Configuration Preparation

Table of Contents

Chapter 1 Configuration Preparation

The chapter mainly describes the following preparatory works before you configure the switch at the first time:

- Port number of the switch
- Preparation before switch startup
- How to get help
- Command mode
- Cancelling a command
- Saving configuration

1.1 Port Number of the Switch

The physical port of the switch is numbered in the **<type><slot>/<port>** form. THE type-to-name table is shown as follows:

Interface Type	Name	Simplified Name
10M Ethernet	Ethernet	e
100M fast Ethernet	FastEthernet	f
1000M Ethernet	GigaEthernet	g

The expansion slot number to mark and set ports must be the number **0**. Other expansion slots are numbered from left to right, starting from **1**.

The ports in the same expansion slot are numbered according to the order from top to bottom and the order from left to right, starting from **1**. If only one port exists, the port number is **1**.

Note:

Ports in each kind of modulars must be numbered sequently from top to bottom and from left to right.

1.2 Preparation Before Switch Startup

Do the following preparatory works before the switch is configured:

(1) Set the switch's hardware according to the requirements of the manual.

(2) Configure a PC terminal simulation program.

(3) Determine the IP address layout for the IP network protocols.

1.3 Acquiring Help

Use the question mark (?) and the direction mark to help you enter commands:

- Enter a question mark. The currently available command list is displayed.

  Switch> ?

- Enter several familiar characters and press the space key. The available command list starting with the entered familiar characters is displayed.

  Switch> s?

- Enter a command, press the space key and enter the question mark. The command parameter list is displayed.

  Switch> show ?

- Press the “up” key and the commands entered before can be displayed. Continue to press the “up” key and more commands are to be displayed. After that, press the “down” key and the next command to be entered is displayed under the current command.

1.4 Command Modes

The command line interfaces for the switch can be classified into several modes. Each command mode enables you to configure different groupware. The command that can be used currently is up to the command mode where you are. You can enter the question mark in different command modes to obtain the available command list. Common command modes are listed in the following table:

Command Mode	Login Mode	Prompt	Exit Mode
System monitoring mode	Enter **Ctrl-p** after the power is on.	monitor#	Run **quit**.
User mode	Log in.	Switch>	Run **exit** or **quit**.
Management mode	Enter **enter** or **enable** in user mode.	Switch#	Run **exit** or **quit**.
Office configuration mode	Enter **config** in management mode.	Switch_config#	Run **exit** or **quit** or **Ctrl-z** to directly back to the management mode.
Port configuration mode	Enter the **interface** command in office configuration mode, such as **interface f0/1**.	Switch_config_f0/1#	Run **exit** or **quit** or **Ctrl-z** to directly back to the management mode.

Each command mode is unsuitable to subsets of some commands. If problem occurswhen you enter commands, check the prompt and enter the question mark to obtain the available command list. Problem may occur when you run in incorrect command mode or you misspelled the command.

Pay attention to the changes of the interface prompt and the relative command mode in the following case:

Switch> enter

Password: <enter password>

Switch# config

Switch_config# interface f0/1

Switch_config_f0/1# quit

Switch_config# quit

Switch#

1.5 Canceling a Command

To cancel a command or resume its default properties, add the keyword “no” before most commands. An example is given as follows:

no ip routing

1.6 Saving Configuration

You need to save configuration in case the system is restarted or the power is suddenly off. Saving configuration can quickly recover the original configuration. You can run write to save configuration in management mode or office configuration mode.

Basic Configuration

Table of Contents

Chapter 1 System Management Configuration

1.1 File Management Configuration

1.1.1 Managing the file system

The filename in flash is no more than 20 characters and filenames are case insensitive.

1.1.2 Commands for the file system

The boldfaces in all commands are keywords. Others are parameters. The content in the square brakcet “[ ]” is optional.

Command	Description
format	Formats the file system and delete all data.
dir [filename]	Displays files and directory names. The file name in the symbol “[]” means to display files starting with several letters. The file is displayed in the following format: Index number file name <FILE> length established time
delete filename	Deletes a file. The system will prompt if the file does not exist.
md dirname	Creates a directory.
rd dirname	Deletes a directory. The system will prompt if the directory is not existed.
more filename	Displays the content of a file. If the file content cannot be displayed by one page, it will be displayed by pages.
cd	Changes the path of the current file system.
pwd	Displays the current path.

1.1.3 Starting up from a file manually

monitor#boot flash <*local_filename*>

The previous command is to start a switch software in the flash, which may contain multiple switch software.

Parameter description

Parameter	Description
local_filename	A file name stored in the flash memory Users must enter the file name.

Example

monitor#boot flash switch.bin

1.1.4 Updating software

User can use this command to download switch system software locally or remotely to obtain version update or the custom-made function version (like data encryption and so on).

There are two ways of software update in monitor mode.

1. Through TFTP

monitor#copy tftp flash [ip_addr]

The previous commad is to copy file from the tftp server to the flash in the system. After you enter the command, the system will prompt you to enter the remote server name and the remote filename.

Parameter description

Parameter	Description
ip_addr	IP address of the tftp server If there is no specified IP address, the system will prompt you to enter the IP address after the **copy** command is run.

Example

The following example shows a **main.bin** file is read from the server, written into the switch and changed into the name **switch. Bin**.

monitor#copy tftp flash

Prompt: Source file name[]?main.bin

Prompt: Remote-server ip address[]?192.168.20.1

Prompt: Destination file name[main.bin]?switch.bin

please wait ...
##
##
##
##
##
##
TFTP:successfully receive 3377 blocks ,1728902 bytes
monitor#

2. Through serial port communication protocol—zmodem

Use the **download** command to update software. Enter **download ?** to obtain help.

monitor#download c0 *<local_filename>*

This command is to copy the file to the flash of system through zmodem. The system will prompt you to enter the port rate after you enter the command.

Parameter description

Parameter	Description
local_filename	Filename stored in the flash Users must enter the filename.

Example

The terminal program can be the Hyper Terminal program in WINDOWS 95, NT 4.0 or the terminal emulation program in WINDOWS 3.X.

monitor#download c0 switch.bin

Prompt: speed[9600]?115200

Then, modify the rate to 115200. After reconnection, select **send file** in the transfer menu of hyper terminal (terminal emulation). The **send file** dialog box appears as follows:

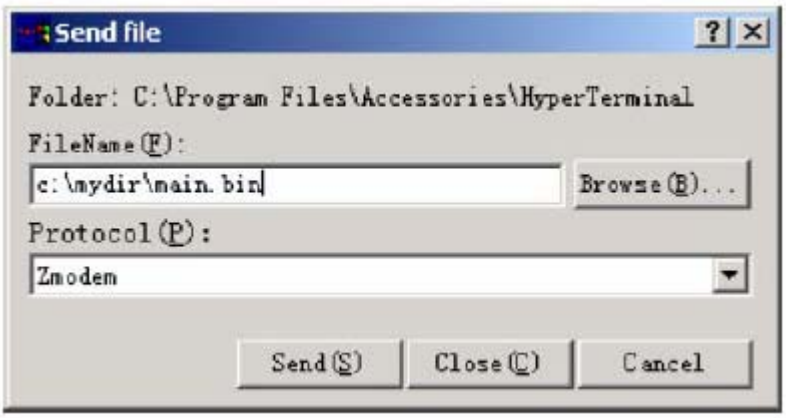


Figure 1-1 Send files

Enter the all-path of the switch software **main.bin** that our company provides in the filename input box, choose Zmodem as the protocol. Click **send** to send the file.

After the file is transferred, the following information appears:

ZMODEM:successfully receive 36 blocks ,18370 bytes

It indicates that the software update is completed, and then the baud rate of the hyper terminal should be reset to 9600.

Note:

The maximum download rate of switch S2026,S2224 is 38400 through the zmodem protocol.

1.1.5 Updating configuration

The switch configuration is saved as a file, the filename is startup-config. You can use commands similar to software update to update the configuration.

1. Through TFTP

monitor#copy tftp flash startup-config

2. Through serial port communication protocol—zmodem.

monitor#download c0 startup-config

1.1.6 Using ftp to perform the update of software and configuration

config #copy ftp flash [ip_addr|option]

Use ftp to perform the update of software and configuration in formal program management. Use the **copy** command to download a file from ftp server to switch, also to upload a file from file system of the switch to ftp server. After you enter the command, the system will prompt you to enter the remote server name and remote filename.

copy{**ftp**:[[[//login-name:[login-password]@]location]/directory]/filename}|**flash**:filename>}{**flash**<:filename>|**ftp**:[[[//login-name:[login-password]@]location]/directory]/filename}<blksize><mode><type>

Parameter description

Parameter	Description
login-nam	Username of the ftp server If there is no specified username, the system will prompt you to enter the username after the **copy** command is run.
login-password	Password of the ftp server If there is no specified password, the system will prompt you to enter the password after the **copy** command is run.
nchecksize	The size of the file is not checked on the server.
vrf	Provides vrf binding function for the device that supports MPLS.
blksize	Size of the data transmission block Default value: 512
ip_addr	IP address of the ftp server If there is no specified IP address, the system will prompt you to enter the IP address after executing the **copy** command.

active	Means to connect the ftp server in active mode.
passive	Means to connect the ftp server in passive mode.
type	Set the data transmission mode (ascii or binary)

Example

The following example shows a **main.bin** file is read from the server, written into the switch and changed into the name **switch. Bin**.

config#copy ftp flash

Prompt: ftp user name[anonymous]? login-nam

Prompt: ftp user password[anonymous]? login-password

Prompt: Source file name[]?main.bin

Prompt: Remote-server ip address[]?192.168.20.1

Prompt: Destination file name[main.bin]?switch.bin

or

config#copy ftp://login-nam:login-password@192.168.20.1/main.bin flash:switch.bin

##

##

FTP:successfully receive 3377 blocks ,1728902 bytes

config#

Note:

1) When the ftp server is out of service, the wait time is long. If this problem is caused by the tcp timeout time (the default value is 75s), you can configure the global command **ip tcp synwait-time** to modify the tcp connection time. However, it is not recommended to use it.

2) When you use ftp in some networking conditions, the rate of data transmission might be relatively slow. You can properly adjust the size of the transmission block to obtain the best effect. The default size is 512 characters, which guarantee a relatively high operation rate in most of the networks.

1.2 Basic System Management Configuration

1.2.1 Configuring Ethernet IP address

monitor#ip address <*ip_addr*> <*net_mask*>

This command is to configure the IP address of the Ethernet. The default IP address is 192.168.0.1, and the network mask is 255.255.255.0.

Parameter description

Parameter	Description
ip_addr	IP address of the Ethernet
net_mask	Mask of the Ethernet

Example

monitor#ip address 192.168.1.1 255.255.255.0

1.2.2 Configuring default route

monitor#ip route default <*ip_addr*>

This command is used to configure the default route. You can configure only one default route.

Parameter description

Parameter	Description
ip_addr	IP address of the gateway

Example

monitor#ip route default 192.168.1.1

1.2.3 Using ping to test network connection state

monitor#ping <*ip_address*>

This command is to test network connection state.

Parameter description

Parameter	Description
ip_address	Destination IP address

Example

monitor#ping 192.168.20.100
PING 192.168.20.100: 56 data bytes
64 bytes from 192.168.20.100: icmp_seq=0. time=0. ms
64 bytes from 192.168.20.100: icmp_seq=1. time=0. ms
64 bytes from 192.168.20.100: icmp_seq=2. time=0. ms
64 bytes from 192.168.20.100: icmp_seq=3. time=0. ms
----192.168.20.100 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss

round-trip (ms) min/avg/max = 0/0/0

Chapter 2 Terminal Configuration

2.1 VTY Configuration Introduction

The system uses the **line** command to configure terminal parameters. Through the command, you can configure the width and height that the terminal displays.

2.2 Configuration Task

The system has four types of lines: console, aid, asynchronous and virtual terminal. Different systems have different numbers of lines of these types. Refer to the following software and hardware configuration guide for the proper configuration.

Line Type	Interface	Description	Numbering
CON(CTY)	Console	To log in to the system for configuration.	0
VTY	Virtual and asynchronous	To connect Telnet, X.25 PAD, HTTP and Rlogin of synchronous ports (such as Ethernet and serial port) on the system	32 numbers starting from 1

2.2.1 Relationship between line and interface

1. Relationship between synchronous interface and VTY line

The virtual terminal line provides a synchronous interface to access to the system. When you connect to the system through VTY line, you actually connects to a virtual port on an interface. For each synchronous interface, there can be many virtual ports.

For example, if several Telnets are connecting to an interface (Ethernet or serial interface), you need to do the following steps for the VTY configuration:

(1) Log in to the line configuration mode.

(1) Configure the terminal parameters.

For VTY configuration, refer to Part 2.4 “VTY configuration example”.

2.3 Monitor and Maintenance

Run **showline** to chek the VTY configuration.

2.4 VTY Configuration Example

It shows how to cancel the limit of the line number per screen for all VTYs without **more** prompt:

config#line vty 0 32

config_line#length 0

Chapter 3 Network Management Configuration

3.1 Configuring SNMP

3.1.1 Introduction

The SNMP system includes the following parts:

- SNMP management side (NMS)
- SNMP agent (AGENT)
- Management information base (MIB)

SNMP is a protocol working on the application layer. It provides the packet format between SNMP management side and agent.

SNMP management side can be part of the network management system (NMS, like CiscoWorks). Agent and MIB are stored on the system. You need to define the relationship between network management side and agent before configuring SNMP on the system.

SNMP agent contains MIB variables. SNMP management side can check or modify value of these variables. The management side can get the variable value from agent or stores the variable value to agent. The agent collects data from MIB. MIB is the database of device parameter and network data. The agent also can respond to the loading of the management side or the request to configure data. SNMP agent can send trap to the management side. Trap sends alarm information to NMS indicating a certain condition of the network. Trap can point out improper user authentication, restart, link layer state(enable or disable), close of TCP connection, lose of the connection to adjacent systems or other important events.

1. SNMP notification

When some special events occur, the system will send ‘inform’ to SNMP management side. For example, when the agent system detects an abnormal condition, it will send information to the management side.

SNMP notification can be treated as trap or inform request to send. Since the receiving side doesn’t send any reply when receiving a trap, this leads to the receiving side cannot be sure that the trap has been received. Therefore the trap is not reliable. In comparison, SNMP management side that receives “inform request” uses PDU that SNMP echoes as the reply for this information. If no “inform request” is received on the management side, no echo will be sent. If the receiving side doesn’t send any reply, then you can resend the “inform request”. Then notifications can reach their destination.

Since inform requests are more reliable, they consume more resources of the system and network. The trap will be discarded when it is sent. The “inform request” has to be

stored in the memory until the echo is received or the request timeouts. In addition, the trap is sent only once, while the “inform request” can be resent for many times. Resending "inform request" adds to network communications and causes more load on network. Therefore, trap and inform request provide balance between reliability and resource. If SNMP management side needs receiving every notification greatly, then the “inform request” can be used. If you give priority to the communication amount of the network and there is no need to receive every notification, then trap can be used.

This switch only supports trap, but we provide the extension for "inform request".

2. SNMP version

System of our company supports the following SNMP versions:

- SNMPv1---simple network management protocol,a complete Internet standard,which is defined in RFC1157.
- SNMPv2C--- Group-based Management framework of SNMPv2, Internet test protocol, which is defined in RFC1901.

Layer 3 switch of our company also supports the following SNMP:

- SNMPv3--- a simple network management protocol version 3, which is defined in RFC3410.

SNMPv1 uses group-based security format. Use IP address access control list and password to define the management side group that can access to agent MIB.

SNMPv3 provides secure access to devices by a combination of authenticating and encrypting packets over the network.

The security features provided in SNMPv3 are:

•Message integrity—Ensuring that a packet has not been tampered with in-transit.

•Authentication—Determining the message is from a valid source.

•Encryption—Scrambling the contents of a packet prevent it from being seen by an unauthorized source.

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the group in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level will determine which security mechanism is employed when handling an SNMP packet. Three security models are available, that is, authentication and encryption, authentication and no encryption, no authentication.

You need to configure SNMP agent to the SNMP version that the management working station supports. The agent can communicate with many management sides.

3. Supported MIB

SNMP of our system supports all MIBII variables (which will be discussed in RFC 1213) and SNMP traps (which will be discussed in RFC 1215).

Our system provides its own MIB extension for each system.

3.1.2 SNMP Configuration Tasks

- Configuring SNMP view
- Creating or modifying the access control for SNMP community
- Configuring the contact method of system administrator and the system's location
- Defining the maximum length of SNMP agent data packet
- Monitoring SNMP state
- Configuring SNMP trap
- Configuring SNMP binding source address
- Configuring NMPv3 group
- Configuring NMPv3 user
- Configuring NMPv3 EngineID

1. Configuring SNMP view

The SNMP view is to regulate the access rights (include or exclude) for MIB. Use the following command to configure the SNMP view.

Command	Description
snmp-server view *name oid*] [exclude | include]	Adds the subtree or table of OID-specified MIB to the name of the SNMP view, and specifies the access right of the object identifier in the name of the SNMB view. Exclude: decline to be accessed Include: allow to be accessed

The subsets that can be accessed in the SNMP view are the remaining objects that "include" MIB objects are divided by "exclude" objects. The objects that are not configured are not accessible by default.

After configuring the SNMP view, you can implement SNMP view to the configurtation of the SNMP group name, limiting the subsets of the objects that the group name can access.

2. Creating or modifying the access control for SNMP community

You can use the SNMP community character string to define the relationship between SNMP management side and agent. The community character string is similar to the password that enables the access system to log in to the agent. You can specify one or multiple properties releavant with the community character string. These properties are optional:

Allowing to use the community character string to obtain the access list of the IP address at the SNMP management side

Defining MIB views of all MIB object subsets that can access the specified community

Specifying the community with the right to read and write the accessible MIB objects

Configure the community character string in global configuration mode using the following command:

Command	Function
snmp-server community *string* [**view** *view-name*] [**ro** | **rw**] [*word*]	Defines the group access character string.

You can configure one or multiple group character strings. Run **no snmp-server community** to remove the specified community character string.

For how to configure the community character string, refer to the part “SNMP Commands”.

3. Configuring the contact method of system administrator and the system’s location

SysContact and sysLocation are the management variables in the MIB’s system group, respectively defining the linkman’s identifer and actual location of the controlled node. These information can be accessed through **config.** files. You can use the following commands in global configuration mode.

Command	Function
snmp-server contact *text*	Sets the character string for the linkman of the node.
snmp-server location *text*	Sets the character string for the node location.

4. Defining the maximum length of SNMP agent data packet

When SNMP agent receives requests or sents respons, you can configure the maximum length of the data packet. Use the following command in global configuration mode:

Command	Function
snmp-server packetsize *byte-count*	Sets the maximum length of the data packet.

5. Monitoring SNMP state

You can run the following command in global configuration mode to monitor SNMP output/input statistics, including illegal community character string items, number of mistakes and request variables.

Command	Function
show snmp	Monitores the SNMP state.

6. Configuring SNMP trap

Use the following command to configure the system to send the SNMP traps (the second task is optional):

- Configuring the system to send trap

  Run the following commands in global configuration mode to configure the system to send trap to a host.

Command	Function
snmp-server host host community-string [trap-type]	Specifies the receiver of the trap message.
snmp-server host *host* [traps|informs]{version {v1 | v2c | v3 {auth | noauth | priv } }}*community-string* [*trap-type*]	Specifies the receiver, version number and username of the trap message. Note: For the trap of SNMPv3, you must configure SNMP engine ID for the host before the host is configured to receive the trap message.

  When the system is started, the SNMP agent will automatically run. All types of traps are activated. You can use the command **snmp-server host** to specify which host will receive which kind of trap.

  Some traps need to be controlled through other commands. For example, if you want SNMP link traps to be sent when an interface is opened or closed, you need to run **snmp trap link-status** in interface configuration mode to activate link traps. To close these traps, run the interface configuration command **snmp trap link-stat**.

  You have to configure the command **snmp-server host** for the host to receive the traps.

- Modifying the running parameter of the trap

  As an optional item, it can specify the source interface where traps originate, queue length of message or value of resending interval for each host.

  To modify the running parameters of traps, you can run the following optional commands in global configuration mode.

Command	Function
snmp-server trap-source *interface*	Specifies the source interface where traps originate and sets the source IP address for the message.
snmp-server queue-length *length*	Creates the queue length of the message for each host that has traps. Default value: 10
snmp-server trap-timeout *seconds*	Defines the frequency to resend traps in the resending queue. Default value: 30 seconds

3.1.3 Configuration example

1. Example 1

```
snmp-server community public RO
```

snmp-server community private RW

snmp-server host 192.168.10.2 public

The above example shows:

- how to set the community string **public** that can only read all MIB variables.
- how to set the community string **private** that can read and write all MIB variables.

You can use the community string **public** to read MIB variables in the system. You can also use the community string **private** to read MIB variables and write writable MIB variables in the system.

The above command specifies the community string **public** to send traps to 192.168.10.2 when a system requires to send traps. For example, when a port of a system is in the **down** state, the system will send a **linkdown** trap information to 192.168.10.2.

2. Example 2

snmp-server engineID remote 90.0.0.3 80000523015a000003

snmp-server group getter v3 auth

snmp-server group setter v3 priv write v-write

snmp-server user get-user getter v3 auth sha 12345678

snmp-server user set-user setter v3 encrypted auth md5 12345678

snmp-server user notifier getter remote 90.0.0.3 v3 auth md5 abcdefghi

snmp-server host 90.0.0.3 informs version v3 auth notifier

snmp-server view v-write internet included

The above example shows how to use SNMPv3 to manage devices. Group **getter** can browse device information, while group **setter** can set devices. User **get-user** belongs to group **getter** while user **set-user** belongs to group **setter**.

For user **get-user**, its security level is **authenticate but not encrypt**, its password is **12345678**, and it uses the sha arithmetic to summarize the password.

For user **set-user**, its security level is **authenticate and encrypt**, its password is **12345678**, and it uses the md5 arithmetic to summarize the password.

When key events occur at a device, use username **notifier** to send **inform** messages to host 90.0.0.3 of the administrator.

3.2 RMON Configuration

3.2.1 RMON configuration task

RMON configuration tasks include:

- Configuring the rMon alarm function for the switch
- Configuring the rMon event function for the switch
- Configuring the rMon statistics function for the switch

- Configuring the rMon history function for the switch
- Displaying the rMon configuration of the switch

1. Configuring rMon alarm for switch

You can configure the rMon alarm function through the command line or SNMP NMS. If you configure through SNMP NMS, you need to configure the SNMP of the switch. After the alarm function is configured, the device can monitor some statistic value in the system. The following table shows how to set the rMon alarm function:

Command	Function
configure	Enter the global configuration mode.
rmon alarm index variable *interval* {**absolute** | **delta**} **rising-threshold** *value* [*eventnumber*] **falling-threshold** *value* [*eventnumber*] [**owner** *string*]	Add a rMon alarm item. **index** is the index of the alarm item. Its effective range is from 1 to 65535. **variable** is the object in the monitored MIB. It must be an effective MIB object in the system. Only obejects in the Integer, Counter, Gauge or TimeTicks type can be detected. **interval** is the time section for sampling. Its unit is second. Its effective value is from 1 to 4294967295. **absolute** is used to directly monitor the value of MIB object. **delta** is used to monitor the value change of the MIB objects between two sampling. **value** is the threshold value when an alarm is generated. **eventnumber** is the index of an event that is generated when a threshold is reached. **eventnumber** is optional. **owner string** is to describe the information about the alarm.
exit	Enter the management mode again.
write	Save the configuration.

After a rMon alarm item is configured, the device will obtain the value of variable-specified oid after an interval. The obtained value will be compared with the previous value according to the alrm type (absolute or delta). If the obtained value is bigger than the previous value and surpasses the threshold value specified by **rising-threshold**, an event whose index is **eventnumber** (If the value of **eventnumber** is 0 or the event whose index is **eventnumber** does not exist in the event table, the event will not occur). If the variable-specified oid cannot be obtained, the state of the alarm item in this line is set to **invalid**. If you run **rmon alarm** many times to configure alarm items with the same index, only the last configuration is effective. You can run **no rmon alarm index** to cancel alarm items whose indexes are **index**.

2. Configuring eMon event for switch

The steps to configure the rMon event are shown in the following table:

Step	Command	Purpose
1.	**configure**	Enter the global configuration mode.

2.	**rmon event index** [**description** *string*] [**log**] [**owner** *string*] [**trap** community]	Add a rMon event item. **index** means the index of the event item. Its effective range is from 1 to 65535. **description** means the information about the event. **log** means to add a piece of information to the log table when a event is triggered. **trap** means a trap message is generated when the event is triggered. **community** means the name of a community. **owner string** is to describe the information about the alarm.
3.	**exit**	Enter the management mode again.
4.	**write**	Save the configuration.

After a rMon event is configured, you must set the domain **eventLastTimeSent** of the rMon event item to **sysUpTime** when a rMon alarm is triggered. If the **log** attribute is set to the rMon event, a message is added to the log table. If the **trap** attribute is set to the rMon event, a trap message is sent out in name of community. If you run **rmon event** many times to configure event items with the same index, only the last configuration is effective. You can run **no rmon event index** to cancel event items whose indexes are **index**.

3. Configuring rMon statistics for switch

The rMon statistics group is used to monitor the statistics information on every port of the device. The steps to configure the rMon statistics are as follows:

Step	Command	Purpose
1.	**configure**	Enter the global configuration mode.
2.	**interface iftype ifid**	Enter the port mode. **iftype** means the type of the port. **ifid** means the ID of the interface.
3.	**rmon collection stat index** [**owner** *string*]	Enable the statistics function on the port. **index** means the index of the statistics. **owner string** is to describe the information about the statistics.
4.	**exit**	Enter the global office mode.
5.	**exit**	Enter the management mode again.
6.	**write**	Save the configuration.

If you run **rmon collection stat** many times to configure statistics items with the same index, only the last configuration is effective. You can run **no rmon collection stats index** to cancel statistics items whose indexes are **index**.

4. Configuring rMon history for switch

The rMon history group is used to collect statistics information of different time sections on a port in a device. The rMon statistics function is configured as follows:

Step	Command	Purpose
1.	configure	Enter the global configuration command.
2.	interface iftype ifid	Enter the port mode. **iftype** means the type of the port. **ifid** means the ID of the interface.
3.	rmon collection history index [buckets bucket-number] [interval second] [owner owner-name]	Enable the history function on the port. **index** means the index of the history item. Among all data collected by history item, the latest **bucket-number** items need to be saved. You can browse the history item of the Ethernet to obtain these statistics values. The default value is 50 items. **second** means the interval to abtain the statistics data every other time. The default value is 1800 seconds. **owner string** is used to describe some information about the history item.
4.	exit	Enter the global office mode again.
5.	exit	Enter the management mode again.
6.	write	Save the configuration.

After a rMon history item is added, the device will obtain statistics values from the specified port every **second** seconds. The statistics value will be added to the history item as a piece of information. If you run **rmon collection history index** many times to configure history items with the same index, only the last configuration is effective. You can run **no rmon history index** to cancel history items whose indexes are **index**.

Note:

Too much system sources will be occupied in the case the value of **bucket-number** is too big or the value of **interval second** is too small.

5. Displaying rMon configuration of switch

Run **show** to display the rMon configuration of the switch.

Command	Purpose
show rmon [alarm] [event] [statistics] [history]	Displays the rmon configuration information. **alarm** means to display the configuration of the alarm item. **event** means to show the configuration of the event item and to show the items that are generated by the occurance of events and are contained in the log table. **statistics** means to display the configuration of the statistics item and statistics values that the device collects from the port. **history** means to display the configuration of the history item and statistics values that the device collects in the latest specified intervals from the port.

Interface Configuration

Table of Contents

Chapter 1 Introduction

This section helps user to learn various kinds of interface that our switch supports and consult configuration information about different interface types.

For detailed description of all interface commands used in this section, refer to *Interface configuration command*. For files of other commands appeared in this section, refer to other parts of the manual.

The introduction includes communication information that can be applied to all interface types.

1.1 Supported Interface Types

For information about interface types, please refer to the following table.

Interface Ttype	Task	Reference
Ethernet interface	Configures Ethernet interface. Configures fast Ethernet interface. Configures gigabit Ethernet interface.	*Configuring Ethernet Interface*
Logical Interface	Loopback interface Null interface VLAN interface SuperVlan interface	*Configuring Logistical Interface* The loopback interface and null interface are only configured on layer-3 switch. User can configure either VLAN or SuperVlan interface on layer-2 switch.
	Aggregation interface	*Configuring Logistical Interface*

The two supported kinds of interface: Ethernet interface and logical interface. The Ethernet interface type depends on one device depends on the standard communication interface and the interface card or interfaced module installed on the switch. The logical interface is the interface without the corresponding physical device, which is established by user manually.

The supported Ethernet interfaces of our switch include:

- Ethernet interface
- Fast Ethernet interface
- Gigabit Ethernet interface

The supported logical interface of our switch include:

- loopback interface
- null interface

- aggregation interface
- VLAN interface

1.2 Interface Configuration Introduction

The following description applies to the configuration process of all interfaces. Take the following steps to perform interface configuration in global configuration mode.

(1) Run the **interface** command to enter the interface configuration mode and start configuring interface. At this time, the switch prompt becomes ‘config_’ plus the shortened form of the interface to be configured. Use these interfaces in terms of their numbers. Numbers are assigned during installation(exworks) or when an interface card are added to the system. Run the **show interface** command to display these interfaces. Each interface that the device supports provides its own state as follows:

```
Switch#show interface
GigaEthernet1/1 is down, line protocol is down
  Hardware is Fast Ethernet, Address is 0009.7cf7.7dc1
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Auto-duplex, Auto-speed
  input flow-control is off, output flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 17:52:52, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    1 packets input, 64 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 0 multicast, 0 pause input
    0 input packets with dribble condition detected
    1 packets output, 64 bytes, 0 underruns
    0 output errors, 0 collisions, 1 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier, 0 PAUSE output
    0 output buffer failures, 0 output buffers swapped out
```

To configure gigabit Ethernet interface g1/1, enter the following content:

interface GigaEthernet0/1

The switch prompts “config_g0/1”.

Note:

There is no need to add blank between interface type and interface number. For example, in the above line, g 1/1 or g 1/1 is both right.

(1) You can configure the interface configuration commands in interface configuration mode. Various commands define protocols and application programs to be executed on the interface. These commands will stay until user exits the interface configuration mode or switches to another interface.

(2) Once the interface configuration has been completed, use the show command in the following chapter ‘Monitoring and Maintaining Interface’ to test the interface state.

Chapter 2 Interface Configuration

2.1 Configuring Interface Common Attribute

The following content describes the command that can be executed on an interface of any type and configures common attributes of interface. The common attributes of interface that can be configured include: interface description, bandwidth and delay and so on.

2.1.1 Adding Description

Adding description about the related interface helps to memorize content attached to the interface. This description only serves as the interface note to help identify uses of the interface and has no effect on any feature of the interface. This description will appear in the output of the following commands: **show running-config** and **show interface**. Use the following command in interface configuration mode if user wants to add a description to any interface.

Command	Description
description *string*	Adds description to the currently-configured interface.

For examples relevant to adding interface description, please refer to the following section ‘Interface Description Example’.

2.1.2 Configuring Bandwidth

The upper protocol uses bandwidth information to perform operation decision. Use the following command to configure bandwidth for the interface:

Command	Description
bandwidth *kilobps*	Configures bandwidth for the currently configured interface.

The bandwidth is just a routing parameter, which doesn’t influence the communication rate of the actual physical interface.

2.1.3 Configuring Time Delay

The upper protocol uses time delay information to perform operation decision. Use the following command to configure time delay for the interface in the interface configuration mode.

Command	Description
delay *tensofmicroseconds*	Configures time delay for the currently configured interface.

The configuration of time delay is just an information parameter. Use this command cannnot adjust the actual time delay of an interface.

2.2 Monitoring and Maintaining Interface

The following tasks can monitor and maintain interface:

- Checking interface state
- Initializing and deleting interface
- Shutting down and enabling interface

2.2.1 Checking Interface State

Our switch supports displaying several commands related to interface information, including version number of software and hardware, interface state. The following table lists a portion of interface monitor commands. For the description of these commands, please refer to 'Interface configuration command'.

Use the following commands:

Command	Description
show interface [**type** [slot|port]]	Displays interface state.
show running-config	Displays current configuration.

2.2.2 Initializing and Deleting Interface

You can dynamically establish and delete logical interfaces. This also applies to the sub interface and channalized interface. Use the following command to initialize and delete interface in global configuration mode:

Command	Description
no interface type [*slot*|*port*]	Initializes physical interface or deletes virtual interface.

2.2.3 Shutting down and Enabling Interface

When an interface is shut down, all features of this interface are disabled, and also this interface is marked as unavailable interface in all monitor command displays. This information can be transmitted to other switches via dynamic routing protocol.

Use the following command to shutdown or enable an interface in the interface configuration mode:

Command	Description
shutdown	Shuts down an interface.
no shutdown	Enables an interface.

You can use the **show interface** command and the **show running-config** command to check whether an interface has been shut down. An interface that has been shut down is displayed as 'administratively down' in the **show interface** command display. For more details, please refer to the following example in 'Interface Shutdown Example'.

2.3 Configuring Logistical Interface

This section describes how to configure a logical interface. The contents are as follows:

- Configuring null interface
- Configuring loopback interface.
- Configuring aggregation interface
- Configuring VLAN interface

2.3.1 Configuring Null Interface

The whole system supports only one null interface. Its functions are similar to those of applied null devices on most operating systems. The null interface is always available, but it never sends or receives communication information. The interface configuration command **no ip unreachable** is the only one command available to the null interface. The null interface provides an optional method to filtrate communication. That is, the unwanted network communication can be routed to the null interface; the null interface can function as the access control list.

You can run the following command in global configuration mode to specify the null interface:

Command	Description
interface null *0*	Enters the null interface configuration state.

The null interface can be applied in any command that takes the interface type as its parameter.

The following case shows how to configure a null interface for the routing of IP 192.168.20.0.

ip route 192.168.20.0 255.255.255.0 null 0

2.3.2 Configuring Loopback Interface

The loopback interface is a logistical interface. It always functions and continues BGP session even in the case that the outward interface is shut down. The loopback interface can be used as the terminal address for BGP session. If other switches try to reach the loopback interface, a dynamic routing protocol should be configured to broadcast the routes with loopback interface address. Messages that are routed to the loopback interface can be re-routed to the switch and be handled locally. For messages that are routed to the loopback interface but whose destination is not the IP address of the loopback interface, they will be dropped. This means that the loopback interface functions as the null interface.

Run the following command in global configuration mode to specify a loopback interface and enter the interface configuration state:

Command	Description
interface loopback *number*	Enter the loopback interface configuration state.

2.3.3 Configuring Aggregation Interface

The inadequate bandwidth of a single Ethernet interface gives rise to the birth of the aggregation interface. It can bind several full-duplex interface with the same rate together, greatly improving the bandwidth.

Run the following command to define the aggregation interface:

Command	Description
Interface port-aggregator *number*	Configures the aggregation interface

2.3.4 Configuring VLAN Interface

V VLAN interface is the routing interface in switch. The VLAN command in global configuration mode only adds layer 2 VLAN to system without defining how to deal with the IP packet whose destination address is itself in the VLAN. If there is no VLAN interface, this kind of packets will be dropped.

Run the following command to define VLAN interface:

Command	Description
Interface vlan *number*	Configures VLAN interface.

2.3.5 Configuring Super VLAN Interface

The Super VLAN technology provides a mechanism: hosts in different VLANs of the same switch can be allocated in the same Ipv4 subnet and use the same default gateway; lots of IP addresses are, therefore, saved. The Super VLAN technology puts different VLANs into a group where VLANs use the same management interface and hosts use the same IPv4 network section and gateway. VLAN belonging to Super VLAN is called as SubVLAN. No SubVLAN can possess the management interface by configuring IP address.

You can configure a Super VLAN interface through a command line. The procedure of configuring a Super VLAN interface is shown as follows:

Command	Description
[no] interface supervlan *index*	Enter the Super VLAN interface configuration mode. If the specified Super VLAN interface does not exist, the system will create a Super VLAN interface.. **index** is the index of the Super VLAN interface. Its effective value ranges from 1 to 32. **no** means to delete Super VLAN interface.
[no] subvlan [*setstr*] **[add** *addstr***] [remove** *remstr***]**	Configure SubVLAN in Super VLAN. The added Sub VLAN cannot possess a management interface or cannot belong to other Super VLANs. In original state, Super VLAN does not contain any Sub VLAN. Only one sub command can only be

	used every time. **setstr** means to set the Sub VLAN list. For example, List 2,4-6 indicate VLAN 2, 4, 5 and 6. **add** means to add VLAN list in the original SubVLAN list. **addstr** means the character string whose format is the same as the above. **remove** means to delete VLAN list in the original SubVLAN list. remstr is the list's character string whose format is the same as the above. **no** means to delete all SubVLANs in SuperVLAN. The **no** command cannot be used with other sub commands.

After you configure the Super VLAN interface, you can configure the IP address for the Super VLAN interface. The Super VLAN interface is also a routing port, which can be configured as other ports are.

Chapter 3 Interface Configuration Example

3.1 Configuring Public Attribute of Interface

3.1.1 Interface Description Example

The following example shows how to add description related to an interface. This description appears in the configuration file and interface command display.

```
interface vlan 1
ip address 192.168.1.23 255.255.255.0
```

3.1.2 Interface Shutdown Example

The following example shows how to shutdown the Ethernet interface 0/1:

```
interface GigaEthernet0/1
shutdown
```

The following example shows how to enable the interface:

```
interface GigaEthernet0/1
no shutdown
```

Port Additional Characteristic Configuration

Table of Contents

Chapter 1 Port Security

1.1 Introduction

You can control the access function of the secure port, enabling the port to run in a certain range according to your configuration. If you enable the security function of a port through configuring the number of secure MAC addresses for the port. If the number of secure MAC addresses exceeds the upper limitation and MAC addresses are insecure, secure port violation occurs. You should take actions according to different violation modes.

The secure port has the following functions:

- Configuring the number of secure MAC addresses
- Configuring static secure MAC addresses
  If the secure port has no static secure MAC address or the number of static secure MAC addresses is smaller than that of secure MAC addresses, the port will learn dynamic MAC addresses.
- Dropping violated packets when secure port violation occurs

The section describes how to configure the secure port for the switch.

1.2 Configuring Secure Port Task List

- Configure MAC addresses and the binding of IP address.

1.3 Configuring Secure Port Task

1.3.1 Configuring MAC Address and Binding of IP Address

The switch can bind both the IP address and the MAC address to the port, or just bind one of them.

Note:

After the IP address is bound to the MAC address on the port, IP messages that are incompatible with the bound MAC addresses are to be filtrated.

Enter the port configuration mode and run the following command to display the configuration information about secure port.

Run…	To…
switchport port-security bind {**ip** *A.B.C.D* **| mac** *H.H.H*}	Bind the IP address to the MAC address on the port.

Chapter 2 Port Congestion

In normal case, the Ethernet interface will broadcast unknown message to the VLAN where the Ethernet interface is located. In some cases, message of the type is forbidden to forward.

Command	Description
switchport block {**unicast|multicast| broadcast**}	The interface does not forward uni-cast, multicast or broadcast message.
no switchport block {**unicast** | **multicast** | **broadcast**}	The interface forwards all message.

Chapter 3 Port Protection

In normal cases, packets between different ports on a switch can be freely forwarded. In some cases, packets between different ports are not allowed to forward. The port isolation function can forbid the packet flow between ports. The ports with the isolation function cannot communicate with each other. Packets can be normally forwarded between ports without isolation function or between isolated ports and non-isolated ports.

Command	Description
switchport protected	Sets port isolation.
no switchport protected	Cancels port isolation.

Chapter 4 Port Storm Control

The port of switch may bear continuous and abnormal attack from Uni-cast (fail to look up the MAC address), multicast or broadcast message. In this case, the port of the switch or the whole switch will break down. A mechanism must be provided to constrain the phenomena.

Command	Description
storm-control {**broadcast** | **multicast** | **unicast**} **threshold count**	Controls the storm of broadcast, multicast or uni-cast message.
no storm-control {**broadcast** | **multicast** | **unicast**} **threshold**	Does not control the storm.

Chapter 5 Port Rate Limitation

You can control the rate of outward/inward traffic through configuration.

Run the following commands in privilege mode to control the traffic rate of the port:

Run…	To…
configure	Enter the global configuration mode.
interface g0/1	Log in to the to-be-configured port.
[**no**] **switchport rate-limit** *band* { ingress|egress}	Configure the traffic rate control for a port. **band** is the traffic rate to be controlled. **ingress** means having effect on the incoming port. **egress** means having effect on the outcoming port.
exit	Enter the global configuration mode again.
exit	Enter the management configuration mode again.

Chapter 6 Port Loop Detection

You can detect whether loop occurs on the port through configuration.

Enter the port configuration in global configuration mode:

Command	Description
[no] keepalive	(Disables) enables port loop detection.
keepalive *period*	Sets the period for port loop detection. Its effective range is from 0 to 32767.

Interface Range Configuration

Table of Contents

Chapter 1 Interface Range Configuration

1.1 Interface Range Configuration Task

1.1.1 Understanding Interface Range

In the process of configuring interface tasks, there are cases when you have to configure the same attribute on ports of the same type. In order to avoid repeated configuration on each port, we provide the **interface range** configuration mode. You can configure ports of the same type and slot number with the same configuration parameters. This reduces the workload.

Note:

when entering the **interface range** mode, all interfaces included in this mode must have been established.

1.1.2 Entering Interface Range Mode

Run the following command to enter the **interface range** mode.

Step	Command	Description
1	**interface range** *type slot*/<*port1* - *port2* | port3>[, <port1 - port2|port3>]	Enters the range mode. All ports included in this mode accord to the following conditions: (1) The slot number is set to **slot**. (2) The port numbers before/after the hyphen must range between port1 and port2, or equal to port3. (3) Port 2 must be less than port 1 (4) There must be space before/after the hyphen or the comma.

1.1.3 Configuration Example

Enter the interface configuration mode via the following commands, including slot 0 and fast Ethernet 1,2,3,6,8,10,11,12:

switch_config#interface range 1 - 3 , 6 , 8 , 10 - 12

switch_config_if_range#

Port Mirroring Configuration

Table of Contents

Chapter 1 Configuring Port Mirroring

1.1 Configuring Port Mirroring Task List

- Configuring port mirroring
- Displaying port mirroring information

1.2 Configuring Port Mirroring Task

1.2.1 Configuring Port Mirroring

Through configuring port mirroring, you can use one port of a switch to observe the traffic on a group of ports.

Enter the privilege mode and perform the following steps to configure port mirroring:

Command	Description
configure	Enters the global configuration mode.
mirror session *session_number* {destination {interface *interface-id*} | source {interface *interface-id* [, | -] [both | rx | tx] }	Configures port mirroring. **session-number** is the number of the port mirroring. **destination** is the destination port of the mirroring. **source** is the source port of mirroring. **both | rx | tx** is the data flow that is to be mirrored. **rx** means the input data of mirroring. **tx** means the output data of mirroring.
exit	Enters the management mode again.
write	Saves the configuration.

1.2.2 Displaying Port Mirroring Information

Run show to display the configuration information of port mirroring.

Command	Description
show mirror [session *session_number]*	Displays the configuration information about port mirroring. **session-number** is the number of the port mirroring.

VLAN Configuration

Table of Contents

Chapter 1 VLAN Configuration

1.1 VLAN Introduction

Virtual LAN (VLAN) refers to a group of logically networked devices on one or more LANs that are configured so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. In 1999 IEEE established IEEE 802.1Q Protocol Standard Draft used to standardize VLAN realization project. Because VLANs are based on logical instead of physical connections, it is very flexible for user/host management, bandwidth allocation and resource optimization.

There are the following types of Virtual LANs:

- Port-Based VLAN: each physical switch port is configured with an access list specifying membership in a set of VLANs.
- 802.1Q trunk mode is supported on the interface.
- Access mode interface is supported.

  Port-Based Vlan is to ascribe port to one subset of vlan that the switch supports. If this vlan subset has only one vlan, then this port is access port. If this vlan subset has multiple vlan, then this port is trunk port. There is one default vlan among the multiple vlan, and the vlan id is the port vlan id (PVID).
- Vlan-allowed range is supported on the interface.

Vlan-allowed parameter is used to control vlan range that the port belongs. Vlan-untagged parameter is used to configure port to send packets without vlan tag to the corresponding vlan.

1.2 VLAN Configuration Task List

- Adding/Deleting VLAN
- Configuring switch port
- Creating/Deleting VLAN interface
- Configuring superVLAN interface
- Monitoring configuration and state of VLAN

1.3 VLAN Configuration Task

1.3.1 Adding/Deleting VLAN

A virtual LAN, commonly known as a VLAN, is a group of hosts with a common set of requirements that communicate as if they were attached to the same wire, regardless of their physical location. A VLAN has the same attributes as a physical LAN, but it allows for end stations to be grouped together even if they are not located on the same LAN segment. A VLAN may have multiple ports and all unicast, multicast and broadcast message can only be forwarded from the same VLAN to the terminal. Each VLAN is a logistical network. If the data wants to reach another VLAN, it must be forwarded by router or bridge.

Run the following command to configure VLAN

Run…	To…
vlan vlan-id	Enter the VLAN configuration mode.
name str	Name in the vlan configuration mode.
Exit	Exit vlan configuration mode, and establish vlan.
vlan vlan-range	Establish multiple VLANs at the same time.
no vlan vlan-id | vlan-range	Delete one or multiple VLANs.

Vlan can perform dynamic addtion and deletion via vlan management protocol GVRP.

1.3.2 Configuring Switch Port

The switch port supports the following modes: access mode, trunk mode and dot1q-tunnel mode.

- The access mode indicates that this port is only subordinate to one vlan and only sends and receives untagged ethernet frame.
- The trunk mode indicates that this port is connected to other switches and can send and receive tagged ethernet frame.
- The dot1q-tunnel mode takes uncontionally the received packets as the ones without tag. The switch chip automatically adds pvid of the port as the new tag, therefore allowing switch to ignore the different vlan partitions that connected to the network. Then the packet will be delivered unchangedly to the other port in the other subnetwork of the same customer. The transparent transmission is realized in this way.

Each port has one default vlan and pvid,and all the data without vlan tag received on the port belong to the data packets of the vlan.

Trunk mode can ascribe port to multiple vlan and also can configure which kind of packet to forward and the number of vlan that belongs, that is, the packet sent on the port is tagged or untagged, and the vlan list that the port belongs.

Run the following command to configure the switch port:

Run…	To…

switchport pvid *vlan-id*	Configure pvid of switch port.
switchport mode access|trunk|dot1q-tunnel	Configure port mode of the switch.
switchport trunk vlan-allowed …	Configure vlan-allowed range of switch port.
switchport trunk vlan-untagged …	Configure vlan-untagged range of switch port.

Note: Not all switches support dot1q-tunnel feature. Some switches only support globally enabling/disabling this feature, and cannot configure different strategies for different ports.

The command to globally enable dot1q-tunnel is as follows:

Command	Description
double-tagging	Globally enables double-tagging feature of the switch.

The capability for switches of various models to support dot1q-tunnel is shown as follows:

Model	Capability to suppor dot1q-tunnel
2116 / 2224 / 2224M / 2226 / 2448B / 3224 / 3224M / 3424 / 6508	Not support
2224D	Global
2448 / 2516 / 2524 / 3448 / 3512	Interface

For those models not listed in the table or the latest models, please consult our technicians or download the latest instructions from our website.

1.3.3 Creating/Deleting VLAN Interface

Vlan interface can be established to realize network management or layer 3 routing feature. The vlan interface can be used to specify ip address and mask. Run the following command to configure vlan interface:

Run…	To…
[no] interface vlan *vlan-id*	Create/Delete a VLAN interface.

1.3.4 Configuring Super VLAN Interface

The Super VLAN technology provides a mechanism: Hosts in different VLANs that run the same switch can be allocated in the same Ipv4 subnet; lots of IP addresses are, therefore, saved. The Super VLAN technology classifies different VLANs into a group. The VLANs in this group uses the same management interface. Hosts in the group use the same IPv4 network section and gateway. VLAN belonging to Super VLAN is called as SubVLAN. No SubVLAN can possess the management interface by configuring IP address.

You can configure a Super VLAN interface through the command line. The procedure of configuring a Super VLAN interface is shown as follows:

Command	Description
[no] interface	Enters the interface configuration mode . If the specified Super VLAN

supervlan *index*	interface does not exists, the system will create a Super VLAN interface. **index** is the index of Super VLAN interface. Its effective value ranges from 1 to 32. **no** means deleting Super VLAN interface.
[**no**] **subvlan** [*setstr*] [**add** *addstr*] [**remove** *remstr*]	Configures SubVlan in Super VLAN. The added Sub VLAN cannot possess the management interface. In original state, Super VLAN does not include Sub VLAN. Only one sub command can be used every time. **setstr** means to set the Sub VLAN list. For example, List 2,4-6 indicate VLAN 2, 4, 5 and 6. **add** means to add VLAN list in the original SubVLAN list. **addstr** means the character string whose format is the same as the above. **remove** means to delete VLAN list in the original SubVLAN list. remstr is the list's character string whose format is the same as the above. **no** means to delete all SubVLANs in SuperVLAN. The **no** command cannot be used with other sub commands.

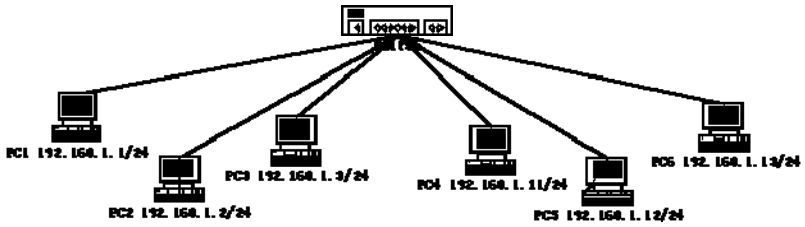
After you configure the Super VLAN interface, you can configure the IP address for the Super VLAN interface. The Super VLAN interface is also a routing port, which can be configured as other ports are.

1.3.5 Monitoring Configuration and State of VLAN

Run the following commands in EXEC mode to monitor configuration and state of VLAN:

Run…	To…
show vlan [**id** *x* | **interface** *intf*]	Display configuration and state of VLAN.
show interface {**vlan** | **supervlan**} *x*	Display the states of vlan/supervlan ports.

1.4 Configuration Examples



Users PC1~PC6 connect the switch through ports 1~6. The IP addresses of these PCs belong to the network section 192.168.1.0/24. Though group PC1~PC3 and group PC4~PC6 are located at different layer-2 broadcast domains, PC1~PC6 can ping each other and manage the switch through the IP address 192.168.1.100. To do this, you need to configure port 1~3 to VLAN1 and port 4~6 to VLAN. Then you need to add VLAN 1 and 2 to a SuperVlan as its SubVLANs. You need to perform the following configuration on the switch:

```
interface fastethernet 0/4
switchport pvid 2
!
interface fastethernet 0/5
switchport pvid 2
!
interface fastethernet 0/6
switchport pvid 2
!
interface supervlan 1
subvlan 1,2
ip address 192.168.1.100 255.255.255.0
ip proxy-arp subvlan
!
```

STP Configuration

Table of Contents

Chapter 1 Configuring STP

1.1 STP Introduction

The standard Spanning Tree Protocol (STP) is based on the IEEE 802.1D standard. A switch stack appears as a single spanning-tree node to the rest of the network, and all stack members use the same bridge ID. Unless otherwise noted, the term switch refers to a standalone switch and to a switch stack.

The STP uses a spanning-tree algorithm to select one switch of a redundantly connected network as the root of the spanning tree. The algorithm calculates the best loop-free path through a switched Layer 2 network by assigning a role to each port based on the role of the port in the active topology.

STP is a Layer 2 link management protocol that provides path redundancy while preventing loops in the network. For a Layer 2 Ethernet network to function properly, only one active path can exist between any two stations. Multiple active paths among end stations cause loops in the network. If a loop exists in the network, end stations might receive duplicate messages. Switches might also learn end-station MAC addresses on multiple Layer 2 interfaces. These conditions result in an unstable network. Spanning-tree operation is transparent to end stations, which cannot detect whether they are connected to a single LAN segment or a switched LAN of multiple segments.

The STP uses a spanning-tree algorithm to select one switch of a redundantly connected network as the root of the spanning tree. The algorithm calculates the best loop-free path through a switched Layer 2 network by assigning a role to each port based on the role of the port in the active topology:

The standard Spanning-Tree Protocol (STP) is defined in IEEE 802.1D. It simplifies the LAN topology comprising several bridges to a sole spinning tree, preventing network loop from occurring and ensuring stable work of the network.

The algorithm of STP and its protocol configure the random bridging LAN to an active topology with simple connections. In the active topology, some bridging ports can forward frames; some ports are in the congestion state and cannot transmit frames. Ports in the congestion state may be concluded in the active topology. When the device is ineffective, added to or removed from the network, the ports may be changed to the transmitting state.

In the STP topology, a bridge can be viewed as root. For every LAN section, a bridging port will forward data from the network section to the root. The port is viewed as the designated port of the network section. The bridge where the port is located is viewed as the designated bridge of the LAN. The root is the designated bridge of all network sections that the root connects. In ports of each bridge, the port which is nearest to the root is the root port of the bridge. Only the root port and the designated port (if available) is in the transmitting state. Ports of another type are not shut down but they are not the root port or the designated port. We call these ports are standby ports.

The following parameters decides the structure of the stabilized active topology:

(1) Identifier of each bridge

(2) Path cost of each port

(3) Port identifier for each port of the bridge

The bridge with highest priority (the identifier value is the smallest) is selected as the root. Ports of each bridge has the attribute **Root Path Cost**, that is, the minimum of path cost summation of all ports from the root to the bridge. The designated port of each network segment refers to the port connecting to the network segment and having the minimum path cost.

When two ports on a switch are part of a loop, the spanning-tree port priority and path cost settings control which port is put in the forwarding state and which is put in the blocking state. The spanning-tree port priority value represents the location of a port in the network topology and how well it is located to pass traffic. The path cost value represents the media speed.

Our switch standard supports two modes of spanning tree protocol 802.1D STP and 802.1w RSTP. Some models of the switch support distributing STP mode according to VLAN and MSTP spanning tree protocol. For more details, please refer to 'STP Mode and Model Table' in chapter 2.

This chapter describes how to configure the standard spanning tree protocol that switch supports.

Note:

802.1D STP and 802.1w RSTP are abbreviated to SSTP and RSTP in this article. SSTP means Single Spanning-tree.

1.2 STP Model-to-Type Table

Model	Single STP	PVST	RSTP	MSTP
S2116, S2224D, S2448	√	√	√	√
S2224, S2448B, S2516, S2524	√	x	√	x
S2224M, S2226	√	√	√	x
S3224, S3224M, S3512	√	x	√	x
S3424, S3448	√	√	√	√
S6508	√	√	√	√
S8500	√	√	√	√

1.3 SSTP Configuratiom Task List

- Selecting STP Mode

- Disabling/Enabling STP
- Configuring the Switch Priority
- Configuring the Hello Time
- Configuring the Max-Age Time
- Configuring the Forward Delay Time
- Configuring Port Priority
- Configuring Path Cost
- Configuring the Auto-Designated port
- Monitoring STP Status

1.4 SSTP Configuration Task

1.4.1 Selecting STP Mode

Run the following command to configure the STP mode:

Run…	To…
spanning-tree mode {sstp | rstp}	Select the STP configuration.

1.4.2 Disabling/Enabling STP

Spanning tree is enabled by default. Disable spanning tree only if you are sure there are no loops in the network topology.

Follow these steps to disable spanning-tree:

command	purpose
no spanning-tree	Disables STP.

To enable spanning-tree, use the following command:

command	purpose
spanning-tree	Enables default mode STP (SSTP).
spanning-tree mode {**sstp** | **rstp**}	Enables a certain mode STP.

1.4.3 Configuring the Switch Priority

You can configure the switch priority and make it more likely that a standalone switch or a switch in the stack will be chosen as the root switch.

Follow these steps to configure the switch priority：

command	purpose

spanning-tree sstp priority *value*	Modifies sstp priority value.
no spanning-tree sstp priority	Returns sstp priority to default value (32768).

1.4.4 Configuring the Hello Time

User can configure the interval between STP data units sent by the root switch through changing the hello time.

Use the following command to configure Hello Time of SSTP：

command	purpose
spanning-tree sstp hello-time *value*	Configures sstp Hello Time.
no spanning-tree sstp hello-time	Returns sstp Hello Time to default value (4s).

1.4.5 Configuring the Max-Age Time

Use the sstp max age to configure the number of seconds a switch waits without receiving spanning-tree configuration messages before attempting a reconfiguration.

Follow these steps to configure the maximum-aging time：

command	purpose
spanning-tree sstp max-age *value*	Configures the sstp max-age time.
no spanning-tree sstp max-age	Returns the max-age time to default value (20s).

1.4.6 Configuring the Forward Delay Time

Configure sstp forward delay to determine the number of seconds an interface waits before changing from its spanning-tree learning and listening states to the forwarding state.

Use the following command to configure sstp forward delay：

command	purpose
spanning-tree sstp *forward-time*	Configures sstp Forward time.
no spanning-tree sstp forward-time	Returns forward time to default value (15s).

1.4.7 Configuring the Port Priority

If a loop occurs, spanning tree uses the port priority when selecting an interface to put into the forwarding state. You can assign higher priority values (lower numerical values) to interfaces that you want selected first and lower priority values (higher numerical values) that you want selected last. If all interfaces have the same priority value, spanning tree puts the interface with the lowest interface number in the forwarding state and blocks the other interfaces.

Follow these steps to configure the port priority of an interface：

command	purpose
spanning-tree port-priority *value*	Configures the port priority for an interface.
spanning-tree sstp port-priority *value*	Modifies sstp port priority.
no spanning-tree sstp port-priority	Returns port priority to default value (128).

1.4.8 Configuring the Path Cost

Follow these steps to configure the cost of an interface：

command	purpose
spanning-tree cost *value*	Configures the cost for an interface.
spanning-tree sstp cost *value*	Modifies sstp path cost.
no spanning-tree sstp cost	Returns path cost to default value.

1.4.9 Configuring Auto-Designated Port

The auto-designated port is a special function of S8500 switches. The function allows line card to automatically send BPDU to the auto-designated port, reducing the load of the MSU.

The auto-designated port function is effective in STP mode.

In global configuration mode, run the following commands to configure the auto-designated port function of S8500 series switches:

Command	Purpose
spanning-tree designated-auto	Enables the auto-designated port function.
no spanning-tree designated-auto	Disables the auto-designated port function.

1.4.10 Monitoring STP State

To monitor the STP configuration and state, use the following command in management mode:

command	purpose
show spanning-tree	Displays spanning-tree information on active interfaces only.
show spanning-tree detail	Displays a detailed summary of interface information.
show spanning-tree interface	Displays spanning-tree information for the specified interface.

1.5 Configuring VLAN STP

1.5.1 Overview

In SSTP mode, the whole network has only one STP entity. The state of the switch port in the STP decides its state in all VLANs. In the case that multiple VLANs exist in the network, the separation of the single STP and the network topology may cause communication congestion in some parts of network.

Our switches run independent SSTP on a certain number of PurposeVLANs, ensuring that the port has different state in different VLANs and that the load balance is realized between VLANs.

Note that the switch can run the independent STP in up to 30 VLANs. Other VLAN topologies is not controlled by the STP.

S2116, S2448, S3448, S6508 and S8500 support the VLAN-based STP case planning. For details, refer to relative device models and software version explanations.

1.5.2 VLAN STP Configuration Task

In global configuration mode, run the following commands to configure SSTP attributes in VLAN:

Command	Purpose
spanning-tree mode pvst	Starts the VLAN-based STP distribution mode.
spanning-tree vlan *vlan-list*	Distributes the STP case for the designated VLAN. vlan-list: the list of VLAN The switch distributes STP case for up to 30 VLANs.
no spanning-tree vlan *vlan-list*	Deletes the STP case in the designated VLA.
spanning-tree vlan *vlan-list* **priority** *value*	Configures the priority for the STP in the designated VLAN.
no spanning-tree *vlan-list* **priority**	Resumes the STP priority in the VLAN to the default configuration.
spanning-tree vlan *vlan-list* **forward-time** *value*	Configures Forward Delay for the designated VLAN.
no spanning-tree vlan *vlan-list* **forward-time**	Resumes Forward Delay of the designated VLAN to the default configuration.
spanning-tree vlan *vlan-list* **max-age** *value*	Configures Max-age for the designated VLAN.
no spanning-tree vlan *vlan-list* **max-age**	Resumes Max-age of the designated VLAN to the default configuration.
spanning-tree vlan *vlan-list* **hello-time** *value*	Configures HELLO-TIME for the designated VLAN.
no spanning-tree vlan *vlan-list* **hello-time**	Resumes HELLO-TIME of the designated VLAN to the default configuration.

In port configuration mode, run the following command to configure attributes of the port:

Command	Purpose
spanning-tree vlan *vlan-list* **cost**	Configures the path cost of the designated VLAN for the port.
no spanning-tree vlan *vlan-list* **cost**	Resumes the default path cost of the designated VLAN for the port.
spanning-tree vlan *vlan-list* **port-priority**	Configures the port priority in the VLAN.
no spanning-tree vlan *vlan-list* **port-priority**	Resumes the default port priority in the VLAN.

In monitor or configuration mode, run the following command to check the STP state in the specified VLAN:

Command	Purpose
show spanning-tree vlan *vlan-list*	Check the STP state in the VLAN.

1.6 RSTP Configuration Task List

- Enabling/Disabling Switch RSTP
- Configuring the Switch Priority
- Configuring the Forward Delay Time
- Configuring the Hello time
- Configuring the Max-Age
- Configuring the Path Cost
- Configuring the Port Priority
- Enabling Protocol Conversation Check

1.7 RSTP Configuration Task

1.7.1 Enabling/Disabling Switch RSTP

Follow these configurations in the global configuration mode:

command	purpose
spanning-tree mode rstp	Enables RSTP
no spanning-tree mode	Returns STP to default mode (SSTP)

1.7.2 Configuring the Switch Priority

You can configure the switch priority and make it more likely that a standalone switch or a switch in the stack will be chosen as the root switch.

Follow these steps to configure the switch priority：

Follow these configurations in the global configuration mode:

command	purpose
spanning-tree rstp priority *value*	Modifies rstp priority value.
no spanning-tree rstp priority	Returns rstp priority to default value.

Note: If the priority of all bridges in the whole switch network uses the same value, then the bridge with the least MAC address will be chosen as the root bridge. In the situation when the RSTP protocol is enabled, if the bridge priority value is modified, it will cause the recalculation of spanning tree.

The bridge priority is configured to 32768 by default.

1.7.3 Configuring the Forward Delay Time

Link failures may cause network to recalculate the spanning tree structure. But the latest configuration message can no be conveyed to the whole network. If the newly selected root port and the specified port immediately start forwarding data, this may cause temporary path loop. Therefore the protocol adopts a kind of state migration mechanism. There is an intermediate state before root port and the specified port starting data forwarding, after the intermediate state passing the Forward Delay Time, the forward state begins. This delay time ensures the newly configured message has been conveyed to the whole network. The Forward Delay characteristic of the bridge is related to the network diameter of the switch network. Generally, the grater the network diameter, the longer the Forward Delay Time should be configured.

Follow these configurations in the global configuration mode:

Command	purpose
spanning-tree rstp forward-time *value*	Configures Forward Delay
no spanning-tree rstp forward-time	Returns Forward Delay Time to default value (15s).

Note: If you configure the Forward Delay Time to a relatively small value, it may leads to a temporary verbose path. If you configure the Forward Delay Time to a relatively big value, the system may not resume connecting for a long time. We recommend user to use the default value.

The Forward Delay Time of the bridge is 15 seconds.

1.7.4 Configuring the Hello Time

The proper hello time value can ensure that the bridge detect link failures in the network without occupying too much network resources.

Follow these configurations in the global configuration mode:

command	purpose
spanning-tree rstp hello-time *value*	Configures Hello Time
no spanning-tree rstp hello-time	Returns Hello Time to default value.

Note: We recommend user to use the default value.

The default Hello Time is 4 seconds.

1.7.5 Configuring the Max-Age

The ma-age is the number of seconds a switch waits without receiving spanning-tree configuration messages before attempting a reconfiguration.

Follow these configurations in the global configuration mode：

command	purpose
spanning-tree rstp max-age *value*	Configures the max-age value.
no spanning-tree rstp max-age	Returns the max-age time to default value (20s).

We recommend user to use the default value. Note: if you configure the Max Age to a relatively small value, then the calculation of the spanning tree will be relatively frequent, and the system may regard the network block as link failure. If you configure the Max Age to a relatively big value, then the link status will go unnoticed in time.

The Max Age of bridge is 20 seconds by default.

1.7.6 Configuring the Path Cost

The spanning-tree path cost default value is derived from the media speed of an interface. If a loop occurs, spanning tree uses cost when selecting an interface to put in the forwarding state. You can assign lower cost values to interfaces that you want selected first and higher cost values to interfaces that you want selected last. If all interfaces have the same cost value, spanning tree puts the interface with the lowest interface number in the forwarding state and blocks the other interfaces.

Beginning in interface configuration mode, follow these steps to configure the cost of an interface:

command	purpose
spanning-tree rstp cost *value*	Configures the cost for an interface.
no spanning-tree rstp cost	Returns path cost to default value.

Note: The modification of the priority of the Ethernet port will arise the recalculation of the spanning tree. We recommend user to use the default value and let RSTP protocol calculate the path cost of the current Ethernet interface.

When the port speed is 10Mbps, the path cost of the Ethernet interface is 2000000.

When the port speed is 100Mbps, the path cost of the Ethernet interface is 200000.

1.7.7 Configuring the Port Priority

If a loop occurs, spanning tree uses the port priority when selecting an interface to put into the forwarding state. You can assign higher priority values (lower numerical values) to interfaces that you want selected first, and lower priority values (higher numerical values) that you want selected last. If all interfaces have the same priority value, spanning tree puts the interface with the lowest interface number in the forwarding state and blocks the other interfaces.

Follow these configurations in the interface configuration mode：

command	purpose
spanning-tree rstp port-priority *value*	Configures the port priority for an interface.
no spanning-tree rstp port-priority	Returns the port priority to the default value.

Note: The modification of the priority of the Ethernet interface will arise the recalculation of the spanning tree.

The default Ethernet interface priority is 128.

1.7.8 Enabling Protocol Conversion Check

RSTP protocol allows switch to cooperate with traditional 802.1D STP switch via a kind of protocol conversion mechanism. If one interface of the switch receives configuration information of STP, then this interface will be converted to the one that only sends STP packet.

When an interface enters STP-compatible state，this interface won't returns to RSTP state even this interface no longer receives 802.1D STP BPDU. To return an interface to RSTP mode, user can use the **spanning-tree rstp migration-check** command to enable protocol conversion check process on an interface.

Note

Only switches supporting IEEE 802.1D 2004 RSTP support the migration-check command.

In global configuration mode, run the following command to restart the RSTP conversion check:

Command	Purpose
spanning-tree rstp migration-check	Restart the protocol conversion check on all ports.

In port configuration mode，run the following command to perform the protocol conversion check on the port:

Command	Purpose
spanning-tree rstp migration-check	Restart the protocol conversion check on the current port.

Chapter 2 Configuring MTSP

2.1 MSTP Overview

2.1.1 Introduction

Multiple Spanning Tree Protocol (MSTP) is used to create simple complete topology in the bridging LAN. MSTP can be compatible with the earlier Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP).

Both STP and RSTP only can create sole STP topology. All VLAN messages are forwarded through the only STP. STP converges too slow, so RSTP ensures a rapid and stable network topology through the handshake mechanism.

MSTP inherits the rapid handshake mechanism of RSTP. At the same time, MST allows different VLAN to be distributed to different STPs, creating multiple topologies in the network. In networks created by MSTP, frames of different VLANs can be forwarded through different paths, realizing the load balance of the VLAN data.

Different from the mechanism that VLAN distributes STP, MSTP allows multiple VLANs to be distributed to one STP topology, effectively reducing STPs required to support lots of VLANs.

S2116, S2448, S3448 and S6508 switches support the MSTP mode. For details, refer to device models and relative software version documents.

2.1.2 MST Domain

In MSTP, the relationship between VLAN and STP is described through the MSTP configuration table. MSTP configuration table, configuration name and configuration edit number makes up of the MST configuration identifier.

In the network, interconnected bridges with same MST configuration identifier are considered in the same MST region. Bridges in the same MST region always have the same VLAN configuration, ensuring VLAN frames are sent in the MST region.

2.1.3 IST, CST, CIST and MSTI

Figure 2.1 shows an MSTP network, including three MST regions and a switch running 802.1D STP.

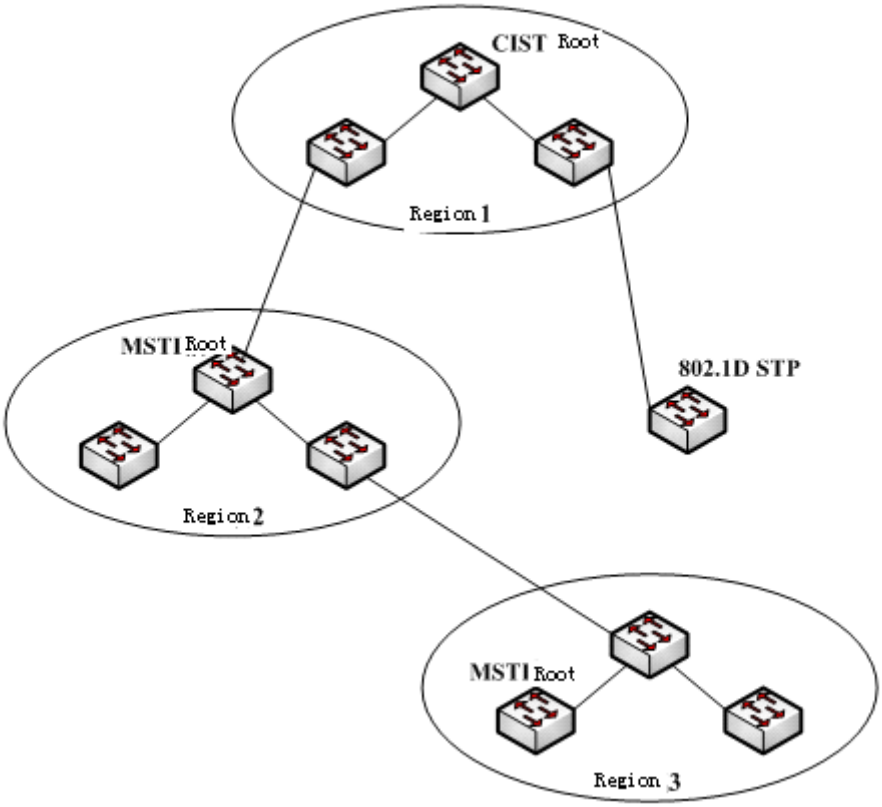


Figure 2.1 MSTP topology

1. CIST

Common and Internal Spanning Tree (CIST) means the spanning tree comprised by all single switches and interconnected LAN. These switches may belong to different MST regions. They may be switches running traditional STP or RSTP. Switches running STP or RSTP in the MST regions are considered to be in their own regions.

After the network topology is stable, the whole CIST chooses a CIST root bridge. An internal CIST root bridge will be choosed in each region, which is the shortest path from the heart of the region to CIST root.

2. CST

If each MST region is viewed as a single switch, Common Spanning Tree (CST) is the spanning tree connecting all “single switches”. As shown in Figure 2.1, region 1, 2 and 3 and STP switches make up of the network CST.

3. IST

Internal Spanning Tree (IST) refers to part of CIST that is in an MST region, that is, IST and CST make up of the CIST.

4. MSTI

The MSTP protocol allows different VLANs to be distributed to different spanning trees. Multiple spanning tree instances are then created. Normally, No.0 spanning tree instance refers to CIST, which can be expanded to the whole network. Every spanning tree instance starting from No.1 is in a certain region. Each spanning tree instance can be distributed with multiple VLANs. In original state, all VLANs are distributed in CIST.

MSTI in the MST region is independent. They can choose different switches as their own roots.

2.1.4 Port Role

Ports in MSTP can function as different roles, similar to ports in RSTP.

1. Root port

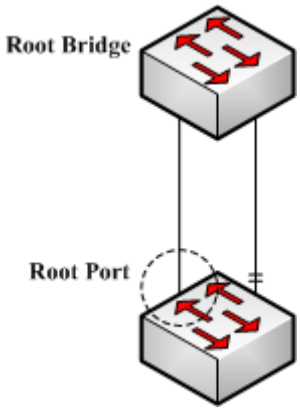


Figure 2.2 Root port

Root port stands for the path between the current switch and the root bridge, which has minimum root path cost.

2. Alternate port

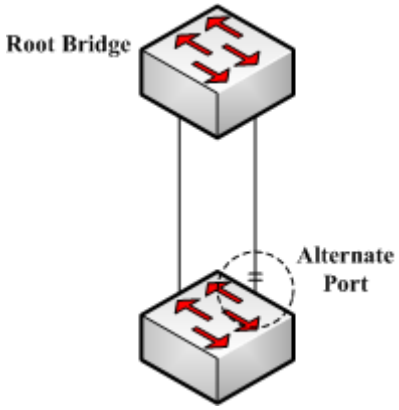


Figure 2.3 Alternate port

The alternate port is a backup path between the current switch and the root bridge. When the connection of root port is out of effect, the alternate port can promptly turn into a new root port without work interruption.

3. Designated port

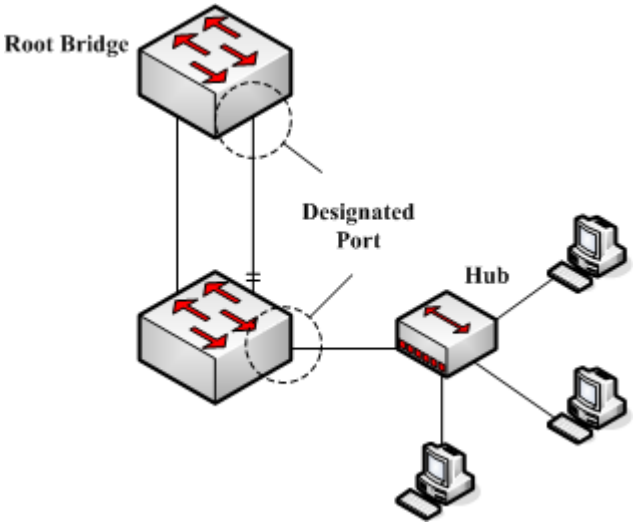


Figure 2.4 Designated port

The designated port can connect switches or LAN in the next region. It is the path between the current LAN and root bridge.

4. Backup port

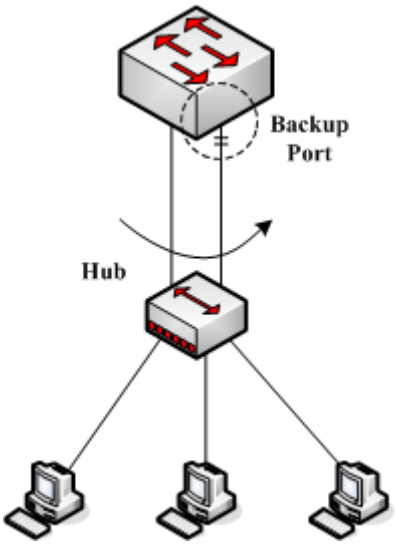


Figure 2.5 Backup port

When two switch ports directly connect or both connect to the same LAN, the port with lower priority is to be the backup port, the other port is to be the designated port. If the designated port breaks down, the backup port becames the designated port to continue working.

5. Master port

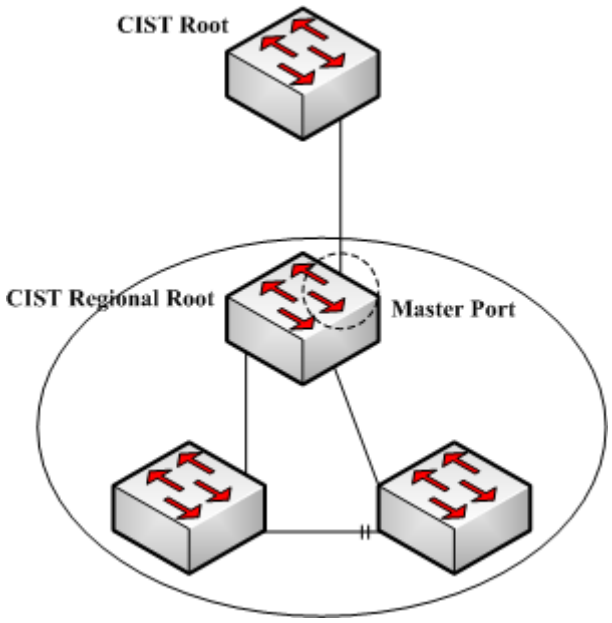


Figure 2.6 Master port

The Master port is the shortest path between MST region and CIST root bridge. Master port is the root port of the root bridge in the CIST region.

6. Boundary port

The concept of boundary port in CIST is a little different from that in each MSTI. In MSTI, the role of the boundary port means that the spanning tree instance does not expand on the port.

7. Edge port

In the RSTP protocol or MSTP protocol, edge port means the port directly connecting the network host. These ports can directly enter the forwarding state without causing any loop in the network.

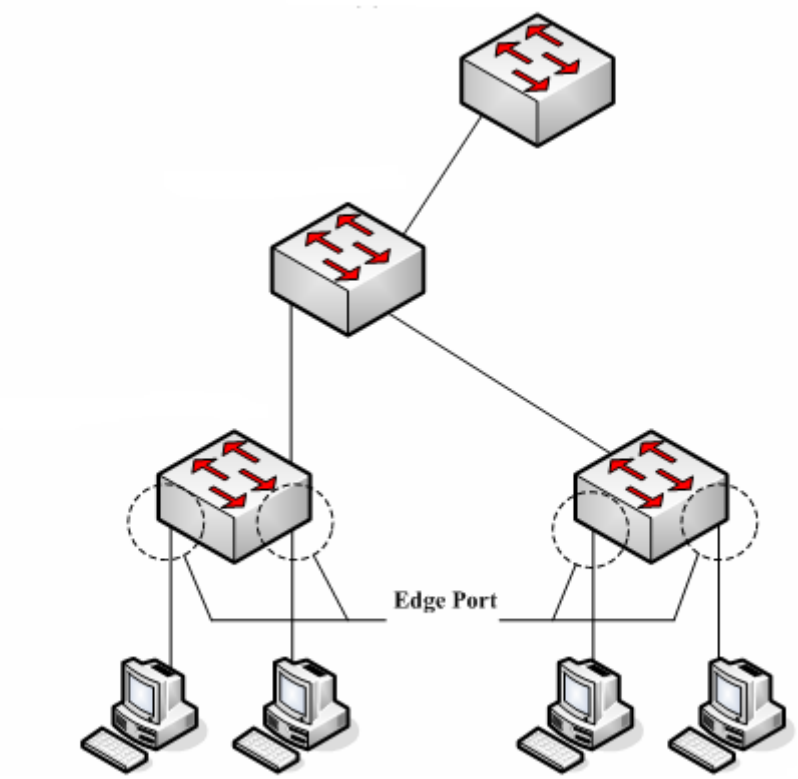


Figure 2.7 Edge port

In original state, MTSP and RSTP do not take all ports as edge ports, ensuring the network topology can be rapidly created. In this case, if a port receives BPDU from other switches, the port is resumed from the edge state to the normal state. If the port receives 802.1D STP BPDU, the port has to wait for double Forward Delay time and then enter the forwarding state.

2.1.5 MSTP BPDU

Similar to STP and RSTP, switches running MSTP can communicate with each other through Bridge Protocol Data Unit (BPDU). All configuration information about the CIST and MSTI can be carried by BPDU. Table 2.1 and Table 2.2 list the structure of BPDU used by the MSTP.

Table 2.1 MSTP BPDU

Field Name	Byte Number
Protocol Identifier	1 – 2
Protocol Version Identifier	3
BPDU Type	4
CIST Flags	5
CIST Root Identifier	6 – 13
CIST External Root Path Cost	14 – 17

CIST Regional Root Identifier	18 – 25
CIST Port Identifier	26 – 27
Message Age	28 – 29
Max Age	30 – 31
Hello Time	32 – 33
Forward Delay	34 – 35
Version 1 Length	36
Version 3 Length	37 – 38
Format Selector	39
Configuration Name	40 – 71
Revision	72 – 73
Configuration Digest	74 – 89
CIST Internal Root Path Cost	90 – 93
CIST Bridge Identifier	94 – 101
CIST Remaining Hops	102
MSTI Configuration Messages	103 ~

Table 2.2 MST configuration information

Field Name	Byte Number
MSTI FLAGS	1
MSTI Regional Root Identifier	2 – 9
MSTI Internal Root Path Cost	10 – 13
MSTI Bridge Priority	14
MSTI Port Priority	15
MSTI Remaining Hops	16

2.1.6 Stable State

The MSTP switch performs calculation and compares operations according to the received BPDU, and finally ensures that:

(1) One switch is selected as the CIST root of the whole network.

(2) Each switch and LAN segment can decide the minimum cost path to the CIST root, ensuring a complete connection and prevent loops.

(3) Each region has a switch as the CIST regional root. The switch has the minimum cost path to the CIST root.

(4) Each MSTI can independently choose a switch as the MSTI regional root.

(5) Each switch in the region and the LAN segment can decide the minimum cost path to the MSTI root.

(6) The root port of CIST provides the minimum-cost path between the CIST regional root and the CIST root.

(7) The designated port of the CIST provided its LAN with the minimum-cost path to the CIST root.

(8) The Alternate port and the Backup port provides connection when the switch, port or the LAN does not work or is removed.

(9) The MSTI root port provides the minimum cost path to the MSTI regional root.

(10) The designated port of MSTI provides the minimum cost path to the MSTI regional root.

(11) A master port provides the connection between the region and the CIST root. In the region, the CIST root port of the CIST regional root functions as the master port of all MSTI in the region.

2.1.7 Hop Count

Different from STP and RSTP, the MSTP protocol does not use Message Age and Max Age in the BPDU configuration message to calculate the network topology. MSTP uses Hop Count to calculate the network topology.

To prevent information from looping, MSTP relates the transmitted information to the attribute of hop count in each spanning tree. The attribute of hop count for BPDU is designated by the CIST regional root or the MSTI regional root and reduced in each receiving port. If the hop count becomes 0 in the port, the information will be dropped and then the port turns to be a designated port.

2.1.8 STP Compatibility

MSTP allows the switch to work with the traditional STP switch through protocol conversion mechanism. If one port of the switch receives the STP configuration message, the port then only transmits the STP message. At the same time, the port that receives the STP information is then considered as a boundary port.

Note：

When a port is in the STP-compatible state, the port will not automatically resume to the MSTP state even if the port does not receive the STP message any more. In this case, you can run spanning-tree mstp migration-check to clear the STP message that the port learned, and make the port to return to the MSTP state.

The switch that runs the RSTP protocol can identify and handle the MSTP message. Therefore, the MSTP switch does not require protocol conversion when it works with the RSTP switch.

2.2 MSTP Configuration Task List

- Default MSTP configuration
- Enabling and disabling MSTP

- Configuring MSTP region
- Configuring network root
- Configuring secondary root
- Configuring bridge priority
- Configuring time parameters of STP
- Configuring network diameter
- Configuring maximum hop count
- Configuring port priority
- Configuring path cost for port
- Configuring port connection type
- Activating MST-compatible mode

2.2.1 Activating MST-Compatible Mode

The MSTP protocol that our switches support is based on IEEE 802.1s. In order to be compatible with other MSTPs, especially MSTP that the Cisco switches support, the MSTP protocol can work in MST-compatible mode. Switches running in MSTP-compatible mode can identify the message structure of other MSTPs, check the contained MST regional identifier and establish the MST region.

The MST-compatible mode and the STP-compatible mode are based on MSTP protocol conversion mechanism. If one port of the switch receives BPDU in compatible mode, the port automatically changes to the mode and sends BPDU in compatible mode. To resume the port to standard MST mode, you can run **spanning-tree mstp migration-check**.

In global configuration mode, run the following commands to activate or disable the MST-compatible mode:

Command	Purpose
spanning-tree mstp mst-compatible	Activates the MST-compatible mode for the switch.
no spanning-tree mstp mst-compatible	Disables the MST-compatible mode for the switch.

Note:

The main function of the compatible mode is to create the MST area for switches and other MSTP-running switches. In actual networking, make sure that the switch has the same configuration name and the same edit number. It is recommended to configure switches running other MSTP protocols to the CIST root, ensuring that the switch enters the compatible mode by receiving message.

If the MST-compatible mode is not activated, the switch will not resolve the whole BPDU-compatible content and take the content as the common RSTP BPDU. In this way, the switch cannot be in the same area with the MST-compatible switch that it connects.

A port in compatible mode cannot automatically resumes to send standard MST BPDU even if the compatible mode is shut down in global configuration mode. In this case, run migration-check.

- Restart the protocol conversion check.
- Check the MSTP message.

2.3 MSTP Configuration Task

2.3.1 Default MSTP Configuration

Attribute	Default Settings
STP mode	SSTP (PVST, RSTP and MSTP is not started)
Area name	Character string of MAC address
Area edit level	0
MST configuration list	All VLANs are mapped in CIST (MST00).
Spanning-tree priority (CIST and all MSTI)	32768
Spanning-tree port priority (CIST and all MSTI)	128
Path cost of the spanning-tree port (CIST and all MSTI)	1000 Mbps：20000 100 Mbps：200000 10 Mbps：2000000
Hello Time	2 seconds
Forward Delay	15 seconds
Maximum-aging Time	20 seconds
Maximum hop count	20

2.3.2 Enabling and Disabling MSTP

The STP protocol can be started in PVST or SSTP mode by default. You can stop it running when the spanning-tree is not required.

Run the following command to set the STP to the MSTP mode:

Command	Purpose
spanning-tree	Enables STP in default mode.
spanning-tree mode mstp	Enables MSTP.

Run the following command to disable STP:

Command	Purpose
no spanning-tree	Disable the STP.

2.3.3 Configuring MST Area

The MST area where the switch resides is decided by three attributes: configuration name, edit number, the mapping relation between VLAN and MSTI. You can configure them through area configuration commands. Note that the change of any of the three attributes will cause the change of the area where the switch resides.

In original state, the MST configuration name is the character string of the MAC address of the switch. The edit number is 0 and all VLANs are mapped in the CIST (MST00). Because different switch has different MAC address, switches that run MSTP are in different areas in original state. You can run **spanning-tree mstp instance *instance-id* vlan *vlan-list*** to create a new MSTI and map the designated VLAN to it. If the MSTI is deleted, all these VLANs are mapped to the CIST again.

Run the following command to set the MST area information:

Command	Purpose
spanning-tree mstp name *string*	Configures the MST configuration name. **string** means the character string of the configuration name. It contains up to 32 characters, capital sensitive. The default value is the character string of the MAC address.
no spanning-tree mstp name	Sets the MST configuration name to the default value.
spanning-tree mstp revision *value*	Sets the MST edit number. **value** represents the edit number, ranging from 0 to 65535. The default value is 0.
no spanning-tree mstp revision	Sets the MST edit number to the default value.
spanning-tree mstp instance *instance-id* **vlan** *vlan-list*	Maps VLAN to MSTI. **instance-id** represents the instance number of the spanning tree, meaning an MSTI. It ranges from 1 to 15. **vlan-list** means the VLAN list that is mapped to the spanning tree. It ranges from 1 to 4094. **instance-id** is an independent value representing a spanning tree instance. **vlan-list** can represent a group of VLANs, such as ”1,2,3”, ”1-5” and “1,2,5-10”.
no spanning-tree mstp instance *instance-id*	Cancels the VLAN mapping of MSTI and disables the spanning tree instance. instance-id represents the instance number of the spanning tree, meaning an MSTI. It ranges from 1 to 15.

Run the following command to check the configuration of the MSTP area:

Command	Purpose
show spanning-tree mstp region	Displays the configuration of the MSTP area.

2.3.4 Configuring Network Root

In MSTP, each spanning tree instance has a bridge ID, containing the priority value and MAC address of the switch. During the establishment of spanning tree topology, the switch with comparatively small bridge ID is selected as the network root.

MSTP can set the switch to the network switch through configuration. You can run the command **Spanning-tree mstp Spanning-tree mstp *instance-id* rootroot** to modify the priority value of the switch in a spanning tree instance from the default value to a sufficiently small value, ensuring the switch turns to be the root in the spanning tree instance.

In general, after the previous command is executed, the protocol automatically check the bridge ID of the current network root and then sets the priority field of the bridge ID to **24576** when the value **24576** ensures that the current switch becomes the root of the spanning tree.

If the network root's priority value is smaller than the value **24576**, MSTP automatically sets the spanning tree's priority of the current bridge to a value that is 4096 smaller than the priority value of the root. Note that the number **4096** is a step length of network priority value.

When setting the root, you can run the **diameter** subcommand to the network diameter of the spanning tree network. The keyword is effective only when the spanning tree instance ID is 0. After the network diameter is set, MSTP automatically calculates proper STP time parameters to ensure the stability of network convergence. Time parameters include Hello Time, Forward Delay and Maximum Age. The subcommand Hello-time can be used to set a new hello time to replace the default settings.

Run the following command to set the switch to the network root:

Command	Purpose
spanning-tree mstp *instance-id* **root primary** [**diameter** *net-diameter* [**hello-time** *seconds*]]	Sets the switch to the root in the designated spanning tree instance. **instance-id** represents the number of the spanning tree instance, ranging from 0 to 15. **net-diameter** represents the network diameter, which is an optional parameter. It is effective when **instance-id** is 0. It ranges from 2 to 7. **seconds** represents the unit of the hello time, ranging from 1 to 10.
no spanning-tree mstp *instance-id* **root**	Cancels the root configuration of the switch in the spanning tree. **instance-id** means the number of the spanning tree instance, ranging from 0 to 15.

Run the following command to check the MSTP message:

Command	Purpose
show spanning-tree mstp [**instance** *instance-id*]	Checks the MSTP message.

2.3.5 Configuring Secondary Root

After the network root is configured, you can run **spanning-tree mstp *instance-id* root secondary** to set one or multiple switches to the secondary roots or the backup roots. If the root does not function for certain reasons, the secondary roots will become the network root.

Different from the primary root configuration, after the command to configure the primary root is run, MSTP sets the spanning tree priority of the switch to **28672**. In the case that the priority value of other switches is the default value **32768**, the current switch can be the secondary root.

When configuring the secondary root, you can run the subcommands **diameter** and **hello-time** to update the STP time parameters. When the secondary root becomes the primary root and starts working, all these parameters starts functioning.

Run the following command to set the switch to the secondary root of the network:

Command	Purpose
spanning-tree mstp *instance-id* **root secondary** [**diameter** *net-diameter* [**hello-time** *seconds*]]	Sets the switch to the secondary root in the designated spanning tree instance. **instance-id** represents the number of the spanning tree instance, ranging from 0 to 15. **net-diameter** represents the network diameter, which is an optional parameter. It is effective when **instance-id** is 0. It ranges from 2 to 7. **seconds** represents the unit of the hello time, ranging from 1 to 10.
no spanning-tree mstp *instance-id* **root**	Cancels the root configuration of the switch in the spanning tree. **instance-id** means the number of the spanning tree instance, ranging from 0 to 15.

Run the following command to check the MSTP message:

Command	Purpose
show spanning-tree mstp [**instance** *instance-id*]	Check the message about the MST instance.

2.3.6 Configuring Bridge Priority

In some cases, you can directly set the switch to the network root by configuring the bridge priority. It means that you can set the switch to the network root without running the subcommand **root**. The priority value of the switch is independent in each spanning tree instance. Therefore, the priority of the switch can be set independently.

Run the following command to configure the priority of the spanning tree:

Command	Purpose
spanning-tree mstp *instance-id* **priority** *value*	Sets the priority of the switch. instance-id represents the number of the spanning tree

	instance, ranging from 0 to 15. **value** represents the priority of the bridge. It can be one of the following values: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440
no spanning-tree mstp *instance-id* **priority**	Resumes the bridge priority of the switch to the default value. **instance-id** means the number of the spanning tree instance, ranging from 0 to 15.

2.3.7 Configuring STP Time Parameters

The following are STP time parameters:

- **Hello Time**:

  The interval to send the configuration message to the designated port when the switch functions as the network root.

- **Forward Delay**:

  Time that the port needs when it changes from the **Blocking** state to the **learning** state and to the **forwarding** state in STP mode.

- **Max Age**:

  The maximum live period of the configuration information about the spanning tree.

To reduce the shock of the network topology, the following requirements for the time parameters must be satisfied:

- 2 x (fwd_delay - 1.0) >= max_age
- max_age >= (hello_time + 1) x 2

Command	Purpose
spanning-tree mstp hello-time *seconds*	Sets the parameter **Hello Time**. The parameter **seconds** is the unit of **Hello Time**, ranging from 1 to 10 seconds. Its default value is two seconds.
no spanning-tree mstp hello-time	Resumes **Hello Time** to the default value.
spanning-tree mstp forward-time *seconds*	Sets the parameter **Forward Delay**. The parameter **seconds** is the unit of **Forward Delay**, ranging from 4 to 30 seconds. Its default value is 15 seconds.
no spanning-tree mstp forward-time	Resumes **Forward Delay** to the default value.
spanning-tree mstp max-age *seconds*	Sets the parameter **Max Age**. The parameter **seconds** is the unit of **Max Age**, ranging from 6 to 40 seconds. Its default value is 20 seconds.
no spanning-tree mstp max-age	Resumes **Max Age** to the default value.

It is recommended to modify STP time parameters by setting root or network diameter, which ensures correct modification of time parameters.

The newly-set time parameters are valid even if they do not comply with the previous formula's requirements. Pay attention to the notification on the console when you perform configuration.

2.3.8 Configuring Network Diameter

Network diameter stands for the maximum number of switches between two hosts in the network, representing the scale of the network.

You can set the MSTP network diameter by running the command **spanning-tree mstp diameter *net-diameter***. The parameter **net-diameter** is valid only to CIST. After configuration, three STP time parameters is automatically updated to comparatively better values.

Run the following command to configure **net-diameter**:

Command	Purpose
spanning-tree mstp diameter *net-diameter*	Configure **net-diameter**. The parameter **net-diameter** ranges from 2 to 7. The default value is 7.
no spanning-tree mstp diameter	Resumes **net-diameter** to the default value.

The parameter **net-diameter** is not saved as an independent setup in the switch. Only when modified by setting the network diameter can the time parameter be saved.

2.3.9 Configuring Maximum Hop Count

Run the following command to configure the maximum hop count.

Command	Purpose
spanning-tree mstp max-hops *hop-count*	Set the maximum hops. **hop-count** ranges from 1 to 40. Its default value is 20.
no spanning-tree mstp *hop-count*	Resume the maximum hop count to the default value.

2.3.10 Configuring Port Priority

If a loop occurs between two ports of the switch, the port with higher priority will enter the **forwarding** state and the port with lower priority is blocked. If all ports have the same priority, the port with smaller port number will first enter the **forwarding** state.

In port configuration mode, run the following command to set the priority of the STP port:

Command	Purpose
spanning-tree mstp *instance-id* **port-priority** *priority*	Sets the priority of the STP port. **instance-id** stands for the number of the spanning tree instance, ranging from 0 to 15.

	priority stands for the port priority. It can be one of the following values: 0, 16, 32, 48, 64, 80, 96, 112 128, 144, 160, 176, 192, 208, 224, 240
spanning-tree port-priority *value*	Sets the port priority in all spanning tree instances. **value** stands for the port priority. It can be one of the following values: 0, 16, 32, 48, 64, 80, 96, 112 128, 144, 160, 176, 192, 208, 224, 240
no spanning-tree mstp *instance-id* **port-priority**	Resumes the port priority to the default value.
no spanning-tree port-priority	Resumes the port priority to the default value in all spanning tree instances.

Run the following command to check the information about the MSTP port.

Command	Purpose
show spanning-tree mstp interface *interface-id*	Check MSTP port information. interface-id stands for the port name, such as “F0/1” and “FastEtnernet0/3”.

2.3.11 Configuring Path Cost of the Port

In MSTP, the default value of the port’s path cost is based on the connection rate. If a loop occurs between two switches, the port with less path cost will enter the forwarding state. The less the path cost is, the higher rate the port is. If all ports have the same path cost, the port with smaller port number will first enter the forwarding state.

In port configuration mode, run the following command to set the path cost of the port:

Command	**Purpose**
spanning-tree mstp *instance-id* **cost** *cost*	Sets the path cost of the port. **instance-id** stands for the number of the spanning tree instance, ranging from 0 to 15. **cost** stands for the path cost of the port, which ranges from 1 to 200000000.
spanning-tree cost *value*	Sets the path cost of the port in all spanning tree instances. **Value** stands for the path cost of the port, which ranges from 1 to 200000000.
no spanning-tree mstp *instance-id* **cost**	Resumes the path cost of the port to the default value.
no spanning-tree cost	Resumes the path cost of the port to the default value in all spanning tree instances.

2.3.12 Configuring Port Connection Type

If the connection between MSTP-supported switches is the point-to-point direct connection, the switches can rapidly establish connection through handshake

mechanism. When you configure the port connection type, set the port connection to the point-to-point type.

The protocol decides whether to use the point-to-point connection or not according to the duplex attribute. If the port works in full-duplex mode, the protocol considers the connection is a point-to-point one. If the port works in the half-duplex mode, the protocol considers the connection is a shared one.

If the switch that the port connects run the RSTP protocol or the MSTP protocol, you can set the port connection type to **point-to-point**, ensuring that a handshake is rapidly established.

In port configuration mode, run the following command to set the port connection type.

Command	Purpose
spanning-tree mstp point-to-point force-true	Sets the port connection type to **point-to-point**.
spanning-tree mstp point-to-point force-false	Sets the port connection type to **shared**.
spanning-tree mstp point-to-point auto	Automatically checks the port connection type.
no spanning-tree mstp point-to-point	Resumes the port connection type to the default settings.

2.3.13 Activating MST-Compatible Mode

The MSTP protocol that our switches support is based on IEEE 802.1s. In order to be compatible with other MSTPs, especially MSTP that the Cisco switches support, the MSTP protocol can work in MST-compatible mode. Switches running in MSTP-compatible mode can identify the message structure of other MSTPs, check the contained MST regional identifier and establish the MST region.

The MST-compatible mode and the STP-compatible mode are based on MSTP protocol conversion mechanism. If one port of the switch receives BPDU in compatible mode, the port automatically changes to the mode and sends BPDU in compatible mode. To resume the port to standard MST mode, you can run **spanning-tree mstp migration-check**.

In global configuration mode, run the following commands to enable or disable the MST-compatible mode:

Command	Purpose
spanning-tree mstp mst-compatible	Enable the MST-compatible mode of the switch.
no spanning-tree mstp mst-compatible	Disable the MST-compatible mode of the switch.

Note:

The main function of the compatible mode is to create the MST area for switches and other MSTP-running switches. In actual networking, make sure that the switch has the same configuration name and the same edit number. It is recommended to configure switches running other MSTP protocols to the CIST root, ensuring that the switch enters the compatible mode by receiving message.

If the MST-compatible mode is not activated, the switch will not resolve the whole BPDU-compatible content and take the content as the common RSTP BPDU. In this way, the switch cannot be in the same area with the MST-compatible switch that it connects.

A port in compatible mode cannot automatically resumes to send standard MST BPDU even if the compatible mode is shut down in global configuration mode. In this case, run migration-check.

2.3.14 Restarting Protocol Conversion Check

MSTP allows the switch to work with the traditional STP switch through protocol conversion mechanism. If one port of the switch receives the STP configuration message, the port then only transmits the STP message. At the same time, the port that receives the STP information is then considered as a boundary port.

Note：

When a port is in the STP-compatible state, the port will not automatically resume to the MSTP state even if the port does not receive the STP message any more. In this case, you can run **spanning-tree mstp migration-check** to clear the STP message that the port learned, and make the port to return to the MSTP state.

The switch that runs the RSTP protocol can identify and handle the MSTP message. Therefore, the MSTP switch does not require protocol conversion when it works with the RSTP switch.

In global configuration mode, run the following command to clear all STP information that is detected by all ports of the switch:

Command	Purpose
spanning-tree mstp migration-check	Clears all STP information that is detected by all ports of the switch.

In port configuration mode, run the following command to clear STP information detected by the port.

Command	Purpose
spanning-tree mstp migration-check	Clears STP information detected by the port.

2.3.15 Check MSTP Information

In monitor command, global configuration command or port configuration command, run the following command to check all information about MSTP.

Command	Purpose
show spanning-tree	Checks MSTP information. (Information about SSTP, PVST, RSTP and MSTP can be checked)
show spanning-tree detail	Checks the details of MSTP information. (Information about SSTP, PVST, RSTP and MSTP can be checked)）
show spanning-tree interface *interface-id*	Checks the STP interface information. (Information about SSTP, PVST, RSTP and MSTP can be checked)）
show spanning-tree mstp	Checks all MST instances.
show spanning-tree mstp region	Checks the MST area configuration.
show spanning-tree mstp instance *instance-id*	Checks information about a MST instance.
show spanning-tree mstp detail	Checks detailed MST information.

show spanning-tree mstp interface *interface-id*	Checks MST port configuration.
show spanning-tree mstp protocol-migration	Checks the protocol conversion state of the port.

STP Optional Characteristic Configuration

Table of Contents

Chapter 1Configuring STP Optional Characteristic

1.1 STP Optional Characteristic Introduction

The spanning tree protocol module of the switch supports seven additional features (the so-called optional features). These features are not configured by default. The supported condition of various spanning tree protocol modes towards the optional characteristics is as follows:

Optional Characteristic	Single STP	PVST	RSTP	MSTP
Port Fast	Yes	Yes	No	No
BPDU Guard	Yes	Yes	Yes	Yes
BPDU Filter	Yes	Yes	No	No
Uplink Fast	Yes	Yes	No	No
Backbone Fast	Yes	Yes	No	No
Root Guard	Yes	Yes	Yes	Yes
Loop Guard	Yes	Yes	Yes	Yes

1.1.1 Port Fast

Port Fast immediately brings an interface configured as an access or trunk port to the forwarding state from a blocking state, bypassing the listening and learning states. You can use Port Fast on interfaces connected to a single workstation or server, to allow those devices to immediately connect to the network, rather than waiting for the spanning tree to converge.

Interfaces connected to a single workstation or server should not receive bridge protocol data units (BPDUs). An interface with Port Fast enabled goes through the normal cycle of spanning-tree status changes when the switch is restarted.

Because the purpose of Port Fast is to minimize the time interfaces must wait for spanning-tree to converge, it is effective only when used on interfaces connected to end stations. If you enable Port Fast on an interface connecting to another switch, you risk creating a spanning-tree loop.

You can enable this feature by using the spanning-tree portfast interface configuration or the spanning-tree portfast default global configuration command.

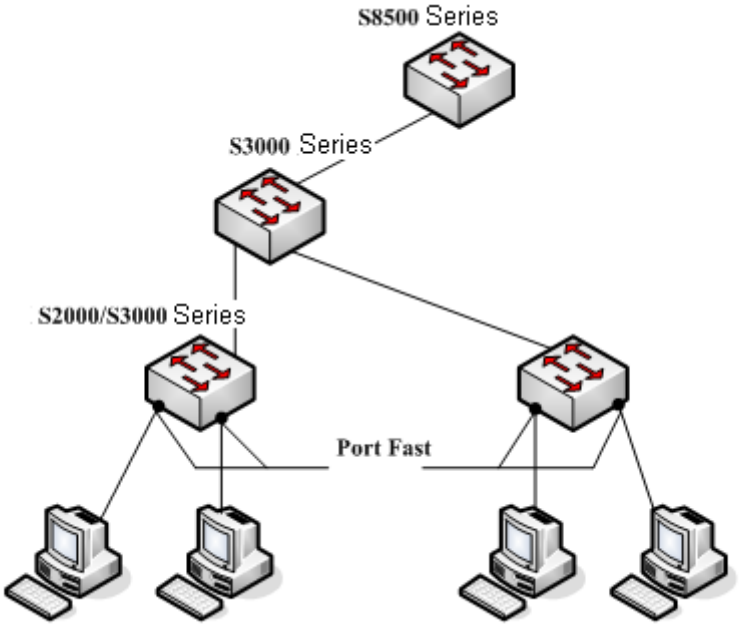


Figure 1.1 Port Fast

Instruction：

For the rapid convergent spanning tree protocol, RSTP and MSTP, can immediately bring an interface to the forwarding state, and therefore there is no need to use Port Fast feature. Series Series Series

1.1.2 BPDU Guard

The BPDU guard feature can be globally enabled on the switch or can be enabled per port, but the feature operates with some differences.

At the global level, you enable BPDU guard on Port Fast-enabled ports by using the spanning-tree portfast bpduguard default global configuration command. Spanning tree shuts down ports that are in a Port Fast-operational state if any BPDU is received on them. In a valid configuration, Port Fast-enabled ports do not receive BPDUs. Receiving a BPDU on a Port Fast-enabled port means an invalid configuration, such as the connection of an unauthorized device, and the BPDU guard feature puts the port in the error-disabled state. When this happens, the switch shuts down the entire port on which the violation occurred.

To prevent the port from shutting down, you can use the errdisable detect cause bpduguard shutdown vlan global configuration command to shut down just the offending VLAN on the port where the violation occurred.

At the interface level, you enable BPDU guard on any port by using the spanning-tree bpduguard enable interface configuration command without also enabling the Port Fast feature. When the port receives a BPDU, it is put in the error-disabled state.

The BPDU guard feature provides a secure response to invalid configurations because you must manually put the interface back in service. Use the BPDU

guard feature in a service-provider network to prevent an access port from participating in the spanning tree.

1.1.3 BPDU Filter

The BPDU filtering feature can be globally enabled on the switch or can be enabled per interface, but the feature operates with some differences.

In SSTP/PVST mode,.if a **Port Fast** port with BPDU filter configured receives the BPDU, the features BPDU Filter and Port Fast at the port will be automatically disabled, resuming the port as a normal port. Before entering the **Forwarding** state, the port must be in the **Listening** state and **Learning** state.

The BPDU Filter feature can be configured in global configuration mode or in port configuration mode. In global configuratiom mode, run the command **spanning-tree portfast bpdufilter** to block all ports to send BPDU out. The port, howerver, can still receive and process BPDU.

1.1.4 Uplink Fast

The feature **Uplink Fast** enables new root ports to rapidly enter the **Forwarding** state when the connection between the switch and the root bridge is disconnected.

A complex network always contains multilayers of devices, as shown in figure 1.2. Both aggregation layer and the access layer of the switch have redundancy connections with the upper layer. These redundancy connections are normally blocked by the STP to avoid loops.

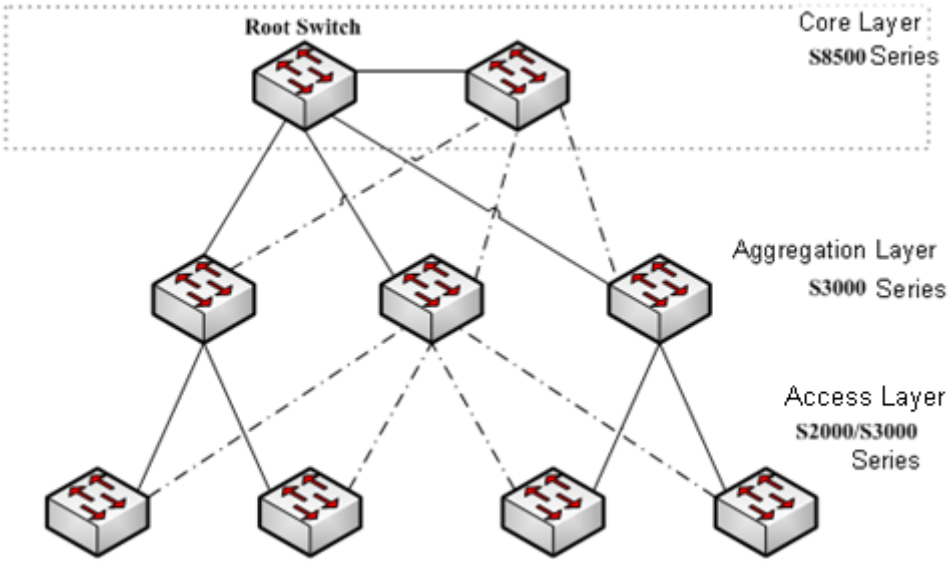


Figure 1.2 switching network topology

Suppose the connection between a switch and the upper layer is disconnected (called as Direct Link Failure), the STP chooses the Alternate port on the redundancy line as the root port. Before entering the **Forwarding** state, the Alternate port must be in the **Listening** state and **Learning** state. If the **Uplink Fast** feature is configured by running the command **spanning-tree uplinkfast** in

global configuration mode, new root port can directly enter the forwarding state, resuming the connection between the switch and the upper layer.

Figure 1.3 shows the working principle of the **Uplink Fast** feature. The port for switch C to connect switch B is the standby port when the port is in the original state. When the connection between switch C and root switch A is disconnected, the previous Alternate port is selected as new root port and immediately start forwarding.

New root port promptly

changes to

the Forwarding state

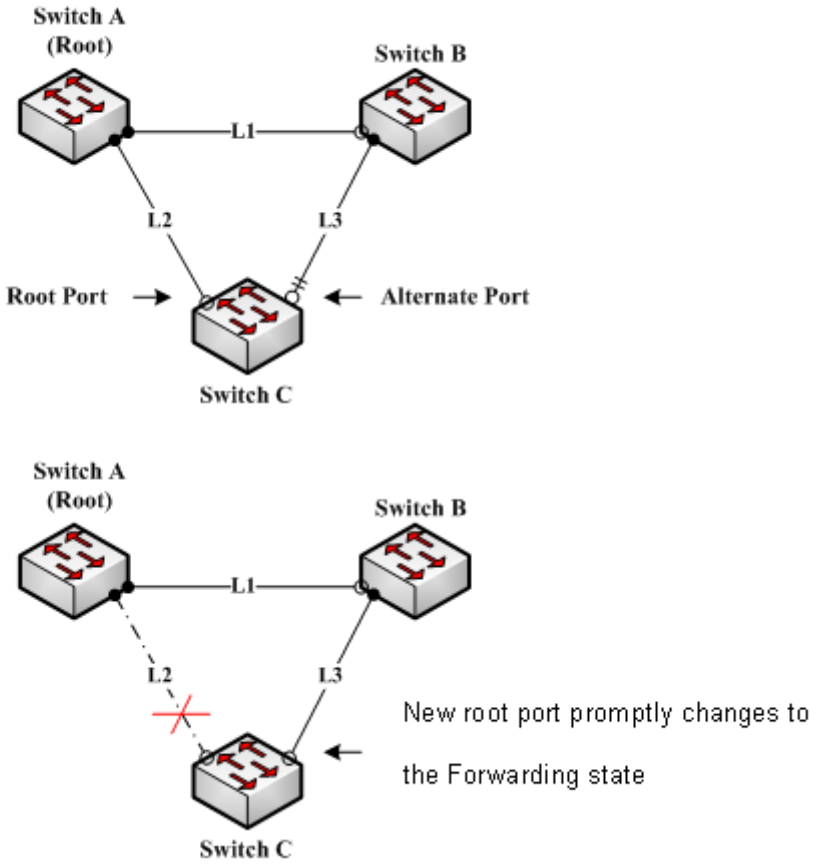


Figure 1.3 Uplink Fast

Note:

The Uplink Fast feature adjusts to the slowly convergent SSTP and PVST. In RSTP and MSTP mode, new root port can rapidly enter the Forwarding state without the Uplink Fast function.

1.1.5 Backbone Fast

The **Backbone Fast** feature is a supplement of the **Uplink Fast** technology. The **Uplink Fast** technology makes the redundancy line rapidly work in case the direct connection to the designated switch is disconnected, while the **Backbone Fast**

technology detects the indirect-link network blackout in the upper-layer network and boosts the change of the port state.

In figure 1.3, Connection L2 between switch C and switch A is called as the direct link between switch C and root switch A. If the connection is disconnected, the **Uplink Fast** function can solve the problem. Connection L1 between switches A and B is called as the indirect link of switch C. The disconnected indirect link is called as indirect failure, which is handled by the **Backbone Fast** function.

The working principle of the Backbone Fast function is shown in Figure 1.4.

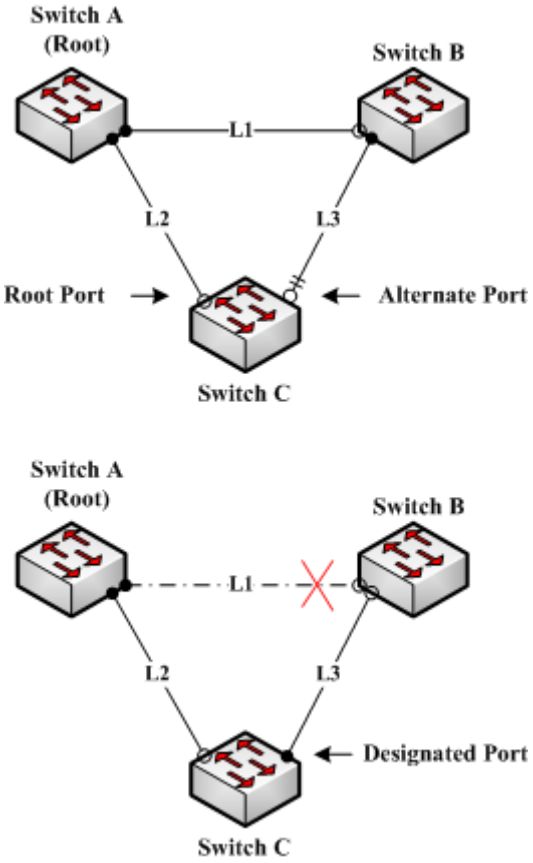


Figure 1.4 Backbone Fast

Suppose the bridge priority of switch C is higher than that of switch B. When L1 is disconnected, switch B is selected to send BPDU to switch C because the bridge priority is used as root priority. To switch C, the information contained by BPDU is not prior to information contained by its own. When Backbone Fast is not enabled, the port between switch C and switch B ages when awaiting the bridge information and then turns to be the designated port. The aging normally takes a few seconds. After the function is configured in global configuration mode by running the command **spanning-tree backbonefast**, when the Alternate port of switch C receives a BPDU with lower priority, switch C thinks that an indirect-link and root-switch-reachable connection on the port is disconnected. Switch C then promptly update the port as the designated port without waiting the aging information.

After the Backbone Fast function is enabled, if BPDU with low priority is received at different ports, the switch will perform different actions. If the Alternate port receives the message, the port is updated to the designated port. If the root port

receives the low-priority message and there is no other standby port, the switch turns to be the root switch.

Note that the Backbone Fast feature just omits the time of information aging. New designated port still needs to follow the state change order: the listening state, then the learning state and finally the forwarding state.

Note:

Similar to Uplink Fast, the Backbone Fast feature is effective in SSTP and PVST modes.

1.1.6 Root Guard

The Root Guard feature prevents a port from turning into a root port because of receiving high-priority BPDU.

The Layer 2 network of a service provider (SP) can include many connections to switches that are not owned by the SP. In such a topology, the spanning tree can reconfigure itself and select a customer switch as the root switch, as shown in Figure 17-8. You can avoid this situation by enabling root guard on SP switch interfaces that connect to switches in your customer's network. If spanning-tree calculations cause an interface in the customer network to be selected as the root port, root guard then places the interface in the root-inconsistent (blocked) state to prevent the customer's switch from becoming the root switch or being in the path to the root.

If a switch outside the SP network becomes the root switch, the interface is blocked (root-inconsistent state), and spanning tree selects a new root switch. The customer's switch does not become the root switch and is not in the path to the root.

If the switch is operating in multiple spanning-tree (MST) modes, root guard forces the interface to be a designated port. If a boundary port is blocked in an internal spanning-tree (IST) instance because of root guard, the interface also is blocked in all MST instances. A boundary port is an interface that connects to a LAN, the designated switch of which is either an IEEE 802.1D switch or a switch with a different MST region configuration.

Root guard enabled on an interface applies to all the VLANs to which the interface belongs. VLANs can be grouped and mapped to an MST instance.

You can enable this feature by using the spanning-tree guard root interface configuration command.

Note：

Root Guard feature acts differently somehow in SSTP/PVST and RSTP/MSTP. In SSTP/PVST mode, Root port is always blocked by Root Guard. In RSTP/MSTP mode, Root port won’t be blocked until receiving higher level BPDU. A port which formerly plays the Root role will not be blocked.

1.1.7 Loop Guard

You can use loop guard to prevent alternate or root ports from becoming designated ports because of a failure that leads to a unidirectional link. This feature is most effective when it is enabled on the entire switched network. Loop

guard prevents alternate and root ports from becoming designated ports, and spanning tree does not send BPDUs on root or alternate ports.

You can enable this feature by using the spanning-tree loopguard default global configuration command.

When the switch is operating in PVST+ or rapid-PVST+ mode, loop guard prevents alternate and root ports from becoming designated ports, and spanning tree does not send BPDUs on root or alternate ports.

When the switch is operating in MST mode, BPDUs are not sent on nonboundary ports only if loop guard in all MST instances blocks the interface. On a boundary port, loop guard blocks the interface in all MST instances.

Note：

Loop Guard feature acts differently somehow in SSTP/PVST and RSTP/MSTP. In SSTP/PVST mode, the designated port is always be blocked by Loop Guard. In RSTP/MSTP mode, the port will be blocked only when it changes into the designated port because of inaccessibility to receiving BPDU. Loop Guard will not block a port, which is provided with the designated role due to receiving the lower level BPDU.

1.2 Configuring STP Optional Characteristic

1.2.1 STP Optional Characteristic Configuration Task

- Configuring Port Fast
- Configuring BPDU Guard
- Configuring BPDU Filter
- Configuring Uplink Fast
- Configuring Backbone Fast
- Configuring Root Guard
- Configuring Loop Guard

1.2.2 Configuring Port Fast

An interface with the Port Fast feature enabled is moved directly to the spanning-tree forwarding state without waiting for the standard forward-time delay.

Use the following command to configure the port fast feature in the global configuration mode：

command	purpose
spanning-tree port fast default	Globally enables port fast feature. It is valid to all interfaces.

no spanning-tree portfast default	Globally disables port fast feature. It has no effect on the interface configuration.

Note：

The port fast feature only applies to the interface that connects to the host. The BPDU Guard or BPDU Filter must be configured at the same time when the port fast feature is configured globally.

Use the following command to configure the port fast feature in the interface configuration mode：

command	purpose
spanning-tree portfast	Enables port fast feature on the interface.
no spanning-tree portfast	Disables port fast feature on the interface. It has no effect on the global configuration.

1.2.3 Configuring BPDU Guard

When you globally enable BPDU guard on ports that are Port Fast-enabled (the ports are in a Port Fast-operational state), spanning tree shuts down Port Fast-enabled ports that receive BPDUs.

In a valid configuration, Port Fast-enabled ports do not receive BPDUs. Receiving a BPDU on a Port Fast-enabled port means an invalid configuration, such as the connection of an unauthorized device, and the BPDU guard feature puts the port in the error-disabled state. When this happens, the switch shuts down the entire port on which the violation occurred.

To prevent the port from shutting down, you can use the errdisable detect cause bpduguard shutdown vlan global configuration command to shut down just the offending VLAN on the port where the violation occurred.

The BPDU guard feature provides a secure response to invalid configurations because you must manually put the port back in service. Use the BPDU guard feature in a service-provider network to prevent an access port from participating in the spanning tree.

Follow these steps to globally enable the BPDU guard feature：

command	purpose
spanning-tree portfast bpduguard	Globally enables bpdu guard feature. It is valid to all interfaces.
no spanning-tree portfast bpduguard	Globally disables bpdu guard feature.

Instruction：

Globally enabling port fast feature may result in broadcast storm. The BPDU Guard or BPDU Filter should be configured for protection sake.

Follow these steps to enable the BPDU guard feature in interface configuration mode：

command	purpose
spanning-tree bpduguard enable	Enables bpdu guard feature on the interface.
spanning-tree bpduguard disable	Disables bpdu guard feature on the interface. It has no effect on the global configuration.
no spanning-tree bpduguard	Disable bpdu guard feature on the interface. It has no effect on the global configuration.

1.2.4 Configuring BPDU Filter

When you globally enable BPDU filtering on Port Fast-enabled interfaces, it prevents interfaces that are in a Port Fast-operational state from sending or receiving BPDUs. The interfaces still send a few BPDUs at link-up before the switch begins to filter outbound BPDUs. You should globally enable BPDU filtering on a switch so that hosts connected to these interfaces do not receive BPDUs. If a BPDU is received on a Port Fast-enabled interface, the interface loses its Port Fast-operational status, and BPDU filtering is disabled.

Follow these steps to globally enable the BPDU filter feature.：

command	purpose
spanning-tree portfast bpdufilter	Globally enables bpdu filter feature. It is valid to all interfaces.
no spanning-tree portfast bpdufilter	Globally disables bpdu filter feature.

Instruction：

Globally enabling port fast feature may result in broadcast storm. The BPDU Guard or BPDU Filter should be configured for protection sake.

Follow these steps to enable the BPDU filter feature in the interface configuration mode ：

command	purpose
spanning-tree bpdufilter enable	Enables bpdu filter feature on the interface.
spanning-tree bpdufilter disable	Disables bpdu filter feature. It has no effect on the global configuration.
no spanning-tree bpdufilter	Disables bpdu filter feature. It has no influence on the global configuration.

1.2.5 Configuring Uplink Fast

If a switch loses connectivity, it begins using the alternate paths as soon as the spanning tree selects a new root port. By enabling UplinkFast with the spanning-tree uplinkfast global configuration command, you can accelerate the choice of a new root port when a link or switch fails or when the spanning tree reconfigures itself. The root port transitions to the forwarding state immediately

without going through the listening and learning states, as it would with the normal spanning-tree procedures.

Uplink Fast feature is only valid in SSTP/PVST mode.

Follow these steps to globally enable UplinkFast.：

command	purpose
spanning-tree uplinkfast	Enables uplink fast feature.
no spanning-tree uplinkfast	Disables uplink fast feature.

1.2.6 Configuring Backbone Fast

BackboneFast is a complementary technology to the UplinkFast feature, which responds to failures on links directly connected to access switches. BackboneFast optimizes the maximum-age timer, which controls the amount of time the switch stores protocol information received on an interface. When a switch receives an inferior BPDU from the designated port of another switch, the BPDU is a signal that the other switch might have lost its path to the root, and BackboneFast tries to find an alternate path to the root.

Backbone fast feature is only valid in SSTP/PVST mode.

Follow these steps to globally enable BackboneFast.：

command	purpose
spanning-tree backbonefast	Enables backbone fast feature.
no spanning-tree backbonefast	Disables backbone fast feature.

1.2.7 Configuring Root Guard

Root guard enabled on an interface applies to all the VLANs to which the interface belongs. Do not enable the root guard on interfaces to be used by the UplinkFast feature. With UplinkFast, the backup interfaces (in the blocked state) replace the root port in the case of a failure. However, if root guard is also enabled, all the backup interfaces used by the UplinkFast feature are placed in the root-inconsistent state (blocked) and are prevented from reaching the forwarding state.

Root Guard feature acts differently somehow in SSTP/PVST and RSTP/MSTP. In SSTP/PVST mode, Root port is always blocked by Root Guard. In RSTP/MSTP mode, Root port won’t be blocked until receiving higher level BPDU. A port which formerly plays the Root role will not be blocked.

Follow these steps to enable root guard on an interface.：

command	purpose
spanning-tree guard root	Enables root guard feature on the interface.

no spanning-tree guard	Disables root guard and loop guard features on the interface.
spanning-tree guard none	Disables root guard and loop guard features on the interface.

1.2.8 Configuring Loop Guard

You can use loop guard to prevent alternate or root ports from becoming designated ports because of a failure that leads to a unidirectional link. This feature is most effective when it is configured on the entire switched network. Loop guard operates only on interfaces that are considered point-to-point by the spanning tree.

Loop Guard feature acts differently somehow in SSTP/PVST. In SSTP/PVST mode,, the designated port is always blocked by Loop Guard. In RSTP/MSTP, the designated port is always blocked by Loop Guard. In RSTP/MSTP mode, the port will be blocked only when it changes into the designated port because of inaccessibility to receiving BPDU. A port which is provided with the designated role due to receiving the lower level BPDU will not be blocked by Loop Guard.

Follow these steps to enable loop guard in global configuration mode.：

command	purpose
spanning-tree loopguard default	Globally enables loop guard feature. It is valid to all interfaces.
no spanning-tree loopguard default	Globally disables loop guard.

Follow these steps to enable loop guard in the interface configuration mode.：

Command	Purpose
spanning-tree guard loop	Enables loop guard feature on the interface.
no spanning-tree guard	Disables root guard and loop guard feature on the interface.
spanning-tree guard none	Disables root guard and loop guard on the interface.

MAC Address Table Attribute Configuration

Table of Contents

Chapter 1 Configuring MAC Address Attribute

1.1 MAC Address Configuration Task List

- Configuring Static Mac Address
- Configuring Mac Address Aging Time
- Configring VLAN-shared MAC Address
- Displaying Mac Address Table
- Clearing Dynamic Mac Address

1.2 MAC Address Configuration Task

1.2.1 Configuring Static Mac Address

Static MAC address entries are MAC address entries that do not age by the switch and can only be deleted manually. According to the actual requirements during the operation process, you can add and delete a static MAC address. Use the following command in privileged level to add and delete a static MAC address.

Command	Purpose
configure	Enters the global configuration mode.
[no] mac address-table static *mac-addr* **vlan** *vlan-id* **interface** *interface-id*	Adds/deletes a static MAC address entry. Mac-addr indicates the MAC address. Vlan-id indicates the VLAN number. Valid value is from 1~4094. Interface-id indicates the interface name.
exit	Returns to EXEC mode.
write	Saves configuration.

1.2.2 Configuring MAC Address Aging Time

When a dynamic MAC address is not used during the specified aging time, the switch will delete this MAC address from the MAC address table. The aging time of the switch MAC address can be configured in terms of needs. The default aging time is 300 seconds.

Configure the aging time of MAC address in the privileged mode as follows:

command	purpose
configure	Enters the global configuration mode

mac address-table aging-time [**0 | 10-1000000**]	Configures the aging time of MAC address. 0 indicates no-age of the MAC address. Valid value is from 10 to 1000000 in seconds.
exit	Returns to the management mode.
write	Saves configuration.

1.2.3 Configring VLAN-shared MAC Address

When a port is configured with the VLAN-shared MAC address, the MAC address learned by the port will be shared by all VLAN, that is, other VLANs will learn the MAC address too.

Perform the following steps in privileged mode to configure the MAC address shared by VLANs.

Command	Purpose
configure	Enters the global configuration mode.
interface q0/1	Enters the to-be-configured interface.
switchport shared-learning	Configures the MAC address shared by VLAN.
exit	Returns to the global configuration mode.
exit	Returns to the management mode.
write	Saves configuration.

1.2.4 Displaying MAC Address

Since debugging and management are required in operation process, we want to know content of the switch MAC address table. Use the show command to display content of the switch MAC address table.

Command	purpose
show mac address-table {**dynamic** [**interface** interface-id **| vlan** vlan-id] **| static**}	Displays content of the MAC address table. Dynamic indicates the MAC address that acquires dynamically. Vlan-id indicates the VLAN number. Valid value is from 1 to 4094. Interface-id indicates the interface name. Static indicates the static MAC address table.

1.2.5 Clearing dynamic MAC Address

The acquired MAC addresses need to be cleared in some circumstances.

Use the following command to delete a dynamic MAC address in privileged mode:

command	purpose

clear mac address-table dynamic [address *mac-addr* | **interface** *interface-id* **| vlan** *vlan-id*]	Deletes a dynamic MAC address entry. Dynamic indicates the MAC address that dynamically acquires. Mac-addr is the MAC address. Interface-id indicates the interface name. Vlan-id indicates the VLAN number. Valid value is from 1 to 4094.

Link Aggregation Configuration

Table of Contents

Chapter 1 Configuring Port Aggregation

1.1 Overview

Link aggregation, also called trunking, is an optional feature available on the Ethernet switch and is used with Layer 2 Bridging. Link aggregation allows logical merge of multiple ports in a single link. Because the full bandwidth of each physical link is available, inefficient routing of traffic does not waste bandwidth. As a result, the entire cluster is utilized more efficiently. Link aggregation offers higher aggregate bandwidth to traffic-heavy servers and reroute capability in case of a single port or cable failure.
Supported Features:

- Static aggregation control is supported

  Bind a physical port to a logical port, regardless whether they can actually bind to a logical port.

  Aggregation control of LACP dynamic negotiation is supported

  Only a physical port that passes the LACP protocol negotiation can bind to a logical port. Other ports won't bind to the logical port.
- Aggregation control of LACP dynamic negotiation is supported

  When a physical port is configured to bind to a logical port, the physical port with LACP negotiation can be bound to a logical port. Other ports cannot be bound to the logical port.
- Flow balance of port aggregation is supported.

  After port aggregation, the data flow of the aggregation port will be distributed to each aggregated physical port.

1.2 Port Aggregation Configuration Task

- Configuring logical channel used for aggregation
- Aggregation of physical port
- Selecting load balance mode after port aggregation
- Monitoring the concrete condition of port aggregation

1.3 Port Aggregation Configuration Task

1.3.1 Configuring logical channel used to aggregation

You should establish a logical port before binding all the physical ports together. The

logical port is used to control the channel formed by these binding physical ports.
Use the following command to configure the logical channel:

command	Description
interface port-aggregator id	Configures aggregated logical channel.

1.3.2 Aggregation of Physical Port

To aggregate multiple physical ports into a logical channel, you can use static aggregation or LACP protocol for negotiation.
In the case when the static aggregation is used, it is required that the link of the physical port should be up, and the VLAN attribute of aggregation port and physical port should be identical, and then this port will be aggregated to the logical channel, regardless of whether the current port accords with the conditions of port aggregation and whether the port that connects with the physical port accords with the aggregation conditions.
Prerequisites for ports to be aggregated:

- The link of the port must be up and the port should be negotiated to full-duplex mode.
- The speed of all physical ports should be same during aggregation process, that is, if there is one physical port that has been aggregated successfully, then the speed of the second physical port must be the same as the first configured one. Also the vlan attributes of all physical ports must be identical to the aggregated port.

LACP packets are exchanged between ports in these modes:

- Active—Places a port into an active negotiating state, in which the port initiates negotiations with remote ports by sending LACP packets.
- Passive—Places a port into a passive negotiating state, in which the port responds to LACP packets it receives but does not initiate LACP negotiation. In this mode, the port channel group attaches the interface to the bundle.

If both ports use Passive method, then the aggregation fails. This is because both sides will wait for the other side to launch aggregation negotiation process.
VALN attributes: PVID, Trunk attribute, vlan-allowed range and vlan-untagged range.
Use the following command to perform aggregation on the physical ports:

command	purpose
aggregator-group *agg-id* **mode** { **lacp** | **static** }	Configures aggregation option of the physical port.

1.3.3 Selecting Load Balance Method After Port Aggregation

You can select the load share method to ensure that all ports can share the data traffic after the aggregation of all physical ports. The switch can provides up to six load balance strategy:

- src-mac

  It is to share the data traffic according to the source MAC address, that is, the message with same MAC address attributes is to get through a physical port.

- dst-mac

  It is to share the data traffic according to the destination MAC address, that is, the message with same MAC address attributes is to get through a physical port.

- both-mac

  It is to share the data traffic according to source and destination MAC addresses, that is, the message with same MAC address attributes is to get through a physical port.

- src-ip

  It is to share the data traffic according to the source IP address, that is, the message with same IP address attributes is to get through a physical port.

- dst-ip

  It is to share the data traffic according to the destination IP address, that is, the message with same IP address attributes is to get through a physical port.

- both-ip

  It is to share the data traffic according to the destination and source IP addresses, that is, the message with same IP address attributes is to get through a physical port.

Use the following command to configure load balance method:

command	purpose
aggregator-group load-balance	Configures load balance method.

Note:

The command is unavailable at the switch that does not support load balance methods or supports only one method. The switch using the command only selects the load balance strategies supported by itself.

The following table shows different switches spport different kinds of load balance strategies:

Model	src-mac	dst-mac	both-mac	src-ip	dst-ip	both-ip
S2008, S2116, S2026B	x	x	x	x	x	x
S2224D	√	√	√	x	x	x
S2224M, S2226, S2448	√	√	√	√	√	√
S2516, S2524, S2524GX	√	√	x	x	x	√
S2448B,S2226C	√	√	√	x	x	x
S3224, S3224M	√	√	√	√	√	√

S3424, S3448 **S3512**						
S6508	√	x	x	x	x	x
S8500	√	√	√	√	√	√

1.3.4 Monitoring the Concrete Conditions of Port Aggregation

Use the following command to monitor port aggregation state in EXEC mode:

command	description
show aggregator-group	Displays port aggregation state.

MAC Access List Configuration

Table of Contents

Chapter 1 Configuring MAC List

1.1 MAC List Configuration Task

1.1.1 Creating MAC List

To apply the MAC list on the port, you must first create the MAC list. After the MAC list is successfully created, you log in to the MAC list configuration mode and then you can configure items of the MAC access list.

Perform the following operations to add and delete a MAC list in privilege mode:

Run…	To…
configure	Log in to the global configuration mode.
[**no**] **mac access-list** *name*	Add or delete a MAC list. **name** means the name of the MAC list.

1.1.2 Configuring Items of MAC List

You can use the **permit** or **deny** command to configure the **permit** or **deny** items of the MAC list. Multiple **permit** or **deny** items can be configured on a MAC list.

The mask of multiple items configured in a MAC list must be the same. Otherwise, the configuration may be out of effect (see the following example). The same item can only be configured once in the same MAC address.

Perform the following operations in MAC list configuration mode to configure the items of the MAC list:

Run…	To…
[no] {deny | permit} {**any** | **host** *src-mac-addr*} {**any** | **host** *dst-mac-addr*}**[**ethertype**]**	Add/Delete an item of the MAC list. You can rerun the command to add or delete multiple items of the MAC list. **any** means any MAC address can be compatible; **src-mac-addr** means the source MAC address; **dst-mac-addr** means the destination MAC address. **ethertype** means the type of matched Ethernet packet.
exit	Log out from the MAC list configuration mode and enter the global configuration mode again.
exit	Enter the management mode again.
write	Save configuration.

MAC list configuration example

Switch_config#mac acce 1

Switch-config-macl#permit host 1.1.1 any
Switch-config-macl#permit host 2.2.2 any

The above configuration is to compare the source MAC address, so the mask is the same. The configuration is successful.

Switch_config#mac acce 1
Switch-config-macl#permit host 1.1.1 any
Switch-config-macl#permit any host 1.1.2
Switch-config-macl#2003-11-19 18:54:25 rule conflict,all the rule in the acl should match!

The first line on the above configuration is to compare source MAC addresses, while the second line is to compare destination MAC addresses. Therefore, the mask is different. The configuration fails.

1.1.3 Applying MAC List

The created MAC list can be applied on any physical port. Only one MAC list can be applied to a port. The same MAC list can be applied to multiple ports.

Enter the privilege mode and perform the following operation to configure the MAC list.

Run…	To…
configure	Enter the global configuration mode.
interface f0/1	Log in to the port that is to be configured.
[**no**] **mac access-group** *name*	Apply the created MAC list to the port or delete the applied MAC list from the port. **name** means the name of the MAC list.
exit	Enter the global configuration mode again.
exit	Enter the management mode again.
write	Save configuration.

Physical Port IP Access List Configuration

Table of Contents

Chapter 1 Configuring Physical Port-based IP Access List

1.1 Filtering IP Message

Filtering message helps control the running of packets in the network. The control can constrain network transmission or limit network usage through user or device. To enable or disable packets on the crossly specified port, our routing switches provide the access list. The access list can be used through the following methods:

- Controlling packet transmission on the port
- Controlling the access of virtual terminal line
- Limiting routing update content

The section describes how to create and use the IP access list.

The IP access list is an orderly set IP of applying the allowed and forbidden conditions of IP address. The ROS software of our routing switches is to test the addresses in the access list one by one. The first match decides whether the software to accept or reject the address. Because the ROS software stops the match rules after the first match, the order of conditions is very important. If rule match does not exist, the address is to be rejected.

You need to perform the following steps before using the access list:

(1) Create the IP access list by specifying the access list name and access conditions.

(2) Apply the IP access list to the port.

1.2 Creating Standard and Extensible IP Access List

Use a character string to create an IP access list.

Note:

The standard IP access list and the extensible IP access list cannot use the same name.

Run the following commands in global configuration mode to create a standard IP access list:

Run…	To…
ip access-list standard *name*	Use name to define a standard IP access list.
deny {*source [source-mask]* | **any**} or **permit** {*source [source-mask]* | **any**}	Specify one or multiple **permit/reject** conditions in standard IP access list configuration mode, which decides whether the packet is approved or disapproved.
Exit	Log out from the IP access list configuration mode.

Run the following commands in global configuration mode to create an extensible IP access list:

Run…	To…
ip access-list extended *name*	Use a name to define an extensible IP access list.
{**deny	permit**} *protocol source source-mask destination destination-mask* [**precedence** *precedence*] [**tos** *tos*] {**deny	permit**} *protocol* **any any**	Specify one or multiple **deny** or **permit** conditions in extensible access list configuration mode, which decides whether the IP packet is passed or not (**precedence** means the priority of the IP packet. **TOS** is the simplified form of Type of Service). If the protocol is TCP/UDP, a single port or port 14 in a certain range can be specified. For details, refer to "Extensible Access List Example".
Exit	Log out of the access list configuration mode.

After the access list is originally created, any part added later (may be entered from the terminal) is put at the end of the list, that is, you cannot add the command line to the designated access list. However, you can run **no permit** and **no deny** to delete items from the name access list.

Note:

When you create the access list, remember that the end of the access list contains the invisible **deny** sentence. In another word, if the mask is not specified in relevant IP address access list, 255.255.255.255 is supposed to be the mask.

After the access list is created, it must be applied to the line or the port. Refer to section 1.3 "Applying the Access List to Port".

1.3 Applying the Access List to Port

After the access list is created, you can apply it to one or multiple ports or entries.

Run the following command in port configuration mode:

Run…	To…
ip access-group *name*	Apply the access list to the port.

For the standard entry access list, when the packet is received, the source address of the access list checking packet will be checked. For the extensible access list, the routing switch also checks the destination address. If the access list permits the destination address, the software continues to handle the packet. If the access list denies the destination address, the software drops the packet and returns a message that the ICMP host is unreachable.

If the designated access list does not exist, all packets are allowed to get through.

1.4 Extensible Access List Example

1.4.1 Port-Based IP Access List Supporting Filtration on TCP/UDP Ports

The example is shown as follows:

{**deny | permit**} {tcp | udp}

source source-mask [{ [src_portrange begin-port end-port] | [{gt | lt } port] }]

destination destination-mask [{ [dst_portrange begin-port end-port] | [{gt | lt } port] }]

[**precedence** *precedence*] [**tos** *tos*]

In this case, port l4 of TCP and UDP can be controlled through the access list. Pay attention to the following problems when you configure the access list by defining the port range:

(1) If the access list is configured at the source and destination by specifying the port range, some configuration may fail because lots of sources are occupied during configuration. To solve the problem, you are recommended to specify the port range at one side and the port at the other side.

(2) Using the port range filtration needs a lot of resources. The access list cannot provide strong support to other applications because the port range filtration is used too much.

1.4.2 Port-Based IP Access List Supporting Filtration of Port-Based IP Access List Supporting Filtration of TCP/UDP-Specified Ports

In the following case, the first command line allows the newly coming TCP to connect SMTP of host 130.2.1.2.

```
ip access-list extended aaa
permit tcp any 130.2.1.2 255.255.255.255 eq 25
interface  g0/10
ip access-group aaa
```

Network Protocol Configuration

Table of Contents

Chapter 1 Configuring IP Addressing

1.1 IP Introduction

1.1.1 IP

Internet Protocol (IP) is a protocol in the network to exchange data in the text form. IP has the functions such as addressing, fragmenting, regrouping and multiplexing. Other IP protocols (IP protocol cluster) are based on IP. As a protocol working on the network layer, IP contains addressing information and control information which are used for routing.

Transmission Control Protocol (TCP) is also based on IP. TCP is a connection-oriented protocol which regulates the format of the data and information in data transmission. TCP also gives the method to acknowledge data is successfully reached. TCP allows multiple applications in a system to communicate simultaneously because it can send received data to each of the applications respectively.

The IP addressing, such as Address Resolution Protocol, are to be described in section 1.3 “Configuring IP Addressing.” IP services such as ICMP, HSRP, IP statistics and performance parameters are to be described in Chapter 4 “Configuring IP Services.”

1.1.2 IP Routing Protocol

Our routing switch supports multiple IP routing dynamic protocols, which will be described in the introduction of each protocol.

IP routing protocols are divided into two groups: Interior Gateway Routing Protocol (IGRP) and Exterior Gateway Routing Protocol (EGRP). Our routing switch supports RIP, OSPF, BGP and BEIGRP. You can configure RIP, OSPF, BGP and BEIGRP respectively according to your requirements. Our switch also supports the process that is to configure multiple routing protocols simultaneously, a random number of OSPF processes (if memory can be distributed), a BGP process, a RIP process and a random number of BEIGRP processes. You can run the **redistribute** command to redistribute the routes of other routing protocols to the database of current routing processes, connecting the routes of multiple protocol processes.

To configure IP dynamic routing protocols, you must first configure relevant processes, make relevant network ports interact with dynamic routing processes, and then designate routing processes to be started up on the ports. To do this, you may check configuration steps in configuration command documents.

1. Choosing routing protocol

It is a complex procedure to choose routing protocol. When you choose the routing protocol, consider the following items:

- Size and complexity of the network
- Whether the length-various network need be supported
- Network traffic
- Safety requirements
- Reliability requirements
- Strategy
- Others

Details of the above items are not described in the section. We just want to remind you that your network requirements must be satisfied when you choose the routing protocols.

2. IGRP

Interior Gateway Routing Protocol (IGRP) is used for network targets in an autonomous system. All IP IGRPs must be connected with networks when they are started up. Each routing process monitors the update message from other routing switches in the network and broadcasts its routing message in the network at the same time. The IGRPs that our routing switches support include:

- RIP
- OSPF
- BEIGRP

3. EGRP

Exterior Gateway Routing Protocol (EGRP) is used to exchange routing information between different autonomonous systems. Neighbors to exchange routes, reachable network and local autonomonous system number generally need to be configured. The EGRP protocol that our switch supports is BGP.

1.2 Configuring IP Address Task List

An essential and mandatory requirement for IP configuration is to configure the IP address on the network interface of the routing switch. Only in this case can the network interface be activated, and the IP address can communicate with other systems. At the same time, you need to confirm the IP network mask.

To configure the IP addressing, you need to finish the following tasks, among which the first task is mandatory and others are optional.

For creating IP addressing in the network, refer to section 1.4 “IP Addressing Example.”

Followed is an IP address configuration task list:

- Configuring IP address at the network interface
- Configuring multiple IP addresses at the network interface
- Configuring address resolution
- Configuring routing process
- Configuring broadcast text management
- Detecting and maintaining IP addressing

1.3 Configuring IP Address

1.3.1 Configuring IP Address at Network Interface

The IP address determines the destination where the IP message is sent to. Some IP special addresses are reserved and they cannot be used as the host IP address or network address. Table 1 lists the range of IP addresses, reserved IP addresses and available IP addresses.

Type	Address or Range	State
A	0.0.0.0 1.0.0.0 to 126.0.0.0 127.0.0.0	Reserved Available Reserved
B	128.0.0.0 to 191.254.0.0 191.255.0.0	Available Reserved
C	192.0.0.0 192.0.1.0 to 223.255.254 223.255.255.0	Reserved Available Reserved
D	224.0.0.0 to 239.255.255.255	Multicast address
E	240.0.0.0 to 255.255.255.254 255.255.255.255	Reserved Broadcast

The official description of the IP address is in RFC 1166 “Internet Digit”. You can contact the Internet service provider.

An interface has only one primary IP address. Run the following command in interface configuration mode to configure the primary IP address and network mask of the network interface:

Run…	To…
ip address *ip-address mask*	Configure the main IP address of the interface.

The mask is a part of the IP address, representing the network.

Note:

Our switches only support masks which are continuously set from the highest byte according to the network character order.

1.3.2 Configuring Multiple IP Addresses on Network Interface

Each interface can possess multiple IP addresses, including a primary IP address and multiple subordinate IP addresses. You need to configure the subordinate IP addresses in the following two cases:

- If IP addresses in a network segment are insufficient.

For example, there are only 254 available IP addresses in a certain logical subnet, however, 300 hosts are needed to connect the physical network. In this case, you can configure the subordinate IP address on the switch or the server, enabling two logical subnets to use the same physical subnet. Most of early-stage networks which are based on the layer-2 bridge are not divided into multiple subnets. You can divide the early-stage network into multiple route-based subnets by correctly using the subordinate IP addresses. Through the configured subordinate IP addresses, the routing switch in the network can know multiple subnets that connect the same physical network.

- If two subnets in one network are physically separated by another network.

In this case, you can take the address of the network as the subordinate IP address. Therefore, two subnets in a logical network that are physically separated, therefore, are logically connected together.

Note:

If you configure a subordinate address for a routing switch in a network segment, you need to do this for other routing switches in the same network segment.

Run the following command in interface configuration mode to configure multiple IP addresses on the network interface.

Run…	To…
ip address *ip-address mask* **secondary**	Configure multiple IP addresses on the network interface.

Note:

When the IP routing protocol is used to send the route update information, subordinate IP addresses may be treated in different ways.

1.3.3 Configuring Address Resolution

IP can realize functions such as IP address resolution control. The following sections show how to configure address resolution:

1. Creating address resolution

An IP device may have two addresses: local address (local network segment or device uniquely identified by LAN) and network address (representing the network where the device is located). The local address is the address of the link layer because the local

address is contained in the message header at the link layer, and is read and used by devices at the link layer. The professionalists always call it as the MAC address. This is because the MAC sub layer in the link layer is used to process addresses.

For example, if you want your host to communicate with a device on Ethernet, you must know the 48-bit MAC address of the device or the local address of the link layer. The process on how to obtain the local address of the link layer from the IP address is called as Address Resolution Protocol (ARP). The process on how to obtain the IP address from the local address of the link layer is called as Reverse Address Resolution (RARP).

Our system adopts address resolution in two types: ARP and proxy ARP. The ARP and proxy ARP are defined in RFC 860 and 1027 respectively.

ARP is used to map IP addresses to media or MAC address. When the IP address is known, ARP will find the corresponding MAC address. When the MAC address is known, the mapping relationship between IP address and MAC address is saved in ARP cache for rapid access. The IP message is then packaged in the message at the link layer and at last is sent to the network.

- Defining a static ARP cache

  ARP and other address resolution protocols provide a dynamic mapping between IP address and MAC address. The static ARP cache item is generally not required because most hosts support dynamic address resolution. You can define it in global configuration mode if necessary. The system utilizes the static ARP cache item to translate the 32-bit IP address into a 48-bit MAC address. Additionally, you can specify the routing switch to respond to the ARP request for other hosts.

  You can set the active period for the ARP items if you do not want the ARP item to exist permanently. The following two types show how to configure the mapping between the static IP address and the MAC address.

  Run one of the following commands in global configuration mode:

Run…	To…
arp ip-address hardware-address	Globally map an IP address to a MAC address in the ARP cache.
arp ip-address hardware-address **alias**	Specify the routing switch to respond to the ARP request of the designated IP address through the MAC address of the routing switch.

  Run the following command in interface configuration mode:

Run…	To…
arp timeout *seconds*	Set the timeout time of the ARP cache item in the ARP cache.

  Run **show interfaces to display the ARP timeout time of the designated interface. Run the show arp to check the content of the ARP cache. Run clear arp-cache to delete all items in the ARP cache.**

- Activating proxy ARP

  The system uses the proxy ARP (defined by RFC 1027) to obtain the host's MAC address on other networks for the hosts without corresponding routes. For example, when the routing switch receives an ARP request and finds that the source host and the destination host are not connected to the same interface and all the routes that the routing switch reaches the destination host are not

through the interface that receives the ARP request, it will send a proxy ARP response that contains its address of the link layer. The source host then sends the message to the routing switch and the switch forwards it to the destination host. The proxy ARP is activates by default.

To activate the proxy ARP, run the following command in interface configuration mode:

Run…	To…
ip proxy-arp	Activate the proxy ARP on the interface.

- Configuring free ARP function

  The switch can know whether the IP addresses of other devices collide with its IP address by sending free ARP message. The source IP address and the destination IP address contained by free ARP message are both the local address of the switch. The source MAC address of the message is the local MAC address.

  The switch processes free ARP message by default. When the switch receives free ARP message from a device and finds that the IP address contained in the message collide with its own IP address, it will return an ARP answer to the device, informing the device that the IP addresses collide with each other. At the same time, the switch will inform users by logs that IP addresses collide.

  The switch's function to send free ARP message is disabled by default. Run the following commands to configure the free ARP function on the port of the switch:

Run…	To…
arp send-gratuitous	Start up free ARP message transmission on the interface.
arp send-gratuitous interval *value*	Set the interval for sending free ARP message on the interface. The default value is 120 seconds.

2. Mapping host name to IP addres

Any IP address can correspond to a host name. The system stores a hostname-to-address mapping cache that you can telnet or ping.

Run the following command in global configuration mode to specify a mapping between host name and IP address:

Run…	To…
ip host *name address*	Statically map the host name to the IP address.

1.3.4 Configuring Routing Process

You can configure one or multiple routing protocols according to your actual network requirements. The routing protocol provides information about the network topology. The details about configuring IP routing protocols such as BGP, RIP and OSPF are shown in the following sections.

1.3.5 Configuring Broadcast Message Handling

The destination addresses of the broadcast message are all the hosts on a physical network. The host can identify the broadcast message through special address. Some protocols, including some important Internet protocols, frequently use the broadcast message. One primary task of the IP network administrator is to control the broadcast message. The system supports the directed broadcast, that is, the broadcast of designated network. The system does not support the broadcast of all subnets in a network.

Some early-stage IP's do not adopt the current broadcast address standard. The broadcast address adopted by these IP's is represented completely by the number "0". The system can simultaneously identify and receive message of the two types.

1. Allowing translating from directed broadcast to physical broadcast

The directed IP broadcast message will be dropped by default, preventing the switch from attacking by message "service rejected".

You can activate the function of forwarding directed IP broadcast on the interface where the directed broadcast is transformed to the physical message. If the forwarding function is activated, all the directed broadcast message of the network that connects the interface will be forwarded to the interface. The message then will be sent as the physical broadcast message.

You can designate an access table to control the forwarding of broadcast message. After the access table is specified, only IP message that the access table allows can be transformed from the directed broadcast to the physical broadcast.

Run the following command in interface configuration mode to activate the forwarding of the directed broadcast.

Run…	To…
ip directed-broadcast [*access-list-name*]	Allow the translation from the directed broadcast to the physical broadcast on the interface.

2. Forwarding UDP broadcast message

Sometimes, the host uses the UDP broadcast message to determine information about the address, configuration and name, and so on. If the network where the host is located has no corresponding server to forward the UDP message, the host cannot receive any of the UDP message. To solve the problem, you can do some configuration on the corresponding interface to forward some types of broadcast message to an assistant address. You can configure multiple assistant addresses for an interface.

You can designate a UDP destination port to decide which UDP message is to be forwarded. Currently, the default forwarding destination port of the system is port 137.

Run the following command in interface configuration mode to allow message forwarding and to specify the destination address:

Run…	To…
ip helper-address *address*	Allow to forward the UDP broadcast message

	and to specify the destination address.

Run the following command in global configuration mode to specify protocols to be forwarded:

Run…	To…
ip forward-protocol udp [*port*]	Specify which interfaces' UDP protocols will be forwarded.

1.3.6 Detecting and Maintaining IP Addressing

Perform the following operations to detect and maintain the network:

1. Clearing cache, list and database

You can clear all content in a cache, list or the database. When you think some content is ineffective, you can clear it.

Run the following command in management mode to clear the cache, list and database:

Run…	To…
clear arp-cache	Clear the IP ARP cache.

2. Displaying statistics data about system and network

The system can display designated statistics data, such as IP routing table, cache and database. All such information helps you know the usage of the systematic resources and solve network problems. The system also can display the reachability of the port and the routes that the message takes when the message runs in the network.

All relative operations are listed in the following table. For how to use these commands, refer to Chapter "IP Addressing Commands".

Run the following commands in management mode:

Run…	To…
show arp	Display content in the ARP table.
show hosts	Display the cache table about hostname-to-IP mapping.
show ip interface [*type number*]	Display the interface state.
show ip route [*protocol*]	Display the current state of the routing table.
ping {**host	address**}	Test the reachability of the network node.

1.4 IP Addressing Example

The following case shows how to configure the IP address on interface VLAN 11.

interface vlan 11

ip address 202.96.2.3 255.255.255.0

Chapter 2 Configuring NAT

2.1 Introduction

The Internet faces two key problems: insufficient IP address space and route measurement. Network Address Translation (NAT) is an attribute. You can find that a group of IP networks with this attribute use different IP address spaces, but you cannot find the actual address space used by the group of networks. By transforming these addresses to the address spaces that can be globally routed, NAT permits an organization without global routing addresses to connect the Internet. NAT also permits good recoding strategy to change the service providers for the organizations or to automatically code to the CIDR module. NAT will be described in RFC 1631.

2.1.1 NAT Application

Main NAT applications are shown as follows:

- All hosts need to connect to the Internet, but no all hosts have a unique global IP address. NAT enables unregistered networks with private IP addresses to connect the Internet. NAT are always configured at the routing switch between inside network and Internet. Before sending message to the Internet, NAT transfers the inside local address to the unique global IP address.

- The inside address has to be modified. You can transform the address by using NAT without too much time.

- The basic TCP transmission load balance need be realized. You can map a single global IP address to multiple IP addresses using TCP load distribution characteristic.

- As a resolution for connection problems, NAT can be used when relatively few hosts in an inside network communicate with the Internet. In this case, the IP addresses of few hosts will be transformed to a unique global IP address when they communicate with the Internet. These addresses can be reused when they are not used any more.

2.1.2 NAT Advantage

An obvious advantage of NAT is that you can perform configuration without modifying host or switch. As said above, NAT is useless if many hosts in a single-connection domain communicate with the outside. What's more, the NAT device is not suitable to translate the embedded IP address. These applications cannot work transparently or completely (without translation) pass through a NAT device. NAT hides the identifier of the host, which may be an advantage or a shortcoming.

The router configured with NAT has at least one inside interface and one outside interface. In typical case, NAT is configured at the router between the single-connection domain and the backbone domain. When a message is leaving the single-connection domain, NAT transforms the effective local address to a unique

global address. When the message reaches the domain, NAT transforms the unique global address to the local address. If multiple interfaces exist, each NAT must have the same the transfer table. If no address is available, the software cannot distribute an address and NAT will drop the message and returns an ICMP message indicating the host cannot be reached.

The switch with NAT configured should not publish the local network. However, the routing information that NAT receives from the outside can be published in the single-connection domain.

2.1.3 NAT Terms

As said above, the term “inside” means those networks which are possessed by organizations and have to be transformed. In this domain, the host has an address in one address space. At the outside, the host will possess an address in another address space when the NAT is configured. The first address space means the local address space, while the second address space means the global address space.

Similarly, the term “outside” means the network that the single network connects, generally out of control of an organization. The addresses of the hosts in the outside network need to translate a certain address and may be classified into two types of addresses: local address and global address.

NAT uses the following definitions:

- Inside local address: IP address that is allocated to a host in the inside network. The address may not be the legal IP address distributed by Network Information Center (NIC) or service provider (SP).
- Inside global address: legal IP address distributed by NIC or SP, describing one or multiple IP addresses for the outside network.
- Outside local address: IP address of the outside host that appears in the inside network. It may be illegal. It can be distributed through the routable address space in the inside network.
- Outside global address: IP address that the owner of the host distributes to the host in the outside network, which can be distributed from the global address space or the network space.

2.1.4 NAT Regulation Matching Order

When NAT translates message, the configured NAT regulations must first be matched. There are three classes of NAT regulations: inside source address mapping, outside source address mapping and inside destination address mapping. Each class has its own subclasses. The following case takes the inside source address mapping as an example to introduce the subclass order of the NAT matching regulations:

- Static TCP/UDP port mapping regulation
- Static single address mapping regulations
- Static network segment mapping regulations

- Dynamic POOL address mapping regulations
- PAT mapping regulations

The regulations in the same subclass in the same class and the three classes are matched according the sequence they are being added. When you run the **show running** command, the order to display the NAT regulations is the same as the actual matching order.

2.2 NAT Configuration Task List

Before configuring any NAT, you must know the range of the inside local address and inside global address. The NAT configuration task list is shown as follows:

- Translating inside source address
- Reloading inside global address
- Translating the overlapping address
- Providing TCP load balance
- Changing translation timeout time and limiting the number of connections
- Monitoring and maintaining NAT

2.3 NAT Configuration Task

2.3.1 Translating Inside Source Address

When the host communicates with the outside network, it uses the attribute (translating inside source address) to translate its IP address to the unique global IP address. You can configure the static or dynamic inside source address translation through the following method:

The static translation creates the one-to-one mapping between inside local address and inside global address. When an inside host is accessed by a fixed outside address, the static translation is useful.

The dynamic translation creates the mapping between inside local address and outside address pool.

The following figure shows a routing switch translates the source address inside a network to the source address outside the network.

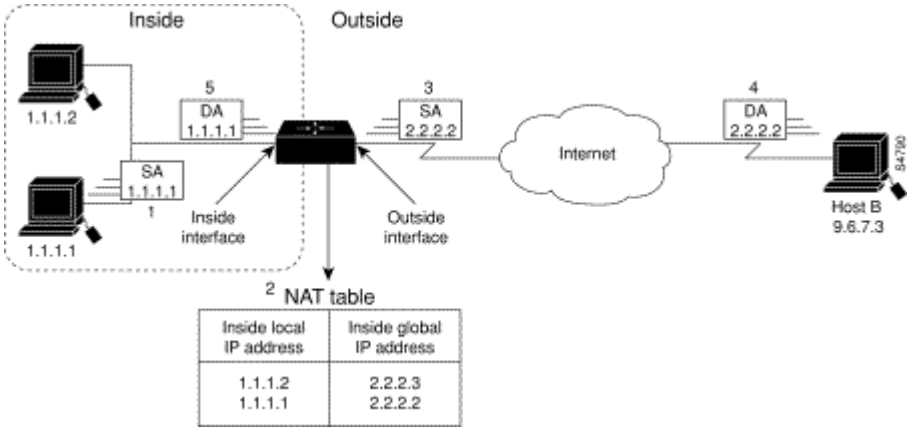


Figure 2-1 NAT Inside Source Address Transfer

The following steps show the inside source address translation.

(1) The user of host 1.1.1.1 creates a connection between host 1.1.1.1 and host B.

(2) The first packet received by the routing switch from host 1.1.1.1 makes the routing switch check the NAT table.

If a static translation item has been configured, the switch is to perform step 3.

If no translation exists, the switch decides that the source address (SA) 1.1.1.1 must be translated dynamically, then chooses a legal global address from the dynamic address pool, and finally generates a translation item. The type item is called as simple item.

(3) The routing switch replaces the inside local source address with the global address of the transfer item and forwards the message.

(4) Host B receives the message through inside global IP destination address (DA) 2.2.2.2 and responds to host 1.1.1.1.

(5) When the routing switch receives message of the inside global IP address, it takes the inside global address as a keyword to query the NAT table, translates the address to the inside local address of host 1.1.1.1, and forwards message to host 1.1.1.1.

(6) Host 1.1.1.1 receives the message and continues the session. The routing switch is to perform step 2 and step 5 for each message.

1. Configuring static transfer

Run the following commands in global configuration mode to configure static inside source address transfer:

Run…	To…
ip nat inside source static *local-ip global-ip*	Create a static transfer between inside local address and inside global address.

interface *type number*	Specify the inside interface.
ip nat inside	Label the interface as one to connect the inside network.
interface *type number*	Specify the outside interface.
ip nat outside	Label the interface as one to connect the outside network.

The above is the minimum configuration. You can configure multiple inside and outside interfaces.

2. Configuring dynamic transfer

Run the following commands in global configuration mode to configure dynamic inside source address translation.

Run…	To…
ip nat pool name start-ip end-ip netmask	Define a to-be-allocated global address pool according to your requirements.
ip access-list standard access-list-name permit source [source-mask]	Define a standard access list to permit which address can be transferred.
ip nat inside source list access-list-name **pool** name	Create dynamic source address transfer and specify the access list that is defined at the previous step.
interface type number	Specify the inside interface.
ip nat inside	Label the interface as one to connect the inside network.
interface type number	Specify the outside interface.
ip nat outside	Label the interface as one to connect the outside network.

Note:

Only those transferable addresses can be contained in the access list (remember that an implicit item “deny all” exists at the end of each access list). The random access list may lead to unexpected results.

Refer to section 2.4.1 “Dynamic Inside Source Address Transfer Example” for details.

2.3.2 Reloading Inside Global Address

Multiple local addresses use one global address through the routing switch. All the addresses can be stored in the inside global address pool. When the reloading is configured, the routing switch maintains sufficient information from high-level protocols (such as TCP or UDP) and transfers the global address to the correct local address. When multiple local addresses are mapped to one global address, TCP or UDP port numbers of each inside host are used to label multiple local addresses.

The following figure shows the NAT operation when an inside global address represents multiple local addresses. TCP port number is used to label the local address.

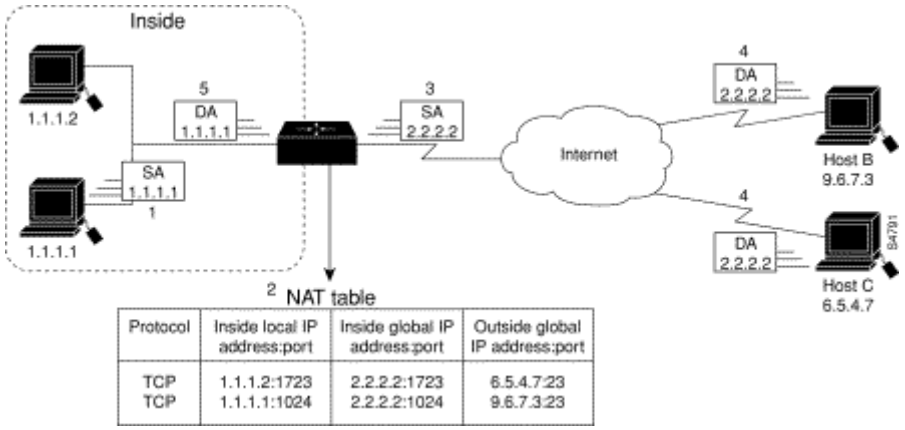


Figure 2-2 NAT Operation During the Reloading of Inside Global Address

The routing switch performs the following steps in the reloaded inside global address. Host B and host C think that they are communicating with host 2.2.2.2. However, they are communicating with different hosts in fact. The port number is the identifier. In fact, multiple inside hosts can share one inside global IP address using different port numbers.

(1) The user of host 1.1.1.1 creates a connection between host 1.1.1.1 and host B.

(2) The routing switch receives the first message from host 1.1.1.1 and then checks its NAT table.

If no transfer items exist, the switch decides that address 1.1.1.1 must be translated, and then creates a translation between inside local address 1.1.1.1 and legal global address. If the reloading is successful, another translation is started up. The switch reuses the global address in the previous translation and saves sufficient transferable information. The item is called as the expansion item.

(3) The routing switch replaces the inside local source address 1.1.1.1 with the selected global address, and then forwards a packet.

(4) Host B receives the packet and responds to host 1.1.1.1 using inside global IP address 2.2.2.2.

(5) When the routing switch receives the packet with the inside global IP address, it uses the protocol, inside global address, outside address and port as the keywords to search the NAT table. After that, it transfers the address to the inside local address 1.1.1.1 and forwards the packet to host 1.1.1.1.

(6) Host 1.1.1.1 receives the packet and continues the session. The routing switch performs step 2 and step 5 for each packet.

Run the following commands in global configuration mode to configure the reloading of the inside global address:

Run…	To…
ip nat pool name start-ip end-ip netmask	Define a to-be-distributed global address pool according to requirements.
ip access-list standard access-list-name **permit** source [source-mask]	Define a standard access list.
ip nat inside source list access-list-name **pool** name overload	Create dynamic inside source address transfer and decide the access list previously defined.
interface type number	Specify the inside interface.
ip nat inside	Label the interface as one to connect the inside network.
interface type number	Specify the outside interface.
ip nat outside	Label the interface as one to connect the outside network.

Note:

Only those transferable addresses can be contained in the access list (remember that an implicit item “deny all” exists at the end of each access list). The random access list may lead to unexpected results.

Refer to section 2.4.2 “Inside Global Address Reloading Example” for details.关

2.3.3 Translating Overlapping Addresses

When an internal local address is the same as the to-be-connected outside address, address overlapping occurs. The following figure shows how NAT translates the overlapping addresses.

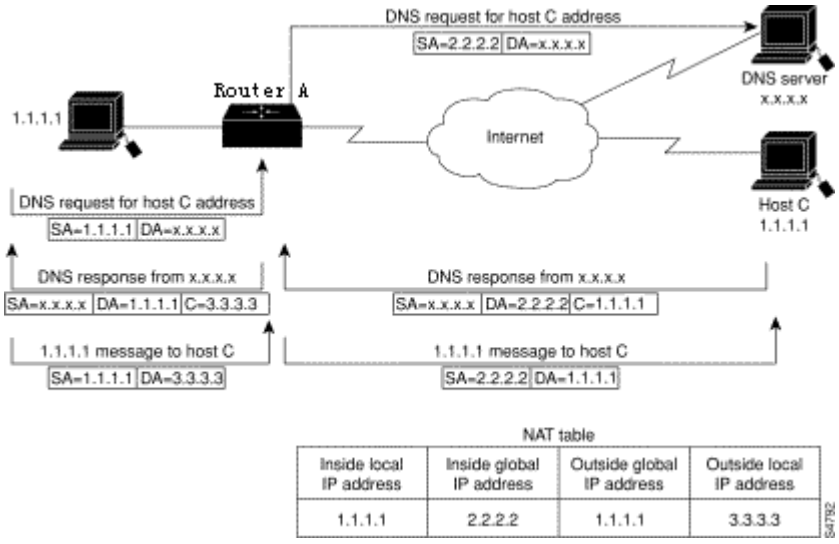


Figure 2-3 Network Condition Where NAT Translates Overlapping Addresses

The routing switch performs the following steps when translating the overlapping addresses:

(1) The user of host 1.1.1.1 uses domain name to send instructions for connecting host C. Host 1.1.1.1 requires DNS server to perform a checkup from domain name to address.

(2) The DNS server responds the request and returns the address 1.1.1.1 of host C. The routing switch intercepts the DNS response message and selects an outside local address from the outside local address pool to replace the source address. In this case, the source address 1.1.1.1 is replaced with address 3.3.3.3.

(3) The routing switch creates a mapping table about address transfer, where inside local addresses and inside global addresses map each other, outside global address and outside local address map each other.

(4) Host 1.1.1.1 sends message to host C . The destination IP address is the outside local address 3.3.3.3.

(5) When switch A receives message whose destination address is the outside local address, switch A transfers the local address to the global address.

(6) Host C receives the packet and continues the session.

1. Configuring static transfer

Run the following commands in global configuration mode to configure static source address translation:

Run…	To…
ip nat outside source static *global-ip local-ip*	Creates static translation between outside local address and outside global address.
interface *type number*	Specify the inside interface.
ip nat inside	Label the interface as one to connect the inside network.
interface *type number*	Specify the outside interface.
ip nat outside	Label the interface as one to connect the outside network.

2. Configuring dynamic transfer

Run the following commands in global configuration mode to configure dynamic outside source address transfer:

Run…	To…
ip nat pool *name start-ip end-ip netmask*	Define a to-be-distributed local address pool according to requirements.
ip access-list standard *access-list-name* **permit** source [*source-mask*]	Define a standard access list.
ip nat outside source list *access-list-name* **pool** *name*	Create dynamic outside source address transfer and decide the access list previously defined.
interface type *number*	Specify the inside interface.

ip nat inside	Label the interface as one to connect the inside network.
interface type *number*	Specify the outside interface.
ip nat outside	Label the interface as one to connect the outside network.

Note:

Only those transferable addresses can be contained in the access list (remember that an implicit item “deny all” exists at the end of each access list). The random access list may lead to unexpected results.

For details, refer to section“Overlapping Address Translation Example”.

2.3.4 Providing TCP Load Balance

Another fashion of using NAT is unrelated to the Internet address. Your organization may have multiple hosts to communicate with a frequently used host. In this case, you can use NAT technology to create a virtual host in the inside network, helping the load balance among actual hosts. You need to replace the destination address of the access list with the address in the cycle address pool. The distribution is complete in a cycle when a new connection from the outside to the inside is opened. The non-TCP communication need not be translated (unless other translations are effective). The following figure illustrates the attribute.

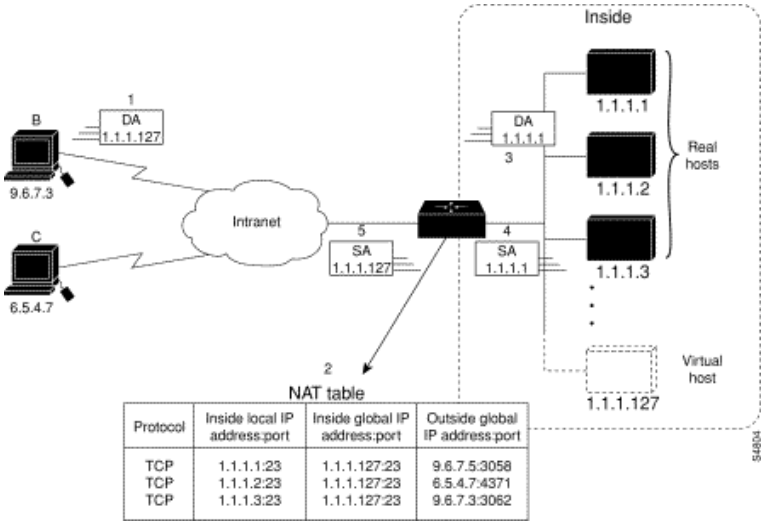


Figure 2-4 NAT TCP load balance

When translating the cycle address, the routing switch performs the following steps:

(1) The user of host B (9.6.7.3) sends instructions for connecting the virtual host 1.1.1.127 in the inside network.

(2) The routing switch receives the connection request and creates a new translation item to allocate the next host 1.1.1.1 for the inside local IP address.

(3) The routing switch replaces the destination address with the selected actual address of the host, and forwards the message.

(4) Host 1.1.1.1 receives the message and makes response.

(5) The routing switch receives the message and uses the inside local addresses and their port numbers, the outside address and port number as keywords to check the NAT table. The routing switch then transfers the source address to the address of the virtual host, and forwards the message.

(6) Next connection request invokes the routing switch to distribute address 1.1.1.2 for the inside local address. To configure the destination address transfer, run the following commands in global configuration mode. These commands permit to map one virtual host to multiple real hosts. Each TCP session with the virtual host will be transferred to the sessions with different real hosts.

(7)

Run...	To...
ip nat pool name start-ip end-ip netmask	Define an address pool containing the addresses of real hosts.
ip access-list standard access-list-name **permit** source [source-mask]	Define an access table permitting addresses of virtual hosts.
ip nat inside destination list access-list-name **pool** name	Create a dynamic inside target transfer mechanism and confirm the previously defined access list.
interface type number	Specify the inside interface.
ip nat inside	Label the interface as one to connect the inside network.
interface type number	Specify the outside interface.
ip nat outside	Label the interface as one to connect the outside interface.

Note:

Only those transferable addresses can be contained in the access list (remember that an implicit item “deny all” exists at the end of each access list). The random access list may lead to unexpected results.

For details, refer to section “TCP Load Configuration Example”.

2.3.5 Changing Translation Timeout Time and Limiting the Number of Connections

After a period of leisure, the dynamic Network Address Translation (NAT) is to time out by default. If the reloading is not configured, the simple translation item is to time out after one hour. You can run the following command to in global configuration mode to change the timeout value.

Run...	To...
ip nat translation timeout *seconds*	Change the timeout value of the dynamic NAT without reloading.

If the reloading is configured, the translation timeout will be better controlled because every translation item contains more contents. To change the timeout value of the expansible item, run one or most of the following commands in global configuration mode.

Run...	To...
ip nat translation udp-timeout *seconds*	Change the UDP timeout value (the default value is five seconds).
ip nat translation dns-timeout *seconds*	Change the DNS timeout value (the default value is one second).
ip nat translation tcp-timeout *seconds*	Change the TCP timeout value (the default value is one hour).
ip nat translation icmp-timeout *seconds*	Set the timeout time of the ICMP NAT (the default time is 60 seconds).
ip nat translation syn-timeout *seconds*	Set the timeout time of the NAT in the TCP SYN state (the default time is 60 seconds).
ip nat translation finrst-timeout *seconds*	Change the TCP FIN/RST timeout value (the default value is 60 seconds).

There are three methods to limit the NAT connections. Run the following commands in global configuration mode to realize the three methods.

Run...	To...
ip nat translation max-entries *numbers*	Set the maximum number of the translation items (the default value is 4000).
ip nat translation max-links A.B.C.D *numbers*	Limit the maximum number of the NAT connection items that the designated inside IP address creates. There is no default value.
ip nat translation max-links all *numbers*	Limit the maximum number of the NAT connection items that a single IP address creates. The default value is the same as max-entries.

2.3.6 Monitoring and Maintaining NAT

The dynamic NAT is to time out by default according to the time regulated by the NAT transfer table. You can run the following commands in management mode to clear up the timeout item before the timeout occurs.

Run...	To...
clear ip nat translation *	Clear up all transfer items from the NAT transfer table.
clear ip nat translation inside *local-ip global-ip* [outside *local-ip global-ip*]	Clear up a simple dynamic translation item containing inside translation, outside translation or both.
clear ip nat translation outside *local-ip global-ip*	Clear up a simple dynamic translation item containing outside translation.
clear ip nat translation inside *local-ip local-port global-ip global-port* [outside *local-ip local-port global-ip global-port*]	Clear up expansible dynamic translation items.

Run one of the following commands in management mode to display the transfer information:

Run...	To...
show ip nat translations [verbose]	Display active translation.
show ip nat statistics	Display translation statistics.

2.4 NAT Configuration Example

2.4.1 Dynamic Inside Source Transfer Example

The following example shows how to transfer all source addresses (192.168.1.0/24) that matches access list a1 to one address in the net-208 pool whose address range is from 171.69.233.208 to 171.69.233.233.

```
ip nat pool net-208 171.69.233.208 171.69.233.233   255.255.255.240
ip nat inside source list a1 pool net-208
!
interface vlan10
 ip address 171.69.232.182 255.255.255.240
 ip nat outside
!
interface vlan11
 ip address 192.168.1.94 255.255.255.0
 ip nat inside
!
ip access-list    standard a1
 permit 192.168.1.0 255.255.255.0
!
```

2.4.2 Inside Global Address Reloading Example

An address pool named net-208 is created in the following example. The address pool contains all addresses from 171.69.233.208 to 171.69.233.233. The a1 access list permits all packets from source addresses from 192.168.1.0 to 192.168.1.255. If there is no transfer, packets matching the a1 access list are to be transferred to one address the net-208 address pool. The routing switch authorizes multiple local addresses (from 192.168.1.0 to 192.168.1.255) to use the same global address. The routing switch stores the port numbers to distinguish every connection.

```
ip nat pool net-208 171.69.233.208 171.69.233.233 255.255.255.240
ip nat inside source list a1 pool net-208 overload
!
interface vlan10
 ip address 171.69.232.182 255.255.255.240
 ip nat outside
!
interface vlan11
 ip address 192.168.1.94 255.255.255.0
```

```
 ip nat inside
!
ip access-list standard a1
 permit 192.168.1.0 255.255.255.0
!
```

2.4.3 Example to overlapping address transfer

The following example shows that other users in the Internet are legally using the address in the local network. Extra transfer is needed to access the outside network. The net-10 address pool is an outside local IP address pool. The sentence **ip nat outside source list 1 pool net-10** transfer the host addresses of the outside overlapping network to the address in the net-10 address pool.

```
ip nat pool net-208 171.69.233.208 171.69.233.223 255.2555.255.240
ip nat pool net-10 10.0.1.0 10.0.1.255 255.255.255.0
ip nat inside source list a1 pool net-208
ip nat outside source list a1 pool net-10
!
interface vlan10
 ip address 171.69.232.192 255.255.255.240
 ip nat outside
!
interface vlan11
 ip address 192.168.1.94 255.255.255.0
 ip nat inside
!
ip access-list standard a1
 permit 192.168.1.0 255.255.255.0
!
```

2.4.4 TCP Load Distribution Example

The following example shows that the connections between a virtual address and a group of actual hosts are distributed. The address pool defines the addresses of actual hosts. The access list defines the virtual address. The TCP packet that matches the access list and is from serial port 1/0 (outside interface) is to be translated to the address in the pool.

```
ip nat pool real-hosts 192.168.15.2 192.168.15.15 255.255.255.240
ip nat inside destination list a2 pool real-hosts
!
interface vlan10
 ip address 192.168.15.129 255.255.255.240
 ip nat outside
!
interface vlan11
 ip address 192.168.15.17 255.255.255.240
  ip nat inside
!
```

```
ip access-list standard a2
 permit 192.168.15.1 255.255.255.0
```

Chapter 3 Configuring DHCP

3.1 Introduction

The Dynamic Host Configuration Protocol (DHCP) provides some parameters of network configuration fro hosts in the Internet. DHCP will be described in RFC 2131. The most important function of DHCP is to distribute IP addresses on the interface. DHCP supports three mechanisms of distributing IP addresses.

- Automatic distribution

  The DHCP server automatically distributes a permanent IP address to a client.

- Dynamic distribution

  The DHCP server distributes an IP address for a client to use for a certain period of time or until the client does not use it.

- Manual distribution

The administrator of the DHCP server manually specifies an IP address and through the DHCP protocol sends it to the client.

3.1.1 DHCP Applications

DHCP has several kinds of applications. You can use DHCP in the following cases:

- You can distribute IP address, network segment and related sources (such as relevant gateway) to an Ethernet interface by configuring the DHCP client.

- When a switch that can access DHCP connects multiple hosts, the switch can obtain an IP address from the DHCP server through the DHCP relay and then distribute the address to the hosts.

3.1.2 DHCP Advantages

In current software version, the DHCP client or the DHCP client on the Ethernet interface is supported. The function to support the DHCP client has the following advantages:

- Reducing the configuration time

- Reducing configuration faults

- Controlling IP addresses of some device ports through the DHCP server

3.1.3 DHCP Terminology

DHCP is based on the Server/Client model. The DHCP-server and DHCP-client exist in the DHCP running conditions.

- DHCP-Server

  It is a device to distribute and recycle the DHCP-related sources such as IP addresses and lease time.

- DHCP-Client

  It is a device to obtain information from the DHCP server for devices of the local system to use, such as IP address information.

As described above, the lease time is a concept appearing in the procedure of DHCP dynamic distribution.

- Lease time—an effective period of an IP address since its distribution. When the effective period is over, the IP address is to be recycled by the DHCP server. To continuously use the IP address, the DHCP client requires re-applying the IP address.

3.2 Configuring DHCP Client

3.2.1 DHCP Client Configuration Tasks

- Obtaining an IP address
- Specifying an address for DHCP server
- Configuring DHCP parameters
- Monitoring DHCP

3.2.2 DHCP Client Configuration Tasks

1. Obtaining an IP address

Run the following command on the VLAN interface to obtain an IP address through the DHCP protocol for an interface.

Run...	To...
ip address dhcp	Specify the DHCP protocol to configure the IP address of the Ethernet interface.

2. Specifying an address for DHCP server

If the addresses of some DHCP servers are known, you can specify the addresses for these DHCP servers on the switch to reduce protocol interaction time. Run the following command in global configuration mode:

Run...	To...
ip dhcp-server *ip-address*	Specify the IP address of the DHCP server.

The command is optional when you perform operations to obtain an IP address.

3. Configuring DHCP parameters

You can adjust the parameters for the DHCP protocol interaction according to requirements. Run the following commands in global configuration mode:

Run...	To...
ip dhcp client minlease *seconds*	Specify the minimum lease time.
ip dhcp client retransmit *count*	Specify the times of resending protocol message.
ip dhcp client select *seconds*	Specify the interval for SELECT.

The command is optional when you perform operations to obtain an IP address.

4. Monitoring DHCP

To check information about DHCP-server currently found by switch, run the following command in management mode:

Run...	To...
show dhcp server	Display information about the DHCP server known by the routing switch.

Run the following command in management mode to check the IP address currently used by the routing switch:

Run...	To...
show dhcp lease	Display the IP address resources currently used by the routing switch and relevant information.

Additionally, if the DHCP protocol is used to distribute an IP address for an Ethernet interface, you can run **show interface** to check whether the IP address required by the Ethernet interface is successfully obtained.

3.2.3 DHCP Client Configuration Example

1. Obtaining an IP address

The following example shows Ethernet1/1 obtains an IP address through DHCP.

```
!
interface vlan 11
ip address dhcp
```

3.3 Configuring DHCP Server

3.3.1 DHCP Server Configuration Tasks

- Enabling DHCP server
- Disabling DHCP server
- Configuring ICMP detection parameter
- Configuring database storage parameter
- Configuring the address pool of DHCP server
- Configuring the parameter for the address pool of DHCP server
- Monitoring DHCP server
- Clearing information about DHCP server

3.3.2 Configuring DHCP Server

1. Enabling DHCP server

To enable the DHCP server and distribute parameters such as IP address for the DHCP client, run the following command in global configuration mode (the DHCP server also supports the relay operation. For the addresses that the DHCP server cannot distribute, the port where **ip helper-address** is configured is to forward the DHCP request):

Run...	To...
ip dhcpd enable	Enabling DHCP server.

2. Disabling DHCP server

To enable DHCP server and stop distributing parameters such as IP address parameter for the DHCP client, run the following command in global configuration mode:

Run...	To...
no ip dhcpd enable	Disable DHCP server.

3. Configuring ICMP detection parameter

You can adjust the parameter of the to-be-sent ICMP message when the server performs address detection. Run the following command in global configuration mode to configure the number of to-be-sent ICMP messages:

Run...	To...
ip dhcpd ping packets *pkgs*	Specify the times of address detection as the number of to-be-sent ICMP message.

Run the following command in global configuration mode to configure the timeout time of ICMP message response:

Run...	To...
ip dhcpd ping timeout *timeout*	Specify the timeout time of ICMP message response.

4. Configuring database storage parameter

To configure the interval when the address distribution information is stored in the agent database, run the following command in global configuration mode.

Run...	To...
ip dhcpd write-time *time*	Specify the interval at which the address distribution information is stored in the agent database.

5. Configuring DHCP server address pool

Run the following command in global configuration mode to add the address pool for the DHCP server:

Run...	To...
ip dhcpd pool *name*	Add the address pool of the DHCP server and enter the configuration mode of the DHCP address pool.

6. Configuring DHCP server address pool

You can run the following commands in DHCP address pool configuration mode to configure related parameters.

Run the following command to configure the network address of the address pool which is used for automatic distribution.

Run...	To...
network *ip-addr netsubnet*	Configure the network address of the address pool which is used for automatic

	distribution.

Run the following command to configure the address range that is used for automatic distribution.

Run...	To...
range *low-addr high-addr*	Configure the address range that is used for automatic distribution.

Run the following command to configure the default route that is distributed to the client:

Run...	To...
default-router *ip-addr …*	Configure the default route that is distributed to the client.

Run the following command to configure the DNS server address that is distributed to the client:

Run...	To...
dns-server *ip-addr …*	Configure the DNS server address that is distributed to the client.

Run the following command to configure domain that is distributed to the client:

Run...	To...
domain-name *name*	Configure domain that is distributed to the client.

Run the following command to configure the lease time of the address that is distributed to the client:

Run...	To...
lease {*days* [*hours*][*minutes*] | *infinite* }	Configure the lease time of the address that is distributed to the client.

Run the following command to configure the netbios server address that is distributed to the client:

Run...	To...
netbios-name-server *ip-addr…*	Configure the netbios server address that is distributed to the client.

You can run the following command to reject to distribute the IP address to the host whose MAC address is hardware-address.

Run…	To…
hw-access deny hardware-address	Reject to distribute IP addresses to the host whose MAC address is hardware-address.

7. Monitoring DHCP server

Run the following command in management mode to check current address distribution information about DHCP server.

Run…	To…
show ip dhcpd binding	Display current address distribution information about DHCP server.

Run the following command in management mode to check current message statistics information about DHCP server.

Run…	To…
show ip dhcpd statistic	Display current message statistics information about DHCP server.

8. Clearing up information about DHCP server

Run the following command in management mode to delete current address distribution information about DHCP server:

Run...	To...
clear ip dhcpd binding {*ip-addr*|*}	Delete the designated address distribution information.

Run the following command in management mode to delete current message statistics information about DHCP server.

Run...	To...
clear ip dhcpd statistic	Delete current message statistics information about DHCP server.

3.3.3 DHCP Server Configuration Example

In the following example, the timeout time of the ICMP detection packet is set to 200ms; Address pool 1 is configured and the DHCP server is enabled.

```
ip dhcpd ping timeout 2
ip dhcpd pool 1
 network 192.168.20.0 255.255.255.0
 range 192.168.20.211 192.168.20.215
 domain-name my315
 default-router 192.168.20.1
 dns-server 192.168.1.3 61.2.2.10
 netbios-name-server 192.168.20.1
 lease 1 12 0
!
ip dhcpd enable
```

Chapter 4 IP Service Configuration

It is to describe how to configure optional IP service. For the details of the IP service commands, refer to section “IP Service Commands”.

4.1 Configuring IP Service

Optional IP service configuration tasks are listed as follows:

- Managing IP connection
- Configuring performance parameters
- Configuring default gateway
- Detecting and maintaining IP network

The above operations are not mandatory. You can perform the operations according to your requirements.

4.1.1 Managing IP Connection

The IP protocol provides a series of services to control and manage IP connections. Most of these services are provided by ICMP. The ICMP message is sent to the host or other routing switches when the routing switch or the access server detects faults in the IP message header. ICMP is mainly defined in RFC 792.

Perform the following different operations according to different IP connection conditions:

1. Sending ICMP unreachable message

If the system receives a message and cannot send it to the destination, such as no routes, the system will send an ICMP-unreachable message to the source host. The function of the system is enabled by default.

If the function is disabled, you can run the following command in interface configuration mode to enable the function.

Run…	To…
ip unreachables	Enable the function to send an ICMP-unreachable message.

2. Sending ICMP redirection message

Sometimes the host selects an unfavorable route. After a routing switch on the route receives a message from the host, it is to check the routing table and then forward the message through the message-receiving interface to another routing switch that is in

the same network segment as the host. In this case, the routing switch notifies the source host of directly sending the message with the destination to another routing switch without winding itself. The redirection message requires the source host to discard the original route and take more direct route suggested in the message. Many host's operating system adds a host route to its routing table. However, the routing switch is more willing to trust information obtained through the routing protocol. Therefore, the routing switch would not add the host route according to the information.

The function is enabled by default. If the hot standby routing switch protocol is configured on the interface, the function is automatically disabled. However, the function will not be automatically enabled even if the hot standby routing switch protocol is cancelled.

To enable the function, run the following command in interface configuration mode:

Run…	To…
ip redirects	Permit sending the ICMP redirection messafge.

3. Sending ICMP mask response message

Sometimes the host must know the network mask. To get the information, the host can send the ICMP mask request message. If the routing switch can confirm the mask of the host, it will respond with the ICMP mask response message. By default, the routing switch can send the ICMP mask response message.

To send the ICMP mask request message, run the following command in interface configuration mode:

Run…	To…
ip mask-reply	Send the ICMP mask response message.

4. Supporting route MTU detection

The system supports the IP route MTU detection mechanism defined by RFC 1191. The IP route MTU detection mechanism enables the host to dynamically find and adjust to the maximum transmission unit (MTU) of different routes. Sometimes the routing switch detects that the received IP message length is larger than the MTU set on the message forwarding interface. The IP message needs to be segmented, but the "unsegmented" bit of the IP message is reset. The message, therefore, cannot be segmented. The message has to be dropped. In this case, the routing switch sends the ICMP message to notify the source host of the reason of failed forwarding, and the MTU on the forwarding interface. The source host then reduces the length of the message sent to the destination to adjust to the minimum MTU of the route.

If a link in the route is disconnected, the message is to take other routes. Its minimum MTU may be different from the original route. The routing switch then notifies the source host of the MTU of the new route. The IP message should be packaged with the minimum MTU of the route as much as possible. In this way, the segmentation is avoided and fewer message is sent, improving the communication efficiency.

Relevant hosts must support the IP route MTU detection. They then can adjust the length of IP message according to the MTU value notified by the routing switch, preventing segmentation during the forwarding process.

5. Setting IP maximum transmission unit

All interfaces have a default IP maximum transmission unit (MTU), that is, the transmissible maximum IP message length. If the IP message length exceeds MTU, the routing switch segments the message.

Changing the MTU value of the interface is to affect the IP MTU value. If IP MTU equals to MTU, IP MTU will automatically adjust itself to be the same as new MTU as MTU changes. The change of IP MTU, however, does not affect MTU. IP MTU cannot bigger than MTU configured on the current interface. Only when all devices connecting the same physical media must have the same MTU protocol can normal communication be created.

To set IP MTU on special interface, run the following command in interface configuration mode:

Run…	To…
ip mtu *bytes*	Set IP MTU of the interface.

6. Authorizing IP source route

The routing switch checks the IP header of every message. The routing switch supports the IP header options defined by RFC 791: strict source route, relax source route, record route and time stamp. If the switch detects that an option is incorrectly selected, it will send message about the ICMP parameter problem to the source host and drop the message. If problems occur in the source route, the routing switch will send ICMP unreachable message (source route fails) to the source host.

IP permits the source host to specify the route of the IP network for the message. The specified route is called as the source route. You can specify it by selecting the source route in the IP header option. The routing switch has to forward the IP message according to the option, or drop the message according to security requirements. The routing switch then sends ICMP unreachable message to the source host. The routing switch supports the source route by default.

If the IP source route is disabled, run the following command in global configuration mode to authorize the IP source route:

Run…	To…
ip source-route	Authorizing IP source route.

7. Allowing IP fast exchange

IP fast exchange uses the route cache to forward the IP message. Before the switch forwards message to a certain destination, its system will check the routing table and then forward the message according to a route. The selected route will be stored in the routing cache of the system software. If latter message will be sent to the same host, the switch will forward latter message according to the route stored in the routing cache. Each time message is forwarded, the value of hit times of the corresponding route item is increasing by 1. When the hit times is equal to the set value, the software routing cache will be stored in the hardware routing cache. The following message to the same host will be forwarded directly by the hardware. If the cache is not used for a period of time, it will be deleted. If the software/hardware cache items reach the upper limitation, new destination hosts are not stored in the cache any more. S3224

series switches can hold 2074 hardware cache items and 1024 software cache items. To allow or forbid fast exchange, run the following command in interface configuration mode:

Run…	To…
ip route-cache	Allow fast exchange (use the routing cache to forward the IP message).
no ip route-cache	Forbid fast exchange.

To configure the hit times required when the software cache items are stored to the hardware cache, run the following command in global configuration.

Run…	To…
ip route-cache hit-numbers *hitnumber*	When the hit times of the routing item in the software cache reaches the value of the parameter **hitnumber**, the routing item in the software cache will be stored as a routing item in the hardware cache.

8. Supporting IP fast exchange on the same interface

You can enable the switch to support IP fast exchange by making the receiving interface the same as the transmitting interface. Generally, it is recommended not to enable the function because it conflicts with the redirection function of the router.

Run the following command in interface configuration mode to allow IP routing cache in the same interface:

Run…	To…
ip route-cache *same-interface*	Allow IP message with the same receiving/transmitting interfaces to be stored in the routing cache.

4.1.2 Configuring Performance Parameters

1. Setting the wait time for TCP connection

When the routing switch performs TCP connection, it considers that the TCP connection fails if the TCP connection is not created during the wait time. The routing switch then notifies the upper-level program of the failed TCP connection. You can set the wait time for TCP connection. The default value of the system is 75 seconds. The previous configuration has no impact on TCP connections that the switch forwards. It only affects TCP connections that are created by the switch itself.

Run the following command in global configuration mode to set the wait time for TCP connections:

Run…	To…
ip tcp synwait-time *seconds*	Set the wait time for TCP connection.

2. Setting the size of TCP windows

The default size of TCP windows is 2000 byte. Run the following command in global configuration mode to change the default window size:

Run…	To…
ip tcp window-size *bytes*	Set the size of TCP windows.

4.1.3 Detecting and Maintaining IP Network

1. Clearing cache, list and database

You can clear all content in a cache, list or database. Incorrect data in a cache, list or database need be cleared.

Run the following command to clear incorrect data:

Run…	To…
clear tcp statistics	Clear TCP statistics data.

2. Clearing TCP connection

To disconnect a TCP connection, run the following command:

Run…	To…
clear tcp {**local** host-name port **remote** host-name port | **tcb** address}	Clear the designated TCP connection. TCB refers to TCP control block.

3. Displaying statistics data about system and network

The system can display the content in the cache, list and database. These statistics data can help you know the usage of systematic sources and solve network problems.

Run the following commands in management mode. For details, refer to “IP Service Command”.

Run…	To…
show ip access-lists *name*	Display the content of one or all access lists.
show ip cache [prefix mask] [type number]	Display the routing cache that is used for fast IP message exchange.
show ip sockets	Display all socket information about the routing switch.
show ip traffic	Display statistics data about IP protocol.
show tcp	Display information about all TCP connection states.
show tcp brief	Briefly display information about TCP

	connection states.
show tcp statistics	Display TCP statistics data.
show tcp tcb	Display information about the designated TCP connection state.

4. Displaying debugging information

When problem occurs on the network, you can run **debug** to display the debugging information.

Run the following command in management mode. For details, refer to “IP Service Command”.

Run…	To…
debug arp	Display the interaction information about ARP.
debug ip icmp	Display the interaction information about ICMP.
debug ip raw	Display the information about received/transmitted IP message.
debug ip packet	Display the interaction information about IP.
debug ip tcp	Display the interaction information about TCP.
debug ip udp	Display the interaction information about UDP.

4.2 Configuring Access List

4.2.1 Filtering IP Message

Filtering message helps control the movement of packet in the network. The control can limit network transmission and network usage through a certain user or device. To make packets valid or invalid through the crossly designated interface, our routing switch provides the access list. The access list can be used in the following modes:

Controlling packet transmission on the interface

Controlling virtual terminal line access

Limiting route update content

The section describes how to create IP access lists and how to use them.

The IP access list is an orderly set of the **permit/forbid** conditions for applying IP addresses. The ROS software of our switch tests the address one by one in the access list according to regulations. The first match determines whether the ROS accepts or declines the address. After the first match, the ROS software terminates the match regulations. The order of the conditions is, therefore, important. If no regulations match, the address is declined.

Use the access list by following the following steps:

(1) Create the access list by designating the access list name and conditions.

(2) Apply the access list to the interface.

4.2.2 Creating Standard and Extensible IP Access List

Use a character string to create an IP access list.

Note:

The standard access list and the extensible access list cannot have the same name.

Run the following command in global configuration mode to create a standard access list:

Run…	To…
ip access-list standard *name*	Use a name to define a standard access list.
deny {*source [source-mask]* | **any**}[**log**] or **permit** {*source [source-mask]* | **any**}[**log**]	Designate one or multiple **permit/deny** conditions in standard access list configuration mode. The previous setting decides whether the packet is approved or disapproved.
Exit	Log out from the access list configuration mode.

Run the following command in global configuration mode to create an extensible access list.

Run…	To…
ip access-list extended *name*	Use a name to define an extensible IP access list.
{**deny | permit**} *protocol source source-mask destination destination-mask* [**precedence** *precedence*] [**tos** *tos*] [**established**] [**log**]{**deny | permit**} *protocol* **any any**	Designate one or multiple **permit/deny** conditions in extensible access list configuration mode. The previous setting decides whether the packet is approved or disapproved. **precedence** means the priority of the IP packet; **TOS** means Type of Service.
Exit	Log out from the access list configuration mode.

After the access list is originally created, any part that is added later can be put at the end of the list. That is to say, you cannot add the command line to the designated access list. However, you can run **no permit** and **no deny** to delete items from the access list.

Note:

When you create the access list, the end of the access list includes the implicit **deny** sentence by default. If the mask is omitted in the relative IP host address access list, 255.255.255.255 is supposed to be the mask.

After the access list is created, the access list must be applied on the route or interface. For details, refer to section 4.2.3 “Applying the Access List to the Interface”.

4.2.3 Applying the Access List to the Interface

After the access list is created, you can apply it to one or multiple interfaces including the **in** interfaces and **out** interfaces.

Run the following command in interface configuration mode.

Run…	To…
ip access-group *name* **{in | out}**	Apply the access list to the interface.

The access list can be used on the **in** interfaces and the **out** interfaces. For the standard access list of the **in** interface, the soured address of the packet is to be checked according to the access list after the packet is received. For the extensible access list, the routing switch also checks the destination. If the access list permits the address, the software goes on processing the packet. If the access list does not permit the address, the software drops the packet and returns an ICMP unreachable message.

For the standard access list of the **out** interfaces, after a packet is received or routed to the control interface, the software checks the source address of the packet according to the access list. For the extensible access list, the routing switch also checks the access list of the receiving side. If the access list permits the address, the software will send the packet. If the access list does not permit the address, the software drops the packet and returns an ICMP unreachable message.

If the designated access list does not exist, all packets allows to pass.

4.2.4 Extensible Access List Example

In the following example, the first line allows any new TCP to connect the destination port after port 1023. The second line allows any new TCP to connect the SMTP port of host 130.2.1.2.

```
ip access-list extended aaa
permit tcp any 130.2.0.0 255.255.0.0 gt 1023
permit tcp any 130.2.1.2 255.255.255.255 eq 25
interface vlan 10
ip access-group aaa in
```

Another example to apply the extensible access list is given. Suppose a network connects the Internet, you expect any host in the Ethernet can create TCP connection with the host in the Internet. However, you expect the host in the Internet cannot create TCP connection with the host in the Ethernet unless it connects the SMTP port of the mail host.

During the connection period, the same two port numbers are used. The mail packet from the Internet has a destination port, that is, port 25. The outgoing packet has a contrary port number. In fact, the security system behind the routing switch always receives mails from port 25. That is the exact reason why the incoming service and the outgoing service can be uniquely controlled. The access list can be configured as the outgoing service or the incoming service.

In the following case, the Ethernet is a B-type network with the address 130.20.0.0. The address of the mail host is 130.20.1.2. The keyword **established** is only used for the TCP protocol, meaning a connection is created. If TCP data has the ACK or RST digit to be set, the match occurs, meaning that the packet belongs to an existing connection.

```
ip access-list aaa
permit tcp any 130.20.0.0 255.255.0.0 established
permit tcp any 130.20.1.2 255.255.255.255 eq 25
interface vlan 10
ip access-group aaa in
```

4.3 Configuring IP Access List Based on Physical Port

4.3.1 Filtering IP Message

4.3.2 Filtering IP Message

Filtering message helps control the movement of packet in the network. The control can limit network transmission and network usage through a certain user or device. To make packets valid or invalid through the crossly designated interface, our routing switch provides the access list. The access list can be used in the following modes:

Controlling packet transmission on the interface

Controlling virtual terminal line access

Limiting route update content

The section describes how to create IP access lists and how to use them.

The IP access list is an orderly set of the **permit/forbid** conditions for applying IP addresses. The ROS software of our switch tests the address one by one in the access list according to regulations. The first match determines whether the ROS accepts or declines the address. After the first match, the ROS software terminates the match regulations. The order of the conditions is, therefore, important. If no regulations match, the address is declined.

Use the access list by following the following steps:

(3) Create the access list by designating the access list name and conditions.

(4) Apply the access list to the interface.

4.3.3 Creating Standard and Extensible IP Access List

Use a character string to create an IP access list.

Note:

The standard access list and the extensible access list cannot have the same name.

Run the following command in global configuration mode to create a standard access list:

Run…	To…
ip access-list standard *name*	Use a name to define a standard access list.
deny {*source [source-mask]* | **any**}[**log**] or **permit** {*source [source-mask]* **| any**}[**log**]	Designate one or multiple **permit/deny** conditions in standard access list configuration mode. The previous setting decides whether the packet is approved or disapproved.
Exit	Log out from the access list configuration mode.

Run the following command in global configuration mode to create an extensible access list.

Run…	To…
ip access-list extended *name*	Use a name to define an extensible IP access list.
{**deny | permit**} *protocol source source-mask destination destination-mask* [**precedence** *precedence*] [**tos** *tos*] [**established**] [**log**]{**deny | permit**} *protocol* **any any**	Designate one or multiple **permit/deny** conditions in extensible access list configuration mode. The previous setting decides whether the packet is approved or disapproved. **precedence** means the priority of the IP packet; **TOS** means Type of Service.
Exit	Log out from the access list configuration mode.

After the access list is originally created, any part that is added later can be put at the end of the list. That is to say, you cannot add the command line to the designated access list. However, you can run **no permit** and **no deny** to delete items from the access list.

Note:

When you create the access list, the end of the access list includes the implicit **deny** sentence by default. If the mask is omitted in the relative IP host address access list, 255.255.255.255 is supposed to be the mask.

After the access list is created, the access list must be applied on the route or interface. For details, refer to section 4.2.3 “Applying the Access List to the Interface”.

4.3.4 Applying the Access List to the Interface

After the access list is created, you can apply it to one or multiple interfaces including the **in** interfaces and **out** interfaces.

Run the following command in interface configuration mode.

Run…	To…

ip access-group *name* **{in | out}**	Apply the access list to the interface.

The access list can be used on the **in** interfaces and the **out** interfaces. For the standard access list of the **in** interface, the soured address of the packet is to be checked according to the access list after the packet is received. For the extensible access list, the routing switch also checks the destination. If the access list permits the address, the software goes on processing the packet. If the access list does not permit the address, the software drops the packet and returns an ICMP unreachable message.

For the standard access list of the **out** interfaces, after a packet is received or routed to the control interface, the software checks the source address of the packet according to the access list. For the extensible access list, the routing switch also checks the access list of the receiving side. If the access list permits the address, the software will send the packet. If the access list does not permit the address, the software drops the packet and returns an ICMP unreachable message.

If the designated access list does not exist, all packets allows to pass.

4.3.5 Extensible Access List Example

1. Port-based IP access list supporting TCP/UDP port filtration

{**deny | permit**} {tcp | udp}

source source-mask [{ [src_portrange begin-port end-port] | [{gt | lt } port] }]

destination destination-mask [{ [dst_portrange begin-port end-port] | [{gt | lt } port] }]

[**precedence** *precedence*] [**tos** *tos*]

If you configure the access list by defining the port range, pay attention to the following:

- If you use the method of designating the port range to configure the access list at the source side and the destination side, some configuration may fail because of massive resource consumption. In this case, you need to use the fashion of designating the port range at one side, and use the fashion of designating the port at another side.
- When the port range filtration is performed, too many resources will be occupied. If the port range filtration is used too much, the access list cannot support other programs as well as before.

2. Port-based IP access list supporting TCP/UDP designated port filtration

In the following example, the first line allows any new TCP to connect the SMTP port of host 130.2.1.2.

```
ip access-list extended aaa
permit tcp any 130.2.1.2 255.255.255.255 eq 25
interface  f0/10
ip access-group aaa
```

Fast Ethernet Ring Protection Configuration

Table of Contents

Chapter 1 Introduction of Fast Ethernet Ring Protection

1.1 Overview

Ethernet ring protection protocol is a special type of link-layer protocol specially designed for constructing the ring Ethernet topology. The Ethernet protection protocol can shut down one link in a complete ring topology, preventing the data loop from forming the broadcast storm. If a link is broken, the protocol immediately resumes the link that is previously shut down. In this way, the nodes among the ring network can communicate with each other.

The Ethernet ring protection protocol can transmit data packets to the correct link by controlling the aging of the switch's MAC address table when the topology changes. In general, the time for a MAC address to age in the MAC address table is 300 seconds. The ring protection protocol can control the aging of the MAC address table in a short time.

The ring protection protocol and STP are both used for topology control on the link layer. STP is suitable for all kinds of complicated networks, which transmits the change of network topology hop by hop. The ring protection protocol is used for ring topology and adopts the pervasion mechanism to transmit the change of network topology. Therefore, the convergence of the ring protection protocol in the ring network is better than STP. In a sound network, the ring protection protocol can resume network communication within less than 50ms.

Note:
ring protection protocol supports that one switch is set to the node of multiple physical ring network, so that the tangency ring can be formed. The ring protection protocol does not support the tangency ring with public link.

1.2 Types of Ring Protection Protocol

Ethernet switch series support two types of ring protection protocol:

- Ethernet Automatic Protection Switching (EAPS), which is based on RFC-3619
- Ethernet Ring Protection Switching（ERPS）

Note:
Both switches of version 2.0.3 and hi-end switches of version 4.0.2B only support EAPS.

1.3 Basic Knowledge About Configuration of Ring Protection Protocol

Before the ring protection protocol is configured on the Ethernet switch, make sure that you have already read the following notices:

- One of important functions of the ring protection protocol is to stop the broadcast storm, so please make sure that before the ring link is reconnected all ring nodes are configured. For example, when EAPS is configured, after the master node and all transit nodes are configured, connect the network cable and the secondary port of the master node; when configuring ERPS, please keep at least one link disconnected until all ring nodes are configured. If the ring network is connected in the case that the configuration is not finished, the broadcast storm may easily occur.

- EAPS and ERPS are both reversible protection shift. For example, if a broken link of a port gets recovered, the protocol will change into the state before the shift.

- EAPS and ERPS can be configured on the same Ethernet switch at the same time, but they have to be used to control different ring networks. That is to say, EAPS and ERPS are incompatible and cannot run at the same time at the same ring network.

- The ring protection protocol can be running along with SSTP and RSTP at the same time and also can be running in the case that the STP is closed. The already set ring port will not take part in the calculation of the state of STP.

- switch software of version 2.0.3A and hi-end switch software of version 4.0.2B only support EAPS; switches of version 202A and hi-end switches of version 402A do not support the case that EAPS and STP are running at the same time.

- If the ring protection protocol is running without STP being shut down, we suggest configuring the **spanning-tree bpdu-terminal** function to prevent all ring nodes from forwarding BPDU and affecting the network performance.

- The ring protection protocol cannot be running along with MSTP at the same time. In case that EAPS or ERPS is configured, MSTP cannot be restarted.

- The ring protection protocol can configure a switch into multiple ring networks. But it does not support the complicated ring network with public links.

Chapter 2 EAPS Introduction

2.1 Related Concepts of EAPS

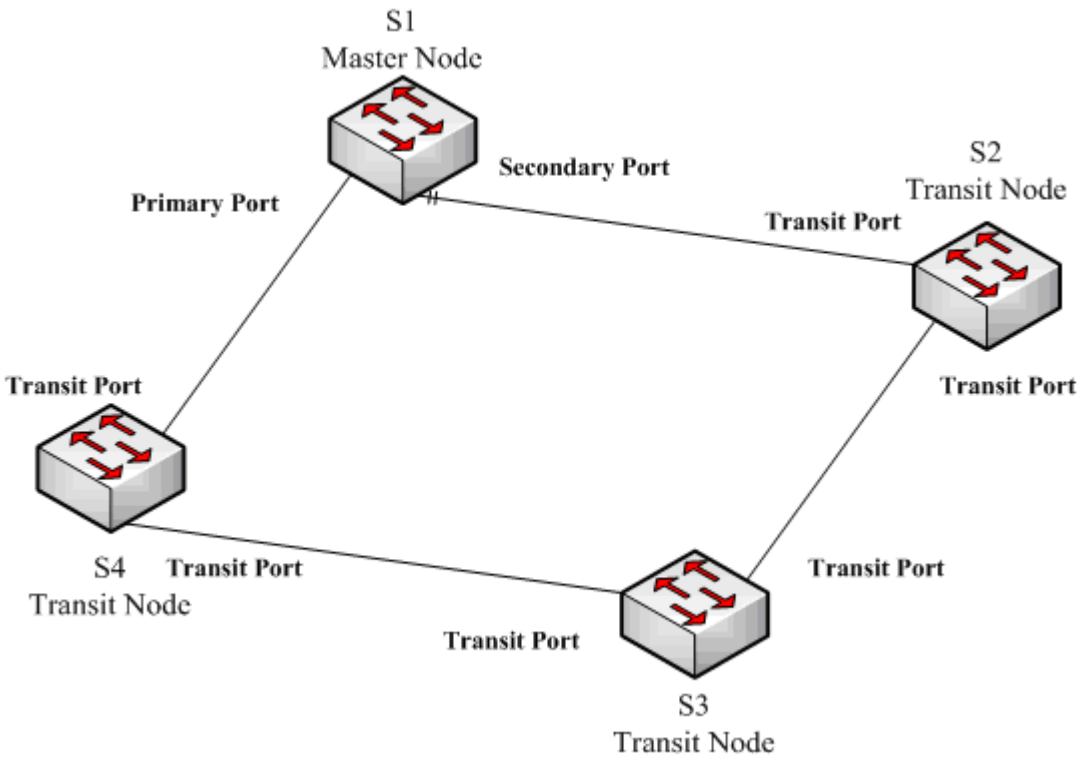


Figure 1.1 EAPS Ethernet ring

2.1.1 Roles of Ring's Nodes

Each switch on an Ethernet ring is a ring node. The ring nodes are classified into master nodes and transit nodes. Only one switch on the Ethernet ring can serve as a mere master node and other switches are worked as transit nodes.

Master node: It positively knows whether the ring's topology is complete, removes loopback, control other switches to update topology information.

Transit node: It only checks the state of the local port of the ring, and notifies the master node of the invalid link.

The role of each node can be specified by user through configuration. The thing is that each switch in the same ring can be set to only one kind of node. In figure 1.1, switch S1 is the master node of ring network, while switches S2, S3 and S4 are transit nodes.

2.1.2 Role of the Ring's Port

EAPS demands each switch has two ports to connect the ring network. Each port of the ring network also needs to be specified through configuration and the protocol supports the following kinds of port roles:

Primary port: the primary port can be configured only on the master node. The master node transmits the ring detection packets through the primary port.

Secondary port: the secondary port can be configured only on the master node. The master node receives the ring detection packets from the secondary port and judges whether the topology of the ring network is complete. In complete topology, the master node blocks the data packets on the secondary port, and prevents loopback from occurring; after a link on the ring network is interrupted, the master node removes the blocking state of the secondary port.

Transit port: the transmit port can only be configured on the transit node. Both ports through which the transit node connects the ring network are all transit ports.

Each port of the ring network can be configured as only one port role after the node's role of the switch and the control VLAN are configured. As shown in figure 1.1, the port through which master node S1 connects transit node S4 is a primary port, the port through which S1 connects S2 is a secondary port, and the ports through which other switches connect the ring network are all transit ports.

Note:
To configure a same switch to belong to multiple rings, the switch must connect different rings through different physical ports.

2.1.3 Control VLAN and Data VLAN

A private control VLAN is used between master node and transit node to transmit protocol packets. This control VLAN is specified by user through configuration and ring's ports are added also by user to the control VLAN, which guarantees that the protocol packets can be normally forwarded. In general, each port of the ring network is in the forwarding state in the control VLAN and the ports which do not belong to the ring network cannot forward the packets of control VLAN.

Note:
You can specify different control VLAN for each ring on a switch. The control VLAN is only used to forward the control packets of the ring network, not for L2/L3 communication. For example, if the VLAN port that corresponds to the control VLAN is established, the IP address of the VLAN port cannot be pinged through other devices.

The VLANs except the control VLAN are all data VLANs, which are used to transmit the packets of normal services or the management packets. It is the ring protection protocol that controls whether the port of the Ethernet ring can forward the packets of the data VLAN; the forwarding state of the non-ring port is controlled by STP.

Note:
The data VLAN can be used for normal L2/L3 communication. For example, you can establish a VLAN port corresponding to data VLAN and configure dynamic routing protocols.

2.1.4 Symbol of a Complete Ring Network

Both the master node and the transit node can show whether the current ring network is complete through the state symbol “COMPLETE”. On the master node, only when all links of the ring network are normal, the primary port is in forwarding state and the secondary port is in blocking state can the "COMPLETE” symbol be real; on the transit node, only when its two transit ports are in forwarding state can the “COMPLETE” symbol be true.

The state symbol of the ring network helps user to judge the topology state of the current network.

2.2 Type of EAPS Packets

The EAPS packets can be classified into the following types, as shown in table 1.1.

Table 1.1 Type of EAPS packets

Type of the packet	**Description**
HEALTH	It is transmitted by the master node to detect whether the topology of the ring network is complete.
LINK-DOWN	It is transmitted by the transit node to indicate that link interruption occurs in the ring network.
RING-DOWN-FLUSH-FDB	It is transmitted by the master node after interruption of the ring network is detected and the packets show the MAC address aging table of the transit node.
RING-UP-FLUSH-FDB	It is transmitted by the master node after interruption of the ring network is resumed and the packets show the MAC address aging table of the transit node.

2.3 EAPS Mechanism

2.3.1 Ring Detection and Control of Master Node

The master node transmits the HEALTH packets to the control VLAN through the primary port in a configurable period. In normal case, the HEALTH packets will pass through all other nodes of the ring network and finally arrive at the secondary port of the master node.

The secondary port blocks all data VLANs in primitive condition. When receiving the HEALTH packets continuously, the secondary port keeps blocking data VLANs and blocking the loop. If the secondary port does not receive the HEALTH packets from the primary port in a certain time (which can be configured), it will regard the ring network is out of effect. Then the master node removes the blocking of data VLANs on the secondary port, ages the local MAC address table, and transmits the RING-DOWN-FLUSH-FDB packets to notify other nodes.

If the master node receives the HEALTH packets at the secondary port that is open to data VLANs, the ring network is resumed. In this case, the master node immediately

blocks data VLANs on the secondary port, updates the local topology information and reports other nodes to age the MAC address table through RING-UP-FLUSH-FDB packets.

You can configure related commands on the Hello-time node and the Fail-time node to modify the interval for the primary port to transmit the HEALTH packets and the time limit for the secondary port to wait for the HEALTH packets.

2.3.2 Notification of Invalid Link of Transit Node

After the transit port of the transit node is out of effect, the LINK-DOWN packet will be immediately transmitted by the other transit port to notify other nodes. In normal case, the packet passes through other transit nodes and finally arrives at one port of the master node.

After the master node receives the LINK-DOWN packet, it thinks that the ring network is invalid. In this case, the master node removes the blocking of data VLANs on its secondary port, ages the local MAC address table, transmits the RING-DOWN-FLUSH-FDB packet and notifies other nodes.

2.3.3 Resuming the Link of the Transit Node

After the transit port is resumed, it does not immediately transmit the packets of data VLANs, but enters the Pre-Forwarding state. A transit port in pre-forwarding state only transmits and receives the control packets from the control VLAN.

If there is only one transit port invalid in the ring network and when the port enters the pre-forwarding state, the secondary port of the master node can receive the HEALTH packet from the primary port again. In this case, the master node blocks data VLANs on the secondary port again and transmits the notification of ageing address table outside. After the node with a transit port in pre-forwarding state receives the notification of aging address table, the node will first modify the pre-forwarding port to the forwarding port and then ages the local MAC address table.

If a transit mode does not receives the notification of aging address table from the master node, it thinks that the link to the master node is already out of effect, the transit node will automatically set the pre-forwarding port to be a forwarding one.

You can configure the related commands through the pre-forward-time node to modify the time for the transit port to keep the pre-forwarding state.

Chapter 3 EAPS Settings

3.1 Reading Before EAPS Configuration

Before configuring EAPS, please read the following items carefully:

- EAPS can be configured along with ERPS or SSTP/RSTP, but not with MSTP, at the same time.
- The configuration of the control VLAN of the ring network does not automatically establish the corresponding systematic VLAN. You need to establish the systematic VLAN manually through global VLAN configuration command.
- The port of each ring can forward the packets from the control VLAN of the ring, while other ports, even in the Trunk mode, cannot forward the packets from the control VLAN.
- By default, Fail-time of the master node is triple longer than Hello-time, so that packet delay is avoided from shocking the ring protection protocol. After Hello-time is modified, Fail-time need be modified accordingly.
- By default, Pre-Forward-Time of the transit node is triple longer than Hello-time of the master node so that it is ensured that the master node can detect the recovery of the ring network before the transit port enters the pre-forwarding state. If Hello-time configured on the master node is longer than Fre-Forward-Time of the transit node, loopback is easily generated and broadcast storm is then triggered.
- By default, the ring's nodes that are configured on S6800 and S8500 are all working on the distributive control mode so that an excellent convergence performance can be obtained. The working mode of the ring protection protocol can be changed through the node configuration commands **distributed-mode** and **centralized-mode**.
- EAPS can set a physical or aggregation port to be a ring port. If link aggregation, 802.1X or port security has been already configured on a physical port, the physical port cannot be set to be a ring's port any more.

3.2 EAPS Configuration Tasks

- Configuring the Master Node
- Configuring the Transit Node
- Configuring the Port of Ethernet Ring
- Browsing the State of the Ring Protection Protocol

3.3 EAPS Settings

3.3.1 Configuring the Master Node

Configure a switch to be the master node of a ring network according to the following steps:

Command	**Purpose**
Switch# **configure**	Enters the switch configuration mode.
Switch_config# **no spanning-tree**	Shuts down the currently running STP.
Switch_config# **spanning-tree bpdu-terminal**	Forbids the switch to forward STP BPDU.
Switch_config# **ether-ring** *id*	Sets a node and enters the node configuration mode. id: ID of the node
Switch_config_ring# **control-vlan** *vlan-id*	Configures the control VLAN. Vlan-id: ID of the control VLAN
Switch_config_ring# **master-node**	Configures the node type to be a master node.
Switch_config_ring# **hello-time** *value*	This step is optional. Configures the cycle for the master node to transmit the HEALTH packets. Value: It is a time value ranging from 1 to 10 seconds and the default value is 1 second.
Switch_config_ring# **fail-time** *value*	This step is optional. Configures the time for the secondary port to wait for the HEALTH packets. Value: It is a time value ranging from 3 to 30 seconds and the default value is 3 second.
Switch_config_ring# **distributed-mode**	This step is optional. Configures the distributive mode for the ring protection protocol. This command is only used for S6800 and S8500.
Switch_config_ring# **centralized-mode**	This step is optional. Configures the centralized mode for the ring protection protocol. This command is only used for S6800 and S8500.
Switch_config_ring# **exit**	Saves the current settings and exits the node configuration mode.
Switch_config# **vlan** *vlan-id*	Establishes the corresponding control VLAN.

Remark:

The **no ether-ring *id*** command is used to delete the node settings and port settings of the Ethernet ring.

3.3.2 Configuring the Transit Node

Configure a switch to be the transit node of a ring network according to the following steps:

Command	**Purpose**
Switch# **configure**	Enters the switch configuration mode.
Switch_config# **no spanning-tree**	Shuts down the currently running STP.
Switch_config**# spanning-tree bpdu-terminal**	Forbids the switch to forward STP BPDU.
Switch_config# **ether-ring** *id*	Sets a node and enters the node configuration mode. id：ID of the node
Switch_config_ring# **control-vlan** *vlan-id*	Configures the control VLAN. vlan-id：ID of the control VLAN
Switch_config_ring# **transit-node**	Configures the node type to be a transit node.
Switch_config_ring# **pre-forward-time** *value*	This step is optional. Configures the time of maintaining the pre-forward state on the transit port. value：It is a time value ranging from 3 to 30 seconds and the default value is 3 second.
Switch_config_ring# **exit**	Saves the current settings and exits the node configuration mode.
Switch_config# **vlan** *vlan-id*	Establishes the corresponding control VLAN.

3.3.3 Configuring the Port of Ethernet Ring

Configure a port of a switch to be the port of Ethernet ring according to the following steps:

Command	**Purpose**
Switch# **configure**	Enters the switch configuration mode.
Switch_config# **interface** *intf-name*	Enters the interface configuration mode. intf-name: Stands for the name of an interface.
Switch_config_intf# **ether-ring** *id* **primary-port** **{ secondary-port | transit-port }**	Configures the type of the port of Ethernet ring. id：ID of the node of Ethernet ring
Switch_config_intf**# exit**	Exits from interface configuration mode.

Remark:

The **no ether-ring *id* primary-port** { **secondary-port** | **transit-port** } command can be used to cancel the port settings of Ethernet ring.

3.3.4 Browsing the State of the Ring Protection Protocol

Run the following command to browse the state of the ring protection protocol:

Command	Purpose
show ether-ring *id*	Browses the summary information about the ring protection protocol and the port of Ethernet ring. id：ID of Ethernet ring
show ether-ring *id* **detail**	Browses the detailed information about the ring protection protocol and the port of Ethernet ring.
show ether-ring *id* **interface** *intf-name*	Browses the state of the Ether-ring port or that of the common port.

3.4 EAPS Configuration Example

3.4.1 Configuration Example

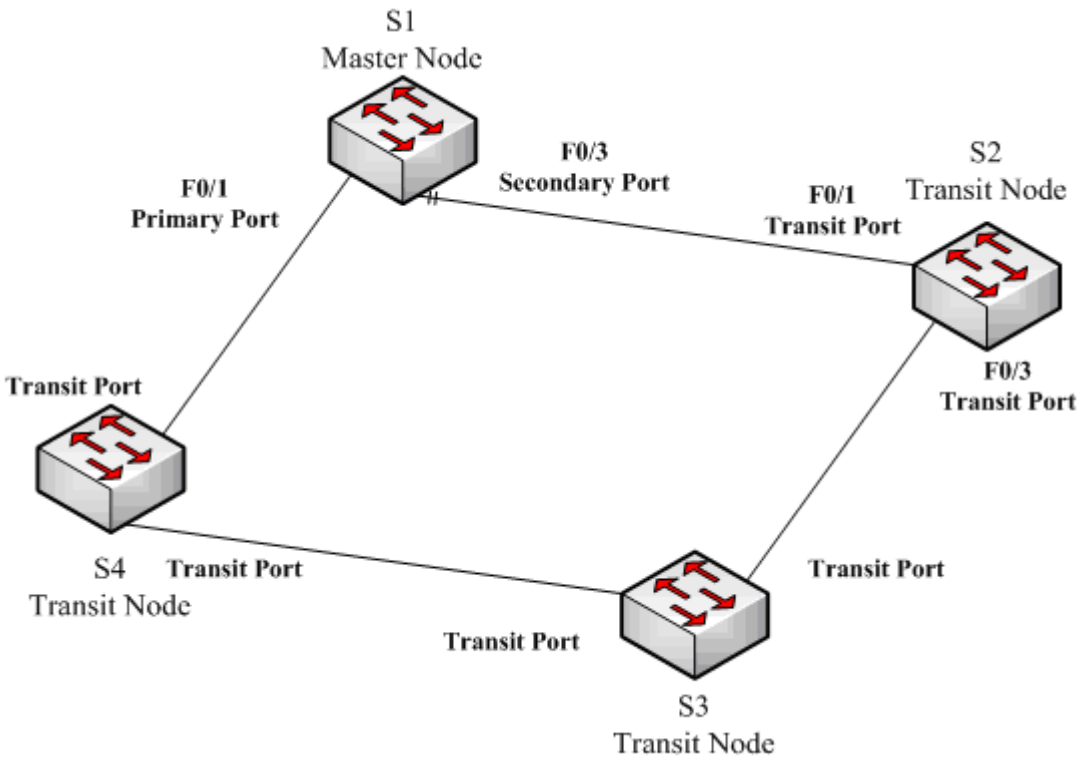


Figure 2.1 Security settings of EAPS Ethernet ring

As shown in figure 2.1, master node S1 and transit node S2 are configured as follows. As to the settings of other nodes, they are same to S2's settings.

Configuring switch S1:

Shuts down STP and configures the Ether-ring node:

```
S1_config# no spanning-tree
S1_config# ether-ring 1
S1_config_ring1# control-vlan 2
S1_config_ring1# master-node
```

Configures the time related parameters:

```
S1_config_ring1# hello-time 2
S1_config_ring1# fail-time 6
```

Exits from the node configuration mode:

```
S1_config_ring1# exit
```

Configures the primary port and the secondary port:

```
S1_config# interface fastEthernet 0/1
S1_config_f0/1# ether-ring 1 primary-port
S1_config_f0/1# exit
S1_config# interface fastEthernet 0/3
S1_config_f0/3# ether-ring 1 secondary-port
S1_config_f0/3# exit
```

Establishes the control VLAN:

```
S1_config# vlan 2
S1_config_vlan2# exit
S1_config# interface range f0/1 , 3
S1_config_if_range# switchport mode trunk
S1_config_if_range# exit
```

Configuring switch S2:

```
S1_config# no spanning-tree
S1_config# ether-ring 1
S1_config_ring1# control-vlan 2
S1_config_ring1# transit-node
S1_config_ring1# pre-forward-time 8
S1_config_ring1# exit
S1_config# interface fastEthernet 0/1
S1_config_f0/1# ether-ring 1 transit-port
S1_config_f0/1# exit
S1_config# interface fastEthernet 0/3
S1_config_f0/3# ether-ring 1 transit-port
S1_config_f0/3# exit
S1_config# vlan 2
S1_config_vlan2# exit
S1_config# interface range fastEthernet 0/1 , 3
S1_config_if_range# switchport mode trunk
S1_config_if_range# exit
```

Chapter 4 ERPS Introduction

4.1 Related Concepts of ERPS

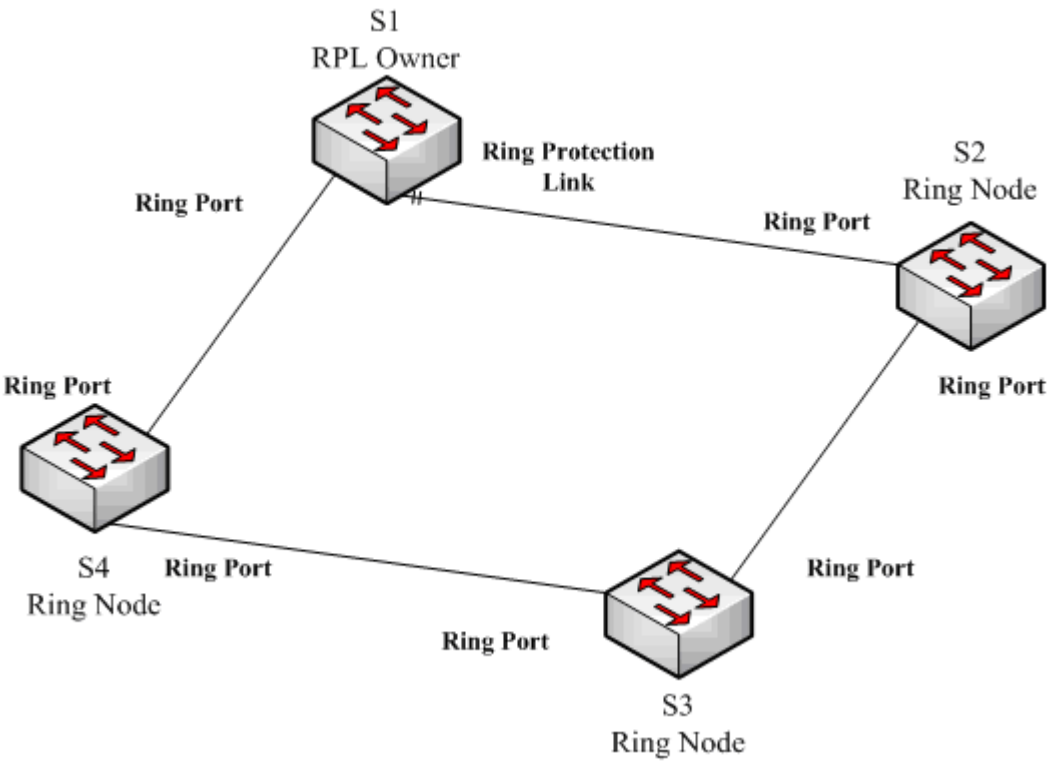


Figure 4.1 ERPS Ethernet Ring

4.1.1 Roles of Ether-Ring Nodes

Each switch on an Ethernet ring is a node on the Ethernet ring.. The nodes of Ethernet ring can be classified into RPL owner and common nodes. Only one switch on the Ethernet ring can serve as a mere RPL owner and other switches are worked as common nodes.

The node type of ERPS does not need the display configuration. By default, all devices on Ethernet ring determine the node with highest priority through the automatic discovery mechanism of ERPS as the RPL owner, one of whose ports is also automatically set as the ring protection link (RPL).

If a port of one device is set through a command to RPL, the priority of the device will be automatically modified so that the device can be the protection node.

The RPL owner is functionally same to a common node, that is, it is used to check the state of the ports of local Ethernet ring and send out the notifications in case of link

breakdown. The difference between RPL owner and common node is that RPL owner blocks the RPL link in normal case.

Note:
The RPL owner is greatly different from the master node of EAPS on the functionality: the RPL owner will not check the completeness of Ethernet ring positively, nor control the MAC address ageing of other nodes.

Note:
In the case that the automatic discovery mechanism of Ethernet ring is enabled, a port of a device is set to RPL through related command. Its functions are equivalent to setting the smallest priority value for the device. In this case, if other devices also have the lowest priority, the RPL owner of Ethernet ring still needs selection.

4.1.2 Role of the Ring's Port

ERPS demands that each node has two ports to connect Ethernet ring and each port is called as the ring port. Additionally, the whole Ethernet ring has a ring port as RPL.

In normal case, all ports on Ethernet ring except RPL are in forwarding state, while the RPL port is blocked to avoid loopback. In case that the link of Ethernet ring is invalid, the RPL owner cancels the blocking of the RPL owner for recovering network communication.

Only one RPL owner can be configured on each ring node on a switch.

Note:
1. ERPS supports setting an aggregation port to be a ring port.
2. To configure a same switch to belong to multiple rings, the switch must connect different rings through different physical ports.

4.1.3 Control VLAN and Data VLAN

ERPS has no need to distinguish control VLAN and data VLAN.

When ERPS runs together with EAPS, the state of the ring port of ERPS will affect all VLANs on this port.

When ERPS and EAPS are configured at the same time, the state of the ring port of ERPS will affect all EAPS data VLANs on this port.

Note:
ERPS always transmits its packets to the default VLAN of a port, so user needs to confirm that the default VLANs of all ports are same.

4.1.4 Automatic Discovery and Consistence Checkup of Ring Port

The automatic discovery mechanism of ERPS is used to determine a node on Ethernet ring as the protection node. Compared with EAPS, automatic discovery makes the deployment of Ethernet-ring devices much easier.

The automatic discovery mechanism uses the priority value and the MAC address to identify a ring node. The smaller the priority value and the MAC address are, the higher the priority is.

After the automatic discovery flow is started, the device begins to transmit the discovery packets to the ring port. In these packets, the local two-tuple information of the device is carried. When a discovery packet is found, please compare the information in the packet and judge whether it is more prior than the local information. If the packet's information is more prior, the device will not function as the RPL owner. If a device has not received a more prior packet before the end of a discovery flow, the device will become the RPL owner.

The **discovery time** command can be used to configure the time of the operation of the discovery flow, while the **discovery disable** command can be used to disable automatic discovery.

The automatic discovery mechanism is used for checking the consistence of the ring port at the same time to prevent incorrect or omitted settings, or incorrect network cable connection from affecting the running of the protocol.

ERPS guarantees that the discovery packets are transmitted only to t he ring port and these packets carry the ID of Ethernet ring. Suppose port P of a device receives a discovery packet and the discovery packet carries an **ID1** ID, it will be regarded, in the following two cases, that port P has the error of consistence and then port P will be set to the **Error-Disable** state.

- Port P has already been set to the ring port, but its ID is not equal to ID1.
- Port P has not been configured to be the ring port, but there are two other ports that have been configured to be ring ports whose IDs are both ID1.

In global configuration mode, the **no erps inconsistence-check** command can be used to forbid the consistence checkup of the ring port, while the **error-disable-recovery** command can be used to configure the time of port recovery.

4.2 Types of the ERPS Packets

The ERPS packets can be classified into the following types, as shown in table 4.1.

Table 4.1 Types of ERPS packets

Type of the packet	**Description**
Signal Fail（SF）	The ring node (including RPL owner) notifies other nodes after the local link is found to be invalid.
No Request（NR）	The ring node notifies other nodes after it detects that all local links are recovered.
No Request, RPL Blocked （NR-RB）	The RPL owner notifies other nodes of the recovery of ring protection shift.

4.3 ERPS Ring Protection Mechanism

4.3.1 Stable State

In stable state, the ring protection node blocks the RPL port and transmits the NR-RB packets in a configurable period.

All common nodes that receive NR-RB packets set the local ring ports to be in forwarding state. In stable state the common nodes do not transmit the protocol packets.

You can run the **send-time** command to modify the cycle time for the protection node to transmit the NR-RB packets.

4.3.2 Handling the Invalid Local Link

After a ring node checks an invalid local link, it first cancels the blocking state of the valid local ports (including the RPL port or the common ring ports that are not in forwarding state), then begins to transmit the SF protocol packets and conducts the ageing of the local MAC address table.

Other nodes that receive the SF packets first stop the transmission of local packets, and then cancel the blocking state of the valid local ports and conduct the ageing of MAC address table.

The node whose link is invalid transmits the SF packets every period of send-time. During the process, if a port of another node is resumed, the node will recover the port to the forwarding state after it receives the SF packets.

4.3.3 Handling the Recovery of Local Link

When the ring node detects that the local ring port recovers from the invalid state, it will maintain the blocking state of the port and begins to transmit the NR packets continuously.

When the NR packets are being transmitted, if the node receives the SF packets from other nodes, it means that the invalid link exists in the network, and the local node will stop the transmission of the NR packets and restore to the forwarding state.

If the local node does not receive new SF packets, it will start shift recovery WTR after the RPL owner receives the NR packets; after WTR times out, the RPL owner blocks the RPL port again, transmits the NR-RB packets and then conducts the ageing of the MAC address table; in this way, the network communication recovers the initial stable state.

4.3.4 Shift Recovery

The RPL owner realizes the ring shift recovery through a wait-to-restore timer (WTR).

WTR is used to avoid protection shift which occurs on Ethernet ring frequently. After the RPL owner receives the NR messages from other nodes, WTR is started; before

WTR times out, the RPL owner maintains the forwarding state of the RPL port and does not transmit the ring recovery notification. If the RPL owner receives the SF messages again, that means Ethernet ring is not fully recovered and in this case WTR is stopped.

After WTR times out, the RPL owner starts to block the RPL port again.

Chapter 5 ERPS Configuration

5.1 Reading Before ERPS Configuration

Before configuring ERPS, please read the following items carefully:

- ERPS can be configured along with EAPS or SSTP/RSTP, but not with MSTP, at the same time.
- The default VLAN for each ring port must be configured to be consistent so that ERPS packets can be normally forwarded.
- When ERPS and EAPS are running at the same time, the default VLAN of the ERPS ring port must be different from the control VLAN of EAPS. The ERPS packets cannot be forwarded in the control VLAN of EAPS.
- One port can not be used as the ERPS ring port and the EAPS ring port at the same time.
- ERPS can set a physical or aggregation port to be a ring port. However, the physical port where link aggregation, 802.1X or port security has been configured can not be set to be an ERPS ring port.
- ERPS chooses the RPL owner through automatic discovery mechanism by default; the automatic discovery mechanism can be forbidden through the **discovery disable** command in ERPS configuration mode. If automatic discovery is forbidden, please make sure that RPL has been configured and displayed on Ethernet ring; otherwise the broadcast storm may occur.
- In order to guarantee the ERPS ring port to recover from the error state, please run the **error-disable-recovery** command in global configuration mode to configure the automatic recovery time of the errable port.
- After the ring port is set to RPL, it has not become the RPL owner unless automatic discovery is forbidden. In the case that automatic discovery is enabled, setting the command is equivalent to setting the priority of the device to 0. Of cause, the RPL owner generates still through election.

5.2 ERPS Configuration Tasks

- Configuring the Ring Node
- Configuring the Ring Port
- Browsing the State of the Ring Protection Protocol

5.2.1 Configuring the Ring Node

In global mode, run the following commands to set a switch to the ERPS node:

Command	Purpose
Switch_config# **error-disable-recovery** *value*	Configures the automatic recovery time of the errable port.
Switch_config# **erps** *id*	Sets an ERPS ring node and enters the node configuration mode. id: ID of an Ethernet ring, which ranges between 0 and 7.
Switch_config# **discovery** [**enable** | **disable**]	Enables or disables the discovery mechanism.
Switch_config# **discovery time** *value*	Set the runtime for the automatic discovery of ERPS. Value: stands for the operation time of automatic discovery, which ranges from 15 to 300 seconds (30 seconds by default).
Switch_config# **discovery interval** *value*	Set the interval of transmission of the discovery packets. value：1-20 seconds (2 seconds by default)
Switch_config# **priority** *value*	Sets the priority of the local node. This value is used to confirm the ring protection node in the discovery mechanism. value：It ranges between 0 and 61440 and must be the integer times of 4096. The default value is 32768.
Switch_config_ring# **wtr-time** *value*	Sets the timeout time of the WTR timer. Value range: 10-720 seconds (300 seconds by default)
Switch_config_ring# **guard-time** *value*	Configures the timeout time of the Guard timer. When a port is recovered from an invalid state, the Guard timer is forbidden to handle the received protocol packets to avoid outdated packets from generating inaccurate protocols. Value: its unit is 10ms and it ranges between 1 and 200 (the default value is 50ms)
Switch_config_ring# **send-time** *value*	Sets the interval of transmission of the protocol packets. Value: the interval for the transmission of packets, which ranges between 1 and 10 and whose default value is 5 seconds.
Switch_config_ring# **exit**	Exits from the node configuration mode and starts the node.

Note:

The **no erps *id*** command is used to delete the node settings and port settings of the Ethernet ring.

5.2.2 Configuring the Ring Port

Configure a port of a switch to be the port of Ethernet ring according to the following steps:

Command	Purpose
Switch_config# **interface** *intf-name*	Enters the interface configuration mode. intf-name: Stands for the name of an interface.
Switch_config_intf# **erps** *id* **ring-port**	Set a port to be a common ring port of a designated node. id: ID of Ethernet ring
Switch_config_intf# **erps** *id* **rpl**	Set a port to be RPL of a designated node. In the case automatic discovery is enabled, the function of the command is as same as the priority value is modified to 10. id: ID of Ethernet ring
Switch_config_intf# **exit**	Exits from interface configuration mode.

Note:

The **no erps *id* rpl** command is used to set an RPL port to be a common ring port.

The **no erps** *id* **ring-port** command is used to delete a common ring port or an RPL port.

In the case that the ring nodes are not configured globally, both the **erps id ring-port** command and the **rpl** command are used to create the ring nodes at the same time.

5.2.3 Browsing the State of the Ring Protection Protocol

Run the following command to browse the state of the ring protection protocol:

Command	Purpose
show erps *id*	Browses the summary information about the ring protection protocol and the port of Ethernet ring. id: ID of Ethernet ring
show erps *id* **detail**	Browses the detailed information about the ring protection protocol and the ports.
show erps interface *intf-name*	Browses the state of the ring port.

5.3 ERPS Configuration Example

5.3.1 Example 1—Fixed RPL Settings

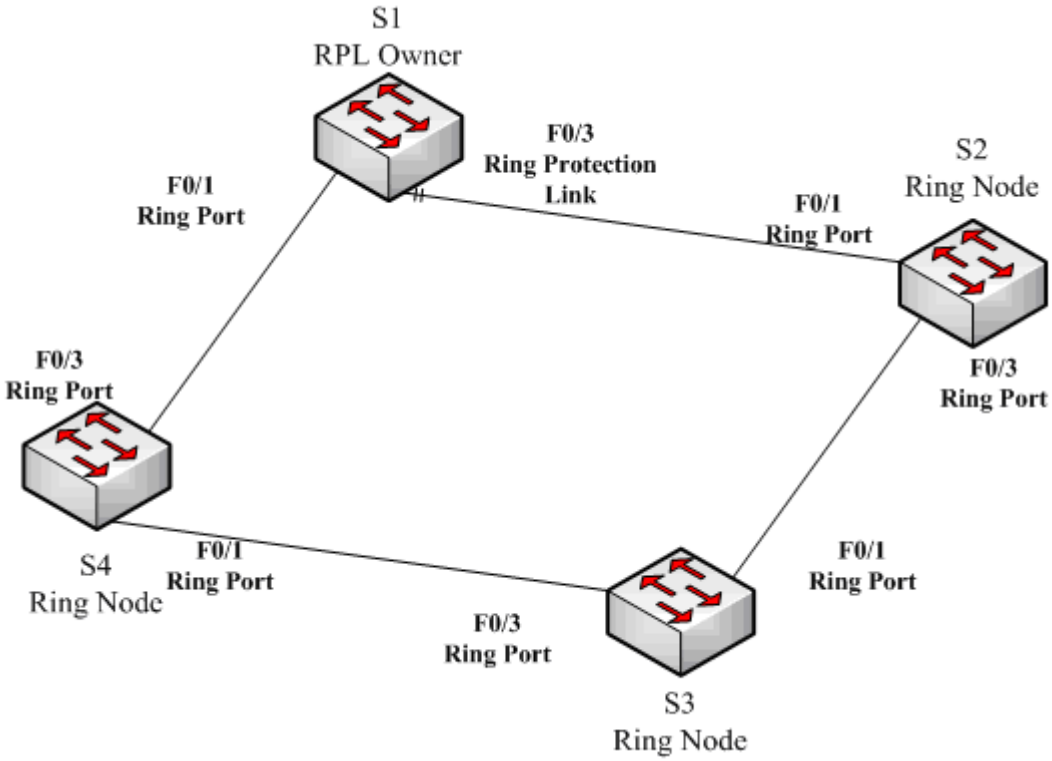


Figure 5.1 Fixed ERPS RPL settings

As shown in figure 5.1, the RPL node (S1) and the common node (S2) are configured.

Configuring switch S1:

The following commands are used to set the recovery time of the errable port:

Switch# config
Switch_config# error-disable-recovery 30

The following command is used to configure the ring node:

Switch_config# erps 1

The following commands are used to set the time related parameters:

Switch_config_ring1# wtr-time 15
Switch_config_ring1# send-time 5
Switch_config_ring1# exit

The following commands are used to set a common port:

Switch_config# interface f0/1
Switch_config_f0/1# erps 1 ring-port

The following commands are used to set the RPL port:

```
Switch_config_f0/1# interface f0/3
Switch_config_f0/3# erps 1 rpl
```

Configuring switch S2:

```
Switch_config# erps 1
Switch_config_ring1# send-time 5
Switch_config_ring1# exit
Switch_config_if_range# interface range fastEthernet 0/1 , 3
Switch_config_if_range# erps 1 ring-port
Switch_config_if_range# exit
```

5.3.2 Example 2 – Simple Settings for Applying Automatic Discovery

As shown in figure 5.1, all nodes are configured as follows:

The following commands are used to configure Ethernet ring and the ring port:

```
Switch_config# error-disable-recovery 30
Switch_config# interface range fastEthernet 0/1 , 3
Switch_config_if_range# erps 1 ring-port
Switch_config_if_range# exit
```

The following command is used to browse the state of ERPS:

```
Switch# show erps
```

QoS Configuration

Table of Contents

Chapter 1 QoS Configuration

If you concern how to fully use the bandwidth of your line and effectively use your network resources, you need to configure the service quality.

1.1 Overview

1.1.1 QoS Concept

The switch is normally in best-effort served mode. In this mode, the switch equally treats all flows and tries its best to forward all flows. In this case, all flows have the same chance to be dropped if congestion occurs. In real network conditions, different flows have different importance. The QoS function of the switch provides different services to different flows according to the importance of the flow, providing more important flows better service.

The current network provides two methods to distinguish the importance of the flow.

- Distinguish the importance based on the tag in the 802.1Q frame. The tag has two bytes. Three bits in the highest byte represent the priority levels. There are eight priority levels, 0 and 7 representing the lowest priority and the highest priority level respectively.
- Distinguish the importance based on the DSCP field in the IP header of the IP message. The DSCP field occupies 6 bits in the TOS domain of the IP header.

In real network application, the verging switches distribute different priorities to different flows according to their importance. Other switches provide different flows different services according to the priority information contained in the flow. The peer-to-peer (P2P) QoS service is realized.

Additionally, you can configure a switch in the network, enabling the switch to specially handle message with special features. The action performed by the switch is called as one-hop action.

The QoS function of the switch makes the network bandwidth effectively use, which greatly improves the performance of the network.

1.1.2 P2P QoS Model

The service model describes the capability of the P2P QoS, that is, the capability to send special network communication from one peer to another peer. The QoS software supports two kinds of service models: best-effort served service and differentiated service.

a. Best-effort service

It is a single service model. In this mode, the application can send any number of data at

necessary time without applying permission or previous notification of network. For the best-effort service, network can transmit data without concerning reliability, delay range or putthrough. The QoS function of the switch in best-effort service model complies with the “first come, first served” order.

b. Differentiated service

For the differentiated service, if the to-be-sent service is special, the corresponding QoS label must be designated in each packet. The designation can be embodied in different modes such as setting IP priority in the IP packet. The switch uses the QoS rule to classify the service and perform intelligent queue. The QoS function of switch provides strict priority, weighted round robin (WRR) and “first come, first served” (FCFS) to send the differentiated service.

1.1.3 Algorithm of QoS Queue of QoS Queue

The algorithm of QoS Queue of QoS queue guarantees the QoS realization. Our switches provide the queue algorithm for the strict priority, weighted round robin (WRR) and “first come, first served” (FCFS).

a. Strict priority

The queue algorithm of the strict priority means first providing service to a flow with the high priority until the flow with the high priority does not exist. The queue algorithm provides better service for the flows with high priority. Its shortcoming is that the flows with low priority cannot get service and die eventually.

b. Weighted round robin

WRR algorithm is an effective way to solve the shortcoming of the queue algorithm of strict priority. A certain bandwidth is distributed to each priority queue. Each priority queue is provided service according to the order from high priority to low priority. When the queue with high priority has already used up all the distributed bandwidth, the WWW algorithm turns to the queue with low priority and provides service to it.

c. First come first served

FCFS algorithm strictly follows the order the message reaches the switch to provide service for the flows. The message flow that first reaches the switch is first provided with service.

1.2 QoS Configuration Task List

Generally, the switch tries its best to deliver every message. When congestion occurs, all messages have the same chance to be dropped. In fact, different message has different

importance. Important message should be provided with better service. The QoS function provides different message with different priorities for providing different services. Therefore, the network has better performance and can be effectively used.

The section describes how to configure the QoS function of the switch.

The QoS configuration tasks are listed as follows:

- Configuring global CoS priority queue
- Configuring the bandwidth of the CoS priority queue
- Configuring the schedule strategy for the CoS priority queue
- Configuring the schedule standard for the CoS priority queue
- Configuring the default CoS value of the port
- Configuring CoS priority queue of the port
- Establishing QoS strategy mapping
- Configuring the description of QoS strategy mapping
- Configuring the matched data flow of the QoS strategy mapping
- Configuring actions for the matched data flow of the QoS strategy mapping
- Applying the QoS strategy on the port
- Displaying the QoS strategy mapping table
- Configuring the limitation for the port flow rate

1.3 QoS Configuration Tasks

1.3.1 Configuring global QoS Priority Queue

Configuring QoS priority queue is to map eight CoS values defined by IEEE802.1p to the priority queue. The switch has eight priority queues. The switch adopts the corresponding strategy according to different queues and makes the QoS service realized.

If you configure the CoS priority queue in global configuration mode, the CoS priority mapping at all ports is to be affected. When the priority queue is configured at the layer-2 port, the port will use the priority queue. Otherwise, the global configuration is to be used.

Perform the following operations in privileged mode to configure the global CoS priority queue:

Command	Purpose
configure	Enters the global configuration mode.
[**no**] **cos map** *quid cos1..cosn* **(1~8)**	Set the COS priority queue. **quid** is the ID of the COS priority. **cos1..cosn** is the cos value defined in IEEE802.1p.
exit	Returns to the management mode.
write	Saves configuration.

1.3.2 Configuring the Bandwidth of the CoS Priority Queue

The bandwidth of the CoS priority queue is the bandwidth distributed for each priority when the schedule strategy of the COS priority queue is WRR.

Using the command affects the bandwidth of the CoS priority queues on all ports. The command is valid only when the schedule strategy is WRR. The command decides the bandwidth value of the Cos priority queue when the wrr schedule strategy is used.

Perform the following operations in privileged mode to configure the bandwidth of the CoS priority queue:

command	description
configure	Enters global configuration mode.
[**no**] **scheduler wrr bandwidth** *weight1...weightn* **(1~8)**	Sets the bandwidth of CoS priority queue. weight1...weightn represent eight CoS CoS priority queue values.
exit	Returns to management configuration mode.
write	Saves configuration.

1.3.3 Configuring the Schedule Strategy for the CoS Priority Queue

Each port of the switch has multiple output queues. This series of switches have eight priority queues. The following methods can be used to schedule the output queue:

- SP (Sheer Priority): sheer priority schedule. The packet of low priority queue will be forwarded only when the high priority queue is vacant. If there are packets in the high priority queue, these packets are to be sent first.
- WRR (Weighted Round Robin): It is to distribute a bandwidth value for each queue and the bandwidth is then distributed to each queue according to their value.

Perform the following operations in privileged mode to configure the schedule strategy of the CoS priority queue.

Command	Purpose
configure	Enter the global configuration mode.
[**no**] **scheduler policy** { **sp** | **wrr** }	Set the schedule strategy for the QoS priority queue. **sp** represents the sp schedule strategy. **wrr** represents the **wrr** schedule strategy.
exit	Returns to the management mode.
write	Saves configuration.

1.3.4 Configuring the Schedule Standard for the CoS Priority Queue

The schedule standard for the priority queue is the standard to value the bandwidth ratio of

the priority queue when the schedule strategy of the COS priority queue is WRR. There are two types of schedule standard.

- packet-count: It uses the number of packets to represent occupied bandwidth.
- latency: It uses the sent time segment to represent occupied bandwidth.

This series of switches only support packet-count. The packet-count is the default schedule standard. Therefore, there is no command to select the schedule strategy standard.

1.3.5 Configuring the Default CoS Value of the Port

If the port receives the frame without label, the switch will add a default COS priority to it. Configuring the default CoS value is to set the default Cos value to the designated value of the unlabelled frame.

Perform the following operations in privileged mode to the default Cos value on the port.

Command	Purpose
configure	Enter the global configuration mode.
interface g0/1	Logs in to the port that will be configured.
[**no**] **cos default** *cos* **(0~7)**	Configures the CoS value for the unlabelled frame. **Cos** represents the corresponding cos value.
exit	Returns to the global configuration mode.
exit	Returns to the management mode.
write	Saves configuration.

1.3.6 Configuring CoS Priority Queue of the Port

When the priority queue is set on the layer-2 port, the port uses the configured priority queue. Otherwise, the global COS priority queue configuration is adopted.

Perform the following operations in privileged mode to configure the default CoS value.

Command	Purpose
configure	Enters the global configuration mode.
interface g0/1	Logs in to the port that will be configured.
[**no**] **cos map** *quid cos1..cosn* **(1~8)**	Sets the cos priority queue. quid is the ID of the COS priority. **cos1..cosn** is the cos value defined in IEEE802.1p.
exit	Returns to the global configuration mode.
exit	Returns to the management mode.

1.3.7 Establishing QoS Strategy Mapping

QoS strategy mapping means to adopt certain requlations to distinguish headers of a certain feature, and to perform the designated operations on the headers.

Only one rule can be used to match the IP access list and the MAC access list of the data flow. If not, the configuration will fail. When the action is **permit**, the rule is used to distinguish data flow. When the action is **deny**, the rule is not used to match the data flow. The port number of IP access list must be fixed.

Perform the following operations in privileged mode to create the QoS strategy mapping:

Command	Purpose
configure	Enters the global configuration mode.
[no]policy-map *name*	Enters the QoS strategy table configuration mode. **name** represents the strategy name.
description description-text	Configures the description of the Qos strategy. **description-text** is the text to describe the strategy.
[**no**]**classify** {**ip access-group** *access-list-name* | **dscp** *dscp-value* | **mac access-group** *mac-access-name* | **vlan** *vlan-id* | **cos** ***cos*** **| any** }	Configures the matched data flow of the QoS strategy table. **access-list-name** is the name of matched IP access list. **dscp-value** stands for the **diffserv** field in the IP message. **mac-list-name** is the name of matched MAC access list. **vlan-id** stands for the ID of the matched VLAN. **cos** stands for the matched cos value. **any** means to match any packet.
action{**bandwidth** *max-band* | **cos** ***cos-value*** **| dscp** *dscp-value* | **redirect** *interface-id* | **drop | monitor** }	Configures the matched data flow strategy of the QoS strategy table. **max-band** stands for the maximum bandwidth occupied by the data flow. **cos-value** means to set the **cos** field of the matched flow to **cos-value**. **dscp-value** means to set the **dscp** field of the matched flow to **dscp-value**. **interface-id** stands for the exit of the redirection match flow. **drop** stands for the dropped message.

	stat stands for statistics information collected by the switch. **monitor** means to send packets to the mirroring port.
exit	Returns to the global configuration mode.
exit	Returns to the management mode.

1.3.8 Configuring Description of QoS Strategy Mapping

Perform the following operations in privileged mode to configure the description of QoS strategy mapping:

Command	Purpose
configure	Enters the global configuration mode.
[**no**]**policy-map** *name*	Enters the QoS strategy list configuration mode. **name** represents the strategy name.
description description-text	Configures the description of the Qos strategy. **description-text** is the text to describe the strategy.
exit	Returns to the global configuration mode.
exit	Returns to the management mode.

1.3.9 Configuring the Matched Data Flow of the QoS Strategy Mapping

The classification rule of the QoS data flow is the filtration rule configured by administrator according to requirements.

Perform the following operations in privileged mode to configure the matched data flow of the strategy. The data flow will replace the previous configuration.

Command	Purpose
configure	Enters the global configuration mode.
[**no**]**policy-map** *name*	Enters the QoS strategy list configuration mode. **name** represents the strategy name.
[**no**]**classify** {**ip access-group** *access-list-name* **| dscp** *dscp-value* | **mac access-group** *mac-access-name* **| vlan** *vlan-id* **| cos** *cos* **| any** }	Configures the matched data flow of the QoS strategy table. **access-list-name** is the name of matched IP access list. **dscp-value** stands for the **diffserv** field in the IP message.

	mac-list-name is the name of matched MAC access list. **vlan-id** stands for the ID of the matched VLAN. **cos** stands for the matched cos value. **any** means to match any packet.
exit	Returns to the global configuration mode.
exit	Returns to the management mode.

1.3.10 Configuring Actions for Matched Data Flow of the QoS Strategy Mapping

Defining the action of the data flow means to take corresponding actions according to the data flow that complies with the filtration rule, including limiting bandwidth, dropping message, updating domains.

Perform the following operations in privileged mode to configure actions for the matched data flow:

Command	Purpose
configure	Enters the global configuration mode.
[**no**]**policy-map** *name*	Enters the QoS strategy list configuration mode. **name** represents the strategy name.
action {**bandwidth** *max-band* | **cos** *cos-value* **| dscp** *dscp-value* | **vlanID** *vlanid-value* | **redirect** *interface-id* **| drop | stat | monitor** }	Configures the matched data flow strategy of the QoS strategy table. **max-band** stands for the maximum bandwidth occupied by the data flow. **cos-value** means to set the **cos** field of the matched flow to **cos-value**. **dscp-value** means to set the **dscp** field of the matched flow to **dscp-value**. **vlanid-value** means to set the **vlanID** field of the matched flow to **vlanid-value**. **interface-id** stands for the exit of the redirection match flow. **drop** stands for the dropped message. **stat** stands for statistics information collected by the switch. **monitor** means to send packets to the mirroring port.
exit	Returns to the global configuration mode.
exit	Returns to the management mode.

1.3.11 Applying the QoS Strategy on the port

You can apply the QOS strategy to a port. Multiple strategies can be applied to one port; one strategy can be applied to multiple ports too. To the strategies applied on a port, the strategies that are first applied have high priority. If the message simultaneously configures two strategies and the configuration actions are conflicted, take the action of firstly matched strategy as standard. After the strategy is applied on the port, the switch adds a strategy by default on the port to block the data flow that is not allowed to pass. When all strategies on the port are deleted, the switch automatically deletes the default default strategy from the port.

Perform the following operations in privileged mode to apply the QoS strategies:

Command	Purpose
configure	Enters the global configuration mode.
interface g0/1	Logs in to the port that will be configured.
[**no**] **qos policy** *name* { **ingress**|**egress**}	Applies the QoS strategy on the port. **name** stands for the name of the QoS strategy. **ingress** means the QoS strategy has impact on the entrance. **egress** means the QoS strategy has impact on the exit.
exit	Returns to the global configuration mode.
exit	Returns to the management mode.

1.3.12 Displaying the QoS Strategy Mapping Table

You can run the **show** command to display all or the designated Qos strategy mapping table.

Perform the following operations in privileged mode to display the QoS strategy mapping table:

Command	Purpose
show policy-map [*policy-map-name*]	Displays all or designated QoS strategy mapping table. **policy-map-name** stands for the name of the trategy mapping table.

1.3.13 Configuring the limitation for the Port Flow Rate

The flow rate of the entrance or exit can be limited through the configuration.

Perform the following operations in privileged mode to limit the flow rate of the port:

Command	Purpose
configure	Enters the global configuration mode.

interface g0/1	Logs in to the port that will be configured.
[**no**] **switchport rate-limit** *band* **(1~1000)** { ingress|egress}	Configures the limitation for the port flow rate. ***band*** stands for the flow rate to be limited. **ingress** means the flow limitation has impact on the entrance. **egress** means the flow limitation has impact on the exit.
exit	Returns to the global configuration mode.
exit	Returns to the management mode.

1.4 QoS Configuration Example

1.4.1 Example for Applying QoS Strategy on the Port

Configure the strategy that change the COS value of the message to 2 on the port. After the corresponding strategy is applied, another strategy to permit all data flows to pass must be configured. Otherwise, all data flows cannot get through:

ip access-list extended ipacl

permit ip 192.168.20.2 255.255.255.255 192.168.20.210 255.255.255.255

policy-map any

classify any

policy-map pmap

classify ip access-group ipacl

action cos 2

interface GigaEthernet0/2

qos policy pmap ingress

qos policy any ingress (pay attention to the order of two strategies applied)

Attack Prevention Configuration

Table of Contents

Chapter 1 Attack Prevention Configuration

1.1 Overview

To guarantee the reasonable usage of network bandwidth, our 6508 series switches provide the function to prevent vicious traffic from occupying lots of network bandwidth. In light of current attack modes, our 6508 series switches can limit the hosts that send lots of ARP, IGMP or IP message in a period of time and do not provide any service to these hosts. The function can prevent malicious message from occuping lots of network bandwidth. Therefore, the network can not be congested.

1.2 Attack Prevention Configuration Tasks

When the number of IGMP, ARP or IP message that is sent by a host in a designated interval exceeds the threshold, we think that the host attack the network.

You can select the type of attack prevention (ARP, IGMP or IP), the attack prevention port and the attack detection parameter. You have the following configuration tasks:

- Configuring the attack prevention type
- Configuring the attack detection parameters

1.3 Attack Prevention Configuration

1.3.1 Configuraing the Attack Detection Parameters

Command	Description
filter period *time*	Sets the attack detection period to **time**, whose unit is second.
filter threshold *vlaue*	Sets the attack detection threshold to **value**. The parameter **value** represents the number of messge at the threshold.
filter block-time *time*	Sets the out-of-service time for the attack source when the attack source is detected. Its unit is second.

1.3.2 Configuring the Attack Prevention Type

Command	Description
filter igmp	Detects the igmp attack.
fileter ip source-ip	Detects the IP attack based on the source IP address.
interface f x/y	Enters interface configuration mode for

	interface y at slot X.
filter arp	Detects the arp attack.

The ARP attack takes the host's MAC address and the source port as the attack source, that is, message from the same MAC address but different ports cannot be calculated together. Both the IGMP attack and IP attack take the host's IP address and source port as the attack source.

Remember that the IGMP attack prevention and the IP attack prevention cannot be started up together.

1.3.3 Starting up the Attack Prevention Function

After all parameters for attack prevention are set, you can start up the attack prevention function. Note that small parts of processor source will be occupied when the attack prevention function is started.

Command	Description
filter enable	Starts up the attack prevention function.

Use the **no filter enable** command to disable the attack prevention function and remove the block to all attack sources.

1.3.4 Checking the State of Attack Prevention

After attack prevention is started, you can run the following command to check the state of attack prevention:

Command	Description
show filter	Checks the state of attack prevention.

1.4 Attack Prevention Configuration Example

To enable the IGMP attack prevention and the ARP attack prevention on port 1/2, consider any host that sends more than 1200 pieces of message within 15 seconds as the attack source and to cut off network service for any attack source.

filter period 15

filter threshold 1200

filter block-time 600

interface f1/2

filter arp

exit

filter enable

Security Configuration

Table of Contents

Chapter 1 AAA Configuration

1.1 AAA Overview

Access control is the way to control access to the network and services. Authentication, authorization, and accounting (AAA) network security services provide the primary framework through which you set up access control on your router or access server.

1.1.1 AAA Security Service

AAA is an architectural framework for configuring a set of three independent security functions in a consistent manner. AAA provides a modular way of performing the following services:

• Authentication—Provides the method of identifying users, including login and password dialog, challenge and response, messaging support, and, depending on the security protocol you select, encryption.

Authentication is the way a user is identified prior to being allowed access to the network and network services. You configure AAA authentication by defining a named list of authentication methods, and then applying that list to various interfaces. The method list defines the types of authentication to be performed and the sequence in which they will be performed; it must be applied to a specific interface before any of the defined authentication methods will be performed. The only exception is the default method list (which is named "default"). The default method list is automatically applied to all interfaces if no other method list is defined. A defined method list overrides the default method list.

All authentication methods, except for local, line password, and enable authentication, must be defined through AAA. For information about configuring all authentication methods, including those implemented outside of the AAA security services, refer to the chapter "Configuring Authentication."

• Authorization—Provides the method for remote access control, including one-time authorization or authorization for each service, per-user account list and profile, user group support, and support of IP, IPX, ARA, and Telnet.

AAA authorization works by assembling a set of attributes that describe what the user is authorized to perform. These attributes are compared to the information contained in a database for a given user and the result is returned to AAA to determine the user's actual capabilities and restrictions. The database can be located locally on the access server or router or it can be hosted remotely on a RADIUS or TACACS+ security server. Remote security servers, such as RADIUS and TACACS+, authorize users for specific rights by associating attribute-value (AV) pairs, which define those rights with the appropriate user. All authorization methods must be defined through AAA.

As with authentication, you configure AAA authorization by defining a named list of authorization methods, and then applying that list to various interfaces. For information about configuring authorization using AAA, refer to the chapter "Configuring Authorization."

• Accounting—Provides the method for collecting and sending security server information used for billing, auditing, and reporting, such as user identities, start and

stop times, executed commands (such as PPP), number of packets, and number of bytes.

Accounting enables you to track the services users are accessing as well as the amount of network resources they are consuming. When AAA accounting is activated, the network access server reports user activity to the RADIUS or TACACS+ security server (depending on which security method you have implemented) in the form of accounting records. Each accounting record is comprised of accounting AV pairs and is stored on the access control server. This data can then be analyzed for network management, client billing, and/or auditing. All accounting methods must be defined through AAA. As with authentication and authorization, you configure AAA accounting by defining a named list of accounting methods, and then applying that list to various interfaces. For information about configuring accounting using AAA, refer to the chapter "Configuring Accounting."

1.1.2 Benefits of Using AAA

AAA provides the following benefits:

- • Increased flexibility and control of access configuration
- • Scalability
- • Standardized authentication methods, such as RADIUS, TACACS+, and Kerberos
- • Multiple backup systems

1.1.3 AAA Principles

AAA is designed to enable you to dynamically configure the type of authentication and authorization you want on a per-line (per-user) or per-service (for example, IP, IPX, or VPDN) basis. You define the type of authentication and authorization you want by creating method lists, then applying those method lists to specific services or interfaces.

1.1.4 Method Lists

A method list is a sequential list that defines the authentication methods used to authenticate a user. Method lists enable you to designate one or more security protocols to be used for authentication, thus ensuring a backup system for authentication in case the initial method fails. Cisco IOS software uses the first method listed to authenticate users; if that method does not respond, Cisco IOS software selects the next authentication method in the method list. This process continues until there is successful communication with a listed authentication method or the authentication method list is exhausted, in which case authentication fails.

The software attempts authentication with the next listed authentication method only when there is no response from the previous method. If authentication fails at any point in this cycle—meaning that the security server or local username database responds by denying the user access—the authentication process stops and no other authentication methods are attempted. The following figures shows a typical AAA network configuration that includes four security servers: R1 and R2 are RADIUS servers, and T1 and T2 are TACACS+ servers.

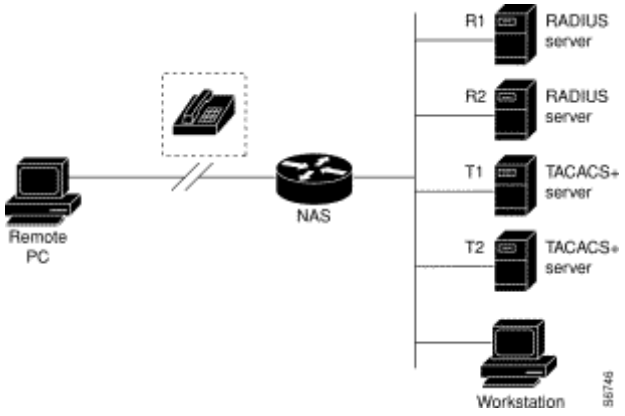


Figure 1-1 Typical AAA Network Configuration

Suppose the system administrator has defined a method list where R1 will be contacted first for authentication information, then R2, T1, T2, and finally the local username database on the access server itself. When a remote user attempts to dial in to the network, the network access server first queries R1 for authentication information. If R1 authenticates the user, it issues a PASS response to the network access server and the user is allowed to access the network. If R1 returns a FAIL response, the user is denied access and the session is terminated. If R1 does not respond, then the network access server processes that as an ERROR and queries R2 for authentication information. This pattern continues through the remaining designated methods until the user is either authenticated or rejected, or until the session is terminated. If all of the authentication methods return errors, the network access server will process the session as a failure, and the session will be terminated.

A FAIL response is significantly different from an ERROR. A FAIL means that the user has not met the criteria contained in the applicable authentication database to be successfully authenticated. Authentication ends with a FAIL response. An ERROR means that the security server has not responded to an authentication query. Because of this, no authentication has been attempted. Only when an ERROR is detected will AAA select the next authentication method defined in the authentication method list.

1.2 AAA Configuration Process

You must first decide what kind of security solution you want to implement. You need to assess the security risks in your particular network and decide on the appropriate means to prevent unauthorized entry and attack.

1.2.1 Overview of the AAA Configuration Process

Configuring AAA is relatively simple after you understand the basic process involved. To configure security on a Cisco router or access server using AAA, follow this process:

- If you decide to use a separate security server, configure security protocol parameters, such as RADIUS, TACACS+, or Kerberos.
- Define the method lists for authentication by using an AAA authentication command.

- Apply the method lists to a particular interface or line, if required.
- (Optional) Configure authorization using the aaa authorization command.
- (Optional) Configure accounting using the aaa accounting command.

1.3 AAA Authentication Configuration Task List

- Configuring Login Authentication Using AAA
- Configuring PPP Authentication Using AAA
- Enabling Password Protection at the Privileged Level
- Configuring Message Banners for AAA Authentication
- AAA authentication username-prompt
- AAA authentication password-prompt
- Establishing Username Authentication
- Enabling Password

1.4 AAA Authentication Configuration Task

To configure AAA authentication, perform the following configuration processes：

(1) If you decide to use a separate security server, configure security protocol parameters, such as RADIUS, TACACS+, or Kerberos.

(2) Define the method lists for authentication by using an AAA authentication command.

(3) Apply the method lists to a particular interface or line, if required.

1.4.1 Configuring Login Authentication Using AAA

The AAA security services facilitate a variety of login authentication methods. Use the aaa authentication login command to enable AAA authentication no matter which of the supported login authentication methods you decide to use. With the aaa authentication login command, you create one or more lists of authentication methods that are tried at login. These lists are applied using the login authentication line configuration command.

To configure login authentication by using AAA, use the following commands beginning in global configuration mode:

command	purpose
aaa authentication login {**default** | *list-name*}*method1* [*method2...*]	Enables AAA globally.

line [**console** | **vty**] *line-number* [*ending-line-number*]	Enters line configuration mode for the lines to which you want to apply the authentication list.
login authentication {**default** | *list-name*}	Applies the authentication list to a line or set of lines.

The list-name is a character string used to name the list you are creating. The method argument refers to the actual method the authentication algorithm tries. The additional methods of authentication are used only if the previous method returns an error, not if it fails. To specify that the authentication should succeed even if all methods return an error, specify none as the final method in the command line.

For example, to specify that authentication should succeed even if (in this example) the TACACS+ server returns an error, enter the following command:

aaa authentication login default group radius

Note：

Because the none keyword enables any user logging in to successfully authenticate, it should be used only as a backup method of authentication.

The following table lists the supported login authentication methods.：

Keyword	description
enable	Uses the enable password for authentication.
group *name*	Uses named server group for authentication.
group radius	Uses the list of all RADIUS servers for authentication.
line	Uses the line password for authentication.
local	Uses the local username database for authentication.
local-case	Uses case-sensitive local username authentication.
none	Uses no authentication.

(1) Login Authentication Using Enable Password

Use the aaa authentication login command with the enable method keyword to specify the enable password as the login authentication method. For example, to specify the enable password as the method of user authentication at login when no other method list has been defined, enter the following command:

aaa authentication login default enable

(2) Login Authentication Using Line Password

Use the aaa authentication login command with the line method keyword to specify the line password as the login authentication method. For example, to specify the line password as the method of user authentication at login when no other method list has been defined, enter the following command:

aaa authentication login default line

Before you can use a line password as the login authentication method, you need to define a line password.

(3) Login Authentication Using Local Password

Use the aaa authentication login command with the local method keyword to specify that the Cisco router or access server will use the local username

database for authentication. For example, to specify the local username database as the method of user authentication at login when no other method list has been defined, enter the following command:

aaa authentication login default local

For information about adding users into the local username database, refer to the section "Establishing Username Authentication" in this chapter.

(4) Login Authentication Using Group RADIUS

Use the aaa authentication login command with the group radius method to specify RADIUS as the login authentication method. For example, to specify RADIUS as the method of user authentication at login when no other method list has been defined, enter the following command:

aaa authentication login default group radius

Before you can use RADIUS as the login authentication method, you need to enable communication with the RADIUS security server. For more information about establishing communication with a RADIUS server, refer to the chapter "Configuring RADIUS."

1.4.2 Enabling Password Protection at the Privileged Level

Use the aaa authentication enable default command to create a series of authentication methods that are used to determine whether a user can access the privileged EXEC command level. You can specify up to four authentication methods. The additional methods of authentication are used only if the previous method returns an error, not if it fails. To specify that the authentication should succeed even if all methods return an error, specify none as the final method in the command line.

Use the following command in global configuration mode:

command	purpose
aaa authentication enable default *method1* [*method2...*]	Enables user ID and password checking for users requesting privileged EXEC level.

The method argument refers to the actual list of methods the authentication algorithm tries, in the sequence entered.

The following table lists the supported enable authentication methods.

Keyword	Description
enable	Uses the enable password for authentication.
group *group-name*	Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the aaa group server radius or aaa group server tacacs+ command.
group radius	Uses the list of all RADIUS hosts for authentication.
line	Uses the line password for authentication.
none	Uses no authentication.

1.4.3 Configuring Message Banners for AAA Authentication

AAA supports the use of configurable, personalized login and failed-login banners. You can configure message banners that will be displayed when a user logs in to the system to be authenticated using AAA and when, for whatever reason, authentication fails.

Configuring a Login Banner

To configure a banner that will be displayed whenever a user logs in (replacing the default message for login), use the following commands in global configuration mode:：

command	purpose
aaa authentication banner *delimiter text-string delimiter*	Creates a personalized login banner.

Configuring a Failed-Login Banner

To configure a message that will be displayed whenever a user fails login (replacing the default message for failed login), use the following commands in global configuration mode:：

command	purpose
aaa authentication fail-message *delimiter text-string delimiter*	Creates a message to be displayed when a user fails login.

Instruction

To create a login banner, you need to configure a delimiting character, which notifies the system that the following text string is to be displayed as the banner, and then the text string itself. The delimiting character is repeated at the end of the text string to signify the end of the banner. The delimiting character can be any single character in the extended ASCII character set, but once defined as the delimiter, that character cannot be used in the text string making up the banner.

1.4.4 AAA authentication username-prompt

To change the text displayed when users are prompted to enter a username, use the aaa authentication username-prompt command in global configuration mode. To return to the default username prompt text, use the no form of this command. username：

The aaa authentication username-prompt command does not change any dialog that is supplied by a remote TACACS+ server. Use the following command to configure in global configuration mode：

command	purpose
aaa authentication username-prompt *text-string*	String of text that will be displayed when the user is prompted to enter an username.

1.4.5 AAA authentication password-prompt

To change the text displayed when users are prompted for a password, use the aaa authentication password-prompt command in global configuration mode. To return to the default password prompt text, use the no form of this command.

password：

The aaa authentication password-prompt command does not change any dialog that is supplied by a remote TACACS+ server. Use the following command to configure in global configuration mode：

command	purpose
aaa authentication password-prompt *text-string*	String of text that will be displayed when the user is prompted to enter a password.

1.4.6 Establishing Username Authentication

You can create a username-based authentication system, which is useful in the following situations:

• To provide a TACACS-like username and encrypted password-authentication system for networks that cannot support TACACS

• To provide special-case logins: for example, access list verification, no password verification, autocommand execution at login, and "no escape" situations

To establish username authentication, use the following commands in global configuration mode as needed for your system configuration:

Use the no form of this command to delete a username.

username *name* {**nopassword** | **password** *password* | **password encryption-type** *encrypted-password*}

username *name* [**autocommand** *command*]

username *name* [**callback-dialstring** *telephone-number*]

username *name* [**callback-rotary** *rotary-group-number*]

username *name* [**callback-line** [**tty** | **aux**] *line-number* [*ending-line-number*]]

username *name* [**noescape**] [**nohangup**]

username *name* [**privilege** *level*]

username *name* [**user-maxlinks** *number*]

no username *name*

1.4.7 Enabling password

To set a local password to control access to various privilege levels, use the enable password command in global configuration mode. To remove the password requirement, use the no form of this command.

enable password { [***encryption-type***] *encrypted-password*} [**level** *level*]

no enable password [**level** *level*]

1.5 AAA Authentication Configuration Example

1. RADIUS Authentication Example

This section provides one sample configuration using RADIUS.

The following example shows how to configure the switch to authenticate and authorize using RADIUS:

aaa authentication login radius-login group radius local

aaa authorization network radius-network radius

line vty

login authentication radius-login

The lines in this sample RADIUS authentication and authorization configuration are defined as follows:：

- The aaa authentication login radius-login radius local command configures the router to use RADIUS for authentication at the login prompt. If RADIUS returns an error, the user is authenticated using the local database.
- The aaa authentication ppp radius-ppp radius command configures the software to use PPP authentication using CHAP or PAP if the user has not already logged in. If the EXEC facility has authenticated the user, PPP authentication is not performed.
- The aaa authorization network radius-network radius command command queries RADIUS for network authorization, address assignment, and other access lists.
- The login authentication radius-login command enables the radius-login method list for line 3.

1.6 AAA Authorization Configuration Task List

- Configuring EXEC Authorization using AAA

1.7 AAA Authorization Configuration Task

To configure AAA authorization, perform the following configuration processes：

(1) If you decide to use a separate security server, configure security protocol parameters, such as RADIUS, TACACS+, or Kerberos.

(2) Define the method lists for authorization by using an AAA authorization command.

(3) Apply the method lists to a particular interface or line, if required.

1.7.1 Configuring EXEC Authorization using AAA

Use the aaa authorization command to enable authorization

Use aaa authorization exec command to run authorization to determine if the user is allowed to run an EXEC shell. This facility might return user profile information such as autocommand information.

Use line configuration command login authorization to apply these lists. Use the following command in global configuration mode:

command	purpose
aaa authorization exec {**default** | *list-name*}*method1* [*method2...*]	Establishes global authorization list.
line [**console** | **vty**] *line-number* [*ending-line-number*]	Enters the line configuration mode for the lines to which you want to apply the authorization method list.
login authorization {**default** | *list-name*}	Applies the authorization list to a line or set of lines(in line configuration mode).

The keyword list-name is the character string used to name the list of authorization methods.

The keyword method specifies the actual method during authorization process. Method lists enable you to designate one or more security protocols to be used for authorization, thus ensuring a backup system in case the initial method fails. The system uses the first method listed to authorize users for specific network services; if that method fails to respond, the system selects the next method listed in the method list. This process continues until there is successful communication with a listed authorization method, or all methods defined are exhausted. If all specified methods fail to respond, and you still want the system to enter the EXEC shell, you should specify none as the last authorization method in command line.

Use default parameter to establish a default list, and the default list will apply to all interfaces automatically. For example, use the following command to specify radius as the default authorization method for exec:

aaa authorization exec default group radius

Note：

If no method list is defined, the local authorization service will be unavailable and the authorization is allowed to pass..

The following table lists the currently supported EXEC authorization mode：

keyword	description
group *WORD*	Uses a named server group for authorization.
group radius	Uses radius authorization.
local	Uses the local database for authorization.
if-authenticated	Allows the user to access the requested function if the user is authenticated.
none	No authorization is performed.

1.8 AAA Authorization Example

1. EXEC local authorization example

```
aaa authentication login default local
aaa authorization exec default local
!
username exec1 password 0 abc privilege 15
username exec2 password 0 abc privilege 10
username exec3 nopassword
username exec4 password 0 abc user-maxlinks 10
username exec5 password 0 abc autocommand telnet 172.16.20.1
!
```

The lines in this sample RADIUS authorization configuration are defined as follows:：

- The aaa authentication login default local command defines the default method list of login authentication. This method list applies to all login authentication servers automatically.
- The aaa authorization exec default local command defines default method list of exec authorization. The method list automatically applies to all users that need to enter exec shell.
- Username is exec1，login password is abc，EXEC privileged level is 15(the highest level)，that is, when user exec1 whose privileged level is 15 logs in exec shell, all commands can be checked and performed.
- Username is exec2，login password is abc，EXEC privileged level is 10，that is, when user exec2 whose privileged level is 10 logs in EXEC shell, commands with privileged level less than 10 can be checked and performed.
- Username is exec3，no password is needed for login.
- Username is exec4，login password is abc，the maximum links of the user is 10.
- Username is exec5，login password is abc, user performs telnet 172.16.20.1 immediately when logging in exec shell.

1.9 AAA Accounting Configuration Task List

- Configuring Connection Accounting using AAA
- Configuring Network Accounting using AAA

1.10 AAA Accounting Configuration Task

To configure AAA accounting, perform the following configuration processes：

(1) If you decide to use a separate security server, configure security protocol parameters, such as RADIUS, TACACS+, or Kerberos.

(2) Define the method lists for accounting by using an AAA accounting command.

(3) Apply the method lists to a particular interface or line, if required.

1.10.1 Configuring Accounting Connection using AAA

Use the aaa accounting command to enable AAA accounting.

To create a method list to provide accounting information about all outbound connections made from the network access server, use the aaa accounting connection command.

command	purpose
aaa accounting connection {**default** | *list-name*} {**start-stop** | **stop-only** | **none**} **group** *groupname*	Establishes global accounting list.

The keyword list-name is used to name any character string of the establishing list. The keyword method specifies the actual method adopted during accounting process.

The following table lists currently supported connection accounting methods：

keyword	description
group *WORD*	Enables named server group for accounting.
group radius	Enables radius accounting.
none	Disables accounting services for the specified line or interface.
stop-only	Sends a "stop" record accounting notice at the end of the requested user process.
start-stop	RADIUS or TACACS+ sends a "start" accounting notice at the beginning of the requested process and a "stop" accounting notice at the end of the process.

1.10.2 Configuring Network Accounting using AAA

Use the aaa accounting command to enable AAA accounting.

To create a method list to provide accounting information for SLIP, PPP, NCPs, and ARAP sessions, use the aaa accounting network command in global configuration mode.

command	purpose
aaa accounting network {**default** | *list-name*} {**start-stop** | **stop-only** | **none**} **group** *groupname*	Enables global accounting list.

The keyword list-name is used to name any character string of the establishing list. The keyword method specifies the actual method adopted during accounting process.

The following table lists currently supported network accounting methods：

keyword	description
group *WORD*	Enables named server group for accounting.
group radius	Enables radius accounting.
none	Disables accounting services for the specified line or interface.
stop-only	Sends a "stop" record accounting notice at the end of the requested user process.
start-stop	RADIUS or TACACS+ sends a "start" accounting notice at the beginning of the requested process and a "stop" accounting notice at the end of the process.

1.10.3 AAA accounting update

To enable periodic interim accounting records to be sent to the accounting server, use the aaa accounting update command in global configuration mode. To disable interim accounting updates, use the no form of this command.

Command	purpose
aaa accounting update [**newinfo**] [**periodic** *number*]	Enables AAA accounting update.

If the newinfo keyword is used, interim accounting records will be sent to the accounting server every time there is new accounting information to report. An example of this would be when IP Control Protocol (IPCP) completes IP address negotiation with the remote peer. The interim accounting record will include the negotiated IP address used by the remote peer.

When used with the periodic keyword, interim accounting records are sent periodically as defined by the argument number. The interim accounting record contains all of the accounting information recorded for that user up to the time the accounting record is sent.

When using both the newinfo and periodic keywords, interim accounting records are sent to the accounting server every time there is new accounting information to report, and accounting records are sent to the accounting server periodically as defined by the argument number. For example, if you configure the aaa accounting update newinfo periodic number command, all users currently logged in will continue to generate periodic interim accounting records while new users will generate accounting records based on the newinfo algorithm.

1.10.4 AAA accounting suppress null-username

To prevent the AAA system from sending accounting records for users whose username string is NULL, use the aaa accounting suppress null-username command in global configuration mode. To allow sending records for users with a NULL username, use the no form of this command.

- **aaa accounting suppress null-username**

Chapter 2 Configuing RADIUS

This chapter describes the Remote Authentication Dial-In User Service (RADIUS) security system, defines its operation, and identifies appropriate and inappropriate network environments for using RADIUS technology. The "RADIUS Configuration Task List" section describes how to configure RADIUS with the authentication, authorization, and accounting (AAA) command set.

2.1 Introduction

2.1.1 RADIUS Introduction

RADIUS is a distributed client/server system that secures networks against unauthorized access. In the implementation, RADIUS clients run on switches and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.

RADIUS has been implemented in a variety of network environments that require high levels of security while maintaining network access for remote users.

Use RADIUS in the following network environments that require access security:：

- Networks with multiple-vendor access servers, each supporting RADIUS. For example, access servers from several vendors use a single RADIUS server-based security database. In an IP-based network with multiple vendors' access servers, dial-in users are authenticated through a RADIUS server that has been customized to work with the Kerberos security system.

- Networks in which a user must only access a single service. Using RADIUS, you can control user access to a single host, to a single utility such as Telnet, or to a single protocol such as Point-to-Point Protocol (PPP). For example, when a user logs in, RADIUS identifies this user as having authorization to run PPP using IP address 10.2.3.4 and the defined access list is started.

- Networks that require resource accounting. You can use RADIUS accounting independent of RADIUS authentication or authorization. The RADIUS accounting functions allow data to be sent at the start and end of services, indicating the amount of resources (such as time, packets, bytes, and so on) used during the session. An Internet service provider (ISP) might use a freeware-based version of RADIUS access control and accounting software to meet special security and billing needs.

RADIUS is not suitable in the following network security situations:：

- Multiprotocol access environments. RADIUS does not support the following protocols:：

  AppleTalk Remote Access (ARA)

  NetBIOS Frame Control Protocol (NBFCP)

- NetWare Asynchronous Services Interface (NASI)
- X.25 PAD connections
- Switch-to-switch situations. RADIUS does not provide two-way authentication.
- Networks using a variety of services. RADIUS generally binds a user to one service model.

2.1.2 RADIUS Operation

When a user attempts to log in and authenticate to an access server using RADIUS, the following steps occur:：

(1) The user is prompted for and enters a username and password.

(2) The username and encrypted password are sent over the network to the RADIUS server.

(3) The user receives one of the following responses from the RADIUS server:

a. ACCEPT—The user is authenticated.

b. REJECT—The user is not authenticated and is prompted to reenter the username and password, or access is denied.

c. CHALLENGE—A challenge is issued by the RADIUS server. The challenge collects additional data from the user.

d. CHANGE PASSWORD—A request is issued by the RADIUS server, asking the user to select a new password.

The ACCEPT or REJECT response is bundled with additional data that is used for EXEC or network authorization. You must first complete RADIUS authentication before using RADIUS authorization. The additional data included with the ACCEPT or REJECT packets consists of the following:

• Services that the user can access, including Telnet, rlogin, or local-area transport (LAT) connections, and PPP, Serial Line Internet Protocol (SLIP), or EXEC services.

• Connection parameters, including the host or client IP address, access list, and user timeouts.

2.2 RADIUS Configuration Task List

To configure RADIUS on your switch or access server, you must perform the following tasks:：

- Use the aaa authentication global configuration command to define method lists for RADIUS authentication. For more information about using the aaa authentication command, refer to the "Configuring Authentication" chapter.
- Use line and interface commands to enable the defined method lists to be used. For more information, refer to the "Configuring Authentication" chapter.

(1) The following configuration tasks are optional:：

- You may use the aaa authorization global command to authorize specific user functions. For more information about using the aaa authorization command, refer to the chapter "Configuring Authorization."

- You may use the aaa accounting command to enable accounting for RADIUS connections. For more information about using the aaa accounting command, refer to the chapter "Configuring Accounting."

2.3 RADIUS Configuration Task List

- Configuring Switch to RADIUS Server Communication
- Configuring Switch to Use Vendor-Specific RADIUS Attributes
- Specifying RADIUS Authentication
- Specifying RADIUS Authorization
- Specifying RADIUS Accounting

2.4 RADIUS Configuration Task

2.4.1 Configuring Switch to RADIUS Server Communication

The RADIUS host is normally a multiuser system running RADIUS server software from Livingston, Merit, Microsoft, or another software provider.

A RADIUS server and a Cisco router use a shared secret text string to encrypt passwords and exchange responses.

To configure RADIUS to use the AAA security commands, you must specify the host running the RADIUS server daemon and a secret text (key) string that it shares with the router.

To configure per-server RADIUS server communication, use the following command in global configuration mode:

command	purpose
radius-server host *ip-address* [**auth-port** *port-number*][**acct-port** *portnumber*]	Specifies the IP address or host name of the remote RADIUS server host and assign authentication and accounting destination port numbers.
radius-server key *string*	Specifies the shared secret text string used between the router and a RADIUS server.

To configure global communication settings between the router and a RADIUS server, use the following radius-server commands in global configuration mode:：

command	purpose
radius-server retransmit *retries*	Specifies how many times the switch transmits each RADIUS request to the server before giving up (the default is 2).

radius-server timeout *seconds*	Specifies for how many seconds a switch waits for a reply to a RADIUS request before retransmitting the request.
radius-server deadtime *minutes*	Specifies for how many minutes a RADIUS server that is not responding to authentication requests is passed over by requests for RADIUS authentication.

2.4.2 Configuring Switch to Use Vendor-Specific RADIUS Attributes

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific information between the network access server and the RADIUS server by using the vendor-specific attribute (attribute 26).

Vendor-specific attributes (VSAs) allow vendors to support their own extended attributes not suitable for general use.

For more information about vendor-IDs and VSAs, refer to RFC 2138, Remote Authentication Dial-In User Service (RADIUS). To configure the network access server to recognize and use VSAs, use the following command in global configuration mode:

command	purpose
radius-server vsa send [authentication]	Enables the network access server to recognize and use VSAs as defined by RADIUS IETF attribute 26.

2.4.3 Specifying RADIUS Authentication

After you have identified the RADIUS server and defined the RADIUS authentication key, you must define method lists for RADIUS authentication. Because RADIUS authentication is facilitated through AAA, you must enter the aaa authentication command, specifying RADIUS as the authentication method. For more information, refer to the chapter "Configuring Authentication."

2.4.4 Specifying RADIUS Authorization

AAA authorization lets you set parameters that restrict a user's access to the network. Authorization using RADIUS provides one method for remote access control, including one-time authorization or authorization for each service, per-user account list and profile, user group support, and support of IP, IPX, ARA, and Telnet. Because RADIUS authorization is facilitated through AAA, you must issue the aaa authorization command, specifying RADIUS as the authorization method. For more information, refer to the chapter "Configuring Authorization."

2.4.5 Specifying RADIUS Accounting

The AAA accounting feature enables you to track the services users are accessing as well as the amount of network resources they are consuming. Because RADIUS accounting is facilitated through AAA, you must issue the aaa accounting command, specifying RADIUS as the accounting method. For more information, refer to the chapter "Configuring Accounting."

2.5 RADIUS Configuration Examples

2.5.1 RADIUS Authentication and Authorization Example

The following example shows how to configure the router to authenticate and authorize using RADIUS:

aaa authentication login use-radius group radius local

The lines in this sample RADIUS authentication and authorization configuration are defined as follows:：

aaa authentication login use-radius radius local configures the router to use RADIUS for authentication at the login prompt. If RADIUS returns an error, the user is authenticated using the local database. In this example, use-radius is the name of the method list, which specifies RADIUS and then local authentication.

RADIUS Authentication, Authorization, and Accounting Example

The following example shows a general configuration using RADIUS with the AAA command set:：

radius-server host 1.2.3.4

radius-server key myRaDiUSpassWoRd

username root password AlongPassword

aaa authentication login admins radius local

line vty 1 16

login authentication admins

The lines in this example RADIUS authentication, authorization, and accounting configuration are defined as follows:：

radius-server host command defines the IP address of the RADIUS server host.；

radius-server key command defines the shared secret text string between the network access server and the RADIUS server host.

aaa authentication login admins group radius local command defines the authentication method list "dialins," which specifies that RADIUS authentication and then (if the RADIUS server does not respond) local authentication will be used on serial lines using PPP.；

login authentication admins command applies the "admins" method list for login authentication.

Chapter 3 Web Authentication Configuration

The section describes the concept of Web authentication and configuration and usage of the Web authentication.

3.1 Overview

3.1.1 Web Authentication

The Web authentication of the switch is a connection control mode as PPPoE and 802.1x. When you use the Web authentication, the login and logout operations can be successfully performed through the interaction of the browser and the builtin portal server of the switch. During the operations of login and logout, no other client software need be installed.

1. Device role

The roles that the network devices take during the Web authentication are shown in Figure 3-1:

- **Client**: It is a user computer that accesses network through the switch. The user computer need be configured the network browser, the function of DHCP client and the function to originate DNS query.
- **DHCP server**: It is to distribute the IP address for users.
- **AAA server**: It is to save user right information and to charge users for their network access.
- **Switch**: It is a switch having Web authentication. It is to control the access right of users and works as an agent between users and AAA server.

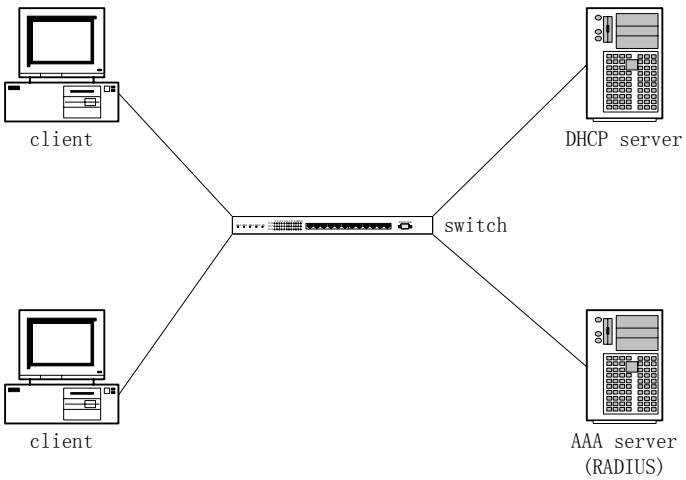


Figure 3-1 Web authentication network

2. Authentication flow

According to different configuration strategies, the Web authentication flow of the switch may relate to protocols such as DHCP and DNS. Its typical flow is shown in Figure 3-2. The Web authentication flow generally contains the following steps:

(1) The DHCP server sends a DHCP confirmation request to a user through the switch after the user originates the process of DHCP address distribution. The switch then identifies and records the user.

(1) The user accesses any Website through the browser (Write down the domain name, not the IP address, in the host part of the **url** column in the browser), which activates the DNS request of the user computer.

(2) The DNS server returns the user a request response. The switch captures the request response message and changes the resolved address to the address of the built-in portal server in the switch.

(3) The DHCP confirmation process continues after the browser captures DNS resolution. The switch returns the corresponding authentication page according to different authentication methods after the switch receives the request.

(4) The user submits the authentication request; the switch authenticates the user through the AAA server after the switch receives information submitted by the user; if the authentication succeeds, the AAA server will be notified to start charging; the switch gives the user the network access right and returns the user a page that the authentication is successful; meanwhile, the switch also returns a **keep alive** page, which periodically sends the **user online** notification to the switch.

(5) The user sends the logout request to the switch through the browser. The switch then notifies the AAA server to stop charging, and withdraws the network access right from the user.

(6) In the period between successful user authentication and logout, the switch periodically detects the user online notification. If the notification is not received in the preset time, the switch consuders that the user abnormally logs off, notifies the AAA server to stop charging and withdraws the network access right from the user.

The above steps may vary a little with configuration strategies and user’s operations. For example, if user directly accesses the portal server of the switch before the authentication is approved, DNS-related processes will not be enabled.

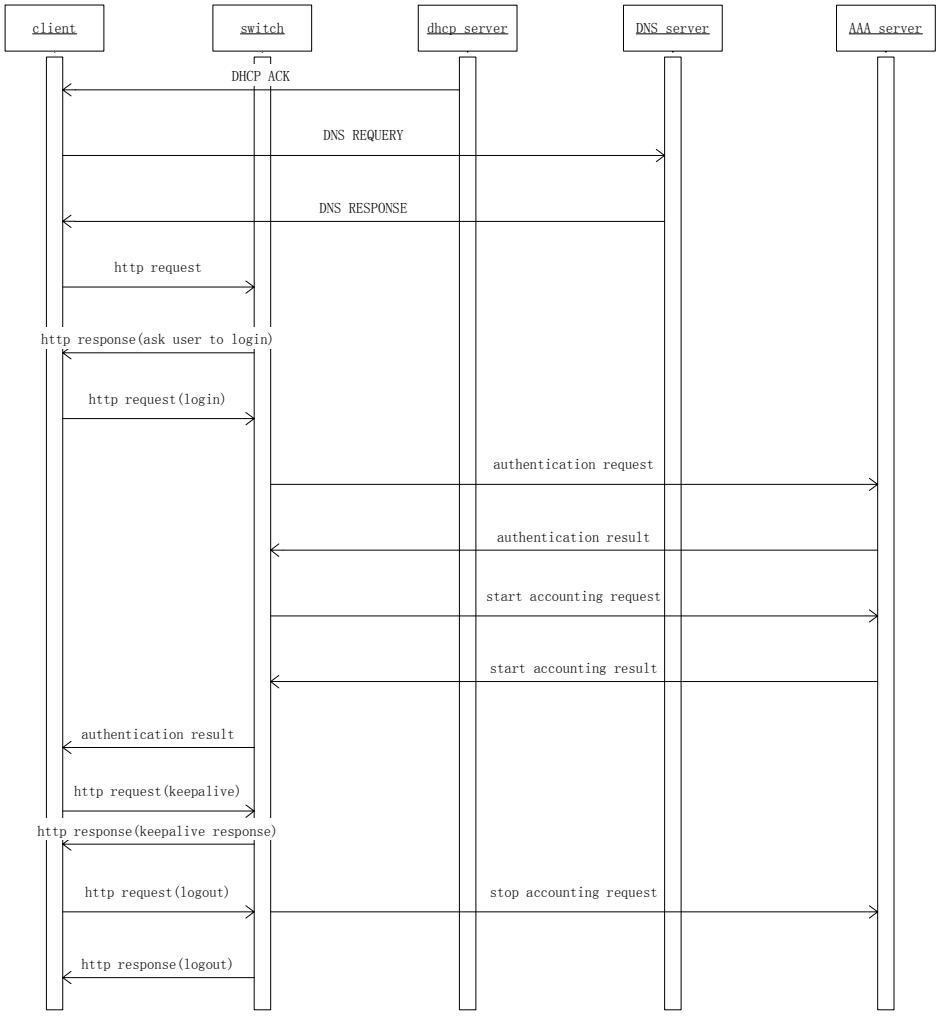


Figure 3-2 web authentication flow

3.1.2 Planning Web Authentication

1. Planning the authentication mode

Two authentication modes are provided to control user's access:

Username/password authentication mode: In this mode, the switch identifies the user through the username and password, and notifies the AAA server to start charging according to username; user needs to enter the username and password through the browser.

VLAN ID authentication mode: In this mode, the switch identifies the user through the VLAN ID the user belongs to, and notifies the AAA server to start charging according to VLAN ID; user only requires to confirm corresponding operations on the Web page before accessing the network.

Different operation strategies adopt different authentication modes. The supported maximum number of users that simultaneously access the network varies with the

authentication mode. For the username/password authentication mode, the switch supports simultaneously accessed users as many as its performance permits. For the VLAN ID authentication mode, the maximum number of simultaneously accessed users equals the number of VLAN that the switch supports.

2. Planning network topology

The switch takes the routing interface as a unit to set the authentication attribute. If the Web authentication function is enabled on a routing interface, network accesses through the routing interface are all controlled by the Web authentication. The DHCP server, DNS server or AAA server should connect the switch through the interface with Web authentication function disabled. Figure 3-3 shows the relative typical network topology.

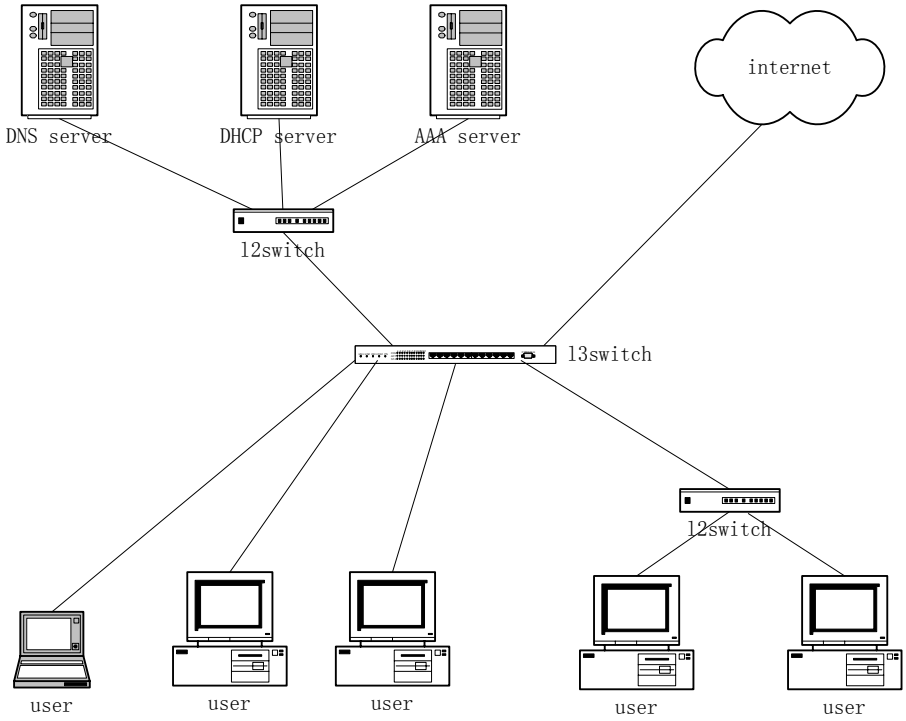


Figure 3-3 Typical network topology

3.2 Configuring Web Authentication

3.2.1 Global Configuration

1. Configuring the address of the portal server

Run the following command in global configuration mode to configure the address of the portal server:

Run…	To...
web-auth portal-server *A.B.C.D*	Configure the IP address of the portal server.

2. Configuring authentication duration

The parameter **authtime** determines the maximum time of user's authentication. If the authentication is not approved within the maximum time, the switch terminates the authentication procedure.

Run the following command in global configuration mode to configure the authentication duration (Unit: second):

Run...	To...
web-auth authtime <60-65535>	Configure the authentication duration.

3. Configuring the transmission period of the online notification

Through the online notification sent by the browser, the switch checks whether the user is online.

Run the following command in global configuration mode to configure the transmission period (unit: second):

Run...	To...
web-auth keep-alive <60-65535>	Configure the transmission period for the online notification.

4. Configuring the duration to detect the abnormal logout

When the switch does not receive the user online notification from the browser in the set duration, the switch considers that user logs out abnormally.

Run the following command in global configuration mode to configure the duration to detect the abnormal logout:

Run...	To...
web-auth holdtime <60-65535>	Configure the duration to detect user's abnormal logout.

5. Configuring password for the VLAN ID authentication

When the authentication mode is set to VLAN ID, the switch takes **vlan n** as the user name, **n** representing the corresponding VLAN serial number. All user names use the same password.

Run the following command in global configuration mode to configure the password for the VLAN ID authentication:

Run...	To...
web-auth vlan-password <WORD>	Configure the password for the VLAN ID authentication.

3.2.2 Interface Configuration

1. Configuring authentication mode

The switch provides two authentication modes: username/password and VLAN ID.

Run the following command in interface configuration mode to configure the authentication mode:

Run...	To...
web-auth mode user | *vlan-id*	Configure the authentication mode.

2. Configuring authentication method list

Different authentication method lists can be applied on each interface. By default, the authentication method list named **default** is applied on each interface.

Run the following command in interface configuration mode to configure the authentication method list:

Run...	To...
web-auth authentication WORD	Configure the authentication method list.

3. Configuring the accounting method list

Different accounting method lists can be applied on each interface. By default, the accounting method list named **default** is applied on each interface.

Run the following command in interface configuration mode to configure the accounting method list:

Run...	To...
web-auth accounting WORD	Configure the accounting method list.

3.2.3 Enabling Web Authentication

If global configuration and interface configuration satisfy the requirements, you can enable the Web authentication on the designated routing switch.

Run the following command in interface configuration mode to enable the Web authentication:

Run...	To...
web-auth enable	Enable the Web authentication.

3.3 Monitoring and Maintaining Web Authentication

3.3.1 Checking the Global Configuration

Run the following command in privileged mode to check the global configuration:

Run...	To...
show web-auth	Check the global configuration.

3.3.2 Checking Interface Configuration

Run the following command in interface configuration mode to check the interface configuration:

Run...	To...
show web-auth interface [**vlan** | **SuperVlan]**	Check the interface configuration.

3.3.3 Checking User State

Run the following command in privileged mode to check the user state:

Run...	To...
show web-auth user	Check the user state.

3.3.4 Mandatorily Kicking Out Users

Run the following command in global configuration mode to mandatorily kick out a user.

Run...	To...
web-auth kick-out user-IP	Mandatorily kick out a user.

3.4 Web Authentication Configuration Example

Network topology

See Figure 3-4:

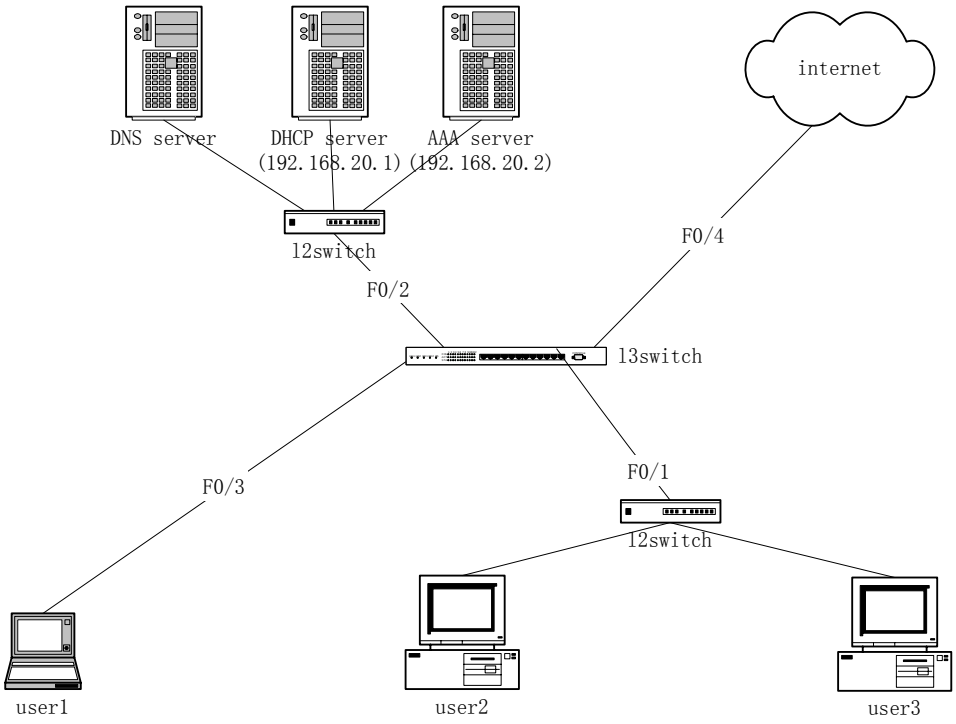


Figure 3-4 Network topology

Global configuration

```
aaa authentication login auth-weba radius
aaa accounting network acct-weba start-stop radius
!
radius-server host 192.168.20.2 auth-port 1812 acct-port 1813
radius-server key 405.10
!
ip dhcpd enable
ip http server
!
vlan 1-4
!
web-auth portal-server 192.168.20.41
web-auth holdtime 3600
web-auth authtime 600
web-auth keep-alive 180
```

Configuration of the layer-2 interface

```
interface FastEthernet0/1
 switchport pvid 1
!
interface FastEthernet0/2
 switchport pvid 2
```

```
!
interface FastEthernet0/3
 switchport pvid 3
!
interface FastEthernet0/4
 switchport pvid 4
```

Configuration of the routing interface

```
interface VLAN1
 no ip directed-broadcast
 ip helper-address 192.168.20.1
 web-auth accounting acct-weba
 web-auth authentication auth-weba
 web-auth mode vlan-id
 web-auth enable
!
interface VLAN2
 ip address 192.168.20.41 255.255.255.0
 no ip directed-broadcast
!
interface VLAN3
 no ip directed-broadcast
 ip helper-address 192.168.20.1
 web-auth accounting acct-weba
 web-auth authentication auth-weba
 web-auth mode user
 web-auth enable
!
interface VLAN4
 no ip directed-broadcast
!
```

EPON OAM Settings

Table of Contents

Chapter 1 **EPON OAM Settings**

1.1 OAM Overview

EFM OAM of IEEE 802.3ah provides point-to-point link trouble/performance detection on the single link. However, EFM OAM cannot be applied to EVC and so terminal-to-terminal Ethernet monitoring cannot be realized. OAM PDU cannot be forwarded to other interfaces. Ethernet OAM regulated by IEEE 802.3ah is a relatively slow protocol. The maximum transmission rate is 10 frames per second and the minimum transmission rate is 1 frame per second.

1.1.1 OAM Protocol's Attributes

- Supporting Ethernet OAM devices and OAM attributes

  The Ethernet OAM connection process is called as the Discovery phase when the OAM entity finds the OAM entity of the remote device and a stable session will be established. During the phase, the connected Ethernet OAM entities report their OAM mode, Ethernet OAM configuration information and local-node-supported Ethernet OAM capacity to each other by interacting the information OAM PDU. If the loopback configuration, unidirectional link detection configuration and link-event configuration have been passed on the Ethernet OAM of the two terminals, the Ethernet OAM protocol will start working on the link layer.

- Link monitoring

  The Ethernet OAM conducts the link monitoring through Event Notification OAM PDU. If the link has troubles and the local link monitors the troubles, the local link will transmits Event Notification OAM PDU to the peer Ethernet OAM to report the normal link event. The administrator can dynamically know the network conditions through link monitoring. The definition of a normal link event is shown in table 1.

Table 1 Definition of the normal link event

Normal Link Event	Definition
Error signal periodical event	Means the threshold that error signals exceed in a period of *N* signals.
Error frame event	Means the threshold that error frames exceed at a time unit.
Error frame periodical event	Means the threshold that error frames exceed in a period of *N* frames.
Error frame second event	Means the threshold that the seconds of error frames exceed in a period of *M* seconds.

- Remote trouble indication

It is difficult to check troubles in the Ethernet, especially the case that the network performance slows down while physical network communication continues. OAM PDU defines a flag domain to allow Ethernet OAM entity to transmit the trouble information to the peer. The flag can stand for the following emergent link events:

- Link Fault: The physical layer detects that the reception direction of the local DTE has no effect. If troubles occur, some devices at the physical layer support unidirectional operations and allows trouble notification from remote OAM.

- Dying Gasp: If an irrecoverable local error occurs, such as OAM shutdown, the interface enters the **error-disabled** state and then is shut down.

- Critical Event: Uncertain critical events occur (critical events are specified by the manufacturer).

Information OAM PDU is continuously transmitted during Ethernet OAM connection. The local OAM entity can report local critical link events to remote OAM entity through Information OAM PDU. The administrator thus can dynamically know the link's state and handle corresponding errors in time.

- Remote loopback

OAM provides an optional link-layer-level loopback mode and conducts error location and link performance testing through non-OAM-PDU loopback. The remote loopback realizes only after OAM connection is created. After the OAM connection is created, the OAM entity in active mode triggers the remote loopback command and the peer entity responses the command. If the remote terminal is in loopback mode, all packets except OAM PDU packets and Pause packets will be sent back through the previous paths. Error location and link performance testing thus can be conducted. When remote DTE is in remote loopback mode, the local or remote statistics data can be queried and compared randomly. The query operation can be conducted before, when or after the loopback frame is transmitted to the remote DTE. Regular loopback check can promptly detect network errors, while segmental loopback check can help locating these network errors and then remove these errors.

1.1.2 OAM Mode

The device can conduct the OAM connection through two modes: active mode and passive mode. The device capacity in different mode is compared in table 1. Only OAM entity in active mode can trigger the connection process, while the OAM entity in passive mode has to wait for the connection request from the peer OAM entity. After the remote OAM discovery process is done, the local entity in active mode can transmit any OAM PDU packet if the remote entity is in active mode, while the local entity's operation in active mode will be limited if the remote entity is in passive mode. This is because the device in active mode does not react on remote loopback commands and variable requests transmitted by the passive remote entity.

Table 2 Comparing device capacity in active and passive modes

Capacity	Active Mode	Passive Mode
Initializing the Ethernet OAM discovery process	Yes	No

Responding to the OAM discovery initialization process	Yes	Yes
Transmitting the Information OAM PDU packet	Yes	Yes
Permitting to transmit the Event Notification OAM PDU packet	Yes	Yes
Allowing to transmit the Variable Request OAM PDU packet	Yes	No
Allowing to transmit Variable Response OAM PDU packet	Yes	Yes
Allowing to transmit the Loopback Control OAM PDU packet	Yes	No
Responding to Loopback Control OAM PDU	Yes, but there is a request that the peer must be in ACTIVE mode.	Yes
Allowing to transmit specified OAM PDU	Yes	Yes

After the Ethernet OAM connection is established, the OAM entities at two terminals maintain connection by transmitting the Information OAM PDU packets. If the Information OAM PDU packet from the peer OAM entity is not received in five seconds, the connection times out and a new OAM connection then requires to be established.

1.1.3 Components of the OAM Packet

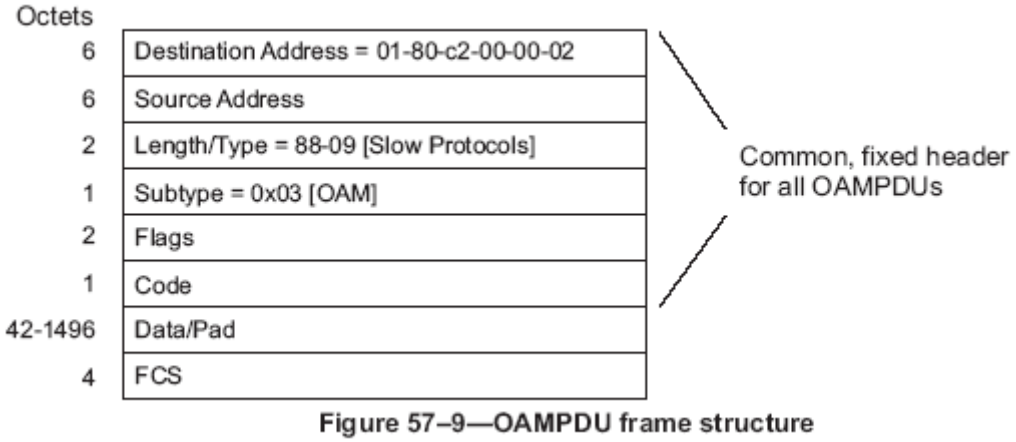


Figure 57–9—OAMPDU frame structure

Figure 1 Components of the OAM packet

The following are the meanings of the fields of the OAM packet:

- Destination address: means the destination MAC address of the Ethernet OAM packet.

- Source address: Source MAC address of the Ethernet OAM packet
  It is the MAC address of the transmitter terminal's port and also a unicast MAC address.
- Length/Type: Always adopts the Type encoding. The protocol type of the Ethernet OAM packet is 0x8809.
- Subtype: The subtype of the protocol for Ethernet OAM packets is 0x03.
- Flags: a domain where the state of Ethernet OAM entity is shown
- Code: a domain where the type of the OAMPDU packet is shown
- Data/Pad: a domain including the OAMPDU data and pad values
- FCS: checksum of the frame

Table 3 Type of the CODE domain

CODE	OAMPDU
00	Information
01	Event Notification
02	Variable Request
03	Variable Response
04	Loopback Control
05-FD	Reserved
FE	Organization Specific
FF	Reserved

The Information OAM PDU packet is used to transmit the information about the state of the OAM entity to the remote OAM entity to maintain the OAM connection.

The Event Notification OAMPDU packet is used to monitor the link and report the troubles occurred on the link between the local and remote OAM entities.

The Loopback control OAMPDU packet is mainly used to control the remote loopback, including the state of the OAM loopback from the remote device. The packet contains the information to enable or disable the loopback function. You can open or shut down the remote loopback according to the contained information.

1.2 EPON OAM Configuration Task List

- Enabling Remote OAM Loopback
- Displaying the Information About OAM Protocol

1.3 EPON OAM Configuration Tasks

1.3.1 Enabling Remote EPON OAM Loopback

The procedure to enable remote loopback on an interface is shown in the following table:

Table 4 Enabling the remote loopback of EPON OAM

Procedure	Command	Purpose
Step1	**ethernet oam remote-loopback {start | stop} interface** intf-type intf-id	Enables or disables remote loopback on an interface.
Step2	**ethernet oam remote-loopback test** num1 num2 **interface** intf-type intf-id	Means transmit num2 frames with num1 bytes on the LLID port.
Step3	**show ethernet oam loopback-test-result interface** intf-type intf-id	Displays the test results.

The remote OAM loopback cannot be enabled on the physical interface that belongs to the aggregation interface.

1.3.2 Setting the Timeout Time of the Discovery State Machine of EPON OAM

The steps to set in the privileged mode the timeout time of the discovery state machine of EPON OAM are shown below:

Table 5 Setting the timeout time of the discovery state machine of EPON OAM

Procedure	Command	Purpose
Step1	**config**	Enters the global configuration mode.
Step2	**ethernet oam timeout** *value*	Sets the timeout time of the discovery state machine of EPON OAM.

1.3.3 Displaying or Restraining the Logs of the Discovery State Machine of EPON OAM

The steps to display in the privileged mode the logs of the discovery state machine of EPON OAM are shown below:

Table 6 Displaying the logs of the discovery state machine of EPON OAM

Procedure	Command	Purpose
Step1	**config**	Enters the global configuration mode.
Step2	**ethernet oam log discovery**	Displays the logs of the discovery state machine of

	{ enable | disable}	EPON OAM.

1.3.4 Displaying or Restraining the Link Monitor Log of EPON OAM.

The procedure to display in the privileged mode the link monitor logs of EPON OAM on an interface is shown in the following table:

Table 7 Displaying the link monitor logs of EPON OAM

Procedure	Command	Purpose
Step1	**config**	Enters the global configuration mode.
Step2	**ethernet oam log link-monitor { enable | disable}**	Displays the link monitor logs of EPON OAM.

1.3.5 Displaying the Information About the EPON OAM Protocol

Table 8 Displaying the information about the EPON OAM protocol

Command	Purpose
show ethernet oam ctc version-negotiation-result interface [intf-type intf-id]	Displays the negotiation result of CTC OAM on all interfaces or a designated interface.
show ethernet oam statistics interface [intf-type intf-id]	Displays on all ports or a certain designated port OAM packet statistics, which is conducted according to the value in the code domain in the OAM packets.
show ethernet oam configuration	Displays global OAM configuration.
show ethernet oam status interface [intf-type intf-id]	Displays on all ports or a designated port the local or peer's OAM status, including the OAM enabling status, OAM discovery state machine's status, OAM mode, allowable maximum size of the OAM packet, edit ID, peer's MAC address, manufacturer's OUI and detailed information of the peer, and supportable OAM function set.
show ethernet oam loopback-test-result interface [intf-type intf-id]	Displays the results of remote OAM loopback test.

1.4 Configuration Example

1.4.1 Network Environment Requirements

Connect an ONU to the EPON0/3 port of IEP3314. Then trigger on IEP3314 the remote loopback test towards ONU. The size of the test packet is 64 bytes and the number of the to-be-sent test packets is 10. After the test packets are completely sent, you can run the related command to display the test results.

1.4.2 Network Topology

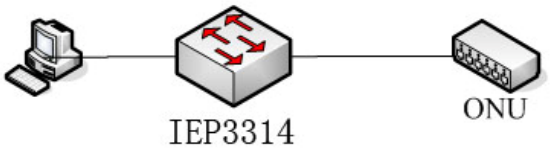


Figure 2 Network topology

1.4.3 Configuration Procedure

Configuring IEP3314:

Switch#**ethernet oam remote-loopback start int e0/3:1**

This is a intrusive loopback.

While loopback, you will be unable to pass traffic across that link.

Proceed with Remote Loopback(y/n)?**y**

Switch#**ethernet oam remote-loopback test 64 10 interface e0/3:1**

Switch#**show ethernet oam loopback-test-result int e0/3:1**

Loopback test result:

Out of Seqance frames: 0

10 packets transmitted, 10 received, 0% packet loss

rtt min/avg/max = 0/0/0 ms

Switch#**ethernet oam remote-loopback stop int e0/3:1**

Encryption Settings

Table of Contents

Chapter 1 **Encryption Settings**

1.1 Setting Encryption

1.1.1 Encryption Principle

At the downlink direction the EPON system adopts the broadcast mode and vicious users are easy to capture the information about other users in this system. In order to improve the safety of user's data, you can adopt the encryption algorithm to encrypt the data.OLT can meet users' requirement at this respect for it supports triple churning.

OLT supports the churning for each LLID and each LLID has independent key. OLT prompts the requirements of updating keys, ONU provides a 3-byte churning key and OLT uses this key to finish the churning function. After the churning function is enabled, all the data frames and the OAM frames will be churned.

The update and synchronization of the key is based on the OAM PDU mode of Organization-Specific Extension.

1.1.2 Encryption Settings on OLT

OLT supports three encryption modes: aes-32, aes-48 and triple churning, among which the update of the keys, Tkey, can be flexibly set and its default value is 10 seconds.

Perform the following steps to conduct the encryption settings towards the downlink packets.

Procedure	Purpose
enable	Enters the privileged configuration mode.
config	Enters the global configuration mode.
epon encryption triple-churning *10000*	Sets the encryption mode of the downlink packets to triple churning, and the key update period to 10000ms.
Interface *slot/port:llid*	Enters the LLID interface configuration mode.
epon encryption enable	Enables the encryption function of the LLID port.
exit	Exits from the LLID interface configuration mode.
exit	Exits from the global configuration mode.
exit	Exits from the privileged configuration mode.

EPON Multicast Settings

Table of Contents

Chapter 1 **EPON Multicast Settings**

1.1 OLT Multicast Introduction

The task of IGMP/MLD snooping is to maintain the correlation of VLAN and group address and to keep up with the change of the multicast group. The main functions of IGMP/MLD snooping include listening the IGMP/MLD packets, maintaining the map of group address and VLAN, and keeping the state of host's IGMP/MLD entity identical with that of the router's IGMP/MLD entity.

When the layer-2 device does not run IGMP/MLD snooping, the multicast data will be broadcasted at the second layer; when the layer-2 device does run IGMP/MLD snooping, the multicast data in the known multicast group will not be broadcast at the second layer, but be transmitted to a designated receiver in the second layer and the unknown multicast data will be discarded.

On the PON port, OLT will over the broadcast LLID channel transmit the multicast data to all ONUs in SCB mode.

OLTs and ONUs of support the multicast VLAN. If the multicast services need be isolated from other services on OLT, you have to plan private VLANs on OLT for multicast to make one multicast VLAN corresponds to one multicast channel or a multicast channel group (a set of multicast channels solely managed by one permission). A multicast channel is designed only for a specific multicast VLAN. The multicast flows being transmitted in the SCN channel all have carried the multicast VLAN tag. Other data flows of a user (including unicast flows and uplink IGMP/MLD packets) are destined to be transmitted to the unicast VLAN/CVLAN.

ONU establishes on the basis of the Add/Del Multicast VLAN OAM message the correlation of the UNI port and the multicast VLAN, and on the basis of IGMP/MLD snooping multicast forward-table the correlation of the UNI port and the specific multicast group.

If ONU receives the following two types of IGMP/MLD general/specific group query packets, it will drop them:

One is the IGMP/MLD general/specific group query packets without VLAN tag;

The other is the IGMP/MLD general/specific group query packets that have carried the VLAN tag but whose VLAN IDs does not belong to the configured multicast VLAN ID set of ONU.

When IEP3310/3314 receives the IGMP report packets after IGMP/MLD snooping is enabled, the VLAN in the multicast forward table is the PVID of the multicast router's port. After the router's port receives the multicast packet, IEP3310/3314 will first check the multicast forward table to confirm which member ports will be forwarded and then change the packet's VLAN tag to the multicast VLAN tag.

Additionally, ONU should under the control of OLT remove/reserve the multicast VLAN tag of the IGMP query packets. As to IGMP/MLD Group-Specific Query packets, OLT should add the multicast VLAN tag to these packets according to the multicast VLAN. As to IGMP/MLD General Query packets, they will be distributed to all multicast VLANs in the EPON system, that is, OLT will copy multiple copies of each IGMP/MLD General Query packet, add different multicast

VLAN tags and at last distribute these copies to all ONUs over the broadcast LLID.

The IGMP/MLD Proxying allows the VLAN where the multicast user is located to receive the multicast source from other VLANs. The IGMP/MLD Proxying runs on layer 2 independently without other multicast routing protocols.IGMP/MLD Proxying will be transmitted by the IGMP/MLD packets of the proxied VLAN to the proxying VLAN and maintain the hardware forward table of the multicast user of the agent VLAN according to these IGMP/MLD packets. IGMP/MLD Proxying divides different VLANs into two kinds: proxied VLANs and proxying VLANs. The downstream multicast VLANs can be set to the proxied VLANs, while the upstream multicast VLANs can be set to the proxying VLANs.

Note:

1. It is to be noted that IGMP/MLD snooping can functions normally only if there is multicast router existing for only by listening the query or report packets can IGMP/MLD snooping realize its functions. That is, a switch has to receive the IGMP/MLD query packets periodically and therefore the router age timer of IGMP/MLD snooping must be set to be bigger than the group query period of the multicast router which connects the switch. You can run **show ip mcst** command to browse the information about the multicast router in each VLAN.

2. The transmitted multicast packets must carry the VLAN tag and the VLAN tag must be same to PVID of the port which connects the multicast router.

Although IGMP/MLD Proxying is based on IGMP/MLD snooping, two are independent in application; IGMP/MLD Snooping will not be affected when IGMP/MLD Proxying is enabled or disabled, while IGMP/MLD Proxying can run only when IGMP/MLD Snooping is enabled.

1.2 OLT IGMP Multicast Configuration Tasks

- Enabling/Disabling DGMP Snooping
- Adding/Removing the Correlation of Multicast VLAN and Multicast IP Group
- Adding/Canceling the Static Multicast Address of VLAN
- Setting the Router Age Timer of IGMP Snooping
- Setting the Response Time Timer of IGMP Snooping
- Setting the Port of the Static Multicast Router
- Monitoring and Maintaining IGMP Snooping
- Enabling/Disabling IGMP-Proxy
- Setting the Querier Address of IGMP Proxy
- Setting the Query Counts and Period of the Special IGMP Proxy Group
- Monitoring and Maintaining DHCP-Proxy
- Setting the Multicast Mode
- Allocating the Multicast Permission for the UNI Port of ONU

1.2.1 Enabling/Disabling IGMP Multicast

Run the following commands in global configuration mode.

Command	Purpose
ip mcst enable	Enables the multicast.
{no ip mcst | ip mcst disable}	Resumes the default settings.

Note:

After IGMP snooping is enabled, when DLF occurs on multicast packets (that is, the destination address is not registered in the swap chip through the igmp-snooping), all multicast packets whose destination addresses are not registered on any port will be dropped.

1.2.2 Adding/Removing the Correlation of Multicast VLAN and Multicast IP Group

This command has two functions: one is that only the Report and Leave packets whose destination IP addresses have been added to a multicast VLAN can be received by IGMP snooping; the other one is that the VLAN tag which transforms the next multicast flow is the multicast VLAN tag. One multicast VLAN can include multiple continuous or discontinuous multicast IP addresses, while one multicast IP address can only belong to one multicast VLAN.

Run the following commands in global configuration mode.

Command	Purpose
ip mcst mc-vlan *vlan_id* **range** *A.B.C.D*&<1-n>	Adds the correlation of multicast VLAN and multicast IP address.
no ip mcst mc-vlan *vlan_id* **[range** *A.B.C.D*&<1-n>**]**	Deletes the correlation of multicast VLAN and multicast IP address.

1.2.3 Adding/Canceling the Static Multicast Address of VLAN

The static multicast address can make some IGMP-incompatible hosts receive the corresponding multicast packets.

Run the following commands in global configuration mode.

Command	Purpose
ip mcst vlan *vlan_id* **static** *A.B.C.D* **interface** *intf*	Adds the static multicast address of VLAN.
no ip mcst vlan *vlan_id* **static** *A.B.C.D* **interface** *intf*	Removes the static multicast address of VLAN.

Note:

1. To make the adding of the static multicast address successful, you have to set A.B.C.D in the correlation of configured multicast VLAN and multicast IP address.

2. On IEP3310/3314 OLT, you have to set the VLAN parameter in this command to be the same as the VLAN tag of the downlink multicast data.

1.2.4 Setting the Router Age Timer of IGMP Snooping

The router age timer is used to monitor whether the IGMP querier exists or not; the IGMP querier maintenance is used to maintain and manage the multicast address by sending the query packets and IGMP snooping works by independence on the communication between IGMP querier and host.

Run the following commands in global configuration mode.

Command	Purpose
ip mcst timer router-age *timer_value*	Sets the value of the router age of IGMP Snooping.
no ip mcst timer router-age	Resumes the default value of the router age of IGMP Snooping.

Note:

The settings of the timer requires to refer to the query period settings of the IGMP querier for it cannot be smaller than the query period; you are recommended to set the router age timer to the triple of the query period.

By default the router age timer is set to be 260 seconds of IGMP snooping.

1.2.5 Setting the Response Timer of IGMP Snooping

The response time timer means the threshold time for the host to report the multicast after IGMP querier sends the query packets; if this report packet is not received after the timer ages, the switch will delete this multicast address.

Run the following commands in global configuration mode.

Command	Purpose
ip mcst timer response-time *timer_value*	Sets the value of the response time of IGMP Snooping.
no ip mcst timer response-time	Resumes the default value of the response time of IGMP Snooping.

Note:

The value of the timer cannot be set too small, or the multicast communication may be unstable.

By default the response time is set to be 15 seconds of IGMP snooping.

1.2.6 Setting the Port of the Static Multicast Router

After a port is set to be a static multicast port, all the IGMP report packets and leave packets, received by OLT, will be transmitted to this port.

Run the following commands in global configuration mode.

Command	Purpose
ip mcst mrouter interface *inft_name*	Sets the port of the static multicast router of IGMP snooping.
no ip mcst mrouter interface *inft_name*	Deletes the port of the static multicast router of IGMP snooping.

1.2.7 Enabling/Disabling IGMP-Proxy

Run the following commands in global configuration mode.

Command	Purpose
ip igmp-proxy enable	Enables IGMP proxy.
{no ip igmp-proxy | ip igmp-proxy disable}	Resumes the default settings.

1.2.8 Setting Querier Port of OLT

Run the following commands in global configuration mode.

Command	Purpose
ip mcst querier *{enable|disable}*	Sets the querier port of OLT to regularly transmit the query packets outward automatically.
{no ip mcst querier| ip mcst querier disable}	Resumes the default settings of the querier port of OLT.

1.2.9 Setting the Querier Address of IGMP Proxy

Run the following commands in global configuration mode.

Command
[**no**] **ip mcst querier address** *[ip_addr*]

The default source IP address of the query packet is 10.0.0.200.

1.2.10 Setting the Query Counts and Period of the Special IGMP Proxy Group

Run the following commands in global configuration mode.

Command	Purpose
[**no**] **ip igmp-proxy last-member-query {count *value1*| interval *value2*}**	Sets the query counts and period of the special IGMP proxy group.

The default query times of the query group is 2 and its default period is also 2.

1.2.11 Setting the Multicast-Incompatible Mode of OLT

Run the following commands in global configuration mode.

Command	Purpose
ip mcst compatible enable	Enables the multicast-compatible function.
{no ip mcst compatible | ip mcst compatible disable}	Resumes the default settings.

Note:

After the multicast compatible function of OLT is enabled, OLT can take the LLID port as the minimum unit and at the same time support IGMP snooping and dynamic controllable multicast.

1.2.12 Switching over the IGMP Multicast Mode

Run the following commands in global configuration mode.

Command	Purpose
ip mcst mode {igmp-snooping | dynamic-controllable}	Switches over the multicast mode.
{no ip mcst mode | ip mcst igmp-snooping}	Resumes the default settings.

Note:

After the OLT multicast mode is switched over, the multicast modes of all ONUs will be automatically switched over to the same mode. The users therefore are free of the trouble of setting ONUs one by one.

1.2.13 Setting the Multicast Preview Time

Run the following commands in global configuration mode.

Command	Purpose

Ip preview time {1-60}	Sets the preview time of the multicast preview channel (the default time is 5 seconds).

1.2.14 Monitoring and Maintaining the IGMP Multicast

Run the following commands in EXEC mode:

Command	Purpose
show ip mcst	Displays the information about IGMP-snooping configuration.
show ip mcst timer	Displays the information about the IGMP-snooping clock.
show ip mcst groups	Displays the information about the multicast group of IGMP-snooping.
show ip mcst statistics	Displays the information about IGMP-snooping statistics.
[**no**] **debug ip mcst** [**packet** | **timer** | **event** | **error**]	Enables/disables the print switch of IGMP snooping packet/timer debug/event/error. If the specific debug switch is not designated, all the debug switches will be enabled or disabled.
show ip igmp-proxy	Displays the information about IGMP proxy.
[**no**] **debug ip igmp-proxy**	Enables or disables the IGMP-proxy debug switch.

The following shows the information about IGMP-snooping running:

```
OLT #show ip mcst

Global multicast configuration:
-----------------------------------
Globally enable          : Enabled
Multicast mode           : IGMP Snooping
Dlf-frames filtering : Enabled
Querier                  : Disabled
Querier address          : 10.0.0.200
Router age               : 260 s
Response time            : 15 s

Router Port List:
-----------------
G0/2(querier);

OLT #
```

This command is used to display the information about the multicast group of IGMP-snooping.

```
OLT #show ip mcst groups

Vlan Group                Type        Port(s)
---- ---------------- -------- ---------------------------------------
   2 225.1.1.1           LEARNING E0/3:1
OLT #
```

The following example shows the timers of IGMP snooping:

```
OLT#show ip mcst timers

Querier on port G0/2: 258

vlan 2 multicast address 0100.5e01.0101 response time : 13

OLT#
```

Querier on port G0/2: 251 means the timeout time of the ageing timer of the router.

vlan 2 multicast address 0100.5e01.0101 response time : This shows the time period from receiving a multicast query packet to the present; if there is no host to respond when the timer times out, the port will be canceled.

The IGMP snooping statistics information is displayed below:

```
OLT#show ip mcst statistics
    v1_packets:0          Number of the IGMPv1 packets
    v2_packets:6          Number of the IGMPv2 packets
    v3_packets:0          Number of the IGMPv3 packets
    general_query_packets:5      Number of the general query packets
    special_query_packets:0      Number of the special query packets
    join_packets:6        Number of the Report packets
    leave_packets:0       Number of the Leave packets
    err_packets:0         Number of the error packets
```

The information about IGMP snooping debug is shown below:

```
OLT#debug ip mcst packet
May 13 05:28:18 MCST: Receive IGMPv2 query from G0/2, diID=331, source ip addr=10.0.0.200, group=0.0.0.0. Type, port, source IP and destination IP of the received packet
May 13 05:28:18 MCST: Flood packet from G0/2 to vlan 2 downstream.
```

The information about IGMP snooping debug timer is shown below:

```
OLT#debug ip mcst timer
OLT#May 13 05:35:22 [MCST] TIMER: Vlan 2 multicast group 225.1.1.1 response time restart, initvalue = 15.
May 13 05:35:36 [MCST] timer: Vlan 2 multicast group 225.1.1.1 response time expiry.
May 13 05:35:36 [MCST]       at port:
May 13 05:35:36 [MCST]       E0/3:1
```

1.3 OLT MLD Multicast Configuration Tasks

- Enabling/Disabling MLD-Snooping
- Enabling/Disabling the Solicitation of Hardware Forward of Multicast Group

- Adding/Removing the Correlation of Multicast VLAN and Multicast IP Group
- Adding/Canceling the Static Multicast Address of VLAN
- Setting the Router Age Timer of MLD Snooping
- Setting the Response Time MLD Snooping
- Setting the Port of the Static Multicast Router
- Monitoring and maintaining MLD Snooping
- Enabling/Disabling IGMP-Proxy
- Setting the Querier Address of MLD Proxying
- Setting the Query Counts and Period of the Special MLD Proxy Group
- Monitoring and maintaining MLD Proxying

1.3.1 Enabling/Disabling MLD Multicast

Run the following commands in global configuration mode.

Command	Purpose
ip mld-snooping enable	Enables MLD snooping multicast.
{no ip mld-snooping | ip mld-snooping disable}	Resumes the default settings.

Note:

After MLD snooping is enabled, when DLF occurs on multicast packets (that is, the destination address is not registered in the swap chip through the MLD-snooping), all multicast packets whose destination addresses are not registered on any port will be dropped.

1.3.2 Enabling/Disabling the Solicitation of Hardware Forward of Multicast Group

Run the following commands in global configuration mode.

Command	Purpose
ip mld-snooping solicitation	Enables the solicitation of hardware forward of multicast group.
no ip mld-snooping solicitation	Disables the solicitation of hardware forward of multicast group.

1.3.3 Adding/Removing the Correlation of Multicast VLAN and Multicast IP Group

This command has two functions: one is that only the Report and Leave packets whose destination IP addresses have been added to a multicast VLAN can be received by MLD snooping; the other one is that the VLAN tag which transforms the next multicast flow is the multicast VLAN tag. One multicast VLAN can include multiple continuous or discontinuous multicast IP addresses, while one multicast IP address can only belong to one multicast VLAN.

Run the following commands in global configuration mode.

Command	Purpose
ip mld-snooping mc-vlan *vlan_id* **range** *X:X:X:X::X* &<1-n>	Adds the correlation of multicast VLAN and multicast IP address.
no ip mld-snooping mc-vlan *vlan_id* **[range** *X:X:X:X::X* &<1-n>**]**	Deletes the correlation of multicast VLAN and multicast IP address.

1.3.4 Adding/Canceling the Static Multicast Address of VLAN

The static multicast address can make some MLD-incompatible hosts receive the corresponding multicast packets.

Run the following commands in global configuration mode.

Command	Purpose
ip mld-snooping vlan *vlan_id* **static** *X:X:X:X::X* **interface** *intf*	Adds the static multicast address of VLAN.
no ip mld-snooping vlan *vlan_id* **static** *X:X:X:X::X* **interface** *intf*	Removes the static multicast address of VLAN.

Note:

1. To make the adding of the static multicast address successful, you have to set X:X:X:X::X in the correlation of configured multicast VLAN and multicast IP address.

2. On IEP3310/3314 OLT, you have to set the VLAN parameter in this command to be the same as the VLAN tag of the downlink multicast data.

1.3.5 Setting the Router Age Timer of MLD Snooping

The router age timer is used to monitor whether the MLD querier exists or not; the MLD querier maintenance is used to maintain and manage the multicast address by sending the query packets and MLD snooping works by independence on the communication between MLD querier and host.

Run the following commands in global configuration mode.

Command	Purpose
ip mld-snooping timer router-age *timer_value*	Sets the value of the router age of MLD Snooping.
no ip mld-snooping timer router-age	Resumes the default value of the router age of MLD Snooping.

Note:

The settings of the timer requires to refer to the query period settings of the MLD querier for it cannot be smaller than the query period; you are recommended to set the router age timer to the triple of the query period.

By default the router age timer is set to be 260 seconds of MLD snooping.

1.3.6 Setting the Response Timer of MLD Snooping

The response time timer means the threshold time for the host to report the multicast after MLD querier sends the query packets; if this report packet is not received after the timer ages, the switch will delete this multicast address.

Run the following commands in global configuration mode.

Command	Purpose
ip mld-snooping timer response-time *timer_value*	Sets the value of the response time of MLD Snooping.
no ip mld-snooping timer response-time	Resumes the default value of the response time of MLD Snooping.

Note:

The value of the timer cannot be set too small, or the multicast communication may be unstable.

By default the response time is set to be 15 seconds of MLD snooping.

1.3.7 Setting the Port of the Static Multicast Router

After a port is set to be a static multicast port, all the MLD report packets and leave packets, received by OLT, will be transmitted to this port.

Run the following commands in global configuration mode.

Command	Purpose
ip mld-snooping mrouter interface *inft_name*	Sets the port of the static multicast router of MLD snooping.
no ip mld-snooping mrouter interface *inft_name*	Deletes the port of the static multicast router of MLD snooping.

1.3.8 Enabling/Disabling MLD-Proxy

Run the following commands in global configuration mode.

Command	Purpose
ip mld-proxying enable	Enables MLD proxying.
no ip mld-proxying enable	Resumes the default settings.

1.3.9 Setting the Querier Address of MLD Proxying

Run the following commands in global configuration mode.

Command	Purpose
[**no**] **ip mld-proxying querier address** *[ip_addr*]	Sets the querier address of MLD proxying to be the source IP address of the query packet.

The default source IP address of the query packet is 10.0.0.200.

1.3.10 Setting the Query Counts and Period of the Special MLD Proxy Group

Run the following commands in global configuration mode.

Command	Purpose
[**no**] **ip mld-proxying last-member-query {count *value1*| interval *value2*}**	Sets the query counts and period of the special MLD proxy group.

The default query times of the query group is 2 and its default period is also 2.

1.3.11 Monitoring and Maintaining the MLD Multicast

Run the following commands in EXEC mode:

Command	Purpose
show ip mld-snooping	Displays the information about MLD-snooping configuration.
show ip mld-snooping timer	Displays the information about the MLD-snooping clock.
show ip mld-snooping groups	Displays the information about the multicast group of MLD-snooping.
show ip mld-snooping statistics	Displays the MLD snooping statistics information.
show ip mld-proxying	Displays the information about MLD proxy.

The following shows the information about MLD-snooping running:

```
OLT#show ip mld-snooping

Global multicast configuration:
----------------------------------
Globally enable          : Disabled
Multicast mode           : MLD Snooping
Dlf-frames filtering : Disabled
Router age               : 260 s
Response time            : 10 s
Handle Solicitation    : Disabled

Router Port PVID VLANMAP=

Router Port List:
-----------------

      None

OLT#
```

The information about the multicast group of MLD-snooping is shown below:

```
OLT#show ip mld-snooping groups

Total Group Counts: 0

Vlan Group                Type        Port(s)
---- ---------------- -------- -------------------------------------
    2 ff12::5           LEARNING E0/3:1
```

The following example shows the timer of MLD snooping:

```
OLT#show ip mcst timers

Querier on port G0/2: 258

vlan 2 multicast address 3333.0000.0005 response time : 13

OLT#
```

Querier on port G0/2: 251 means the timeout time of the ageing timer of the router.

vlan 2 multicast address 3333.0000.0005 response time : This shows the time period from receiving a multicast query packet to the present; if there is no host to respond when the timer times out, the port will be canceled.

The MLD snooping statistics information is displayed below:

```
OLT#show ip mld-snooping statistics
      v1_packets:0          Number of the MLDv1 packets
      v2_packets:6          Number of the MLDv2 packets
      v3_packets:0          Number of the MLDv3 packets
      general_query_packets:5      Number of the general query packets
```

```
special_query_packets:0       Number of the special query packets
listener_packets:6        Number of the Report packets
leave_packets:0       Number of the Leave packets
err_packets:0         Number of the error packets
```

The information about MLD proxying is shown below:

```
OLT #show ip mld-proxying
Global MLD Proxying configuration
--------------------------------
Status                          : Disable
Last member query interval: 1
Last member query count     : 2
Querier address                 : FE80::3FF:FEFE:FD00:1

OLT#
```

1.4 Remote Configuration Commands for ONU Multicast

OLT can set the multicast of ONU remotely.The detailed configuration content is shown below:

- Enabling/Disabling IGMP-Snooping
- Setting the Fast-Leave of IGMP Snooping
- Setting the Query Counts and Period of the Special IGMP Proxy Group
- Monitoring and Maintaining IGMP-Snooping
- Setting the Example of IGMP Proxy

China Telecom stipulates that the OLT can set the multicast of ONU through the CTC OAM channel.

1.4.1 Enabling/Disabling IGMP Snooping

Run the following commands in LLID interface configuration mode.

Command	Purpose
epon onu mcst enable	Enables IGMP snooping.
{no epon onu mcst | epon onu mcst disable}	Resumes the default settings.

Note:

1. After IGMP snooping is enabled, when DLF occurs on multicast packets (that is, the destination address is not registered in the swap chip through the igmp-snooping), all multicast packets whose destination addresses are not registered on any port will be dropped. ONU only supports IGMP snooping V1 and IGMP snooping V2.

2. Because this command is not defined by China Telecom, it only takes effect on ONU.

1.4.2 Setting the Multicast Mode of ONU

ONU has two kinds of multicast modes: IGMP snooping and controllable multicast defined by China Telecom.The multicast mode of ONU must kept same with that of OLT.

Run the following commands in LLID interface configuration mode.

Command	Purpose
epon onu ctc mcst switch { dynamic-controllable | igmp-snooping}	Switches over the multicast mode of ONU.
no epon onu ctc mcst switch	Switches the multicast mode of ONU over to the default mode.

The ONU multicast mode is IGMP snooping by default.

1.4.3 Setting Fast-Leave

The configuration of the **fast-leave** attribute makes the ONU delete the corresponding port in the port list of the corresponding multicast group shortly after ONU receives the **leave** packet, while the timer is not enabled any more for waiting to see whether other hosts will be added to the multicast group; if other hosts of a same port also belong to this multicast group and are reluctant to leave, the multicast communication of these hosts may be affected and in this case the **fast-leave** function should not be enabled.

Run the following commands in LLID interface configuration mode.

Command	Purpose
epon onu ctc mcst fast-leave enable	Enables fast-leave.
{no epon onu ctc mcst fast-leave | epon onu ctc mcst fast-leave disable}	Disables Fast-leave.

The fast-leave function of ONU is enabled by default.

1.4.4 Setting Tag-Stripe

The tag-stripe attribute is used to remove the VLAN tag of the next multicast packet that ONU receives.

Run the following commands in LLID interface configuration mode.

Command	Purpose
epon onu port *port_id* ctc mcst tag-stripe enable	Enables the tag-stripe function of the UNI port.

{no epon onu port *port_id* ctc mcsttag-stripe | epon onu port *port_id* ctc mcst tag-stripe disable}	Disables the tag-stripe function of the UNI port.

The tag-stripe function of the ONU UNI port is disabled by default.

1.4.5 Setting the Permission of Multicast

If OLT is in dynamic controllable multicast mode or in multicast-compatible mode and the LLID port supports the dynamic controllable multicast, you have to set the permission of the multicast channel for related UNI ports.

Run the following commands in LLID interface configuration mode.

Command	Purpose
ip mcst permission uni uni-index **range** *A.B.C.D*&<1-n> **{permit | preview| forbidden}**	Sets the permission of the multicast channel for the related UNI port.
no ip mcst permission uni *uni-index* **range** *A.B.C.D*&<1-n>	Disables the preview permission of the UNI port.

1.4.6 Setting Max-Group-Number

The **max-group-number** attribute can enable the UNI port of ONU to limit the number of the to-be-forwarded multicast groups.

Run the following commands in LLID interface configuration mode.

Command	Purpose
epon onu port *port_id* ctc mcst max-group-number *value*	Sets the value of max-group-number of a UNI port.
no epon onu port *port_id* ctc mcst max-group-number	Resumes the default value of max-group-number of a UNI port.

The default value of max-group-number of the ONU UNI port is 128.

1.4.7 Setting the Correlation of UNI port and Multicast VLAN

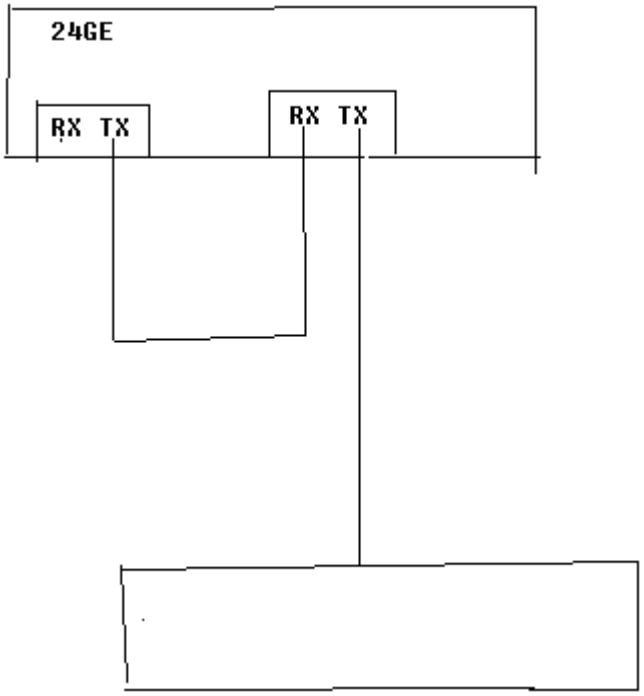
To configure the correlation of the UNI port and the multicast VLAN so that ONU can remove the VLAN tag of the downlink multicast packets, run the command above.

Run the following commands in LLID interface configuration mode.

Command	Purpose
epon onu port *port_id* ctc mcst mc-vlan {add *vlanmap*| delete *vlanmap*|clear}	Sets the correlation of UNI port and multicast VLAN.

1.5 Forced Multicast Forwarding

To set a forced-forward port to be in forced mode, you need not conduct other settings if you connect the optical fiber as shown in the following figure.



1.6 EPON Multicast Configuration Examples

1.6.1 IGMP-Snooping Configuration Example

ONU is connected to the EPON0/3 port of IEP3310/3314.And then the G0/2 port of IEP3310/3314 is connected with the multicast router.

The network topology is shown in figure 1.

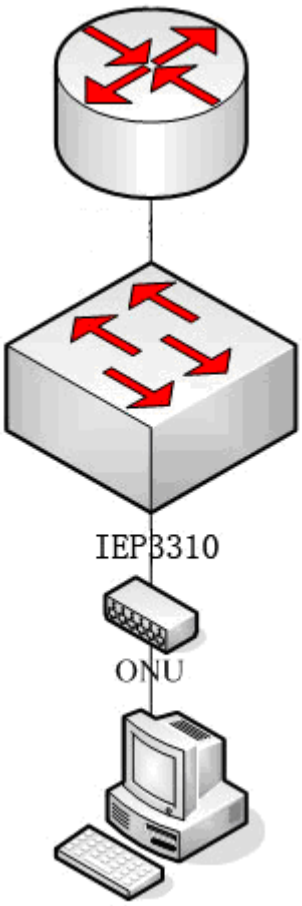


Figure 1 IGMP-Snooping configuration

(1) Enable the multicast function of IEP3310/3314:

OLT_config#ip mcst enable

(2) Set the correlation of multicast VLAN 2 and multicast group 225.1.1.1:

OLT_config#ip mcst mc-vlan 2 range 225.1.1.1

(3) Set the G0/2 port, which connects IEP3310/3314 and the multicast router, to belong to the multicast VLAN 2:

OLT_config_g0/2#switchport mode trunk

OLT_config_g0/2#switchport trunk vlan-allowed 1-2

(4) Set the UNI port of ONU to forward the multicast packets of multicast VLAN 2:

OLT_config_e0/3:1#epon onu port 1 ctc mcst mc-vlan add 2

1.6.2 IGMP-Proxy Configuration Example

ONU is connected to the EPON0/3 port of IEP3310/3314.And then the G0/2 port of IEP3310/3314 is connected with the multicast router.

The network topology is shown in figure 2.

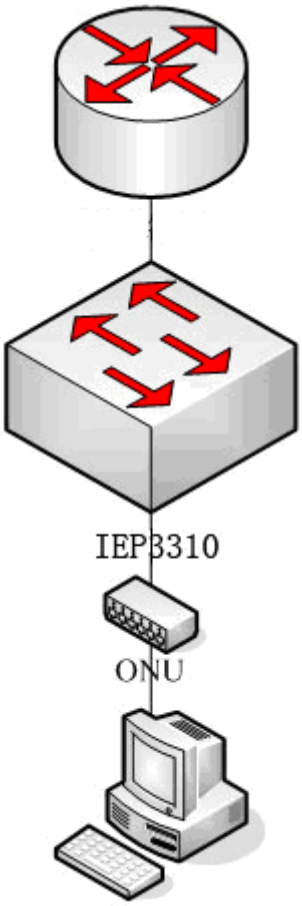


Figure 2 IGMP-Proxy configuration

(1) Enable the multicast function of IEP3310/3314:

OLT_config#ip mcst enable

(2) Enable the IGMP proxy of IEP3310/3314:

OLT_config#ip proxy enable

(3) Set the correlation of multicast VLAN 2 and multicast group 225.1.1.1:

OLT_config#ip mcst mc-vlan 2 range 225.1.1.1

(4) Set the G0/2 port, which connects IEP3310/3314 and the multicast router, to belong to the multicast VLAN 2:

OLT_config_g0/2#switchport mode trunk
OLT_config_g0/2#switchport trunk vlan-allowed 1-2

(5) Set the UNI port of ONU to forward the multicast packets of multicast VLAN 2:

OLT_config_e0/3:1#epon onu port 1 ctc mcst mc-vlan add 2

1.6.3 Controllable IGMP Multicast Configuration Example

ONU is connected to the EPON0/3 port of IEP3310/3314.And then the G0/2 port of IEP3310/3314 is connected with the multicast router.

The network topology is shown in figure 3.

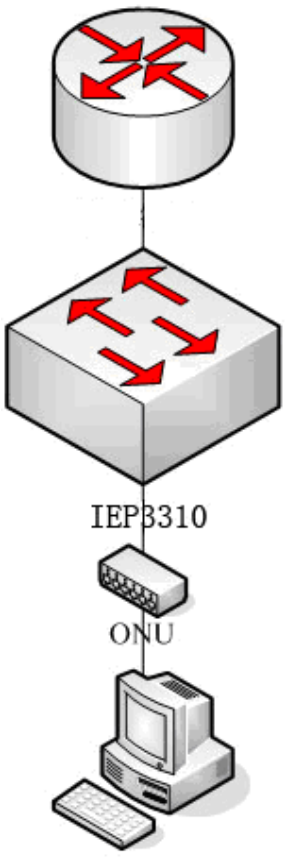


Figure 3 IGMP-Proxy configuration

(1) Enable the multicast function of IEP3310/3314:

OLT_config#ip mcst enable

(2) Set the multicast mode of IEP3310/3314 to be controllable multicast:

OLT_config#ip mcst mode dynamic-controllable

(3) Set the correlation of multicast VLAN 2 and multicast group 225.1.1.1:

OLT_config#ip mcst mc-vlan 2 range 225.1.1.1

(4) Set the G0/2 port, which connects IEP3310/3314 and the multicast router, to belong to the multicast VLAN 2:

OLT_config_g0/2#switchport mode trunk

OLT_config_g0/2#switchport trunk vlan-allowed 1-2

(5) Set UNI port 1 of ONU to forward the multicast packets of multicast 225.1.1.1:

OLT_config#ip mcst permission interface E0/1:2 uni 1 range 225.1.1.1 permit

1.6.4 Example of MLD-Snooping Configuration Example

ONU is connected to the EPON0/3 port of IEP3310/3314.And then the G0/2 port of IEP3310/3314 is connected with the multicast router.

The network topology is shown in figure 4.

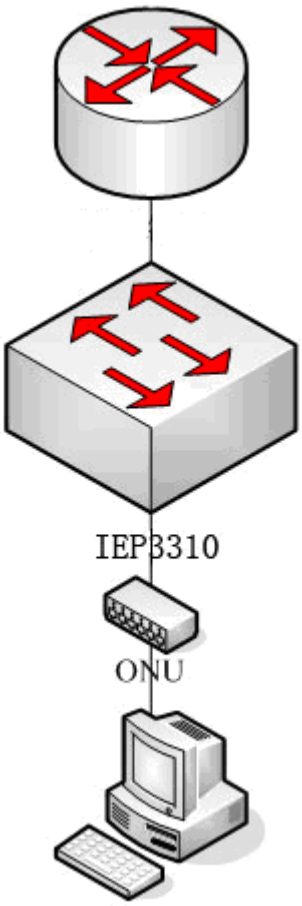


Figure 4 IGMP-Snooping configuration

(6) Enable the multicast function of IEP3310/3314:

OLT_config#ip mld-snooping enable

(7) Set the correlation of multicast VLAN 2 and multicast group ff12::5:

OLT_config#ip mld-snooping mc-vlan 2 range ff12::5

(8) Set the G0/2 port, which connects IEP3310/3314 and the multicast router, to belong to the multicast VLAN 2:

OLT_config_g0/2#switchport mode trunk

OLT_config_g0/2#switchport trunk vlan-allowed 1-2

(9) Set the UNI port of ONU to forward the multicast packets of multicast VLAN 2:

OLT_config_e0/3:1#epon onu port 1 ctc mcst mc-vlan add 2

1.6.5 MLD-Proxy Configuration Example

ONU is connected to the EPON0/3 port of IEP3310/3314.And then the G0/2 port of IEP3310/3314 is connected with the multicast router.

The network topology is shown in figure 5.

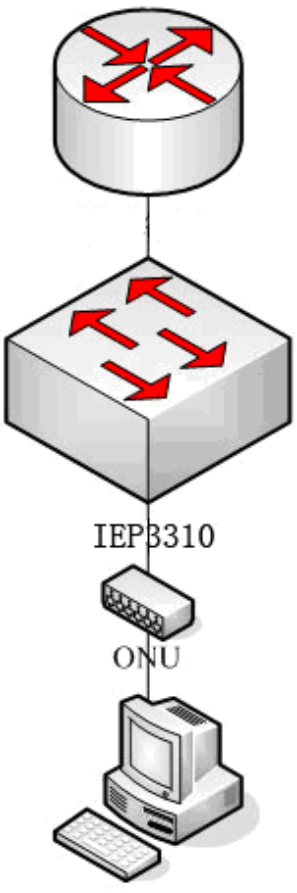


Figure 5 IGMP-Proxy configuration

(10) Enable the multicast function of IEP3310/3314:

OLT_config#ip mld-snooping enable

(11) Enable the MLD proxy of IEP3310/3314:

OLT_config#ip mld-proxying enable

(12) Set the correlation of multicast VLAN 2 and multicast group ff12::5:

OLT_config#ip mld-snooping mc-vlan 2 range ff12::5

(13) Set the G0/2 port, which connects IEP3310/3314 and the multicast router, to belong to the multicast VLAN 2:

OLT_config_g0/2#switchport mode trunk

OLT_config_g0/2#switchport trunk vlan-allowed 1-2

(14) Set the UNI port of ONU to forward the multicast packets of multicast VLAN 2:

OLT_config_e0/3:1#epon onu port 1 ctc mcst mc-vlan add 2

Optical Fiber Protection Shift Configuration

Table of Contents

Chapter 1 **Optical Fiber Protection Shift Settings**

1.1 Overview of Optical Fiber Protection Shift

In order to improve the reliability and life of the network, the EPON system adopts the optical-fiber protection shift mechanism. The optical fiber protection shift can be conducted in the following two methods:

a) Automatic shift: It is triggered by the faults such as signal loss or signal worsening.

b) Mandatory shift: It is triggered by administration events.

OLT supports the following two kinds of optical fiber protection:

1) Type B: OLT PON port, bus optical-fiber redundancy protection (as shown in figure 1-1):

- OLT: The standby OLT PON port is in cold backup state, OLT in line check state and OLT PON in port state. The protection shift is finished by OLT.
- Optical splitter: The 2:N optical splitter is used.
- ONU: There are no special requirements.

2) Type C: full protection (OLT PON port, optical-fiber bus, optical splitter, distributive optical-fiber redundancy protection) (as shown in figure 1-2):

- OLT: The active and standby OLT PON ports are both in working state.
- Optical splitter: Two 2:N optical splitters are used.
- ONU: The optical switch fitting is set before the PON port, its line state is checked by ONU, its main line is also decided by ONU, and its protection shift is conducted by ONU.

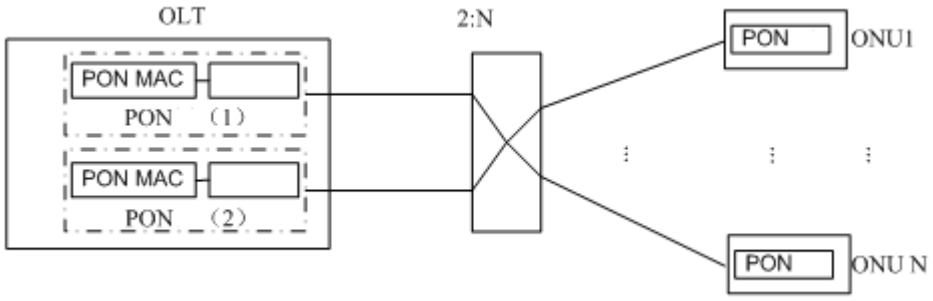


Figure 1-1 Type B

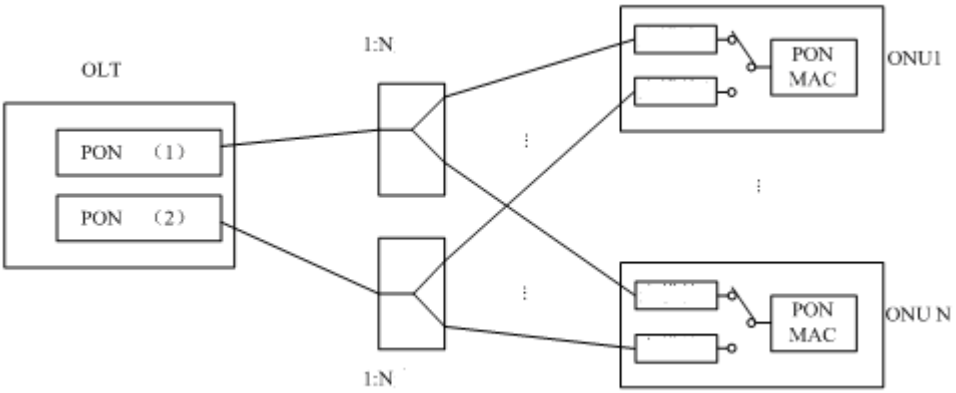


Figure 1-2 Type C

1.2 Setting the Optical-Fiber Protection Shift

1.2.1 Setting the Optical-Fiber Protection Port

You can run **epon {b-psg|c-psg} slot** on OLT to create a virtual optical-fiber protection port, that is, the PSG port. After the PSG port is created, you should run **epon psg member** immediately to add two to-be-protected actual PON ports for the virtual PSG port.

The following steps are recommended to set optical-fiber protection:

Procedure	Purpose
enable	Enters the privileged configuration mode.
config	Enters the global configuration mode.
epon {b-psg|c-psg} slot *slot* **[sequence** *seq***]**	Creates a type-B or type-C virtual PSG port. ***slot*** stands by the ID of the slot where the EPON line card is located. ***seq*** stands for the ID of the logic port.
Interface psg *slot*/*seq*	Enters the psg port configuration mode.
epon psg member active *epon-port* **standby** *epon-port*	Binds the to-be-protected active/standby PON ports.
exit	Exits from the psg interface configuration mode.
exit	Exits from the global configuration mode.
exit	Exits from the privileged configuration mode.

1.2.2 Switching the Optical-Fiber Protection Port Manually

OLT only supports the manual switchover of the type-B optical-fiber protection.

Procedure	Purpose
enable	Enters the privileged configuration mode.
epon psg switch interface *psg-port*	Switches over the PSG port manually.

ONU Management Settings

Table of Contents

Chapter 1 **Local ONU Management Settings**

1.1 Local ONU Management Configuration Tasks

Local ONU Management settings includes the following tasks :

- Authenticating and Registering ONU
- Setting the delay of MPCP
- Adding the Description String for ONU
- Canceling ONU registration
- Removing the Dynamic ONU Binding Manually
- Removing Dynamic ONU Binding Automatically
- Setting the Timeout Time of the Automatic Removal Dynamic ONU Binding
- Enabling or Disabling ONU Registration when the Successful Discovery of CTC OAM of ONU Times out
- Setting the Timeout Time for Waiting for Successful CTC OAM Discovery of ONU
- Setting the Waiting Time and Transmission Times of OAM Transmission after the Initial Registration of ACE ONU is Resumed
- Enabling and Disabling the Print of ONU Power-Off Alarm Log
- Setting the IP Address of OLT Manager
- Setting the IP Address of the Bridge of the ONU Serial Interface

1.2 Authenticating and Registering ONU

You can run **epon onu-registration-method mac** on OLT to enable the ONU MAC detection mechanism at MPCP registration. After the ONU MAC detection mechanism is enabled, ONUs without static binding settings cannot be registered to OLT. If you want to add static binding entries, run **epon bind-onu *mac-address llid-sequence***. One LLID port maps to only one ONU's MAC address.

By default, the ONU MAC detection mechanism at MPCP registration is disabled; in this case all ONUs can be registered freely.

If you have set **epon onu-authemethod manun-al** for manual ONU authentication, ONU registration still needs the manual confirmation of the administration for being authenticated.

As to the authenticated ONU, OLT will automatically obtain the type and number of the ONU ports and release the saved settings to ONU; before this, ONU can obtain only one 10Kbps bandwidth and cannot be set remotely. You can run **epon conform-onu {mac-address *value* | interface epon *slot/port:sequence*}** to let ONU pass through the authentication. Authentication is not required by ONU by default.

The ONU information, including the LLID number, ONU's MAC address, ONU description character string, binding type (static or dynamic) and ONU states (deregistered, registered, authenticated, or automatically configured), can be browsed if you run **show epon onu-information [interface epon** *slot/port***]**.

Note:

Once ONU passes through the authentication, or it is set not to base on the authentication and the registration is successful, the MAC address of ONU and the static binding entries of the LLID number will be automatically added; when this settings is saved and the system is restarted, this ONU will not be re-authenticated.

Run the following commands to control ONU registration and authentication:

Procedure	Purpose
enable	Enters the privileged configuration mode.
config	Enters the global configuration mode.
Interface epon *slot/port*	Enters the EPON port configuration mode.
epon onu-authen-method manual	Conducts manual authentication to the successfully registered ONU.
epon conform-onu {mac-address *value* **| interface epon** *slot/port:sequence***}**	Enables the successfully registered ONU to pass through the authentication.
epon bind-onu *mac-address llid-sequence*	Adds static binding entries.
epon onu-registration-method mac	Opens the checkup mechanism of the ONU MAC address during MPCP registration.
Show epon onu-information [interface epon *slot/port***]**	Displays the ONU information.
exit	Exits from the EPON interface configuration mode.
exit	Exits from the global configuration mode.
exit	Exits from the privileged configuration mode.

1.3 Setting the Delay Time of MPCP

To set the delay time of MPCP, you can use the **epon mpcp-registration-mode {normal | ctc** *value***}** command.

Conduct the following steps:

Procedure	Purpose

enable	Enters the privileged configuration mode.
config	Enters the global configuration mode.
Interface EPON *slot/port*	Enters the EPON interface configuration mode.
epon mpcp-registration-mode {normal | ctc *value***}**	Sets the delay of MPCP.
exit	Exits from the EPON interface configuration mode.
exit	Exits from the global configuration mode.
exit	Exits from the privileged configuration mode.

1.4 Adding the Description String for ONU

To add the description character string for ONU, you can use the command, **epon onu description *string***.

Conduct the following steps:

Procedure	Purpose
enable	Enters the privileged configuration mode.
config	Enters the global configuration mode.
Interface EPON *slot/port:llid*	Enters the LLID interface configuration mode.
epon onu description *string*	Adds the description string for ONU.
exit	Exits from the LLID interface configuration mode.
exit	Exits from the global configuration mode.
exit	Exits from the privileged configuration mode.

1.5 Canceling ONU Registration

To cancel ONU registration, you can use this command, **epon reset onu {mac-address *value* | interface epon *slot/port:sequence*}**.

Its detailed procedure is shown below:

Procedure	Purpose
enable	Enters the privileged configuration mode.
epon epon deregister-onu {interface epon *slot/port:sequence***}**	Deregisters an ONU.
exit	Exits from the privileged configuration mode.

Note: After ONU is deregistered, registration will be conducted automatically.

1.6 Removing the Dynamic ONU Binding

If you want to clear the dynamic ONU binding manually, you can use this command, **clear epon dynamic-binding [interface epon *slot/port*]**.

The detailed procedure is shown below:

Procedure	Purpose
enable	Enters the privileged configuration mode.
clear epon dynamic-binding [interface epon *slot/port***]**	Removes the information about dynamic ONU binding manually.
exit	Exits from the privileged configuration mode.

Note: Only when ONU does not pass authentication and after ONU is deregistered can the information about dynamic ONU binding be known.

1.7 Removing Dynamic ONU Binding Automatically

If you want this system to clear the dynamic ONU binding automatically, you can use this command, **epon dynamic-binding-timeout {disable | enable}**.

The detailed procedure is shown below:

Procedure	Purpose
enable	Enters the privileged configuration mode.
config	Enters the global configuration mode.
epon dynamic-binding-timeout {disable | enable}	Sets whether to clear the dynamic ONU binding automatically or not.
exit	Exits from the global configuration mode.
exit	Exits from the privileged configuration mode.

Note: Only when ONU does not pass authentication and after ONU is deregistered can the information about dynamic ONU binding be known.

1.8 Setting the Timeout Time of Automatic Removal of Dynamic ONU Binding

If you want this system to clear the timeout time of the automatic removal of dynamic ONU binding, you can use this command, **epon dynamic-binding-timeout *value***.

The detailed procedure is shown below:

Procedure	Purpose
enable	Enters the privileged configuration mode.
config	Enters the global configuration mode.
epon dynamic-binding-timeout *value*	Sets the timeout time of the automatic removal of dynamic ONU binding.
exit	Exits from the global configuration mode.
exit	Exits from the privileged configuration mode.

Note: Only when ONU does not pass authentication and after ONU is deregistered can the information about dynamic ONU binding be known.

1.9 Enabling or Disabling ONU Registration when the Successful Discovery of CTC OAM of ONU Times out

If you want to enable or disable ONU deregistration when the discovery of CTC OAM of ONU times out, run **epon ctc-oam-discovery-timeout {disable | enable}**.

The detailed procedure is shown below:

Procedure	Purpose
enable	Enters the privileged configuration mode.
config	Enters the global configuration mode.
epon ctc-oam-discovery-timeout {disable | enable}	Enables or disables ONU deregistration when the discovery of CTC OAM of ONU times out.
exit	Exits from the global configuration mode.
exit	Exits from the privileged configuration mode.

1.10 Setting the Timeout Time for Waiting for Successful ONU CTC OAM Discovery

If you want to set the timeout time for waiting for successful CTC OAM discovery of ONU, run **epon ctc-oam-discovery-timeout *value***. If it times out, OLT will try to deregister ONU to resume the fault that makes CTC OAM discovery unsuccessful.

The detailed procedure is shown below:

Procedure	Purpose
enable	Enters the privileged configuration mode.
config	Enters the global configuration mode.
epon ctc-oam-discovery-timeout	Sets the timeout time for waiting for successful CTC OAM discovery of ONU.

value	
exit	Exits from the global configuration mode.
exit	Exits from the privileged configuration mode.

1.11 Setting the Waiting Time and Transmission Times of OAM Transmission after the Initial Registration of ACE ONU is Resumed

If you want to set the waiting time and transmission times of OAM transmission after the initial registration of ACE ONU is resumed, run **epon ace-reset-delay *value count***.

The detailed procedure is shown below:

Procedure	Purpose
enable	Enters the privileged configuration mode.
config	Enters the global configuration mode.
epon ace-reset-delay *value count*	Sets the waiting time and transmission times of OAM transmission after the initial registration of ACE ONU is resumed.
exit	Exits from the global configuration mode.
exit	Exits from the privileged configuration mode.

1.12 Enabling or Disabling the Print of ONU Power-Off Alarm Log

If you want to enable or disable the print of ONU power-off alarm log, run **epon dying-gasp-log {disable | enable}**.

The detailed procedure is shown below:

Procedure	Purpose
enable	Enters the privileged configuration mode.
config	Enters the global configuration mode.
epon dying-gasp-log {disable | enable}	Enables or disables the print of ONU power-off alarm log.
exit	Exits from the global configuration mode.
exit	Exits from the privileged configuration mode.

1.13 Setting the IP Address of OLT Manager

If you want to set the IP address of OLT network manager, run **epon snmp-ipaddress *ip-address***.

The detailed procedure is shown below:

Procedure	Purpose
enable	Enters the privileged configuration mode.
config	Enters the global configuration mode.
epon snmp-ipaddress *ip-address*	Sets the IP address of OLT network manager.
exit	Exits from the global configuration mode.
exit	Exits from the privileged configuration mode.

1.14 Setting the IP Address of the Serial Bridge of ONU

If you establish the correlation of the bridge's IP address and the index and then apply the index in LLID interface configuration mode, you can enable the IP address of the bridge, which corresponds to the index, to be reported to ONU.

Procedure	Purpose
enable	Enters the privileged configuration mode.
config	Enters the global configuration mode.
[no] serial-bridge remote *index* **address** *A.B.C.D*	Sets the correlation of the bridge's IP address and the index. **index** stands for the index of the serial bridge; **A.B.C.D** stands for the IP address of the serial bridge.
exit	Exits from the global configuration mode.
exit	Exits from the privileged configuration mode.

Chapter 2 **Remote Global Control Commands of ONU**

2.1 Global Remote ONU Management Configuration Tasks

Remote global ONU management configuration tasks include:

- Restarting ONU
- Updating the ONU Version
- Updating ONU EEPROM
- Resuming the Default Settings of ACE ONU
- Switching over the ONU with Dual PON Ports
- Encrypting ONU
- Configuring the Static MAC Address of ONU
- Removing the Dynamic MAC Address of ONU
- Configuring the Learning Mode of the ONU MAC Address Table
- Setting the Aging Time of the MAC Address Table of ONU
- Setting the Schedule Policy of the ONU CoS Priority Queue
- Setting the Schedule Policy of the CoS Priority Queue of the ONU PON Port
- Setting the Bandwidth of the ONU CoS Priority Queue
- Setting the Bandwidth of the CoS Priority Queue of the ONU PON Port
- Setting the ONU CoS Priority Queue
- Setting the CoS Priority Queue ONU PON Port
- Setting the Isolation of the ONU Port
- Setting the ONU IP Address
- Setting the ONU Mirror
- Setting the Attack Prevention of ONU
- Setting the Serial Interface Mode of ONU
- Setting the IP Address of the Serial Bridge of ONU

- Creating VLAN on ONU
- Displaying the Basic ONU Information
- Displaying the CTC-defined Basic ONU Information
- Displaying the ONU MAC Address Table

Remote ONU management is realized through OAM; OAM includes the CTC-defined OAM and the private OAM defined by the manufacturer.

2.2 Restarting ONU

To restart an ONU, you can use this command, **epon reset onu {mac-address** *value* **| interface epon** *slot/port: sequence***}**.

This command can be realized through CTC OAM, and all ONUs that support CTC OAM support this command.

The detailed procedure is shown below:

Procedure	Purpose
enable	Enters the privileged configuration mode.
epon reboot onu {mac-address *value* **| interface epon** *slot/port:sequence***}**	Restarts an ONU.
exit	Exits from the privileged configuration mode.

2.3 Updating the ONU version

IEP3310/3314 supports to update the ONU version remotely from OLT. The ONU update software need be downloaded to the flash memory of IEP3310/3314. For the detailed download procedure, please see the chapter related to software update in *Basic Configuration* in the configuration volume. The detailed command is shown below:

epon update onu image *image_name* **interface epon** *slot/port*[*:sequence*]。

The detailed procedure is shown below:

Command	Purpose
enable	Enters the privileged configuration mode.
epon update onu image *image_name* **interface epon** *slot/port*[*:sequence*]	Updates the ONU version. If the **port** parameter is the EPON port, all ONU software on this port can be upgraded synchronously; if the **port** parameter is the LLID port, a single ONU software will be upgraded.
epon commit-onu-image-update	Confirms the upgrade of this version after ONU is restarted

interface epon *slot/port*[*:sequence*]	and registered again.
exit	Exits from the privileged configuration mode.

Note:

1. Unless the to-be-updated software matches the corresponding ONU type can this software not be updated.

2. During the update process of ONU software, do not cut off the power of ONU. After the completion of ONU update, OLT will notify users of the successful ONU update by the way of log, and ONU will use the updated version for rebooting.

3. After the ONU version is updated and restarted, you need to run epon commit-onu-image-update on OLT to confirm the ONU version.

2.4 Updating ONU EEPROM

The ONU EEPROM file has saved the MAC address and the sequence ID of ONU. If the information need be altered, the ONU EEPROM file need be updated. IEP3310/3314 supports to update the ONU EEPROM configuration file remotely from OLT and the command is **epon update onu eeprom-image *file-name* interface epon *slot/port:sequence***.

This command is realized through the private OAM and only ONU supports this kind of version download.

The detailed procedure is shown below:

Procedure	Purpose
enable	Enters the privileged configuration mode.
epon update onu eeprom-image *file-name* **interface epon** *slot/port:sequence*	Updates the ONU EEPROM file.
epon reboot onu {mac-address *value* **| interface epon** *slot/port:sequence***}**	Restarts an ONU.
exit	Exits from the privileged configuration mode.

Note:

1. After the ONU EEPROM file is updated, ONU need be restarted and then the newly configured information takes effect.

2. During the update process of ONU software, do not cut off the power of ONU.

2.5 Resuming the Default Settings of ACE ONU

At its first registration ACE ONU needs to resume its default settings through the private OAM. The resuming of the default settings can be conducted automatically in normal cases, or can be realized through the **epon ace-recover** command.

This command is realized through the private OAM and only ACE ONU supports this command.

The detailed procedure is shown below:

Procedure	Purpose
enable	Enters the privileged configuration mode.
epon ace-recover {mac-address *value* **| interface epon** *slot/port:sequence***}**	Resumes the default settings.
exit	Exits from the privileged configuration mode.

Note:

After the default settings is resumed, ONU need be restarted.

2.6 Switching over the ONU with Dual PON Ports

ONU with two PON ports can use this two commands, **epon switch-onu-pon** and **epon switch-onu-pon-and-back**, to conduct the switchover of the PON ports.

This command is realized through the private OAM and only ACE ONU supports this command.

The detailed procedure is shown below:

Procedure	Purpose
enable	Enters the privileged configuration mode.
epon switch-onu-pon interface epon *slot/port:sequence*	Switches over one PON port to the other one.
epon switch-onu-pon-and-back interface epon *slot/port:sequence*	Switches ONU to use the other PON port, conducts registration on this PON port successfully and then switches back to the original PON port.
exit	Exits from the privileged configuration mode.

2.7 Encrypting ONU

ONU has to enable its encryption function and its encryption mode must be the same as that of OLT, so the downlink packets can be encrypted.

This command is realized through the private OAM and only ONU supports this command.

In general, the encryption function of ONU is enabled by default. You can enable or disable the encryption function of ONU on OLT and this need not be set.

The detailed procedure is shown below:

Procedure	Purpose
enable	Enters the privileged configuration mode.
config	Enters the global configuration mode.
Interface EPON *slot/port:llid*	Enters the LLID interface configuration mode.
epon onu encryption triple-churning	Enables the Triple Churning encryption of ONU in LLID interface configuration mode.
exit	Exits from the LLID interface configuration mode.
exit	Exits from the global configuration mode.
exit	Exits from the privileged configuration mode.

2.8 Configuring the Static MAC Address of ONU

The static MAC address entries mean those MAC address entries that cannot be aged by ONU but only be removed manually. According to actual requirements of ONU, you can decide whether to add or remove static MAC addresses.

This command is realized through the private OAM and only ONU supports this command.

The detailed procedure is shown below:

Command	Purpose
configure	Enters the global configuration mode.
Interface epon 0/1:1	Enters the LLID interface configuration mode.
[no]epon onu mac address-table static *mac-addr* **port** *port-num*	Configures the static MAC address of ONU. **mac-addr** means a MAC address. **port-num** stands for an egress. If it is the multicast packet, multiple egresses can be set at the same time.
exit	Goes back to the global configuration mode.

exit	Goes back to the EXEC mode.
write	Saves the settings.

2.9 Removing the Dynamic MAC Address of ONU

In some cases, some learned MAC addresses on ONU need be removed.

This command is realized through the private OAM and only ONU supports this command.

The detailed procedure is shown below:

Command	Purpose
configure	Enters the global configuration mode.
Interface EPON *slot/port:llid*	Enters the LLID interface configuration mode.
[no]epon onu clear mac address-table dynamic [address *H.H.H* | **port** *port-num*]	Deletes a dynamic MAC address of ONU. ***H.H.H*** stands for the MAC address. ***port-num*** stands for the UNI port.
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.
write	Saves the settings.

2.10 Configuring the Learning Mode of the ONU MAC Address Table

MAC address learning can generally fall into three modes:

- IVL: Stands for the independent VLAN learning mode. In this mode, VLAN ID and SRC MAC will be used as indexes to add the entry of the MAC address; VLAN ID and DST MAC will be used as indexes to search the MAC address table.
- SVL: Stands for the sharing VLAN learning mode. In this mode, SRC MAC will be used as the index to add the entry of the MAC address; DST MAC will be used as the index to search the MAC address table.
- No learning: In this mode, the MAC address table will not be learned after the packets enter the system, but at packet forwarding the MAC address table will be searched according to VLAN ID and DST MAC.

This command is realized through the private OAM and only ONU supports this command.

The detailed procedure is shown below:

Note:

ONU 暂时不支持 IVL 模式。

Command	Purpose
configure	Enters the global configuration mode.
Interface EPON *slot/port:llid*	Enters the LLID interface configuration mode.
[no] epon onu mac address-table learning { ivl | svl | disable }	Configures the learning mode of ONU MAC address table. **ivl** stands for the independent VLAN learning mode. **svl** stands for the sharing VLAN learning mode. **disable** means to shut down the learning function.
Exit	Goes back to the global configuration mode.
Exit	Goes back to the EXEC mode.
Write	Saves the settings.

2.11 Setting the Aging Time of the MAC Address Table of ONU

When a dynamically learned MAC address is not used during a designated aging time, ONU will remove this MAC address from the MAC address table. The MAC aging time of ONU can be set according to actual needs, and the default aging time is 300 seconds.

This command is realized through the private OAM and only ONU supports this command.

The detailed procedure is shown below:

Command	Purpose
Configure	Enters the global configuration mode.
Interface EPON *slot/port:llid*	Enters the LLID interface configuration mode.
[no] epon onu mac address-table aging-time [**0 | 15-3825**]	Sets the aging time of the ONU MAC address. **0** means that the MAC addresses will not age. **15-3828** means the value range of the MAC aging time, whose unit is second.
Exit	Goes back to the global configuration mode.
Exit	Goes back to the EXEC mode.
Write	Saves the settings.

2.12 Setting the Schedule Policy of the ONU CoS Priority Queue

ONU currently supports two kinds of port queue schedule algorithms: SP and WRR.

- SP (Sheer Priority): In this algorithm, only when the high-priority queue is null can the packets in the low-priority queue be forwarded, and if there are packets in the high-priority queue these packets will be unconditionally forwarded.

- WRR (Deficit Round Robin): Each priority queue is distributed with a certain bandwidth and each priority queue will be provided service from high priority to low priority in turn; when the high-priority queue uses up its own bandwidth, the next-priority queue will be provided with service.

This command is realized through the private OAM and only ONU supports this command.

The detailed procedure is shown below:

Command	Purpose
Configure	Enters the global configuration mode.
Interface EPON *slot/port:llid*	Enters the LLID interface configuration mode.
[no] epon onu scheduler policy { sp | wrr }	Sets the queue schedule mode of ONU to **sp** or **wrr**.
Exit	Goes back to the global configuration mode.
Exit	Goes back to the EXEC mode.
Write	Saves the settings.

2.13 Setting the Schedule Policy of the CoS Priority Queue of the ONU PON Port

The PON port of ONU currently supports two kinds of port queue schedule algorithms: SP and WRR.

- SP (Sheer Priority): In this algorithm, only when the high-priority queue is null can the packets in the low-priority queue be forwarded, and if there are packets in the high-priority queue these packets will be unconditionally forwarded.

- WRR (Deficit Round Robin): Each priority queue is distributed with a certain bandwidth and each priority queue will be provided service from high priority to low priority in turn; when the high-priority queue uses up its own bandwidth, the next-priority queue will be provided with service.

This command is realized through the private OAM and only ONU supports this command.

The detailed procedure is shown below:

Command	Purpose
Configure	Enters the global configuration mode.
Interface EPON *slot/port:llid*	Enters the LLID interface configuration mode.
[no] epon onu scheduler-pon policy { sp | wrr }	Sets the uplink queue schedule mode of ONU to **sp** or **wrr**.
Exit	Goes back to the global configuration mode.

Exit	Goes back to the EXEC mode.
Write	Saves the settings.

2.14 Setting the Bandwidth of the ONU CoS Priority Queue

If this command is run, the bandwidth of all priority queues on all interfaces are affected. This command validates only when the queue schedule mode is set to WRR. This command decides the bandwidth weight value of the CoS priority queue when the WRR schedule policy is used.

This command is realized through the private OAM and only ONU supports this command.

The detailed procedure is shown below:

Note:

At present, ONU supports 4 priority queues but not the queue bandwidth settings; when the queue schedule mode is **wrr**, the bandwidth ratio of 4 queues is 1:2:4:8, so the following commands are invalid.

Command	Purpose
Configure	Enters the global configuration mode.
Interface EPON *slot/port:llid*	Enters the LLID interface configuration mode.
[no] epon onu scheduler wrr bandwidth ***weight1...weightn***	Sets the bandwidth for each queue of ONU. **weight1~weightn** means the bandwidth of the corresponding queue.
Exit	Goes back to the global configuration mode.
Exit	Goes back to the EXEC mode.
Write	Saves the settings.

2.15 Setting the Bandwidth of the CoS Priority Queue of the ONU PON Port

If this command is run, the bandwidth of all priority queues on all interfaces are affected. This command validates only when the queue schedule mode is set to WRR. This command decides the bandwidth weight value of the CoS priority queue when the WRR schedule policy is used.

This command is realized through the private OAM and only ONU supports this command.

The detailed procedure is shown below:

Command	Purpose
Configure	Enters the global configuration mode.
Interface EPON *slot/port:llid*	Enters the LLID interface configuration mode.

[no] epon onu scheduler-pon wrr bandwidth *weight1...weightn*	Sets the bandwidth for each uplink queue of ONU. **weight1~weightn** means the bandwidth of the corresponding queue.
Exit	Goes back to the global configuration mode.
Exit	Goes back to the EXEC mode.
Write	Saves the settings.

2.16 Setting the ONU CoS Priority Queue

The function of the priority queue is to transmits the packets to the designated priority queue according to the CoS value of these packets. The packets of which CoS values are 0 or 1 will be sent to queue 1, those of which CoS values are 2 or 3 to queue 2, those of which CoS values are 4 or 5 to queue 3 and those of which CoS values are 6 or 7 to queue 4.

If this command is set, the correlation of the CoS value and the priority queue will be changed and the packets with the designated CoS value will be sent to the designated priority queue.

This command is realized through the private OAM and only ONU supports this command.

The detailed procedure is shown below:

Command	Purpose
Configure	Enters the global configuration mode.
Interface EPON *slot/port:llid*	Enters the LLID interface configuration mode.
[no] epon onu cos map *quid cos1 ... cosn*	To set the ONU CoS priority queue, run **epon onu cos map *quid cos1..cosn***. **quid** stands for the priority queue. **cos1…cosn** stand for the CoS values.
Exit	Goes back to the global configuration mode.
Exit	Goes back to the EXEC mode.
Write	Saves the settings.

2.17 Setting the CoS Priority Queue ONU PON Port

The function of the priority queue is to sent the packets to the designated priority queue according to the CoS value of the packets. By default, the packets of which CoS values are 0 will be sent to queue 1, those of which CoS values are 1 to queue 2, those of which CoS values are 2 to queue 3 and those of which CoS values are 3 to queue 4, and so on.

If this command is set, the correlation of the CoS value and the priority queue will be changed and the packets with the designated CoS value will be sent to the designated priority queue.

This command is realized through the private OAM and only ONU supports this command.

The detailed procedure is shown below:

Command	Purpose
Configure	Enters the global configuration mode.
Interface EPON *slot/port:llid*	Enters the LLID interface configuration mode.
[no] epon onu cos-pon map *quid cos1 ... cosn*	Sets the uplink CoS priority queue of ONU. **quid** stands for the priority queue. **cos1…cosn** stand for the CoS values.
Exit	Goes back to the global configuration mode.
Exit	Goes back to the EXEC mode.
Write	Saves the settings.

2.18 Setting the Isolation of the ONU Port

In normal cases the packets between different UNI ports of ONU can be freely forwarded. However, in some special cases, you have to set port isolation to forbid the data flows between UNI ports.

This command is realized through the private OAM and only ONU supports this command.

The detailed procedure is shown below:

Command	Purpose
Configure	Enters the global configuration mode.
Interface EPON *slot/port:llid*	Enters the LLID interface configuration mode.
[no] epon onu port-protect	Configures ONU port isolation.
Exit	Goes back to the global configuration mode.
Exit	Goes back to the EXEC mode.
Write	Saves the settings.

2.19 Setting the IP Address of ONU

Before you access ONU through the telnet mode, you have to set the IP address of ONU.

The IP address is realized through the private OAM.

To conduct this settings on ONU, you need to run the commands in the following table:

Command	Purpose
Configure	Enters the global configuration mode.
Interface EPON *slot/port:llid*	Enters the LLID interface configuration mode.
[no] epon onu ip address { dhcp | static *ip-address netmask***}**	Sets the IP address of ONU. **dhcp** means to obtain the IP address through the DHCP mode. **static** means to set the IP address statically. ***ip-address*** stands for the IP address. **netmask** stands for the mask of the network.
Exit	Goes back to the global configuration mode.
Exit	Goes back to the EXEC mode.
Write	Saves the settings.

As to ONUs which locate at the bandwidth center, you need to run the commands in the following table:

Command	Purpose
Configure	Enters the global configuration mode.
Interface EPON *slot/port:llid*	Enters the LLID interface configuration mode.
[no] epon onu ip address *A.B.C.D* **netmask** *A.B.C.D* **gateway** *A.B.C.D* **vlan** *value*	Sets the IP address of ONU. **A.B.C.D** in this command in turn stands for the IP address, the mask and address of the network manager. **Vlan** stands for the ID of VLAN.
Exit	Goes back to the global configuration mode.
Exit	Goes back to the EXEC mode.
Write	Saves the settings.

2.20 Setting the ONU Mirror

To make ONU management easy or to monitor the data of a UNI port, you can copy the data of a UNI port and save these data on another UNI port for storage or analysis.

This command is realized through the private OAM and only ONU supports this command.

The detailed procedure is shown in the following table.

Note:

The mirror function supports the “multiple-to-one” relation, that is, one session has only one destination port but multiple source ports.

The answer of how many source ports are supported depends on the detailed ONU.

Command	Purpose
Configure	Enters the global configuration mode.
Interface EPON *slot/port:llid*	Enters the LLID interface configuration mode.
[no] epon onu mirror session *num* **destination** *dest-port* **source** *src-port* **[both | rx | tx]**	Sets the ONU mirror. **num** stands for the session ID. **dest-port** stands for the destination port of the mirror, which is a port to connect the network analyzer. **src-port** stands for the source port of mirror, which is always the client port. **both | rx | tx** stands fpr the direction of the mirror packets, that is, **both** stands for the outgoing and incoming packets of the source port, **rx** stands for the packets getting in from the source port and **tx** stands for the packets sent out from the source port. The default settings is **both**.
Exit	Goes back to the global configuration mode.
Exit	Goes back to the EXEC mode.
Write	Saves the settings.

2.21 Setting the Attack Prevention of ONU

Network devices need to capture some protocol packets to make sure their normal running, such as BPDU packets and IGMP packets; however, due to the limitation of CPU processing ability, the instant reception of lots of protocol packets will cause CPU to overload or the system to break down. Vicious users may transmit special protocol packets to attack network devices to cause the whole network to paralyze.

ONU supports the rate limit of the special packets. If the received flow exceeds the threshold value, this kind of flow will be limited for avoiding abnormity from occurring in this system.

This command is realized through the private OAM and only ONU supports this command.

The detailed procedure is shown below:

Command	Purpose
Configure	Enters the global configuration mode.
Interface EPON *slot/port:llid*	Enters the LLID interface configuration mode.
[no] epon onu filter {icmp | arp | bpdu | igmp} threshold *value*	Sets the attack prevention of ONU. **value** stands for the number of the packets which are received in a second.
Exit	Goes back to the global configuration mode.

Exit	Goes back to the EXEC mode.
Write	Saves the settings.

2.22 Setting the Serial Interface Mode of ONU

Some ONUs support the serial interface. ONU encapsulates the data of the serial interface as the Ethernet packets and transmits them to the serial bridge, and then the serial bridge decapsulates into the data of the serial interface for storage and display.

The communication between ONU and serial bridge is conducted through TCP or UDP. In TCP mode, ONU can work as the client or in server mode. In total, ONU has three working modes:

- TCP-Server: In this mode, the TCP connection will be established between ONU and serial interface, and ONU works as the server to wait for the serial bridge to trigger the connection request.
- TCP-Client: In this mode, the TCP connection will be established between ONU and serial interface, and the serial bridge enables the TCP listening port and ONU positively triggers the connection request to the serial bridge.
- UDP: The packets will be transmitted between ONU and serial bridge through the UDP mode.

This command is realized through the private OAM and only ONU which supports the serial interface supports this command.

The detailed procedure is shown in the following table.

Note:

At present, both ONU and OLT supports only the TCP-Server mode.

Command	Purpose
Configure	Enters the global configuration mode.
Interface EPON *slot/port:llid*	Enters the LLID interface configuration mode.
[no] epon onu serial-mode {tcp-server | tcp-client | udp} port *port-value* [**timeout** *timeout-value*]	Sets the serial-interface working mode of ONU. **port-value** stands for the ID of the TCP or UDP port. **timeout-value** stands for the connection timeout time, which can be set only in tcp-server mode.
Exit	Goes back to the global configuration mode.
Exit	Goes back to the EXEC mode.
Write	Saves the settings.

2.23 Setting the IP Address of the Serial Bridge of ONU

When ONU is set to be in TCP-Client mode or UDP mode, the IP address of the remote serial bridge should be known. This command is used to notify ONU of the serial bridge's IP address.

The detailed procedure is shown below:

Command	Purpose
Configure	Enters the global configuration mode.
Interface EPON *slot/port:llid*	Enters the LLID interface configuration mode.
[no] epon onu serial-remote *index*	Sets the IP address of the serial bridge of ONU. **index** stands for the index of the serial bridge.
Exit	Goes back to the global configuration mode.
Exit	Goes back to the EXEC mode.
Write	Saves the settings.

2.24 Creating VLAN on ONU

You have to create VLAN on ONU 1208 before the VLAN transparent transmission mode is realized on it.

This command is realized through the private OAM and only 1208 ONU supports this command.

The detailed procedure is shown below:

Command	Purpose
Configure	Enters the global configuration mode.
Interface EPON *slot/port:llid*	Enters the LLID interface configuration mode.
[no] epon onu vlan *word*	Creates or deletes VLAN on an ONU.
Exit	Goes back to the global configuration mode.
Exit	Goes back to the EXEC mode.
Write	Saves the settings.

2.25 Displaying the Basic ONU Information

IEP3310/3314 supports the remote display of ONU's basic information on OLT. The detailed command is shown below:

show epon interface *slot/port:sequence* **onu basic-info**

The detailed procedure is shown below:

Command	Purpose
enable	Enters the global configuration mode.
show epon interface *slot/port:sequence* **onu basic-info**	Displays the basic ONU information.
exit	Exits from the privileged mode.

2.26 Displaying the CTC-defined Basic ONU Information

IEP3310/3314 supports the remote display of CTC-defined ONU's basic information on OLT. The detailed command is shown below:

show epon interface *slot/port:sequence* **onu ctc basic-info**

The detailed procedure is shown below:

Command	Purpose
enable	Enters the privileged configuration mode.
show epon interface *slot/port:sequence* **onu ctc basic-info**	Displays the CTC-defined basic ONU information.
exit	Exits from the privileged configuration mode.

2.27 Displaying the ONU MAC Address Table

During the operation of ONU, we, due to debugging or management, want to know the content of the MAC address table of ONU. Run the following command to display the content in the MAC address table of ONU:

This command is realized through the private OAM and only ONU supports this command.

Command	Purpose
show epon interface *interface-id* **onu mac address-table**	Displays the content in the MAC address table of ONU. **interface-id** means the ID of the LLID port that ONU corresponds to.

Chapter 3 **Remote UNI Control Configuration of ONU**

3.1 Remote UNI Management Configuration Tasks

Remote UNI control configuration tasks include:

- Setting the VLAN Mode of ONU
- Setting the VLAN Translation Entry of the ONU Port
- Setting the VLAN Aggregation Entry of the ONU Port
- Setting Flow Control on the ONU Port
- Limiting the Maximum Number of MAC addresses of the ONU Port
- Setting Storm Control on the ONU Port
- Setting the Rate Limit of the ONU Port
- Setting Loopback Detection of the ONU Port
- Setting the Duplex Mode of the ONU Port
- Setting the Speed of ONU Port
- Setting the Auto-Negotiation of the ONU Port
- Setting the Frame Filtration of the ONU Port
- Setting the Default CoS Value of the ONU Port
- Enabling or Disabling the ONU UNI Port
- Applying the Standard CTC QoS Policy on the ONU Port
- Applying the QoS Policy on the ONU Port
- Applying the MAC Access List on the ONU Port
- Applying the IP Access List on the ONU Port
- Setting the Attributes of a Serial Interface of ONU
- Setting the Buffer of the Serial Interface of ONU
- Setting the Keepalive of the Serial Interface of ONU
- Setting Loopback Detection of the Serial Interface of ONU

- Displaying Packet Statistics on the ONU Port
- Displaying the Status of the ONU Port
- Displaying the VLAN Information on the ONU Port

3.2 Setting the VLAN Mode of ONU

The UNI VLAN tag of ONU has four kinds of modes to be processed: Transparent, Tag, Translation, and STACKING

Downlink means OLT transmits packets to ONU, while uplink means ONU transmits packets to OLT.

- The define of the transparent mode is shown as follows:

Direction	Having the tag in the Ethernet packet or not	Processing mode
Uplink	Having the VLAN tag	Make no change of the Ethernet packet (the previous VLAN tag is preserved) and forward it.
	Not having the VLAN tag	Make no change of the Ethernet packet and forward it.
Downlink	Having the VLAN tag	Make no change of the Ethernet packet (the previous VLAN tag is preserved) and forward it.
	Not having the VLAN tag	Make no change of the Ethernet packet and forward it.

- The definition of the tag mode is shown as follows:

Direction	Having the tag in the Ethernet packet or not	Processing mode
Uplink	Having the VLAN tag	Discard
	Not having the VLAN tag	Add a new VLAN tag (the main parameter is VID) to the packet and forward this packet. Currently, the only requirement that the VID value can be set on ONU, the fields, TPID and Pri which are in the VLANConfig Parameters domain of the received VLAN VariableContainer, can be omitted and the tagged TPID and Pri can be set to the default values (TPID=0x8100, Pri

		=0).
Downlink	Having the VLAN tag	Forward the packet to the corresponding UNI port according to VID, remove the tag; if the VLAN ID of a downlink tagged packet is not the configured VID, this packet will be dropped.
	Not having the VLAN tag	Discard

- The define of the transparent mode is shown as follows:

Direction	Having the tag in the Ethernet packet or not	Processing mode
Uplink	Having the VLAN tag	If a VID of the previous tag has the corresponding entry (equal to the incoming VID) in the VLAN translation list of the corresponding port, this VID will be transformed to the corresponding VID (outgoing VID) according to the entry and then this corresponding VID will be forwarded; if not, this VID will be dropped. At present, only ONU is required to conduct VID transformation, while the transformation of other fields such as TPID, CFI and Pri is not required; ONU will omit the TPID and Pri fields in the **VLANConfig Parameters** domain of the received **VLAN Variable Container**, and set the transformed TPID and Pri to be the default values (the TPID value and Pri value before transformation will not be reserved).
	Not having the VLAN tag	Adds the default VLAN to the untagged packets and forwards them.
Downlink	Having the VLAN tag	If a VID of the previous tag has the corresponding entry (equal to the outgoing VID) in the VLAN translation list of the corresponding port, this VID will be transformed to the corresponding VID (incoming VID) according to this entry and then this corresponding VID will be forwarded; if the VID of the previous tag has the default VID, this tag will be removed and then forwarded; If the VID of the previous tag has no the corresponding entry in the VLAN translation list of the corresponding port, it will be dropped; at present, only ONU is required to conduct VID transformation, while the transformation of other fields such as TPID, CFI and Pri is

		not required. During the transformation at the downlink direction, ONU keeps the original TPID value and the original Pri value unchanged.
	Not having the VLAN tag	Discard

- The STACKING mode is shown in the following table:

Direction	Having the tag in the Ethernet packet or not	Processing mode
Uplink	Having the VLAN tag	If it is in the translation list, the out-layer tag in the translation entry should be added and sent to OLT, or PVID should be added.
	Not having the VLAN tag	Adds the PVID of the port and sends it to OLT.
Downlink	Having the VLAN tag	If it is in the translation list or the tag is equal to PVID, the tag will be removed, or dropped.
	Not having the VLAN tag	Discard

- The aggregation mode is shown in the following table:

Direction	Having the tag in the Ethernet packet or not	Processing mode
Uplink	Having the VLAN tag	If the VLAN ID carried by a packet is equal to an aggregated VLAN in the VLAN aggregation list of a port, this VLAN ID of this packet will be transformed to the corresponding “vlan to be aggr”, and at the same time the source MAC address of this packet will be recorded and forwarded; if the VLAN ID carried by this packet is not equal to any aggregated VLAN in the VLAN aggregation list of this port, the VLAN ID will be dropped. At present, only ONU is required to conduct VID transformation, while the transformation of other fields such as TPID, CFI and Pri is not required; ONU will omit the TPID and Pri fields in the **VLANConfig Parameters** domain of the received **VLAN Variable Container** and set the transformed TPID to be the default

		value (TPID=0x8100), but keep **pri** to be the original value.
	Not having the VLAN tag	Adds the default VLAN to the untagged packets and forwards them.
Downlink	Having the VLAN tag	If the VLAN ID carried by a packet is equal to “vlan to be aggr” in the VLAN aggregation entry of a port, this VLAN ID will be transformed to the corresponding “aggregated VLAN” according to this entry, and then forwarded; if the VLAN ID of the original tag is not the default VLAN ID, this tag will be removed and forwarded; if this VLAN ID is equal to neigther “vlan to be aggr” nor the default VLAN ID, the VLAN ID will be dropped. At present, only ONU is required to conduct VID transformation, while the transformation of other fields such as TPID, CFI and Pri is not required. ONU will omit the TPID and Pri fields in the **VLANConfig Parameters** domain of the received VLAN Variable Container and set the TPID of the transformed VLAN tag to be the default value (TPID=0x8100), but keep pri to be the original value.
	Not having the VLAN tag	Discard

The four modes are realized through CTC OAM, and ONUs, if they support CTC OAM, support this command.

STACKING is realized through the private OAM and only ONU supports this command.

The detailed procedure is shown in the following table:

Procedure	Purpose
Enable	Enters the privileged configuration mode.
Config	Enters the global configuration mode.
Interface EPON *slot/port:llid*	Enters the LLID interface configuration mode.
epon onu port *port-num* **ctc vlan mode {transparent | tag pvid** *value* **| translation pvid** *value* **|**	Sets the processing mode of the ONU UNI VLAN Tag. **port-num** stands for the ID of the UNI port. **transparent** stands for the transparent transmission mode. **tag** stands for the tag mode.

vlan-stacking pvid *value* **| aggregation pvid** *value* **}**	**translation** stands for the translation mode. **vlan-stacking** stands for the STACKING mode. **aggregation** stands for the aggregation mode. **value** stands for the pvid of a port.
exit	Exits from the privileged configuration mode.

3.3 Setting the VLAN Translation Entry of the ONU Port

If the VLAN mode of the ONU UNI port is the translation mode or the STACKING mode, you have to set the translation entry for the designated VLAN to modify or add its out-layer tag.

The detailed procedure is shown in the following table.

Note:

The mode of the ONU port must first be set to the translation mode.

Command	Purpose
Configure	Enters the global configuration mode.
Interface epon *slot/port:llid*	Enters the LLID interface configuration mode.
epon onu port ***num*** **ctc vlan translation-entry** ***old-vid new-vid***	Sets the VLAN translation entry of the ONU port. **num** stands for the UNI port number. **old-vid** stands for the previous vlan, also called as cvlan. **new-vid** stands for the translated vlan, also called as svlan.
Exit	Goes back to the global configuration mode.
Exit	Goes back to the EXEC mode.
Write	Saves the settings.

3.4 Setting the VLAN Aggregation Entry of the ONU Port

If the VLAN mode of the ONU UNI port is the aggregation mode, you have to set the translation entry for the designated VLAN to modify or add its out-layer tag.

The detailed procedure is shown in the following table.

Note:

The mode of the ONU port must first be set to the translation mode.

Command	Purpose
Configure	Enters the global configuration mode.

Interface epon *slot/port:llid*	Enters the LLID interface configuration mode.
epon onu port ***num*** **ctc vlan translation-entry** ***old-vid-range new-vid***	Sets the VLAN translation entry of the ONU port. **num uni** stands for the port number. **old-vid-range** stands fpr the range of the previous vlan. **new-vid** stands for the translated vlan, also called as svlan.
Exit	Goes back to the global configuration mode.
Exit	Goes back to the EXEC mode.
Write	Saves the settings.

3.5 Setting Flow Control on the ONU Port

The flow control in full duplex mode is realized through the 802.3X-defined PAUSE frame, while the flow control in half duplex mode is realized through the backpressure.

This command can be realized through CTC OAM, and all ONUs that support CTC OAM support this command.

The detailed procedure is shown below:

Command	Purpose
Configure	Enters the global configuration mode.
Interface epon 0/1:1	Enters the LLID interface configuration mode.
[no] epon onu port ***num*** **ctc flow-control**	Enables or disables flow control on the ONU UNI port. **num** stands for the ID of the ONU UNI port.
Exit	Goes back to the global configuration mode.
Exit	Goes back to the EXEC mode.
Write	Saves the settings.

3.6 Limiting the Maximum Number of MAC addresses of the ONU Port

The security port can control the port access, enabling a port to be used in an allowable range that you set. You can enable the security function of a port by setting the maximum number (threshold) of secure MAC addresses and enabling the secure MAC address; if the MAC addresses which enters the port exceed the threshold and the MAC addresses are not the secure MAC addresses, we define this phenomenon as port security violation; if this phenomenon happens, different actions will be acted according to different violation modes.

The security port has two functions: setting the maximum number of MAC addresses for the security port and setting the static secure MAC address. If the security port has no static secure MAC address or the number of the static secure MAC addresses is smaller than that of the secure MAC addresses, the dynamic learning of the secure MAC addresses will be conducted. If security port violation appears, the packets will be dropped until security port violation disappears.

At present, ONU only supports the setting of the number of secure MAC addresses.

This command is realized through the private OAM and only ONU supports this command.

The detailed procedure is shown below:

Command	Purpose
Configure	Enters the global configuration mode.
Interface EPON *slot/port:llid*	Enters the LLID interface configuration mode.
[no] epon onu port *port-num* **mac address-table dynamic maximum** *addr-num*	Limits the maximum number of MAC addresses of the ONU port. ***port-num*** stands for the UNI port. ***addr-num*** means the maximum number of MAC addresses that are allowed to pass through.
Exit	Goes back to the global configuration mode.
Exit	Goes back to the EXEC mode.
Write	Saves the settings.

3.7 Setting Storm Control on the ONU Port

The port of ONU may bear continuous and abnormal impact from unicast (MAC address fails to be found), multicast or broadcast packets, and therefore gets paralyzed even to the extent that the whole ONU breaks down. Therefore it is necessary to provide a mechanism to constrain this phenomenon and limit the bandwidth in the allowable range.

This command is realized through the private OAM and only ONU supports this command.

The detailed procedure is shown in the following table.

Note:

Due to the limitation of the hardware, among four storm control modes (the broadcast storm control, the broadcast and multicast storm control, the “broadcast + multicast + unknown unicast” storm control and the storm control for all packets) you can choose only one storm control mode.

Command	Purpose
Configure	Enters the global configuration mode.

Interface EPON *slot/port:llid*	Enters the LLID interface configuration mode.
[no] epon onu port *port-num* **storm-control mode** *mode-num* **threshold** *count*	Sets storm control on an ONU port. ***port-num*** stands for the UNI port. mode-num means the mode: 1:broadcast 2: broadcast and multicast 3: broadcast, multicast and unknown unicast 4: all packets **count** stands for the threshold of storm control.
Exit	Goes back to the global configuration mode.
Exit	Goes back to the EXEC mode.
Write	Saves the settings.

3.8 Setting the Rate Limit of the ONU Port

The limitation of the rate of the ONU UNI port is used to limit the packet transmission rate of the UNI port.

This command can be realized through CTC OAM, and all ONUs that support CTC OAM support this command.

The detailed procedure is shown below:

Command	Purpose
configure	Enters the global configuration mode.
Interface EPON *slot/port:llid*	Enters the LLID interface configuration mode.
[no] epon onu port *port-num* **ctc rate-limit** *band* **{ ingress | egress}**	SetS the rate limit of the ONU port. **port-num** stands for the ID of the UNI port. **band** stands for the threshold of the rate limit.
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.
write	Saves the settings.

3.9 Setting Loopback Detection of the ONU Port

You can confirm whether there is loopback occurring on a port by transmitting a special packet on this port and detecting whether this packet comes back to this port from which it is sent out.

Due to the continuous change of the network, it is certain that the loopback detection is a continuous process, that is, loopback detection will be conducted every a fixed time.

This command is realized through the private OAM and only ONU supports this command.

The detailed procedure is shown below:

Command	Purpose
Configure	Enters the global configuration mode.
Interface EPON *slot/port:llid*	Enters the LLID interface configuration mode.
[no] epon onu port *port-num* **loopback detect**	Sets loopback detection of the ONU port. ***port-num*** stands for the UNI port.
Exit	Goes back to the global configuration mode.
Exit	Goes back to the EXEC mode.
Write	Saves the settings.

3.10 Setting the Duplex Mode of the ONU Port

This command is realized through the private OAM and only ONU supports this command.

The detailed procedure is shown below:

Command	Purpose
Configure	Enters the global configuration mode.
Interface EPON *slot/port:llid*	Enters the LLID interface configuration mode.
[no] epon onu port *port-num* **duplex { half | full | auto }**	Sets the duplex mode of the ONU UNI port. ***port-num*** stands for the UNI port.
Exit	Goes back to the global configuration mode.
Exit	Goes back to the EXEC mode.
Write	Saves the settings.

3.11 Setting the Speed of ONU Port

This command is realized through the private OAM and only ONU supports this command.

The detailed procedure is shown below:

Command	Purpose

Configure	Enters the global configuration mode.
Interface EPON *slot/port:llid*	Enters the LLID interface configuration mode.
[no] epon onu port *port-num* **speed { 10 | 100 | auto }**	Sets the speed of ONU port. ***port-num*** stands for the UNI port.
Exit	Goes back to the global configuration mode.
Exit	Goes back to the EXEC mode.
Write	Saves the settings.

3.12 Setting the Auto-Negotiation of the ONU Port

ONUs that are not produced by do not support to set the rate and duplex mode of the UNI port, but this command helps these ONUs to enable or disable the auto-negotiation of this port.

This command can be realized through CTC OAM, and all ONUs that support CTC OAM support this command.

The detailed procedure is shown below:

Command	Purpose
Configure	Enters the global configuration mode.
Interface EPON *slot/port:llid*	Enters the LLID interface configuration mode.
[no] epon onu port *port-num* **ctc auto-negotiation**	Sets the auto-negotiation of the ONU port. ***port-num*** stands for the UNI port.
Exit	Goes back to the global configuration mode.
Exit	Goes back to the EXEC mode.
Write	Saves the settings.

3.13 Setting the Frame Filtration of the ONU Port

This function can limit some illegal users to access the network or some services by limiting the source or destination MAC address.

The detailed procedure is shown in the following table.

Note:

ONU only supports the frame filtration of the source MAC address.

Command	Purpose
Configure	Enters the global configuration mode.
Interface EPON *slot/port:llid*	Enters the LLID interface configuration mode.
[no] epon onu port *port-num* **block mac {src** *H.H.H* **| dest** *H.H.H***}**	Sets the frame filtration of the ONU port.

	port-num stands for the UNI port. **H.H.H** means an MAC address.
Exit	Goes back to the global configuration mode.
Exit	Goes back to the EXEC mode.
Write	Saves the settings.

3.14 Setting the Default CoS Value of the ONU Port

If the UNI port is set to be in tag or translation mode and the uplink packets do not carry the tag when they enters the UNI port, ONU has to add the default tag of this UNI port to these packets and then sends them to OLT. In this case, the CoS value of the tag is the default CoS value of the UNI port.

This command is realized through the private OAM and only ONU supports this command.

The detailed procedure is shown below:

Command	Purpose
Configure	Enters the global configuration mode.
Interface EPON *slot/port:llid*	Enters the LLID interface configuration mode.
[no] epon onu port *port-num* **default-cos** *value*	Sets the default CoS value of the ONU port. ***port-num*** stands for the UNI port. **value** means the default CoS value.
Exit	Goes back to the global configuration mode.
Exit	Goes back to the EXEC mode.
Write	Saves the settings.

3.15 Enabling or Disabling the ONU UNI Port

You can disable the ONU UNI port to disable all functions on this port, and then all monitor commands will label this port as unavailable. This information can be transmitted to other devices through the dynamic routing protocol. The modification on any route will not affect this port.

This command can be realized through CTC OAM, and all ONUs that support CTC OAM support this command.

The detailed procedure is shown below:

Command	Purpose
configure	Enters the global configuration mode.
Interface EPON *slot/port:llid*	Enters the LLID interface configuration mode.
[no] epon onu port *num* shutdown	Enables or disables the ONU UNI port.

	num stands for the ID of the ONU UNI port.
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.
write	Saves the settings.

3.16 Applying the Standard CTC QoS Policy on the ONU Port

This function is used to classify and queue the uplink flows, modify the priority of the packets, designate the incoming queue of packets and schedule the packets by setting the queue schedule algorithm.

Some ONUs only support the incoming queue but not to modify the CoS value. As to supporting which functions, it depends on ONU.

This command can be realized through CTC OAM, and all ONUs that support CTC OAM support this command.

The detailed procedure is shown below:

Command	Purpose
configure	Enters the global configuration mode.
Interface EPON *slot/port:llid*	Enters the LLID interface configuration mode.
[no] epon onu port *num* ctc qos policy *name*	Applies the QoS policy on the ONU UNI port. **num** stands for the ID of the UNI port. **name** stands for the name of QoS policy map.
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.
write	Saves the settings.

3.17 Applying the QoS Policy on the ONU Port

This function realizes the classification of uplink flows; it helps to conduct the following actions to the packets: forward, drop, rate limit and modify the out-layer VLAN tag.

This command is realized through the private OAM and only ONU supports this command.

The detailed procedure is shown below:

Command	Purpose
configure	Enters the global configuration mode.
Interface EPON *slot/port:llid*	Enters the LLID interface configuration mode.
[no] epon onu port *num* qos policy *name*	Applies the QoS policy on the ONU UNI port. **num** stands for the ID of the UNI port.

	name stands for the name of QoS policy map.
Exit	Goes back to the global configuration mode.
Exit	Goes back to the EXEC mode.
write	Saves the settings.

3.18 Applying the MAC Access List on the ONU Port

The MAC access control list is used to match such attributes as special source MAC addresses, destination MAC addresses, vlan tag or Ethernet types to realize packet filtration which is based on these attributes.

This command is realized through the private OAM and only ONU supports this command.

The detailed procedure is shown below:

Command	Purpose
configure	Enters the global configuration mode.
Interface EPON *slot/port:llid*	Enters the LLID interface configuration mode.
[no] epon onu port *num* mac access-group *name*	Applies the MAC access list on the ONU port. **num** stands for the ID of the UNI port. **name** stands for the name of the MAC access list.
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.
write	Saves the settings.

3.19 Applying the IP Access List on the ONU Port

The IP access control list is used to realize the filtration of special packets by matching the L3/L4 attributes of the packets.

This command is realized through the private OAM and only ONU supports this command.

The detailed procedure is shown below:

Command	Purpose
configure	Enters the global configuration mode.
Interface EPON *slot/port:llid*	Enters the LLID interface configuration mode.
[no] epon onu port *num* ip access-group *name*	Applies the IP access list on the ONU UNI port. **num** stands for the ID of the UNI port. **name** stands for the name of the IP access

	list.
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.
write	Saves the settings.

3.20 Setting the attributes of a Serial Interface of ONU

The serial interface of ONU supports the following attributes: speed, databits, stopbits, parity and flow-control.

This command is realized through the private OAM and only ONU supports this command.

The detailed procedure is shown below:

Command	Purpose
Configure	Enters the global configuration mode.
Interface EPON *slot/port:llid*	Enters the LLID interface configuration mode.
[no] epon onu serial ***num*** **serial-attribute {speed** ***speed-value*** **| databits** ***databits-value*** **| stopbits** ***stopbits-value*** **| parity {none | odd | even | space | mark} | flow-control {none | software | hardware} | bus-type { RS232 | RS485} | duplex {half | full}}**	Sets the attributes of a serial interface of ONU. **num** stands for the number of a serial interface. **speed-value** stands for the speed of the serial interface. **databits-value** stands for the value of the data bit of the serial interface. **stopbits-value** stands for the value of the stop bit of the serial interface. **none | odd | even | space | mark** stands for five checkup modes of the serial interface, among which **none** means no checkup. **none | software | hardware** stands for the flow control modes, among which **none** means no flow control. RS232 | RS485 stands for the serial interface mode. **half | full** stands for the duplex mode.
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.
write	Saves the settings.

3.21 Setting the Buffer of the Serial Interface of ONU

When the data of the serial interface arrives at ONU, these data will be temporally stored in the local, encapsulated into the Ethernet packets and then sent out. The detailed buffer is up to the time and bytes. If the bytes of the local buffer reach a certain number (read-bytes), or the interval of the buffer reaches to a certain time (read-interval), ONU will send all the data out for just one time.

This command is realized through the private OAM and only ONU supports this command.

The detailed procedure is shown below:

Command	Purpose
Configure	Enters the global configuration mode.
Interface EPON *slot/port:llid*	Enters the LLID interface configuration mode.
[no] epon onu serial ***num*** **serial-buffer {read-interval** ***time*** **| read-bytes** ***bytes*****}**	Sets the buffer of the ONU serial interface. **num** stands for the number of a serial interface. **time** stands for the maximum buffer time. **bytes** stands for the bytes of the maximum buffer.
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.
write	Saves the settings.

3.22 Setting the Keepalive of the Serial Interface of ONU

To confirm whether the link between serial bridge and ONU is normal, you should monitor the status the link continuously. ONU can monitor this link continuously through its keepalive function. If there is no packet transmission between ONU and serial bridge at the designated time (idle), ONU will positively transmit the keepalive packets; if ONU does not receive the keepalive packets or data packets from the serial bridge in a certain time (timeout), ONU continues transmitting the keepalive packets; if ONU does not receive the keepalive packets from the serial bridge after a designated times (count), the link will be cut off and OLT will be reported of the network interruption event.

This command is realized through the private OAM and only ONU supports this command.

The detailed procedure is shown below:

Command	Purpose
Configure	Enters the global configuration mode.
Interface EPON *slot/port:llid*	Enters the LLID interface configuration mode.
[no] epon onu serial *num* **serial-keepalive**	Sets the keepalive function of the serial

idle *idle-value* **timeout** *timeout-value* **count** *count-value*	interface of ONU. **num** stands for the number of a serial interface. **idle-value** stands for the maximum idle time between ONU and serial bridge; if there is no packets to be transmitted between ONU and serial bridge during the idle-value time, ONU will transmit the keepalive packet to monitor the status of the link. **timeout-value** stands for the timeout time of the keepalive packet; if onu still receives no response packets from the serial bridge after the keepalive-value time, ONU will transmit the next keepalive packet. **count** stands for the transmission times of the keepalive packet; if the response packet from the serial bridge is still not received after **count** packets are being transmitted, ONU regards that the network is interrupted and notifies OLT.
Exit	Goes back to the global configuration mode.
Exit	Goes back to the EXEC mode.
Write	Saves the settings.

3.23 Setting Loopback Detection of the Serial Interface of ONU

You can confirm whether there is loopback occurring on a port by transmitting a special packet on this port and detecting whether this packet comes back to this port from which it is sent out.

When the loopback on the serial interface is detected by ONU, ONU will report this loopback to the current serial interface.

This command is realized through the private OAM and only ONU supports this command.

The detailed procedure is shown below:

Command	Purpose
Configure	Enters the global configuration mode.
Interface EPON *slot/port:llid*	Enters the LLID interface configuration mode.
[no] epon onu serial *serial-num* **loopback detect**	Sets loopback detection of the ONU port. **serial-num** stands for the ID of the serial interface.
Exit	Goes back to the global configuration mode.

Exit	Goes back to the EXEC mode.
Write	Saves the settings.

3.24 Displaying Packet Statistics on the ONU Port

The administrator needs to know the packet statistics on the ONU port to further know the running state of the current ONU. Packet statistics includes the total number of packets, the number of multicast packets, the number of the broadcast packets, pause frames, error frames and so on.

Command	Purpose
show epon interface *interface-id* **onu {port | serial}** *num* **statistics**	Displays packet statistics on the ONU port. **interface-id** means the ID of the LLID port that ONU corresponds to. **num** stands for the ID of the ONU port or the serial interface.

3.25 Displaying the Status of the ONU Port

During the operation of ONU, the administrator needs to know the information about the configuration and state of the current ONU port through related commands.

The displayed information includes the port type, the link's state, shutdown or not, flow control, the duplex mode, the rate limit and the storm control. Different ONUs have different information to show.

Command	Purpose
show epon interface *interface-id* **onu {port | serial}** *num* **state**	Displays the state of the ONU port. **interface-id** means the ID of the LLID port that ONU corresponds to. **num** stands for the ID of the ONU port or the serial interface.

3.26 Displaying the VLAN Information on the ONU Port

During the operation of ONU, the administrator needs to know the information about VLAN configuration and the state of the current ONU port through related commands.

Command	Purpose
show epon interface *interface-id* **onu {port | serial}** *num* **ctc vlan**	Displays the VLAN information of the ONU port. **interface-id** means the ID of the LLID port that ONU corresponds to. **num** stands for the ID of the ONU port.

Chapter 4 **Basic EPON Networking Examples**

4.1 Networking Requirements

The EPON0/1 port of OLT connects two ONUs: ONU1 and ONU2. After ONU registration the information about the two ONUs will be displayed.

4.2 Network Topology

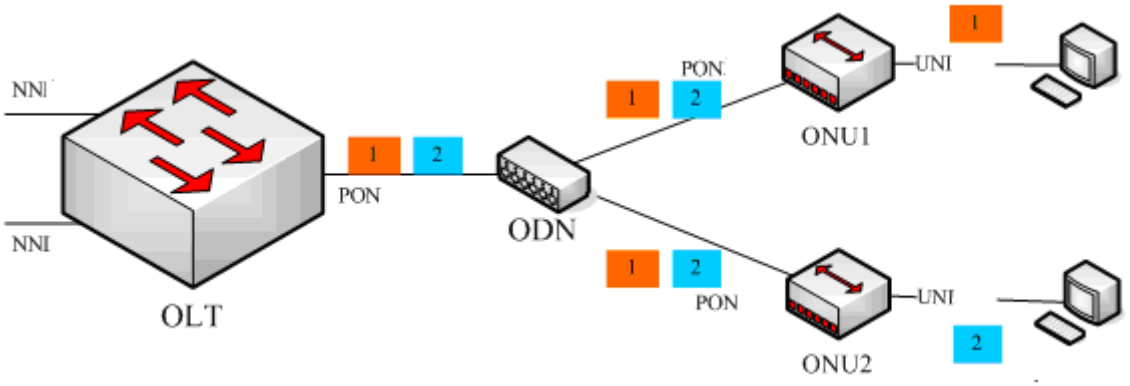


Figure 4-1 Basic EPON network topology

4.3 Configuration Procedure

By default OLT does not enable the ONU MAC checkup and the manual authentication.
ONU registration means to pass through the authentication and add the MAC-LLID binding table.

Run **show epon onu-information** in any OLT mode. The following information is shown:

Intf Name MAC Address ONU Type Bind Type Status distance(m)

---------- ---------- ---------- --------- ---------- ----------

E0/1:1 00e0.0f00.0001 1208 Static auto_configured 32

E0/1:2 00e0.0f00.0002 1004 Static auto_configured 33

Table 4-1 Described ONU Information

Field	Description
Intf Name	Stands for the LLID that ONU is bound to.
MAC Address	Stands for the MAC address of ONU.

ONU Type	Stands for the ONU type.
Bind Type	Stands for the ONU binding type.
Status	Stands for the status of ONU.