Command
Enable the current port to transmit the trap information	`enable snmp trap updown`
Disable the current port from transmitting trap information	`undo enable snmp trap updown`

Disabling the SNMP Agent

To disable the SNMP Agent, perform the following configuration in system view.

Table 311 Disabling SNMP Agent

Operation	Command
Disable snmp agent	`undo snmp-agent`

If a user disables an NMP Agent, it is enabled whatever the `snmp-agent` command is configured.

Displaying and Debugging SNMP

Execute the `display` command to view the SNMP configuration and to verify the effect of the configuration. Execute the `debugging` command in user view to debug the SNMP configuration.

Table 312 Displaying and Debugging SNMP

Operation	Command
Display the statistics information about SNMP packets	`display snmp-agent statisitcs`
Display the engine ID of the active device	`display snmp-agent { local-engineid	remote-engineid }`
Display the group name, the security mode, the states for all types of views, and the storage mode of each group of the switch.	`display snmp-agent group`
Display the names of all users in the group user table	`display snmp-agent usm-user [{ local	{ engineid engineid } }	username groupname]`
Display the current community name	`display snmp-agent community [read	write]`
Display the current MIB view	`display snmp-agent mib-view [exclude	include	viewname mib-view]`
Display the contact character string of the system	`display snmp-agent sys-info contact`
Display the location character string of the system	`display snmp-agent sys-info location`
Display the version character string of the system	`display snmp-agent sys-info version`

Table 312   Displaying and Debugging SNMP (continued)

Operation	Command
Display the contact character string of the system	`display snmp-agent sys-info contact`
Display the location character strng of the system	`display snmp-agent sys-info location`
Display the version character string of the system	`display snmp-agent sys-info version`

Example: SNMP Configuration

A Network Management Station (NMS) and the Ethernet switch are connected by the Ethernet. The IP address of NMS is 129.102.149.23 and the IP address of the VLAN interface on the switch is 129.102.0.1.

Perform the following configurations on the switch:

- Set the community name and access authority
- Set the administrator ID, contact and switch location
- Enable the switch to send a trap packet.

Figure 63   SNMP Configuration Example
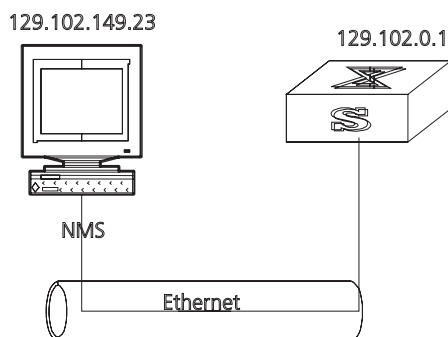
1 Enter the system view.

```
<SW7750>system-view
```

2 Set the community name, group name, and user.

```
[SW7750]snmp-agent sys-info version all
[SW7750]snmp-agent community write public
[SW7750]snmp-agent mib include internet 1.3.6.1
[SW7750]snmp-agent group v3 managev3group write internet
[SW7750]snmp-agent usm v3 managev3user managev3group
```

3 Set the administrator ID, contact and the physical location of the Ethernet switch.

```
[SW7750]snmp-agent sys-info contact Mr.Smith-Tel:3306
[SW7750]snmp-agent sys-info location telephone-closet, 3rd-floor
```

4 Set the VLAN interface 2 as the interface used by network management. Add Ethernet port 2/0/3 to the VLAN 2. This port will be used for network management. Set the IP address of VLAN interface 2 as 129.102.0.1.

```
[SW7750]vlan 2
[SW7750-vlan2]port ethernet 2/0/3
[SW7750-vlan2]interface vlan 2
[SW7750-Vlan-interface2]ip address 129.102.0.1 255.255.255.0
```

5 Set the administrator ID, contact and the physical location of the Ethernet switch.

```
[SW7750]snmp-agent sys-info contact Mr.Smith-Tel:3306
[SW7750]snmp-agent sys-info location telephone-closet,3rd-floor
```

6 Enable the SNMP agent to send the trap to Network Management Station whose IP address is 129.102.149.23. The SNMP community is public.

```
[SW7750]snmp-agent trap enable standard authentication
[SW7750]snmp-agent trap enable standard coldstart
[SW7750]snmp-agent trap enable standard linkup
[SW7750]snmp-agent trap enable standard linkdown
[SW7750]snmp-agent target-host trap address udp-domain
129.102.149.23 udp-port 5000 params securityname public
```

RMON

Remote Network Monitoring (RMON) is a type of IETF-defined MIB. It is the most important enhancement to the MIB II standard. It is used for monitoring the data traffic on a segment and even on a whole network. It is one of the most widely used network management standards.

RMON is based on the SNMP architecture and is compatible with the existing SNMP framework, so it is not necessary to adjust the protocol. RMON includes NMS and the agent running on the network devices. On the network monitor or detector, RMON agent tracks and accounts for different traffic information on the segment connected to its port. For example, the total number of packets on a segment in a certain period of time or that of the correct packets sent to a host.

RMON helps the SNMP monitor the remote network device more actively and effectively, which provides a highly efficient means for monitoring subnet operations. RMON can reduce communication traffic between the NMS and the agent, thus facilitating an effective management over large interconnected networks.

RMON allows multiple monitors. It can collect data in two ways.

1 The first way is with a special RMON probe. NMS directly obtains the management information from the RMON probe and controls the network resource. In this way, it obtains all the information of RMON MIB.

2 The second way is to implant the RMON Agent directly into the network devices, such as routers, switches, hubs, and so on, so that the devices become network facilities with RMON probe functions. RMON NMS uses the basic SNMP commands to exchange data information with the SNMP Agent and to collect NM information. However, not all the data of the RMON MIB can be obtained with this method, depending on resources. In most cases, only four groups of information can be collected. The four groups are: trap information, event information, history information and statistics information.

The Switch 7750 implements RMON using the second method. With the RMON-supported SNMP agent running on the network monitor, NMS can obtain such information as the overall traffic of the segment connected to the managed network device port, the error statistics and performance statistics, thereby implementing the management (usually remote) over the network.

Configuring RMON

RMON configuration includes tasks described in the following sections:

- Adding and Deleting an Entry to or from the Alarm Table
- Adding and Deleting an Entry to or from the Event Table
- Adding and Deleting an Entry to or from the History Control Table
- Adding and Deleting an Entry to or from the Extended RMON Alarm Table
- Adding and Deleting an Entry to or from the Statistics Table
- Displaying the RMON Configuration

Adding and Deleting an Entry to or from the Alarm Table

RMON alarm management can monitor the specified alarm variables, such as, statistics on a port. When a value of the monitored data exceeds the defined threshold, an alarm event will be generated. Generally, the event will be recorded in the device log table and a Trap message will be sent to NMS. The events are defined in event management. The alarm management includes browsing, adding and deleting alarm entries.

Use the following commands to add or delete an entry to or from the alarm table.

Perform the following configuration in system view.

Table 313 Adding or Delete an Entry to or from the Alarm Table

Operation	Command
Add an entry to the alarm table.	**rmon alarm** entry-number alarm-variable sampling-time { **delta** | **absolute** } **rising-threshold** threshold-value1 event-entry1 **falling-threshold** threshold-value2 event-entry2 [**owner** text]
Delete an entry from the alarm table.	**undo rmon alarm** entry-number

Adding and Deleting an Entry to or from the Event Table

RMON event management defines the event ID and handling of the event by keeping logs, sending trap messages to NMS, or performing both at the same time.

Use the following commands to add or delete an entry to or from the event table.

Perform the following configuration in system view.

Table 314 Add or Delete an Entry to or from the Event Table

Operation	Command
Add an entry to the event table	**rmon event** event-entry [**description** string] { **log** | **trap** trap-community | **log-trap** log-trapcommunity | **none** } [**owner** rmon-station]
Delete an entry from the event table	**undo rmon event** event-entry

Adding and Deleting an Entry to or from the History Control Table

The history data management helps you set the history data collection, periodical data collection, and storage of the specified ports. The sampling information includes the utilization ratio, error counts, and the total number of packets.

Use the following commands to add or delete an entry to or from the history control table.

Perform the following configuration in Ethernet port view.

Table 315 Adding or Deleting an Entry to or from the History Control Table

Operation	Command
Add an entry to the history control table	**rmon history** entry-number **buckets** number **interval** sampling-interval [**owner** text-string]
Delete an entry from the history control table	**undo rmon history** *entry-number*

Adding and Deleting an Entry to or from the Extended RMON Alarm Table

You can use the command to add or delete an entry to or from the extended RMON alarm table.

Perform the following configuration in system view.

Table 316 Add or Delete an Entry to or from the Extended RMON AlarmTable

Operation	Command
Add an entry to the extended RMON alarm table	**rmon prialarm** entry-number alarm-var [alarm-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]
Delete an entry from the extended RMON alarm table	**undo rmon prialarm** entry-number

Adding and Deleting an Entry to or from the Statistics Table

The RMON statistics management concerns port usage monitoring and error statistics when using the ports. The statistics include collision, CRC and queuing, undersize packets or oversize packets, timeout transmission, fragments, broadcast, multicast and unicast messages, and the usage ratio of bandwidth.

Use the following commands to add or delete an entry to or from the statistics table.

Perform the following configuration in Ethernet port view.

Table 317 Add or Delete an Entry to or from the Statistics Table

Operation	Command
Add an entry to the statistics table	**rmon statistics** entry-number [**owner** text-string]
Delete an entry from the statistics table	**undo rmon statistics** entry-number

Displaying the RMON Configuration

Execute the **display** command in all views to display the RMON configuration, and to verify the configuration.

Table 318   Displaying and Debugging RMON

Operation	Command
Display the RMON statistics	**display rmon statistics** [port-num]
Display the history information of RMON	**display rmon history** [port-num]
Display the alarm information of RMON	**display rmon alarm** [alarm-table-entry]
Display the extended alarm information of RMON	**display rmon prialarm** [prialarm-table-entry]
Display the RMON event	**display rmon event** [event-table-entry]
Display the event log of RMON	**display rmon eventlog** [event-number]

Example: RMON Configuration

Set an entry in the RMON Ethernet statistics table for Ethernet port performance, which is convenient for network administrators' query.

Figure 64   RMON Configuration Networking
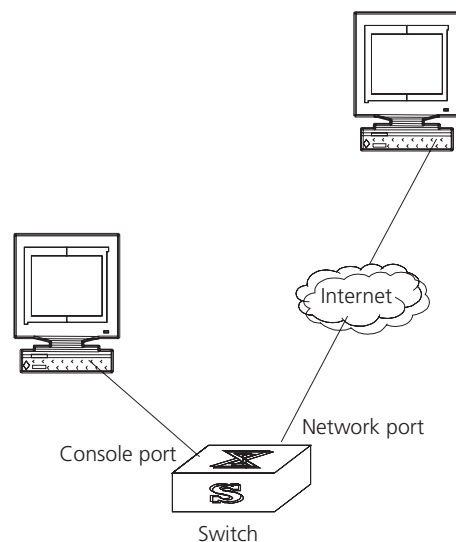
1 Configure RMON.

```
[SW7750-Ethernet2/0/1]rmon statistics 1 owner 3com-rmon
```

2 View the configurations in user view.

```
<SW7750>display rmon statistics Ethernet2/0/1
Statistics entry 1 owned by 3com-rmon is VALID.
  Gathers statistics of interface Ethernet2/0/1. Received:
  octets            : 270149,packets         : 1954
  broadcast packets :1570   ,multicast packets:365
  undersized packets :0      ,oversized packets:0
  fragments packets  :0      ,jabbers packets  :0
  CRC alignment errors:0      ,collisions       :0
```

```
Dropped packet events (due to lack of resources):0
Packets received according to length (in octets):
64      :644      ,  65-127  :518      ,  128-255  :688
256-511:101       ,  512-1023:3        ,  1024-1518:0
```

NTP

As the network topology gets more and more complex, it becomes important to synchronize the clocks of the equipment on the entire network. Network Time Protocol (NTP) is a TCP/IP feature that advertises the accurate time throughout the network.

NTP ensures the consistency of the following applications:

■ Synchronizing the clock between two systems for incremental backup between the backup server and client.

■ Referencing the same clock and guaranteeing correct processing for multiple systems that coordinate to process a complex event.

■ Guaranteeing the normal operation of the inter-system (Remote Procedure Call).

■ Recording an application when a user logs into a system, a file is modified, or some other operation is performed.

Figure 65 illustrates the basic operating principle of NTP:

Figure 65   Basic Operating Principle of NTP
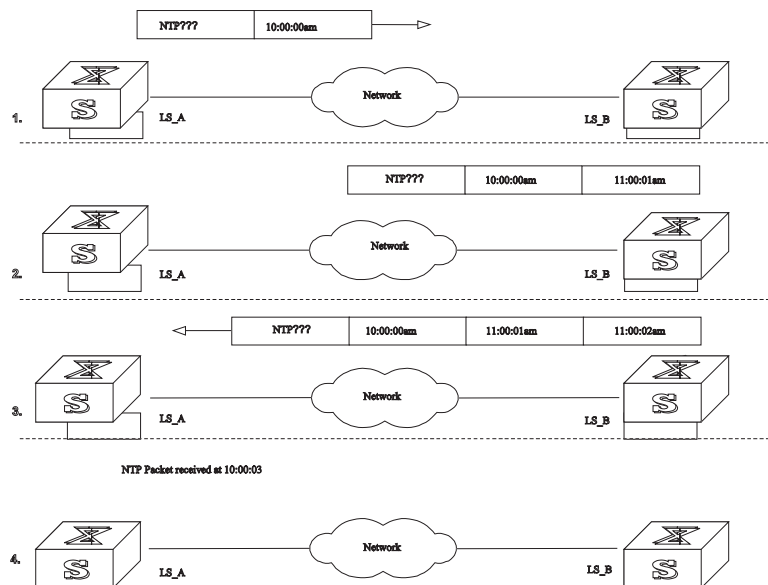
In Figure 65, Ethernet Switch A and Ethernet Switch B are connected to the Ethernet port. They have independent system clocks. Before implementing automatic clock synchronization on both switches. Note that:

■ Before synchronizing the system clocks on Ethernet Switch A and B, the clock on Ethernet Switch A is set to 10:00:00am, and the clock on B is set to 11:00:00am.

- Ethernet Switch B serves as an NTP time server and Ethernet Switch A synchronizes the local clock with the clock of B.

- It takes 1 second to transmit a data packet from either A or B to the opposite end.

The system clocks are synchronized as follows:

- Ethernet Switch A sends an NTP packet to Ethernet Switch B. The packet carries the timestamp 10:00:00am (T1) that tells when it left Ethernet Switch A.

- When the NTP packet arrives at Ethernet Switch B, Ethernet Switch B adds a local timestamp 11:00:01am (T2) to it.

- When the NTP packet leaves Ethernet Switch B, Ethernet Switch B adds another local timestamp 11:00:02am (T3) to it.

- When Ethernet Switch A receives the acknowledgement packet, it adds a new timestamp 10:00:03am (T4) to it.

Next, Ethernet Switch A collects enough information to calculate the following two important parameters:

- The delay for a round trip of an NTP packet traveling between the Switch A and B: Delay= (T4-T1) - (T3-T2).

- Offset of Ethernet Switch A clock relative to Ethernet Switch B clock: offset= ((T2-T1) + (T3-T4)) /2.

Ethernet Switch A uses this information to set the local clock and to synchronize it with the clock on Ethernet Switch B.

Configuring NTP is described in the following sections:

- Configuring NTP
- NTP Configuration Examples

Configuring NTP   NTP configuration includes the tasks described in the following sections:

- Configuring NTP Operating Mode
- Configuring NTP ID Authentication
- Setting the NTP Authentication Key
- Setting the Specified Key to Be Reliable
- Designating an Interface to Transmit the NTP Message
- Setting the NTP Master Clock
- Enabling or Disabling an Interface to Receive an NTP Message
- Setting the Authority to Access a Local Switch
- Setting Maximum Local Sessions
- Displaying and Debugging NTP

Configuring NTP Operating Mode

The Switch 7750 can serve as an NTP client but not as an NTP server.

You can set the NTP operating mode of the Switch 7750 according to its location in the network, and the network structure. For example, you can set a remote server as the time server of the local equipment. In this case the local Ethernet Switch works as an NTP client. If you set a remote server as a peer of the local Ethernet Switch, the local equipment operates in symmetric active mode. If you configure an interface on the local switch to transmit NTP broadcast packets, the local switch will operate in broadcast mode. If you configure an interface on the local switch to receive NTP broadcast packets, the local switch will operate in broadcast client mode. If you configure an interface on the local switch to transmit NTP multicast packets, the local switch will operate in multicast mode. You may also configure an interface on the local switch to receive NTP multicast packets, the local switch will operate in multicast client mode.

The following sections describe how to configure NTP modes:

- Configuring NTP Server Mode
- Configuring NTP Peer Mode
- Configuring NTP Broadcast Server Mode
- Configuring NTP Broadcast Client Mode
- Configuring NTP Multicast Server Mode
- Configuring NTP Multicast Client Mode

Configuring NTP Server Mode   Set a remote server whose IP address is *ip-address* as the local time server. *ip-address* specifies a host address other than a broadcast, multicast, or reference clock IP address. In this case, the local switch operates in client mode. In this mode, only the local client synchronizes its clock with the clock of the remote server, while the reverse synchronization will not happen.

Perform the following configurations in system view.

Table 319   Configuring NTP Time Server

Operation	Command
Configure NTP time server	**ntp-service unicast-server** ip-address [**version** number | **authentication-keyid** keyid | **source-interface** { interface-name | interface-type interface-number } | **priority**]*
Cancel NTP server mode	**undo ntp-service unicast-server** ip-address

NTP version number `number` ranges from 1 to 3 and defaults to 3; the authentication key ID *keyid* ranges from 0 to 4294967295; `interface-name` or `interface-type interface-number` specifies the IP address of an interface, from which the source IP address of the NTP packets sent from the local switch to the time server will be taken; **priority** indicates the time server will be the first choice.

Configuring NTP Peer Mode   Set a remote server whose IP address is `ip-address` as the peer of the local equipment. In this case, the local equipment operates in symmetric active mode. `ip-address` specifies a host address other

than a broadcast, multicast, or reference clock IP address. In this mode, both the local switch and the remote server can synchronize their clocks with the clock of the opposite end.

Perform the following configurations in system view.

Table 320 Configuring NTP Peer Mode

Operation	Command
Configure NTP peer mode	`ntp-service unicast-peer` ip-address [**version** number | **authentication-key** keyid | **source-interface** { interface-name | interface-type interface-number } | **priority**]*
Cancel NTP peer mode	`undo ntp-service unicast-peer` ip-address

NTP version number `number` ranges from 1 to 3 and defaults to 3; the authentication key ID `keyid` ranges from 1 to 4294967295; `interface-name` or `interface-type interface-number` specifies the IP address of an interface, from which the source IP address of the NTP packets sent from the local switch to the peer will be taken; **priority** indicates that the peer will be the first choice for time server.

Configuring NTP Broadcast Server Mode   Designate an interface on the local switch to transmit NTP broadcast packets. In this case, the local equipment operates in broadcast mode and serves as a broadcast server to broadcast messages to its clients regularly.

Perform the following configurations in VLAN interface view.

Table 321 Configuring NTP Broadcast Server Mode

Operation	Command
Configure NTP broadcast server mode	`ntp-service broadcast-server` [**authentication-keyid** keyid] [**version** number]
Cancel NTP broadcast server mode	`undo ntp-service broadcast-server`

NTP version number `number` ranges from 1 to 3 and defaults to 3; the authentication key ID `keyid` ranges from 0 to 4294967295. This command can only be configured on the interface where the NTP broadcast packets will be transmitted.

Configuring NTP Broadcast Client Mode   Designate an interface on the local switch to receive NTP broadcast messages and operate in broadcast client mode. The local switch listens to the broadcast from the server. When it receives the first broadcast packets, it starts a brief client/server mode to switch messages with a remote server for estimating the network delay. Thereafter, the local switch enters broadcast client mode and continues listening to the broadcast, and synchronizes the local clock according to the arrived broadcast message.

Perform the following configurations in VLAN interface view.

Table 322   Configuring NTP Broadcast Client Mode

Operation	Command
Configure NTP broadcast client mode	`ntp-service broadcast-client`
Disable NTP broadcast client mode	`undo ntp-service broadcast-client`

This command can only be configured on the interface where the NTP broadcast packets are received.

Configuring NTP Multicast Server Mode   Designate an interface on the local switch to transmit NTP multicast packets. In this case, the local equipment operates in multicast mode and serves as a multicast server to multicast messages to its clients regularly.

Perform the following configurations in VLAN interface view.

Table 323   Configuring NTP Multicast Server Mode

Operation	Command
Configure NTP multicast server mode	`ntp-service multicast-server [ ip-address ] [ authentication-keyid keyid ] [ ttl ttl-number ] [ version number ]`
Cancel NTP multicast server mode	`undo ntp-service multicast-server`

NTP version number `number` ranges from 1 to 3 and defaults to 3; the authentication key ID `keyid` ranges from 0 to 4294967295; `ttl-number` of the multicast packets ranges from 1 to 255; And the multicast IP address defaults to 224.0.1.1.

This command can only be configured on the interface where the NTP multicast packet is transmitted.

Configuring NTP Multicast Client Mode   Designate an interface on the local switch to receive NTP multicast messages and operate in multicast client mode. The local switch listens to the multicast from the server. When it receives the first multicast packets, it starts a brief client/server mode to switch messages with a remote server for estimating the network delay. Thereafter, the local switch enters multicast client mode and continues listening to the multicast and synchronizes the local clock by the arrived multicast message.

Perform the following configurations in VLAN interface view.

Table 324   Configuring NTP Multicast Client Mode

Operation	Command
Configure NTP multicast client mode	`ntp-service multicast-client [ ip-address ]`
Cancel NTP multicast client mode	`undo ntp-service multicast-client`

Multicast IP address `ip-address` defaults to 224.0.1.1. This command can only be configured on the interface where the NTP multicast packets is received.

Configuring NTP ID Authentication

Enable NTP authentication, set the MD5 authentication key, and specify the reliable key. A client will synchronize itself by a server only if the server can provide a reliable key.

Perform the following configurations in system view.

Table 325   Configuring NTP Authentication

Operation	Command
Enable NTP authentication	`ntp-service authentication enable`
Disable NTP authentication	`undo ntp-service authentication enable`

Setting the NTP Authentication Key

This configuration task sets the NTP authentication key.

Perform the following configurations in system view.

Table 326   Configuring the NTP Authentication Key

Operation	Command
Configure the NTP authentication key	`ntp-service authentication-keyid` number `authentication-mode md5` value
Remove the NTP authentication key	`undo ntp-service authentication-keyid` number

Key number `number` ranges from 1 to 4294967295; the key `value` contains 1 to 32 ASCII characters.

Setting the Specified Key to Be Reliable

This configuration task is to set the specified key as reliable.

Perform the following configurations in system view.

Table 327   Setting the Specified Key as Reliable

Operation	Command
Set the specified key as reliable	`ntp-service reliable authentication-keyid` key-number
Cancel the specified reliable key.	`undo ntp-service reliable authentication-keyid` key-number

Key number `key-number` ranges from 1 to 4294967295

Designating an Interface to Transmit the NTP Message

If the local equipment is configured to transmit all NTP messages, these packets have the same source IP address, which is taken from the IP address of the designated interface.

Perform the following configurations in system view.

Table 328 Designating an Interface to Transmit NTP Message

Operation	Command
Designate an interface to transmit NTP message	`ntp-service source-interface {` `interface-name	interface-type` `interface-number }`
Cancel the interface to transmit NTP message	`undo ntp-service source-interface`

An interface is specified by `interface-name` or `interface-type`
`interface-number`. The source address of the packets will be taken from the IP
address of the interface. If the **`ntp-service unicast-server`** or **`ntp-service`**
`unicast-peer` command also designates a transmitting interface, use the one
designated by them.

Setting the NTP Master Clock

This configuration task sets the external reference clock or the local clock as the
NTP master clock.

Perform the following configurations in system view.

Table 329 Setting the External Reference Clock or the Local Clock as the NTP Master
Clock

Operation	Command
Set the external reference clock or the local clock as the NTP master clock.	`ntp-service refclock-master [` `ip-address ] [ stratum ]`
Cancel the NTP master clock settings	`undo ntp-service refclock-master` `[ ip-address ]`

`ip-address` specifies the IP address 127.127.1.u of a reference clock, in which `u`
ranges from 0 to 3. `stratum` specifies how many strata the local clock belongs to
and ranges from 1 to 15. If no IP address is specified, the system defaults to
setting the local clock as the NTP master clock. You can specify the `stratum`
parameter.

Enabling or Disabling an Interface to Receive an NTP Message

This configuration task enables or disables an interface to receive the NTP
message.

Perform the following configurations in VLAN interface view.

Table 330 Enabling or Disabling an Interface to Receive an NTP Message

Operation	Command
Enable an interface to receive an NTP message	`undo ntp-service in-interface` `disable`
Disable an interface from receiving an NTP message	`ntp-service in-interface disable`

This configuration task must be performed on the interface to be disabled from
receiving an NTP message.

Setting the Authority to Access a Local Switch

Set the authority to access the NTP services on a local switch. This is a basic security measure. An access request will be matched with **peer, serve, serve only**, and **query only** in an ascending order of the limitation. The first matched authority will be granted.

Perform the following configurations in system view.

Table 331 Setting the Authority to Access a Local Ethernet Switch

Operation	Command
Set authority to access a local Ethernet switch	**ntp-service access** { **query** | **synchronization** | **serve** | **peer** } acl-number
Cancel settings of the authority to access a local Ethernet switch	**undo ntp-service access** { **query** | **synchronization** | **serve** | **peer** }

IP address ACL number is specified through the acl-number parameter and ranges from 2000 to 2999. The meanings of other authority levels are as follows:

- **query**: Allow control query for the local NTP service only.
- **synchronization**: Allow request for local NTP time service only.
- **serve**: Allow local NTP time service request and control query. However, the local clock will not be synchronized by a remote server.
- **peer**: Allow local NTP time service request and control query. And the local clock will also be synchronized by a remote server.

Setting Maximum Local Sessions

This configuration task sets the maximum local sessions.

Perform the following configurations in system view.

Table 332 Setting the Maximum Local Sessions

Operation	Command
Set the maximum local sessions	**ntp-service max-dynamic-sessions** number
Resume the maximum number of local sessions	**undo ntp-service max-dynamic-sessions**

number specifies the maximum number of local sessions, ranges from 0 to 100, and defaults to 100.

Displaying and Debugging NTP

After completing the previous configurations, you can use the **display** command to show how NTP runs and verify the configurations according to the outputs. You can use the **debugging** command, in user view, to debug NTP. See Table 333 for the details of these commands.

Table 333 Displaying and Debugging NTP

Operation	Command
Display the status of NTP service	**display ntp-service status**

Table 333 Displaying and Debugging NTP

| Operation	Command
Display the status of sessions maintained by NTP service	`display ntp-service sessions [ verbose ]`
Display the brief information about every NTP time server on the way from the local equipment to the reference clock source.	`display ntp-service trace`
Debug NTP	`debugging ntp-service`

NTP Configuration Examples

NTP configuration examples are shown in the following:

- Example: Configuring NTP Servers
- Example: Configuring NTP Peers
- Example: Configuring NTP Broadcast Mode
- Example: Configuring NTP Multicast Mode
- Example: Configuring Authentication-Enabled NTP Server Mode

Example: Configuring NTP Servers

On SW77501, set the local clock as the NTP master clock at stratum 2. On SW77502, configure SW77501 as the time server in server mode and set the local equipment as in client mode.

Figure 66 Typical NTP Configuration Networking Diagram
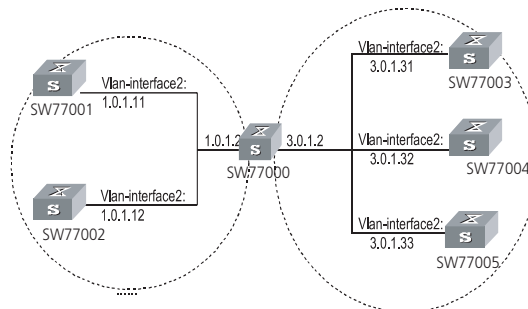
Configure the Switch SW77501:

1 Enter system view.

```
<SW77501>system-view
```

2 Set the local clock as the NTP master clock at stratum 2.

```
[SW77501]ntp-service refclock-master 2
```

Configure Ethernet Switch SW77502:

1 Enter system view.

```
<SW77502>system-view
```

2 Set SW77501 as the NTP server.

```
[SW77502]ntp-service unicast-server 1.0.1.11
```

The above examples synchronized SW77502 by SW77501. Before the synchronization, the SW77502 is shown in the following status:

```
[SW77502]display ntp-service status

clock status: unsynchronized

 clock stratum: 16

 reference clock ID: none

 nominal frequency: 100.0000 Hz

 actual frequency: 100.0000 Hz

 clock precision: 2^17

 clock offset: 0.0000 ms

 root delay: 0.00 ms

 root dispersion: 0.00 ms

 peer dispersion: 0.00 ms

 reference time: 00:00:00.000 UTC Jan 1 1900(00000000.00000000)
```

After the synchronization, SW77502 turns into the following status:

```
[SW77502]display ntp-service status

clock status: synchronized

 clock stratum: 8

 reference clock ID: LOCAL(0)

 nominal frequency: 100.0000 Hz

 actual frequency: 100.0000 Hz

 clock precision: 2^17

 clock offset: 0.0000 ms

 root delay: 0.00 ms

 root dispersion: 10.94 ms

 peer dispersion: 10.00 ms

 reference time: 20:54:25.156 UTC Mar 7 2002(C0325201.2811A112)
```

By this time, SW77502 has been synchronized by SW77501 and is at stratum 3, higher than SW77501 by 1.

Display the sessions of SW77502 and you will see SW77502 has been connected with SW77501.

```
[SW77502]display ntp-service sessions

    source          reference      stra reach poll  now offset  delay
disper

**********************************************************************
****** [12345]127.127.1.0     LOCAL(0)            7   377   64   57
0.0    0.0    1.0

    [5]1.0.1.11        0.0.0.0          16    0   64    -    0.0
0.0    0.0

    [5]128.108.22.44   0.0.0.0          16    0   64    -    0.0
0.0    0.0

note: 1 source(master),2 source(peer),3 selected,4 candidate,5
configured
```

Example: Configuring NTP Peers

On SW77503, set local clock as the NTP master clock at stratum 2. On SW77502, configure SW77501 as the time server in server mode and set the local equipment as in client mode. At the same time, SW77505 sets SW77504 as its peer. See Figure 66.

Configure Ethernet Switch SW77503:

1 Enter system view.

```
<SW77503>system-view
```

2 Set the local clock as the NTP master clock at stratum 2.

```
[SW77503]ntp-service refclock-master 2
```

Configure Ethernet Switch SW77504:

1 Enter system view.

```
<SW77504>system-view
```

2 Set SW77501 as the NTP server at stratum 3 after synchronization.

```
[SW77504]ntp-service unicast-server 3.0.1.31
```

Configure Ethernet Switch SW77505: (SW77504 has been synchronized by SW77503)

1 Enter system view.

```
<SW77505>system-view
```

2 Set the local clock as the NTP master clock at stratum 1.

```
[SW77505]ntp-service refclock-master 1
```

3 After performing local synchronization, set SW77504 as a peer.

```
[SW77505]ntp-service unicast-peer 3.0.1.32
```

The previous examples configure SW77504 and SW77505 as peers and configure SW77505 as in active peer mode and SW77504 in passive peer mode. Since SW77505 is at stratum 1 and SW77504 is at stratum 3, synchronize SW77504 by SW77505.

After synchronization, SW77504 status is shown as follows:

```
[SW77504]display ntp-service status

clock status: synchronized

 clock stratum: 8

 reference clock ID: LOCAL(0)

 nominal frequency: 100.0000 Hz

 actual frequency: 100.0000 Hz

 clock precision: 2^17

 clock offset: 0.0000 ms

 root delay: 0.00 ms

 root dispersion: 10.94 ms

 peer dispersion: 10.00 ms

 reference time: 20:54:25.156 UTC Mar 7 2002(C0325201.2811A112)
```

By this time, SW77504 has been synchronized by SW77505 and it is at stratum 2, or higher than SW77505 by 1.

Display the sessions of SW77504 and you will see SW77504 has been connected with SW77505.

```
[SW77504]display ntp-service sessions

    source          reference       stra reach poll  now offset  delay
disper

********************************************************************
****** [12345]127.127.1.0     LOCAL(0)           7   377   64    57
0.0    0.0    1.0

    [5]1.0.1.11        0.0.0.0            16    0    64    -    0.0
0.0    0.0

    [5]128.108.22.44   0.0.0.0            16    0    64    -    0.0
0.0    0.0

note: 1 source(master),2 source(peer),3 selected,4 candidate,5
configured
```

Example: Configuring NTP Broadcast Mode

On SW77503, set local clock as the NTP master clock at stratum 2, and configure to broadcast packets from Vlan-interface2. Configure SW77504 and SW77501 to listen to the broadcast from their Vlan-interface2. See Figure 66.

Configure Ethernet Switch SW77503:

1 Enter system view.

```
<SW77503>system-view
```

2 Set the local clock as the NTP master clock at stratum 2.

```
[SW77503]ntp-service refclock-master 2
```

3 Enter Vlan-interface2 view.

```
[SW77503]interface vlan-interface 2
```

4 Set it as broadcast server.

```
[SW77503-Vlan-Interface2]ntp-service broadcast-server
```

Configure Ethernet Switch SW77504:

1 Enter system view.

```
<SW77504>system-view
```

2 Enter Vlan-interface2 view.

```
[SW77504]interface vlan-interface 2
[SW77504-Vlan-Interface2]ntp-service broadcast-client
```

Configure Ethernet Switch SW77501:

1 Enter system view.

```
<SW77501>system-view
```

2 Enter Vlan-interface2 view.

```
[SW77501]interface vlan-interface 2
[SW77501-Vlan-Interface2]ntp-service broadcast-client
```

The above examples configured SW77504 and SW77501 to listen to the broadcast through Vlan-interface2, SW77503 to broadcast packets from Vlan-interface2. Since SW77501 and SW77503 are not located on the same segment, they cannot receive any broadcast packets from SW77503, while SW77504 is synchronized by SW77503 after receiving its broadcast packet.

After the synchronization, you can find the state of SW77504 as follows:

```
[SW77504]display ntp-service status

clock status: synchronized

 clock stratum: 8

 reference clock ID: LOCAL(0)

 nominal frequency: 100.0000 Hz

 actual frequency: 100.0000 Hz

 clock precision: 2^17
```

```
 clock offset: 0.0000 ms

 root delay: 0.00 ms

 root dispersion: 10.94 ms

 peer dispersion: 10.00 ms

 reference time: 20:54:25.156 UTC Mar 7 2002(C0325201.2811A112)
```

By this time, SW77504 has been synchronized by SW77503 and it is at stratum 3, higher than SW77503 by 1.

Display the status of SW77504 sessions and you will see SW77504 has been connected to SW77503:

```
[SW77502]display ntp-service sessions

    source          reference     stra reach poll  now offset  delay
disper

*********************************************************************
****** [12345]127.127.1.0     LOCAL(0)            7   377   64   57
0.0    0.0    1.0

   [5]1.0.1.11        0.0.0.0            16    0   64    -    0.0
0.0    0.0

   [5]128.108.22.44  0.0.0.0            16    0   64    -    0.0
0.0    0.0

note: 1 source(master),2 source(peer),3 selected,4 candidate,5
configured
```

Example: Configuring NTP Multicast Mode

SW77503 sets the local clock as the master clock at stratum 2, and multicast packets from Vlan-interface2. Set SW77504 and SW77501 to receive multicast messages from their respective Vlan-interface2. See Figure 66.

Configure Ethernet Switch SW77503:

1 Enter system view.

```
<SW77503>system-view
```

2 # Set the local clock as a master NTP clock at stratum 2.

```
[SW77503]ntp-service refclock-master 2
```

3 Enter Vlan-interface2 view.

```
[SW77503]interface vlan-interface 2
```

4 Set it as a multicast server.

```
[SW77503-Vlan-Interface2]ntp-service multicast-server
```

Configure Ethernet Switch SW77504:

1 Enter system view.

```
<SW77504>system-view
```

2 Enter Vlan-interface2 view.

```
[SW77504]interface vlan-interface 2
```

3 Enable multicast client mode.

```
[SW77504-Vlan-Interface2]ntp-service multicast-client
```

Configure Ethernet Switch SW77501:

1 Enter system view.

```
<SW77501>system-view
```

2 Enter Vlan-interface2 view.

```
[SW77501]interface vlan-interface 2
```

3 Enable multicast client mode.

```
[SW77501-Vlan-Interface2]ntp-service multicast-client
```

The previous examples configure SW77504 and SW77501 to receive multicast messages from Vlan-interface2, SW77503 multicast messages from Vlan-interface2. Since SW77501 and SW77503 are not located on the same segments, SW77501 cannot receive the multicast packets from SW77503, while SW77504 is synchronized by SW77503 after receiving the multicast packet.

Example: Configuring Authentication-Enabled NTP Server Mode

SW77501 sets the local clock as the NTP master clock at stratum 2. SW77502 sets SW77501 as its time server in server mode and itself in client mode and enables authentication. See Figure 66.

Configure Ethernet Switch SW77501:

1 Enter system view.

```
<SW77501>system-view
```

2 Set the local clock as the master NTP clock at stratum 2.

```
[SW77501]ntp-service refclcok-master 2
```

Configure Ethernet Switch SW77502:

1 Enter system view.

```
<SW77502>system-view
```

2 Set SW77501 as time server.

```
[SW77502]ntp-service unicast-server 1.0.1.11
```

3 Enable authentication.

```
[SW77502]ntp-service authentication enable
```

4 Set the key.

```
[SW77502]ntp-service authentication-keyid 42 authentication-mode md5
aNiceKey
```

5 Set the key as reliable.

```
[SW77502]ntp-service reliable authentication-keyid 42
```

The previous examples synchronized SW77502 by SW77501. Since SW77501 has not been enabled authentication, it cannot synchronize SW77502.

Perform the following additional configurations on SW77501:

1 Enable authentication.

```
[SW77501]ntp-service authentication enable
```

2 Set the key.

```
[SW77501]ntp-service authentication-keyid 42 authentication-mode md5
aNiceKey
```

3 Configure the key as reliable.

```
[SW77501]ntp-service reliable authentication-keyid 42
```