D-Link®

Version 1.00 | 04/08/2025

CLI Reference Guide

L2 Industrial Smart Switch

DIS-210G Series

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

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 bottom to top 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 bottom from to top and from left to right.

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.

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.

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#
```

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
```

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.

2. Basic Configuration

System Management Configuration

File Management Configuration

Managing the file system

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

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.

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

Parameter	Description
Flash	A file stored in the flash memory.

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

Example

```
monitor#boot flash switch.bin
```

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.

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

Parameter	Description
flash	Store device in the flash memory.
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#
```

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.

Through TFTP

```
monitor#copy tftp flash startup-config
```

Using ftp to perform the update of software and configuration

```
switch #copy ftp {flash|cf} [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

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.
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.

Basic System Management Configuration

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

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
```

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

Parameter	Description
ip_addr	IP address of the gateway

Example

```
monitor#ip route default 192.168.1.1
```

Using ping to test network connection state

```
monitor#ping <ip_address>
```

This command is to test network connection state.

Parameter

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
```

Terminal Configuration

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.

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

Relationship between line and interface

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.

(2) Configure the terminal parameters.

For VTY configuration, refer to Part 2.4 "VTY configuration example".

Monitor and Maintenance

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

VTY Configuration Example

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

```
Switch_config# line vty 0 31
Switch_config_line# length 0
```

SSH Configuration commands

Introduction

Ssh server

A scure and encrypted communication connection can be created between SSH client and the device through SSH server. The connection has telnet-like functions. SSH server supports the encryption algorithms including des, 3des and blowfish.

Ssh client

SSH client is an application running under the ssh protocol. SSH client can provide authentication and encryption, so SSH client gurantees secure communication between communication devices or devices supporting SSH server even if these devices run in unsafe network conditions. SSH client supports the encryption algorithms including des, 3des and blowfish.

Function

SSH server and SSH client supports version 1.5. Both of them only support the shell application.

Configuration Tasks

Configuring the authentication method list

SSH server adopts the login authentication mode. SSH server uses the **default** authentication method list by default.

Run the following command in global configuration command mode to configure the authentication method list:

Command	Purpose
Ip sshd auth_method STRING	Configures the authentication method list. The length of the authentication method name is no more than 20 characters.

Configuring the access control list

To control the access to the device’s SSH server, you need to configure the access control list for SSH server.

Run the following command in global configuration mode to configure the access control list:

Command	Purpose
Ip sshd access-class STRING	Configures the access control list. The length of the access control list name is no more than 19 characters.

Configuring the authentication timeout value

After a connection is established between client and server, server cuts off the connection if authentication cannot be approved within the set time.

Run the following command in global configuration mode to configure the configuration timeout value:

Command	Purpose
Ip sshd timeout <60-65535>	Configures the authentication timeout value.

Configuring the times of authentication retrying

If the times for failed authentications exeed the maximum times, SSH server will not allow you to retry authentication unless a new connction is established. The maximum times for retrying authentication is 6 by default.

Run the following command in global configuration mode to configure the maximum times for retrying authentication:

Command	Purpose
Ip sshd auth-retries <0-65535>	Configures the maximum times for retrying authentication.

Configuring the login silence period

When the failure login times exceed the threshold, the device enters the login silence period. The silence period is 60s.

Run the following command to configure the login silence period in the global configuration mode:

Command	Purpose
ip sshd silence-period <0-3600>	Configures the login silence period.

Enabling sftp

Stp is a security file transmission system based on the ssh protocol whose authentication and data transmission are encrypted. Though its transmition rate is slow, it has a strong network security.

Sftp is diabled by default. Run the following command to enable sftp in the global configuration mode:

Command	Purpose
ip sshd sftp	Enables sftp.

Enabling sshd

It takes one to two minutes to calculate the initial password when enabling ssh server. The initial password will be saved in **flash** when enabling the function. The device will read the encryption key from **flash** when reenabling ssh server. Thus, the start time is shortened.

The sshd (encryption key saving) is disabled by default. Run the following command to enable sshd (encryption key saving) in the global configuration mode:

Command	Purpose
ip sshd save	Enables sshd

Enabling SSH server

SSH server is disabled by default. When SSH server is enabled, the device will generate a rsa password pair, and then listen connection requests from the client. The process takes one or two minutes.

Run the following command in global configuration mode to enable SSH server:

Command	Purpose
Ip sshd enable	Enables SSH server. The digit of the password is 1024.

SSH server Configuration Example

The following configuration only allows the host whose IP address is 192.168.20.40 to access SSH server. The local user database is used to distinguish user ID.

Access control list

```
ip access-list standard ssh-acl
permit 192.168.20.40
```

Global configuration

```
aaa authentication login ssh-auth local
ip sshd auth-method ssh-auth
ip sshd access-class ssh-acl
ip sshd enable
```

3. Network Management ConfigurationConfiguring SNMP

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.

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".

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 NMP:

- 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.

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.

SNMP Configuration Tasks

SNMP configuration commands include:

- 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 local engine
- Configuring SNMP trap
- Configuring SNMPv3 group
- Configuring SNMPv3 user
- Configuring snmp-server encryption
- Configuring snmp-server trap-source
- Configuring snmp-server trap-timeout
- Configuring snmp-server trap-add-hostname
- Configuring snmp-server trap-logs
- Configuring snmp -dos-max retry times
- Configuring keep-alive times
- Configuring snmp-server necode
- Configuring snmp-server event-id
- Configuring snmp-server getbulk-timeout
- Configuring snmp-server getbulk-delay
- Showing snmp running information
- Showing snmp debug information

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	Purpose
snmp-server view *name oid* [**excluded** | **included**]	Adds the subtree or table of OID-specified MIB t the name of the SNMP view, and specifies th access right of the object identifier in the name of th SNMB view.

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 configuration of the SNMP group name, limiting the subsets of the objects that the group name can access.

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 relevant 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	Purpose
snmp-server community [0|7] *string* [**view** *view-name*] [**ro | rw**] [*word*]	Defines the group access character string.

You can configure one or multiple group character strings. Run command “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”.

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	Purpose
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.

Defining the maximum length of SNMP agent data packet

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

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

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	Purpose
show snmp	Monitor the SNMP state.

Configuring SNMP local engine

Use the following command to configure the system to send the SNMP local engine:

Command	Purpose
snmp-server engineID local *engineID*	Configuring SNMP local engine

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	Purpose
snmp-server host|hostv6 host community-string [trap-type]	Specifies the receiver of the trap message.
snmp-server host|hostv6 *host* **[vrf** *word***]** **[udp-port** *port-num***]** **[permit|deny** *event- id***]** **{{version [v1 | v2c | v3]} | {[informs | traps] | [auth |noauth]}}** *community-string/user* **[authentication | configure| snmp]**	Specifies the receiver, version number and username of 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	Purpose
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

Configuring the SNMP binding source address

Run the following command in the global configuration mode to set the source address for the SNMP message.

Command	Purpose
snmp source-addr *ipaddress*	Set the source address for the SNMP message.

Configuring snmp-server udp-port

Run the following command in the global mode to configure snmp-server udp-port.

Command	Purpose
snmp-server udp-port *portnum*	Set SNMP server udp-port number

Configuring SNMPv3 group

Run the following command to configure a group.

Command	Purpose
snmp-server group [*groupname* { **v3** [**auth** | **noauth** | **priv**]}][**read** readview][**write** writeview] [**notify** notifyview] [**access** access-list]	Configure a SNMPv3 group. You can only read all items in the subtree of the Internet by default.

Configuring SNMPv3 user

You can run the following command to configure a local user. When an administrator logs in to a device, he has to user the username and password that are configured on the device. The security level of a user must be higher than or equals to that of the group which the user belongs to. Otherwise, the user cannot pass authentication.

Command	Purpose
snmp-server user *username groupname* **{v3 [encrypted|auth] [md5|sha]** *auth-password***}**	Configures a local SNMPv3 user.

Configuring snmp-server encryption

You can run the following command in global configuration mode to configure snmp-server encryption. Use ciphertext to show SHA password and MD5 password. The command is one-off and it cannot be cancelled with command “NO”.

Command	Purpose
snmp-server encryption	Use ciphertext to show SHA password and MD5 password.

Configuring snmp-server trap-source

You can run the following command in global configuration mode to configure snmp-server trap-source. Use command “no” to delete such an interface.

Command1	Purpose
snmp-server trap-source *interface*	Any SNMP server is with a trap address no matter from which interface SNMP server sends the SNMP trap.

Configuring snmp-server trap-timeout

You can run the following command in global configuration mode to configure snmp-server trap-timeout.

Command	Purpose
snmp-server trap-timeout *seconds*	Before sending the trap, the switch software will find the route of the destination address. If there is no route, the trap will be saved into the retransmission queue. The command “server trap-timeout” determines the retransmission interval.

Configuring snmp-server trap-add-hostname

Run the following command to configure snmp-server trap-add-hostname.

Command	Purpose
snmp-server trap-add-hostname	In a specific time, the network management host needs to locate which host the trap comes from.

Configuring snmp-server trap-logs

Using the following command to configure snmp-server trap-logs.

Command	Purpose
snmp-server trap-logs	Enable snmp-server trap-logs to record the forwarding record of trap as logs.

Configuring snmp -dos-max retry times

Set password retry times for logging in snmp in five minutes.

Command	Purpose

snmp-server set-snmp-dos-max *retry times*	Set password retry times for logging in snmp in five minutes.

It should be used cooperatively with snmp-server host.

Configuring keep-alive times

You can run the following command in global configuration mode to configure snmp-server keep-alive times.

Command	Purpose
snmp-server keep-alive *times*	Send keep-alive times regularly to the trap host.

Configuring snmp-server necode

You can run the following command in global configuration mode to configure snmp-server encode information (This is the only tag of the device.). Use command “no” to remove the tag information.

Command	Purpose
snmp-server necode *text*	Corresponds to snmp private MIB variables.

Configuring snmp-server event-id

You can run the following command in global configuration mode to configure snmp-server event-id. Use Command “no” to delete the configuration.

Command	Purpose
snmp-server event-id *number* **trap-oid** *oid*	It is used in host configuration and for filtering in forwarding trap.

Configuring snmp-server getbulk-timeout

You can run the following command in global configuration mode to configure snmp-server getbulk-timeout. If it is timeout, all request from getbulk will not be deal with. Use command “no” to delete the configuration.

Command	Purpose
snmp-server getbulk-timeout *seconds*	Set getbulk-timeout. If it is timeout, all request from getbulk will not be deal with.

Configuring snmp-server getbulk-delay

You can run the following command in global configuration mode to configure snmp-server getbulk-delay. Unit is centisecond. Use the no form of the command to delete.

Command	Purpose

snmp-server getbulk-delay *ticks*	To avoid snmp occupies excessive CPU,set snmp-server getbulk-delay ticks. Unit: centisecond.

Showing snmp running information

Use the show snmp command to monitor SNMP input and output statistics, including illegal community string entries, errors, and the number of request variables. Use the show snmp engineID command to display SNMP engine information. Use the show snmp host command to display SNMP trap host information. Use the show snmp view command to display SNMP view information. Use the show snmp mibs command to display mib registration information. Use the show snmp group command to display SNMP group information. Use the show snmp user command to display SNMP user information.

Command	Purpose
show snmp *engineID*	Show SNMP trap local engine information.
show snmp *host*	Show SNMP trap host information.
show snmp *view*	Show snmp view information.
show snmp *mibs*	Show snmp mibs registration information.
show snmp *group*	Show snmp group information
show snmp *user*	Show snmp user information.

Showing snmp debug information

Showing information about SNMP error, snmp event and snmp packet.

Command	Purpose
debug snmp *error*	Enable the debug switch of SNMP error.
debug snmp *event*	Enable the debug switch of snmp event.
debug snmp *packet*	Enable the debug switch of snmp packet

Configuration Example

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. 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.

Example 2

```
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 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.

RMON Configuration

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

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	Purpose
config	Enter the global configuration mode.
rmon alarm index variable *interval* {**absolute** | **delta**} **rising-threshold** *value* [*eventnumber*] **falling-threshold** *value* [*eventnumber*] [**owner** *string*] **[repeat]**	Add an 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 objects in the Integer, Counter, Gauge or Time Ticks type can be detected. **interval** is the time section for sampling. Its unit is second. Its effective value is from 1 to 2147483647.

	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. **Event number** is the index of an event that is generated when a threshold is reached. Event number is optional. **Owner string** is to describe the information about the alarm. **Repeat** is to repeat trigger event.
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.

Configuring rMon event for switch

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

Step	Command	Purpose
1.	**config**	Enter the global configuration mode.
2.	**rmon event index** [**description** *string*] [**log**] [**owner** *string*] [**trap** community] [**ifctrl** *interface*]	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. **ifctrl interface** is the interface controlling event shutdown.

		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.

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.	**config**	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 stats 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.

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.	config	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 abtain 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.

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 occurrence 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.

4. Security ConfigurationAAA Configuration

AAA Overview

Access control is used to control the users to access OLT or NAS and to limit their service types. Authentication, authorization, and accounting (AAA) network security services provide the primary framework through which you set up access control on your OLT or access server.

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: It is a method of identifying users, including username/password inquiry and encryption according to the chosen security protocol.

  Authentication is a method to distinguish the user's identity before users access the network and enjoy network services. AAA authentication can be configured through the definition of an authentication method list and then application of this method list on all interfaces. This method list defines the authentication type and the execution order; any defined authentication method list must be applied on a specific interface before it is executed. The only exception is the default authentication method list (which is named default). If there are no other authentication method lists, the default one will be applied on all interfaces automatically. If anyone is defined, it will replace the default one. For how to configure all authentications, see "Authentication Configuration".

- Authorization: it is a remote access control method to limit user's permissions.

  AAA authorization takes effect through a group of features in which a user is authorized with some permissions. Firstly, the features in this group will be compared with the information about a specific user in the database, then the comparison result will be returned to AAA to confirm the actual permissions of this user. This database can be at the accessed local server or OLT, or remote Radius/TACACS+ server. The Radius or TACACS+ server conducts user authorization through a user-related attribute-value peer. The attribute value (AV) defines the allowably authorized permissions. All authorization methods are defined through AAA. Like authentication, an authorization method list will be first defined and then this list will be applied on all kinds of interfaces. For how to carry on the authorization configuration, see "Authorization Configuration".

- Accounting: it is a method to collect user's information and send the information to the security server. The collected information can be used to open an account sheet, make auditing and form report lists, such as the user ID, start/end time, execution commands, and the number of packets or bytes.

The accounting function can track the services that users access, and at the same time track the service-consumed network resource number. When AAA accounting is activated, the access server can report user’s activities to the TACACS+ or Radius server in way of accounting. Each account contains an AV peer, which is stored on the security server. The data can be used for network management, client's accounting analysis or audit. Like authentication and authorization, an accounting method list must be first defined and then applied on different interfaces. For how to carry on the accounting configuration, see “Accounting Configuration”.

Benefits of Using AAA

AAA provides the following benefits:

- Increased flexibility and control of access configuration
- Scalability
- Standardized authentication methods, such as RADIUS, TACACS+
- Multiple backup systems

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.

AAA Method List

To configure AAA, define a named method list first and then apply it to the concrete service or interface. This method list defines the running AAA type and their running sequence. Any defined method list must be applied to a concrete interface or service before running. The only exception is the default method list. The default method list is automatically applied to all interfaces or services. Unless the interface applies other method list explicitly, the method list will replace the default method list.

A method list is a sequential list that defines the authentication methods used to authenticate a user. In AAA method list you can specify one or more security protocols. Thus, it provides with a backup authentication system, in case the initial method is failed. Our switch software uses the first method listed to authenticate users; if that method does not respond, the 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.

It is important to notice that the switch 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 user name 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. Take the authentication as an example to demonstrate the relation between AAA service and AAA method list.

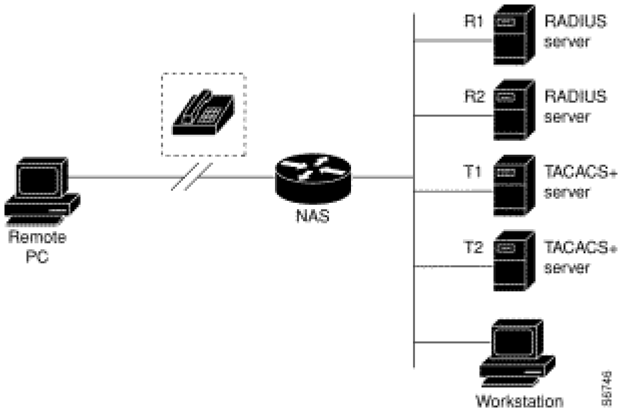


Figure Typical AAA Network Configuration

In this example, default is the name of the method list, including the protocol in the method list and the request sequence of the method list follows the name. The default method list is automatically applied to all interfaces.

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.

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. Only when an ERROR is detected will AAA select the next authentication method defined in the authentication method list.

Suppose the system administrator wants to apply the method list to a certain or a specific port. In such case, the system administrator should create a non-default method list and then apply the list of this name to an appropriate port.

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. Before you configure AAA, you need know the basic configuration procedure. To do AAA security configuration on XXCOM OLT or access servers, perform the following steps:

- If you decide to use a security server, configure security protocol parameters first, such as RADIUS, TACACS+.
- 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.

Authentication Configuration

AAA Authentication Configuration Task List

- Configuring Login Authentication Using AAA
- Enabling Password Protection at the Privileged Level
- Configuring Message Banners for AAA Authentication
- Modifying the Notification Character String for Username Input
- Modifying AAA authentication password-prompt
- Creating local user name authentication database

AAA Authentication Configuration Task

General configuration process of AAA authentication

To configure AAA authentication, perform the following configuration processes:

(3) If you decide to use a separate security server, configure security protocol parameters, such as RADIUS, or TACACS+. Refer to the relevant section for the concrete configuration methods.

(4) Configuring Authentication Method List Using aaa authentication

(5) If necessary, apply the accounting method list to a specific interface or line.

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. After the authentication method lists are configured, you can apply these lists by running login authentication. You can run the following command in global configuration mode to start the configuration:

Command	Purpose
aaa authentication login {**default** | *list-name*}*method1* [*method2...*]	Enables AAA globally.
line { **console** | **vty** } *line-number* [*ending-line-number*]	Enter the configuration mode of a line.
login authentication {**default** | *list-name*}	Applies the authentication list to a line or set of lines. (In the line configuration mode)

The list-name is a character string used to name the list you are creating. The key word method specifies the actual method of the authentication method. 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.

The default parameter can create a default authentication list, which will be automatically applied to all interfaces. 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 keyword **none** enables any user logging in to successfully authenticate, it should be used only as a backup method of authentication.

If you cannot find the authentication method list, you can only login through the console port. Any other way of login is in accessible.

The following table lists the supported login authentication methods:

Keyword	Notes:
enable	Uses the enable password for authentication.
group *name*	Uses named server group for authentication.
group radius	Uses RADIUS for authentication.
group tacacs+	Uses group tacacs+ for authentication.
line	Uses the line password for authentication.
local	Uses the local username database for authentication.
localgroup	Uses the local strategy group username database for authentication.
local-case	Uses case-sensitive local user name authentication.
none	Passes the authentication unconditionally.

(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.

(6) 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.

(7) 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."

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	Notes
enable	Uses the enable password for authentication.
group *group-name*	Uses named server group for authentication.
group radius	Uses RADIUS authentication.
group tacacs+	Uses tacacs+ for authentication.
line	Uses the line password for authentication.
none	Passes the authentication unconditionally.

When configuring enable authentication method as the remote authentication, use RADIUS for authentication. Do as follows:

(1) Uses RADIUS for enable authentication:

The user name for authentication is $ENABLE*level*$; level is the privileged level the user enters, that is, the number of the privileged level after enable command. For instance, if the user wants to enter the privileged level 7, enter command enable 7; if configuring RADIUS for authentication, the user name presenting to Radius-server host is $ENABLE7$; the privileged level of enable is 15 by default, that is, the user name presenting to Radius-server host in using RADIUS for authentication is $ENABLE15$. The user name and the password need to configure on Radius-server host in advance. The point is that in user database of Radius-server host, the Service-Type of the user specifying the privileged authentication is 6, that is, Admin-User.

Configuring Message Banners for AAA Authentication

The banner of configurable, personal logon or failed logon is supported. When AAA authentication fails during system login, the configured message banner will be displayed no matter what the reason of the failed authentication is.

Configuring the registration banner

Run the following command in global configuration mode.

Command	Purpose
aaa authentication banner *delimiter text-string delimiter*	Configures a personal logon registration banner.

Configuring the banner of failed logon

Run the following command in global configuration mode.

Command	Purpose
aaa authentication fail-message *delimiter text-string delimiter*	Configures a personal banner about failed logon.

Usage Guidelines

When creating a banner, you need to configure a delimiter and then to configure the text string itself. The delimiter is to notify that the following text string will be displayed as the banner. The delimiter appears repeatedly at the end of the text character string, indicating that the banner is ended.

Modifying the Notification Character String for Username Input

To modify the default text of the username input prompt, run aaa authentication username-prompt. You can run no aaa authentication username-prompt to resume the password input prompt.

username:

The aaa authentication username-prompt command does not change any prompt information provided by the remote TACACS+ server or the RADIUS server. Run the following command in global configuration mode:

Command	Purpose

aaa authentication username-prompt *text-string*	Modifies the default text of the username input prompt.

Modifying AAA authentication password-prompt

To change the text displayed when users are prompted for a password, use the aaa authentication password-prompt command. To return to the default password prompt text, use the no form of this command. You can run no aaa authentication username-prompt to resume the password input prompt.

password:

The aaa authentication password-prompt command does not change any prompt information provided by the remote TACACS+ server or the RADIUS server. Run the following command 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.

Creating the Authentication Database with the Local Privilege

To create the enable password database with the local privilege level, run **enable password** in global configuration mode. To cancel the enable password database, run **no enable password**.

enable password { [*encryption-type*] *encrypted-password*} [**level** *level*]

no enable password [**level** *level*]

AAA Authentication Configuration Example

RADIUS Authentication Example

The following example shows how to configure the OLT to authenticate and authorize using RADIUS:

```
aaa authentication login radius-login group radius local
aaa authorization network radius-network group radius
line vty 3
login authentication radius-login
```

The meaning of each command line is shown below:

- The aaa authentication login radius-login group radius local command configures the OLT to use RADIUS for authentication at the login prompt. If RADIUS returns an error, the user is authenticated using the local database.
- The aaa authorization network radius-network group radius 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.

Authorization Configuration

AAA Authorization Configuration Task List

- Configuring EXEC authorization through AAA

AAA Authorization Configuration Task

General configuration process of AAA authorization

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, or TACACS+. Refer to the relevant section for the concrete configuration methods.

(8) Run aaa authorization to define the authorization method list. The authorization service is not provided by default.

(9) If necessary, apply the accounting method list to a specific interface or line.

Configuring EXEC authorization through AAA

To enable AAA authorization, run aaa authorization. The aaa authorization exec command can create one or several authorization method lists and enable the EXEC authorization to decide whether the EXEC hull program is run by the users or not, or decide whether the users are authorized with the privilege when entering the EXEC hull program. After the authorization method lists are configured, you can apply these lists by running login authorization. You can run the following command in global configuration mode to start the configuration:

Command	Purpose
aaa authorization exec {**default** | *list-name*}*method1* [*method2...*]	Creates the global authorization list.
line [**console** | **vty**] *line-number* [*ending-line-number*]	Enter the configuration mode of a line.
login authorization {**default** | *list-name*}	Applies the authorization list to a line or set of lines. (In the line configuration mode)

The list-name is a character string used to name the list you are creating. The method keyword is used to designate the real method for the authorization process. Only when the previously-used method returns the authorization error can other authorization methods be used. If the authorization fails because of the previous method, other authorization methods will not be used. If you requires the EXEC shell to be entered even when all authorization methods returns the authorization errors, designate none as the last authorization method in the command line.

The default parameter can create a default authentication list, which will be automatically applied to all interfaces. For example, you can run the following command to designate RADIUS as the default authorization method of EXEC:

```
aaa authorization exec default group radius
```

Note:

If the authorization method list cannot be found during authorization, the authorization will be directly passed without the authorization service conducted.

The following table lists currently-supported EXEC authorization methods:

Keyword	Notes:
group *WORD*	Uses the named server group to conduct authorization.
group radius	Uses RADIUS authorization.
group tacacs+	Uses tacacs+ authorization.
local	Uses the local database to perform authorization.
if-authenticated	Automatically authorizes the authencated user with all required functions.
none	Passes the authorization unconditionally.

AAA Authorization Examples

Example of Local EXEC Authorization

The following example shows how to perform the local authorization and local authorization by configuring the OLT:

```
aaa authentication login default local
aaa authorization exec default local
!
localauthor a1
  exec privilege default 15
!
local author-group a1
username exec1 password 0 abc
username exec2 password 0 abc author-group a1
username exec3 password 0 abc maxlinks 10
username exec4 password 0 abc autocommand telnet 172.16.20.1
!
```

The following shows the meaning of each command line:

- The aaa authentication login default local command is used to define the default login-authentication method list, which will be automatically applied to all login authentication services.
- The command is used to define the default EXEC authorization method list, which will be automatically applied to all users requiring to enter the EXEC shell.
- Command localauthor al defines a local authority policy named al. Command exec privilege default 15 means the privileged level of exec login user is 15 by default.
- Command local author-group a1 means apply the local authorization policy a1 to global configuration (the default local policy group).
- Command username exec1 password 0 abc defines an account exec1 with password abc in the global configuration mode.

- Command username exec2 password 0 abc author-group a1 defines an account exec 2 with password abc in the global configuration mode. The account is applied to the local authorization policy a1.
- Command username exec3 password 0 abc maxlinks 10 defines an account exec 3 with password abc in the global configuration mode. The account makes 10 users available simultaneously.
- Command username exec4 password 0 abc autocommand telnet 172.16.20.1 defines an account exec4 with password abc. telnet 172.16.20.1 is automatically run when the user login the account.

AAA Accounting Configuration

AAA Accounting Configuration Task List

- Configuring Connection Accounting using AAA
- Configuring Network Accounting using AAA
- Configuring Accounting Update using AAA
- Accounting Suppress Null-username

AAA Accounting Configuration Task

General configuration process of AAA accounting

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, or TACACS+. Refer to the relevant section for the concrete configuration methods.

(10) Apply the method lists to a particular interface or line, if required. The accounting service is not provided by default.

(11) If necessary, apply the accounting method list to a specific interface or line.

Configuring Connection Accounting Using AAA

To enable AAA accounting, run command aaa accounting. To create a or multiple method list(s) to provide accounting information about all outbound connections made from the OLT, use the aaa accounting connection command. The outbound connections include Telnet, PAD, H323 and rlogin. Only H323 is supported currently. You can run the following command in global configuration mode to start the configuration:

Command	Purpose
aaa accounting connection {**default** | *list-name*} {{{**start-stop** | **stop-only**} **group** *groupname}* | **none**}	Establishes the global accounting list.

The list-name is a character string used to name the list you are creating. The method keyword is used to designate the real method for the accounting process.

The following table lists currently-supported connection accounting methods:

Keyword	Notes:
group *WORD*	Uses the named server group to conduct accounting.
group radius	Uses the RADIUS for accounting.
group tacacs+	Uses the TACACS+ for 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.

Configuring Network Accounting using AAA

To enable AAA accounting, run command aaa accounting. The aaa accounting network command can be used to establish one or multiple accounting method lists. The network accounting is enabled to provide information to all PPP/SLIP sessions, these information including packets, bytes and time accounting. You can run the following command in global configuration mode to start the configuration:

Command	Purpose
aaa accounting network {**default** | *list-name*} {{{**start-stop** | **stop-only**} **group** *groupname}* | **none**}	Establishes the global accounting list.

The list-name is a character string used to name the list you are creating. The method keyword is used to designate the real method for the accounting process.

The following table lists currently-supported network accounting methods:

Keyword	Notes:
group *WORD*	Uses the named server group to conduct accounting.
group radius	Uses the RADIUS for accounting.
group tacacs+	Uses the TACACS+ for 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.

Configuring Accounting Update through AAA

To activate the AAA accounting update function for AAA to send the temporary accounting record to all users in the system, run the following command: You can run the following command in global configuration mode to start the configuration:

Command	Purpose
aaa accounting update [**newinfo**] [**periodic** *number*]	Enables AAA accounting update.

If the newinfo keyword is used, the temporary accounting record will be sent to the accounting server when there is new accounting information to be reported. For example, after IPCP negotiates with the IP address of the remote terminal, the temporary accounting record, including the IP address of the remote terminal, will be sent to the accounting server.

When the periodic keyword is used, the temporary accounting record will be sent periodically. The period is defined by the number parameter. The temporary accounting record includes all accounting information occurred before the accounting record is sent.

The two keywords are contradictable, that is, the previously-configured parameter will replace the latter-configured one. For example, if aaa accounting update periodic and then aaa accounting update new info are configured, all currently-registered users will generate temporary accounting records periodically. All new users have accounting records generated according to the new info algorithm.

Limiting User Accounting Without Username

To prevent the AAA system from sending the accounting record to the users whose username character string is null, run the following command in global configuration mode:

- **aaa accounting suppress null-username**

Local Account Policy Configuration

Local Account Policy Configuration Task List

- Local authentication policy configuration
- Local authorization policy configuration
- Local password policy configuration
- Local policy group   configuration

Local Account Policy Configuration Task

Local authentication policy configuration

To enter local authentication configuration, run command localauthen WORD in global configuration mode.

(1) The max login tries within a certain time

login max-tries *<1-9>* **try-duration** *1d2h3m4s*

The configured local authentication policy can be applied to a local policy group or directly applied to a local account. It gives priority to some local account directly.

Local authorization policy configuration

To enter local authorization configuration, run command localauthor *WORD* in global configuration mode.

(1) To authorize priority for login users.

exec privilege {**default | console | ssh | telnet}** *<1-15>*

The configured local authorization policy can be applied to a local policy group or directly applied to a local account. It gives priority to some local account directly.

Local password policy configuration

To enter local authorization configuration, run command localpass *WORD* in global configuration mode.

(1) The password cannot be the same with the user name

non-user

(2) The history password check (The new password cannot be the same with the history password. The history password record is 20.)

non-history

(3) Specify the components of the password (complicate the password)

element *[number] [lower-letter] [upper-letter] [special-character]*

(4) Specify the components of the password (complicate the password)

min-length *<1-127>*

(5) password validity period (the validity of the password)

validity 1d2h3m4s

The configured local authorization policy can be applied to a local policy group or directly applied to a local account. It gives priority to some local account directly.

Local policy group configuration

To configure the local group policy, use the **localgroup WORD** command in global configuration mode. (The global configuration mode is considered as the default local policy configuration mode).

(1) local authentication configuration: apply the configured local authentication policy to the policy group

local authen-group *WORD*

(2) local authorization configuration: apply the configured local authorization policy to the policy group

local author-group *WORD*

(3) local password configuration: apply the configured local password policy to the policy group

local pass-group *WORD*

(4) local account configuration: set the max links and freeze for the policy group

local user {{maxlinks *<1-255>***} | { freeze** *WORD* **}}**

(5) account configuration: set the account for the policy group and establish the local database

username *username* [**password** *password* | {**encryption-type** *encrypted-password*}] [**maxlinks** *number*] [**authen-group** *WORD*] [**author-group** *WORD*] [**pass-group** *WORD*] [**autocommand** *command*]

The configured local policy group can be used in local authentication and authorization. Local method is applicable to the default policy group and

localgroup word is to a local policy group.

Local Account Policy Example

This section provides one sample configuration using local account policy. The following example shows how to configure the local authentication and local authorization.

```
aaa authentication login default local
aaa authorization exec default local
!
localpass a3
 non-user
 non-history
 element number lower-letter upper-letter special-character
 min-length 10
 validity 2d
!
localauthen a1
 login max-tries 4 try-duration 2m
!
localauthor a2
 exec privilege default 15
!
local pass-group a3
local authen-group a1
local author-group a2
!
```

The meaning of each command line is shown below:

- The aaa authentication login default local command is used to define the default login-authentication method list, which will be automatically applied to all login authentication services.
- The command is used to define the default EXEC authorization method list, which will be automatically applied to all users requiring to enter the EXEC shell.
- The command localpass a3 defines the password policy named a3.
- The command localauthen a1 defines the authentication policy named a1.
- The command localauthor a2 defines the authorization policy named a2.
- The command local pass-group a3 applies the password policy named a3 to the default policy group.
- The command localauthen a1 applies the authentication policy named a1 to the default policy group.

- The command localauthor a2 applies the authorization policy named a2 to the default policy group.

Configuring 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. The last section in this chapter-RADIUS Configuration Examples-provides with two examples. Refer to RADIUS Configuration Commands for more details of RADIUS command.

Overview

RADIUS Overview

RADIUS is a distributed client/server system that secures networks against unauthorized access. In the implementation, RADIUS clients run on OLTs 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.
- 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.

RADIUS is not suitable in the following network security situations:

- 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

- Conditions of OLT to other switching devices. RADIUS does not provide two-way authentication. On the OLT only incoming call authentication is available when running RADIUS. The outbound call is impossible.
- Networks using a variety of services. RADIUS generally binds a user to one service model.

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.

(12) The username and encrypted password are sent over the network to the RADIUS server.

(13) The user receives one of the following responses from the RADIUS server:

ACCEPT: The user is authenticated.

REJECT: The user is not authenticated and is prompted to reenter the username and password, or access is denied.

CHALLENGE: A challenge is issued by the RADIUS server. The challenge collects additional data from the user.

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:

a. Services that the user can access, including Telnet or rlogin.

b. Connection parameters, including the host or client IP address, access list, and user timeouts.

RADIUS Configuration Steps

To configure RADIUS on your OLT 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.

The following configuration tasks are optional:

- If necessary, run aaa authorization in global configuration mode to authorize the user’s service request. For more information about using the aaa authorization command, refer to the "Configuring Autorization" chapter.
- If necessary, run aaa accounting in global configuration mode to record the whole service procedure. For more information about running aaa accounting, see Record Configuration.

RADIUS Configuration Task List

- Configuring OLT to RADIUS Server Communication
- Configuring OLT to Use Vendor-Specific RADIUS Attributes
- Specifying RADIUS Authentication
- Specifying RADIUS Authorization
- Specifying RADIUS Accounting

RADIUS Configuration Task

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 switch use a shared secret text string to encrypt passwords and exchange responses. Use the **radius-server host** command to specify RADIUS server, Use the **radius-server key** command to specify a shared secret text (key) string.

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.

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.

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."

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."

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."

RADIUS Configuration Examples

RADIUS Authentication Example

The following example shows how to configure the switch 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 OLT 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 Application in AAA

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 group radius local
line vty 1 16
login authentication admins
```

The meaning of each command line is shown below:

radius-server host is used to define the IP address of the RADIUS server.

radius-server key is used to define the shared key between network access server and RADIUS server.

aaa authentication login admins group radius local command defines the authentication method list "admins," 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 is used to designate to apply the admins method list during login.

TACACS+ Configuration

TACACS+ Overview

As an access security control protocol, TACACS+ provides the centralized verification of acquiring the network access server's access right for users. . The communication's safety is guaranteed because the information exchange between network access server and TACACS+ service program is encrypted

Before using TACACS+ configured on network access server, TACACS+'s server has to be accessed and configured. TACACS+ provides independent modularized authentication, authorization and accounting.

Authentication—supporting multiple authentication ways (ASCII, PAP, CHAP and etc), provides the ability of processing any conversation with users (for example, bringing forward probing questions like family address, service type, ID number and etc. after providing login username and password). Moreover, TACACS+ authentication service supports sending information to user's screen, like sending information to notify user that their password has to be changed because of the company's password aging policy.

Authorization—detailed controlling of user's service limitation during service time, including setting up automatic commands, access control, dialog continuing time and etc. It can also limit the command enforcement which user might execute.

Accounting—collecting and sending the information of creating bills, auditing, or counting the usage status of network resources. Network manager can use accounting ability to track user's activities for security auditing or provide information for user's bills. The accounting function keeps track of user authentication, beginning and starting time, executed commands, packets' quantity and bytes' quantities, and etc.

The Operation of TACACS+ Protocol

Authentication in ASCII Form

When user logs in network access server which uses TACACS+, and asking for simple authentication in ASCII form, the following process might happen under typical circumstances:

When the connection is built up, network access server communicates with TACACS+ service program to acquire username prompt, and then gives it to user. User enters username, and network access server communicates with TACACS+ service program again to acquire password prompt. It shows password prompt to user. User enters password and then the password is sent to TACACS+ service program.

Note:

TACACS+ allows any dialogues between server's program and user until it collects enough information to identify user. Normally it is accomplished by the combination of prompting username and password, but it can also include other items, like ID number. All of these are under the control of TACACS+ server's program.

Network access server finally gets one of the following responses from TACACS+ server:

ACCEPT	User passes authentication, and service begins. If network access server is configured as requiring service authorization, authorization begins at this moment.
REJECT	User does not pass authentication. User might be rejected for further access or prompted to access again. It depends on the treatment of TACACS+ server.
ERROR	Error happens during authentication, and the cause might be at server. It also might happen at the network connection between server and network access server. If ERROR response is received, normally network access tries another way to identify user.
CONTINUE	It prompts user to enter additional authentication information.

Authentication in PAP and CHAP Ways

PAP login is similar with ASCII login, but the difference is that username and password of network access server is in PAP message not entered by user, thus it would not prompt user to enter relative information. CHAP login is similar in the main parts. After authentication, user need to enter authorization stage if network access server asks for the authorization for user. But before TACACS+ authorization is handled, TACACS+ authentication has to be finished.

If TACACS+ authorization needs to be processed, it needs to contact with TACACS+ server program again and go back to the authorization response of ACCEPT or REJECT. If back to ACCEPT, AV (attribute-value) for data, which is used for specifying the user's EXEC or NETWORK dialogue and confirming services which user can access, might be included.

TACACS+ Configuration Process

In order to configure as supporting TACACS+, the following tasks must be processed:

Using command **tacacs-server** to assign one or multiple IP addresses of TACACS+ server. Using command tacacs key to assign encrypted secret key for all the exchanged information between network access server and TACACS+ server. The same secret key has to be configured in TACACS+ server program.

Use the global configuration command aaa authentication to define the method table which uses TACACS+ to do authentication. More information about command aaa authentication, please refer to “Authentication Configuration”.

Use commands line and interface to apply the defined method table on interfaces or lines. More relative information, please refer to “Authentication Configuration”.

TACACS+ Configuration Task List

- Assigning TACACS+ server
- Setting up TACACS+ encrypted secret key
- Assigning to use TACACS+ for authentication
- Assigning to use TACACS+ for authorization
- Assigning to use TACACS+ for accounting

TACACS+ Configuration Task

Assigning TACACS+ Server

Command **Tacacs-server** could help to assign the IP address of TACACSC+ server. Because TACACS+ searching host in the configured order, this characteristic is useful for servers which configured with different priorities. In order to assign TACACS+ host, use the following commands under global configuration mode:

Command	Purpose
tacacs-server host *ip-address* [**single-connection**| **multi-connection**] [**port** *integer*] [**timeout** *integer*] [**key** *string*]	To assign the IP address of TACACS+ server and relative features.

Use command tacacs-server to configure the following as well:

- Use single-connection key word to assign the adoption of single connection. This would allow server program to deal with more TACACS+ operations and be more efficient. multi-connection means the adoption of multiple TCP connection.
- Use parameter port to assign TCP interface number which is used by TACACS+ server program. The default interface number is 49.
- Use parameter timeout to assign the time’s upper limit (taken second as the unit) for OLT’s waiting response from server.
- Use parameter key to assign the encrypted and decrypted secret keys for messages.

Note:

Connect host after using tacacs-server, and connect the timeout value defined by command timeout to cover the global timeout value configured by command tacacs-server timeout. Use the encrypted secret key assigned by tacacs-server to cover the default secret key configured by global configuration command tacacs-server key. Therefore, this command could be used to configure the unique TACACS+ connection to enhance the network security.

Setting up TACACS+ Encrypted Secret Key

In order to set up the encrypted secret key of TACACS+ message, use the following command under the global configuration mode:

Command	Purpose
tacacs-server key *keystring*	To set up the encrypted secret key matched with the encrypted secret key used by TACACS+ server.

Note:

In order to encrypt successfully, the same secret key should also be configured for TACACS+ server program.

Assigning to Use TACACS+ for Authentication

After having marked the TACACS+ server and defined its related encrypted secret key, method table need to be defined for TACACS+ authentication. Because TACACS+ authentication is by AAA, command aaa authentication should be assigned as TACACS+'s authentication way. More information, please refer to "Authentication Configuration".

Assigning to Use TACACS+ for Authorization

AAA authorization could help to set up parameter to confine user's network access limitation. TACACS+ authorization could be applied to services like command, network connection, EXEC dialogue and etc. Because TACACS+ authorization is by AAA, command aaa authorization should be assigned as TACACS+'s authentication way. More information, please refer to "Authorization Configuration".

Assigning to Use TACACS+ for Accounting

AAA accounting is able to track user's current service and their consumed network resources' quantity. Because TACACS+ authorization is by AAA, command aaa accounting should be assigned as TACACS+'s accounting way. More information, please refer to "Accounting Configuration".

TACACS+ Configuration Example

This chapter includes the following TACACS+ configuration example.

TACACS+ Authentication Examples

The following configuring login authentication is accomplished by TACACS+:

```
aaa authentication login test group tacacs+ local

tacacs-server host 1.2.3.4

tacacs-server key testkey

line vty 0
```

```
login authentication test
```

In this example:

Command **aaa authentication** defines the authentication method table test used on vty0. Key word tacacs+ means the authentication is processed by TACACS+, and if TACACS+ does not respond during authentication, key word local indicates to use the local database on the network access server to do authentication.

Command **tacacs-server host** marks TACACS+ server's IP address as 1.2.3.4. command tacacs-server key defines the shared encrypted secret key as testkey.

The following example is the security protocol used when configuring TACACS+ as login authentication, with the usage of method table default not test:

```
aaa authentication login default group tacacs+ local
tacacs-server host 1.2.3.4
tacacs-server key goaway
```

In this example:

Command **aaa authentication** defines the default authentication method table default during login authentication. If authentication required, keyword tacacs+ means authentication is by TACACS+. If TACACS+ does not respond, keyword local indicates to use the local database on the network access server for authentication.

Command **tacacs-server host** marks TACACS+ server program's IP address as 1.2.3.4. Command **tacacs-server key** defines the shared encrypted secret key as goaway.

TACACS+ Authorization Examples

```
aaa authentication login default group tacacs+ local
aaa authorization exec default group tacacs+
tacacs-server host 10.1.2.3
tacacs-server key goaway
```

In this example:

Command aaa authentication defines the default authentication method table default during login authentication. If authentication required, keyword tacacs+ means authentication is by TACACS+. If TACACS+ does not respond, keyword local indicates to use the local database on the network access server for authentication.

Command aaa authorization does network service authorization by TACACS+.

Command tacacs-server host marks TACACS+ server's IP as 10.1.2.3. Command tacacs-server key defines the shared encrypted secret key as goaway.

TACACS+ Accounting Examples

The following configuration of login authentication's method table uses TACACS+ as one of the methods to configure the accounting by TACACS+:

```
aaa authentication login default group tacacs+ local
aaa accounting exec default start-stop group tacacs+
tacacs-server host 10.1.2.3
tacacs-server key goaway
```

In this example:

Command **aaa authentication** defines the default authentication method table default during login authentication. If authentication required, keyword tacacs+ means authentication is by TACACS+. If TACACS+ does not respond, keyword local indicates to use the local database on the network access server for authentication.

Command **aaa accounting** does accounting of network service by TACACS+. In this example, the relative information of starting and beginning time is accounted and sent to TACACS+ server.

Command **tacacs-server host** marks TACACS+ server's IP address as 10.1.2.3. Command **tacacs-server key** defines the share

5. Interface ConfigurationTable of Contents

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.

Supported Interface Types

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

Interface Type	Task	Reference
Ethernet interface	Configures fast Ethernet interface. Configures gigabit Ethernet interface.	*Configuring Ethernet Interface*
Logical Interface	Aggregation interface VLAN 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:

- Fast Ethernet interface
- Gigabit Ethernet interface

The supported logical interface of our switch include:

- aggregation interface
- VLAN interface

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_config#show interface g0/2
GigaEthernet0/2 is administratively down, line protocol is down
  Hardware is Giga-Combo-FX, address is 00e0.0f8d.e0e1 (bia 00e0.0f8d.e0e1)
  MTU 1500 bytes, BW 10000 kbit, DLY 10 usec
  Encapsulation ARPA
  port info 1 0 2 1
  Auto-duplex,    Auto-speed
  flow-control off
     Received 0 packets, 0 bytes
     0 broadcasts, 0 multicasts
     0 discard, 0 error, 0 PAUSE
     0 align, 0 FCS, 0 symbol
     0 jabber, 0 oversize, 0 undersize
     0 carriersense, 0 collision, 0 fragment
     0 L3 packets, 0 discards, 0 Header errors
     Transmited 0 packets, 0 bytes
     0 broadcasts, 0 multicasts
     0 discard, 0 error, 0 PAUSE
     0 sqettest, 0 deferred
     0 single, 0 multiple, 0 excessive, 0 late
     0 L3 forwards
```

Note:

There is no need to add blank between interface type and interface number. For example, in the above line, g0/2 or g 0/2 is both right.

(2) 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.

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

Interface Configuration

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.

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'.

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.

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 cannot adjust the actual time delay of an interface.

Monitoring and Maintaining Interface

The following tasks can monitor and maintain interface:

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

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.
show version	Displays memory configuration, software version, start-up image and so on.

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.

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’.

Setting the Ethernet Interface

In this section the procedure of setting the Enthernet interface will be described. The detailed configuration includes the following steps, among which step 1 is obligatory while other steps are optional.

Choosing an Ethernet Interface

Run the following command in global configuration mode to enter the Ethernet interface configuration mode:

Command	Purpose
interface gigaethernet [*slot|port*]	Enters the gigabit-Ethernet interface configuration mode.

The **show interface gigaethernet** [*slot*|*port*] command can be used to show the state of the gigabit-Ethernet interface.

Configuring the Rate

The Ethernet rate can be realized not only through auto-negotiation but also through interface configuration.

Command	Purpose
show interface gigaethernet [*slot*|*port*]	Sets the rate of fast Ethernet to 10M, 100M, 1000M or auto-negotiation.
show interface gigaethernet [*slot*|*port*]	Resumes the default settings. The rate is auto-negotiation

Note：

The speed of the optical interface varies according to the model. For example, the speed of GE-FX is 1000M, but it can also be specified as 100M through configuration. The speed of FE-FX is 100M. If there is auto parameter after the speed command of the optical interface, the interface can enable the automatic negotiation function. Otherwise, The speed of the optical interface is fixed and cannot negotiate. The gigabit port can support 10,100,1000 mode in auto mode.The specific configuration is subject to the prompt from each port.

Configuring the Duplex Mode of an Interface

By default, Ethernet interfaces can automatically negotiate whether to be half duplex or full duplex. The duplex mode for the gigbit interface is always auto.

Command	Purpose
duplex {**full**|**half**|**auto**}	Sets the duplex mode of an Ethernet interface.
No duplex	Resumes the default settings. The duplex mode is auto-negotiation.

Configuring Flow Control on an Interface

When an interface is in full duplex mode, flow control is realized through the 802.3X-defined PAUSE frame. In half duplex mode, it is implemented by back pressure.

Command	Purpose
flow-control *on/off /auto*	Enables or disables flow control on an interface.
no flow-control	Resumes the default settings, that is, there is no flow control on an interface.

Configuring Logistical Interface

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

- Configuring aggregation interface

- Configuring VLAN interface

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

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.

Interface Configuration Example

Configuring Public Attribute of Interface

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
```

Interface Shutdown Example

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

```
interface GigaEthernet0/1
shutdown
```

The following example shows how to enable the interface:

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

6. Interface Range ConfigurationInterface Range Configuration Task

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.

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 no space before/after the hyphen or the comma.

Configuration Example

Enter the interface configuration mode via the following commands, including slot 0 and fast Ethernet 1,2,3,4:

```
switch_config# interface range gigaEthernet 0/1-4
switch_config_if_range#
```

7. Port Physical Characteristics ConfigurationConfiguring the Ethernet Interface

Configuring Rate

The Ethernet rate can be realized through auto-negotiation or configuration on the interface.

Run the following command to configure the Ethernet rate:

Command	Purpose
Speed {**10**|**100**|**auto**} (T port) **Speed** {**100**|**1000**|**auto**} (SFP port)	Set the rate of fast Ethernet to 10M, 100M, 1000M or auto-negotiation.
No speed	Resume the default settings—auto-negotiation.

Note:

The speed of the optical interface is fixed. For example, the rate of GBIC and GE-FX is 1000M; the rate of FE-FX is 100M. If the **auto** parameter is behind the **speed** command, it means that you can enable the auto-negotiation function on the optical interface. Otherwise, you cannot enable the auto-negotiation function on the optical interface.

Configuring the Duplex Mode of an Interface

By default, the Ethernet interface can be auto, half duplex or full duplex. The gigabit combo SFP/TX ports does not support speed 1000 and compulsory duplex mode simultaneously.

Command	Purpose
duplex {**full** | **half** | **auto**}	Sets the duplex mode of the Ethernet.
No duplex	Resumes the default setting. The duplex mode is auto-negotiation.

Configuring Flow Control on the Interface

When the interface is in full-duplex mode, the flow control is achieved through the PAUSE frame defined by 802.3X. When the interface is in half-duplex mode, the flow control is achieved through back pressure.

Command	Purpose
flow-control {on | off | auto}	Enable or disable the flow control on the interface.
no flow-control	Resume the default settings. The default settings have no flow control.

Note:

The difference between “flow-control auto” and “flow-control on” is that the flow control frame is compulsory received. The flow control frame is forwarded when the peer negotiation is successful in “auto” mode.

8. Port's Additional Features ConfigurationPort Isolation

Under normal condition, data packet could be forwarded among different ports of switches. Under some circumstances, flows among ports need to be forbidden, and port isolation function is the one to provide this kind of control. For isolation which is not based on group, data communication could not work between isolated ports, but data packets among non-isolated ports and isolated and non-isolated ports could be forwarded normally. For isolation based on group, isolated ports in group cannot do data communication, but they can do data communication with any ports outside group. To be noticed, port isolation function works for layer 2 messages, but it does not support isolation based on group.

Isolation based on non-group:

Command	Purpose
config	Entering global configuration mode
interface g0/1	Entering the interface which to be configured
[no] **switchport protected**	Enable/cancel port isolation function
exit	Back to global configuration mode
exit	Back to management configuration mode

Isolation based on group:

Command	Purpose
config	Entering global configuration mode.
[no] **port-protected** *group-id*	Create and enable the isolation group mode. *group-id* means to configure the the isolation group ID.
[no] **description** *word*	Description of the group. *Word* stand for the character string of the group.
exit	Back to global configuration mode.
interface g0/1	Entering the interface which to be configured
[no] **switchport protected** *group-id*	Add/remove isolation group. *group-id stand for* the isolation group ID that is configured.
exit	Back to global configuration mode.
exit	Back to management configuration mode.

Storm Control

Switch's ports could be attacked by constant abnormal unicast (MAC address locating failure), multicast or broadcast messages. It might cause switch's ports and even the whole switch's failure. Therefore, a mechanism has be provided to restrain this phenomenon. Storm control function could set different rates at the ingress for different kinds of messages which are allowed to enter switch.

Command	Purpose
config	Entering global configuration mode
interface g0/1	Entering the interface which to be configured
[no] **storm-control** {**broadcast** | **multicast** | **unicast**} **threshold** *count*	Configuring port's storm control function. **Unicast** means it works for unknown unicast. **Multicast** means it works for multicast. **Broadcast** means it works for broadcast. **Count** means the threshold which is to be configured.
exit	Back to global configuration mode
exit	Back to management configuration mode

Port's Rate Limitation

Port's rate limitation is used for limiting the rate of flow which comes in and goes out of ports. Use the following commands to limit port's flow rate after entering management mode:

Command	Purpose
config	Entering global configuration mode
interface g0/1	Entering the interface which to be configured
[no] **switchport rate-limit {***band* **| Bandwidth** *percent }* { **ingress** | **egress**}	Configuring the flow rate limitation for port. Band is the limited flow rate. *Percent* is the limited flow percentage. **Ingress** means it works for ingress; **Egress** means it works for egress.
exit	Back to global configuration mode
exit	Back to management configuration mode

Port Loop Detection

Port loop detection function is used for detecting whether port has loop. Time interval of loop detection messages sent by port could be configured. Use the following command to set time interval of loop detection messages sent by port after entering management mode.

Command	Purpose

config	Entering global configuration mode
Interface g0/1	Entering the interface which to be configured
[no] **keepalive [***second* **]**	Configuring time interval of loop detection messages sent by port. *Second* is the time interval of sending messages.
exit	Back to global configuration mode
exit	Back to management configuration mode

Port MAC-address learning

Port MAC address learning is used to enable/disable port MAC address learning. The configuration method is as follows:

Command	Purpose
config	Entering global configuration mode
interface g0/1	Entering the interface which to be configured
[no] **switchport disable-learning**	Configure port MAC address learning. Enable/disable port MAC address learning function.
exit	Back to global configuration mode
exit	Back to management configuration mode

Port's Security

Port's security does controlling by accessing port according to MAC address. Port's security has three kinds of modes: dynamic security mode, static accepting mode, and static rejecting mode. Under dynamic security mode, maximum MAC address quantity which is allowed to be learnt by ports can be configured. When the maximum mac quantity has been learnt from some port by switch, mac address would not be learnt; at the meantime, switch drops all the DLF messages. Under static security mode, static security MAC address can be configured at port. Under static accepting mode, only messages which source MAC is safe MAC address are allowed to get in, and others would be dropped. Under static rejecting mode, messages which source MAC is safe MAC address would be dropped, and other messages would be allowed to get in.

Command	Purpose
config	Entering global configuration mode
interface g0/1	Entering the interface which to be configured
[no] **switchport port-security mode** {**dynamic | static** *accept*|*reject* | **sticky**}	Configuring port's security mode. **Dynamic** means dynamic security mode.

	static *accept* means static accepting mode **static** *reject* means static rejecting mode
[no] **switchport port-security dynamic maximum** *num*	Configuring maximum learnable MAC address quantity
[**no**] **switchport port-security static mac-address** *H.H.H*	Configuring static security address
[**no**] **switchport port-security sticky** {**maximum** *sticky_number* | **mac-address** *H.H.H* | **aging-time** *aging_time* }	Configuring port MAC address sticky. **maximum** *sticky_number* means maximum sticky MAC address quantity. **mac-address** *H.H.H* means to configure sticky MAC address manually. **aging-time** *aging_time* means to configure aging time of sticky MAC address manually.
exit	Back to global configuration mode
exit	Back to management configuration mode

Interface's binding

This switch could be bind with IP address and MAC address on interface at the same time, or be bind with only IP address or MAC address. It works for IP and ARP messages.

Use the following commands to do configuration after entering management mode:

Command	Purpose
config	Entering global configuration mode
interface g0/1	Entering the interface which to be configured
[no] **switchport port-security bind|block** {**ip|arp| both-arp-ip** *A.B.C.D* **| mac** *H.H.H* }	Configuring interface's binding function. **Bind** only allows messages which conform to binding requirements to pass, and other messages would not be allowed to pass. Block only reject messages which conform to binding requirements, and others would be allowed to pass.

	Ip means it would only work for IP messages which conform to binding requirements; **Arp** means it would only work for arp messages which conform to binding requirements; **both-arp-ip** means it would work for ip and arp messages conforming to binding requirements.
exit	Back to global configuration mode
exit	Back to management configuration mode

SVL/IVL

This switch can be configured with Shared (SVL)/independent (IVL) vlan learning mode. By default, the ports are all in IVL mode.

This switch could be bind with IP address and MAC address on interface at the same time, or be bind with only IP address or MAC address. It works for IP and ARP messages.

Use the following commands to do configuration after entering management mode:

Command	Purpose
config	Entering global configuration mode
[no]**vlan shared-learning**	Configuring SVL/IVL
exit	Back to management configuration mode

Configuring Link Scan

Overview

Configuring port’s scanning time interval is to scan port’s up/down status quickly.

Link scan Configuration Task

- Configuring port's scanning time interval.

1. Setting up port's scanning time interval

When setting up port's scanning time interval, use the following command under global configuration mode:

Command	Purpose
[no] Link scan {normal *interval* | **fast** *interval***}**	Mode means to choose optical port's scanning mode. **Normal** means standard link scanning mode. **Fast** means quick link scanning mode. Fast mode mainly applies to service protocol, like rstp. **Interval** means configuring port's scanning time interval.

Configuration Example

Configuring standard scanning interval as 20 millisecond

```
link scan normal 20
```

Configuring Port Enhanced Link Status Check

Overview

Configuring port's enhanced link status check is to scan port's link status quickly.

Configuration Task

- Enable/disable port's enhanced link status check.

Enable/disable port's enhanced link status check

When enable/disable port's enhanced link status check, use the following command under interface configuration mode:

Command	Purpose
[no] switchport enhanced-link	Enable/disable port's enhanced link status check.

Configuration Example

Enable enhanced link status check of interface g0/1.

```
Switch_config#interface g0/1
Switch_config_g0/1#switchport enhanced-link
```

Configuring system mtu

Overview

Configuring system mtu

Configuration Task

- Configuring system mtu

Setting up mtu

Use the following command under global configuration mode:

Command	Purpose
[no] system mtu *mtu*	Configuring system mtu value

Configuration Example

Configuring system mtu 2000 bytes

```
Switch_config#system mtu 2000
```

9. Port Mirroring Configuration Configuring Port Mirroring

Configuring Port Mirroring Task List

- Configuring port mirroring
- Displaying port mirroring information

Configuring Port Mirroring Task

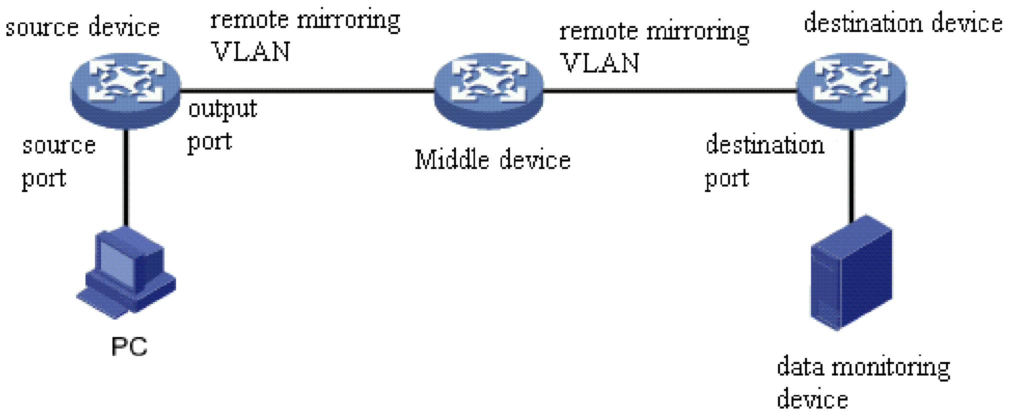
Configuring Port Mirroring

In order to make switch management easy, you can set port mirror and use a port of the switch to observe the flux that runs through a group of ports.

Port mirroring could be divided like local mirroring and remote mirroring. Local mirroring means copying message to this device's port, and remote mirroring function means transferring message to remote device across multiple network devices. Port mirroring is configured by the way of mirroring group, and relative concepts include port, destination port, remote mirroring VLAN, remote mirroring TPID, VLAN DISABLE-LEARNING and etc.

In the remote mirroring, the local device would add a vlan tag in the mirroring message. Messages from different mirroring's remote groups are detected by setting the tag's vid (remote mirroring vlan) and tpid. In order to achieve remote mirroring function, it is required that the middle device could transfer messages within remote mirroring's vlan to remote device.

Remote mirroring's schemetic plot is like following:



Configuring remote mirroring function on source device, and mirroring source port's message to the output port while adding configuring RSPAN TAG on the message. Vlan id in this tag is the remote mirroring VLAN. Middle device transfer mirroring message to the destination port by broadcasting. The destination device transfer message from destination port to data monitoring device by configuration. If the destination device supports port mirroring function, the message could be transferred from destination port to data monitoring device by configuring local mirroring. If the destination device supports the configuration of mac address learning based on vlan, the message could be transferred to data monitoring device by shutting down remote mirroring vlan address learning. If the destination device's qos policy mapping supports the matching of vlan, the message could be transferred to monitoring device by qos policy mapping.

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

Command	Description
config	Enters the global configuration mode.
mirror session *session_number* {**destination** {**interface** *interface-id*} { **rspan** *vid tpid*} | **source** {**interface** *interface-id* [, | -] rx | tx | both] }	Configures port mirroring. **session-number** is the number of the port mirroring. **destination** is the destination port of the mirroring. Vid of the remote mirroring tag. tpid of the remote mirroring tag. **source** is the source port of mirroring. **rx** means the input data of mirroring. Tx means the output data of mirroring. Both means the input and output data of mirroring.
exit	Enters the management mode again.
write	Saves the configuration.

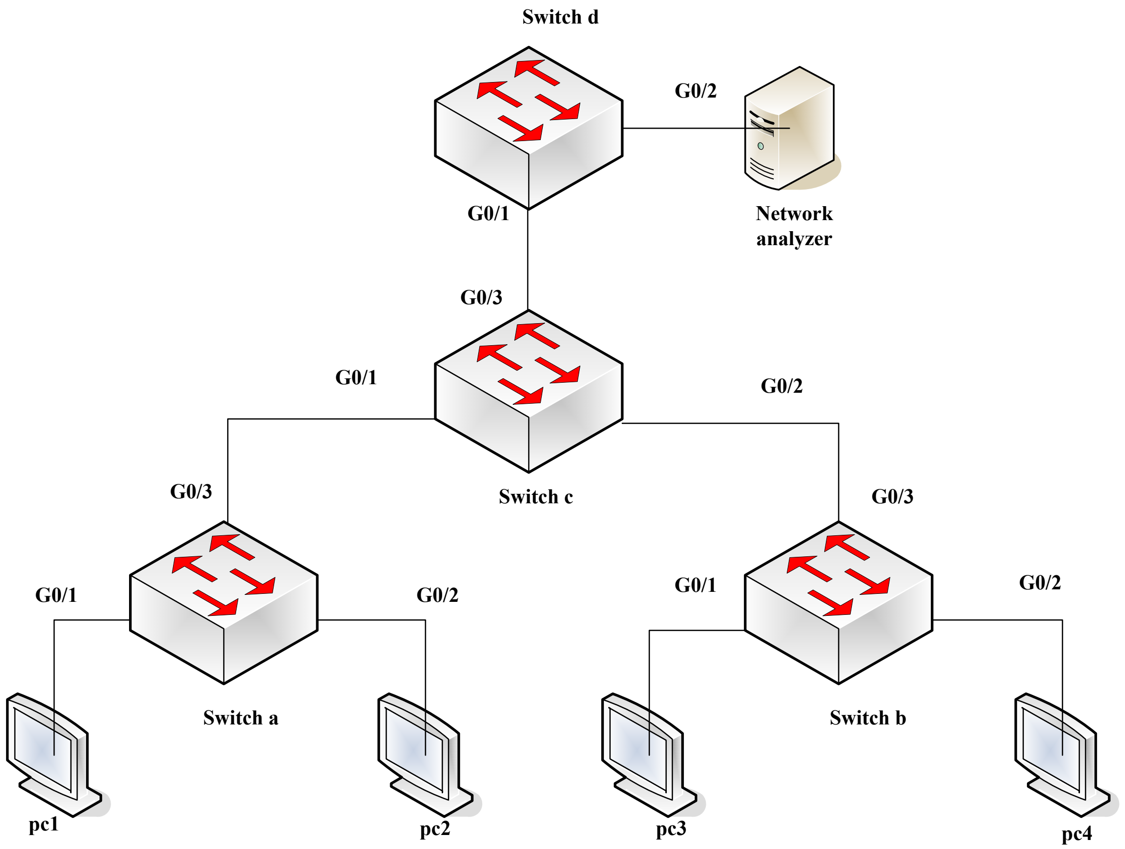
Displaying Port Mirroring Information

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.

Remote Mirroring Configuration Example

The network environment is as shown in following figure:



Users need to monitor the flow of the g0/1 port in switch a and the g0/1 port in switch b at the network analyzer, which can be realize through remote mirroring. The configuration is as follows:

switch a:

```
mirror session 1 destination interface g0/3 rspan 100 0x8100
mirror session 1 source interface g0/1 both
```

switch b:

```
mirror session 1 destination interface g0/3 rspan 1000 0x8100
mirror session 1 source interface g0/1 both
```

switch c:

```
interface GigaEthernet0/1
 switchport mode trunk
!
interface GigaEthernet0/2
 switchport mode trunk
!
interface GigaEthernet0/3
 switchport mode trunk
!
```

```
!
vlan 1,100,1000
!
```

switch d:

```
mirror session 1 destination interface g0/2
mirror session 1 source interface g0/1 both
```

10. MAC Address Table Attribute Configuration Configuring MAC Address Attribute

MAC Address Configuration Task List

- Configuring Static Mac Address
- Configuring Mac Address Aging Time
- Configuring blackhole Mac Address
- Displaying Mac Address Table
- Clearing Dynamic Mac Address

MAC address Configuration Task

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.

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.

Displaying blackhole Mac Address

Blackhole MAC address table entries refer to those entries that are not allowed to communicate and can only be manually deleted. Blackhole MAC addresses can be added and removed according to the actual needs of the use of the switch. Configure the following commands to add and remove a blackhole MAC address:

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

Displaying MAC Address Table

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 | brief | multicast | interface** *interface-id* **| vlan** *vlan-id* **| H.H.H | blackhole]**	**Dynamic** indicates the MAC address that acquires dynamically. **Interface-id** indicates the interface name. **Vlan-id** indicates the VLAN number. Valid value is from 1 to 4094. **Static** indicates the static MAC address table. **Brief** indicates the brief information of the MAC address. **Multicast** indicates multicast MAC address table. **Interface** indicates interface MAC address table. **Vlan** indicates MAC address table in VLAN. **H.H.H** indicates specific address. **Blackhole** indicates BLACKHOLE MAC address table.

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.

11. MAC Access-List Configuration

Access-list configuration includes:

- Creating MAC access-list
- Configuring items of MAC access-list
- Applying MAC access-list

Creating MAC Access-List

A MAC access-list must be created first before applying it on the port. When a MAC access-list has been created, it enters MAC access-list configuration mode, under which items of MAC access-list can be configured.

Enter privilege mode and use the following steps to add or delete a MAC access-list.

Command	Purpose
config	Enters the global configuration mode.
[**no**] **mac access-list** *name*	To add or cancel a MAC access list, run the previous command. **name** stands for the name of theMACaccess list.

Configuring Items of MAC Access-List

In MAC access-list configuration mode, specify to permit or deny any source MAC address or a specific host source MAC address and any destination MAC address. The same items can be configured in a MAC access list only once.

Enter MAC access list configuration mode and use the following steps to set MAC access list entry.

Command	Purpose
[**no**] {**permit | deny}** {**any** | **host** *src-mac-addr* | *src-mac-addr src-mac-mask* } {**any** | **host** *dst-mac-addr* | *dst-mac-addr dst-mac-mask*}[**arp** [{*any* | *src-ip-addr*} {*any* | *dst-ip-addr* }] | *ethertype* |*cos value*]	To add/delete a MAC access list entry, run the previous command. You can repeat this command to add/delete multiple MAC access list entry. **any** means match with any MAC address; **src-mac-addr** stands for source MAC address; ***src-mac-mask*** *stands for source mac mask;* **dst-mac-addr** stands for the destination MAC address; ***dst-mac-mask*** stands for destination mac mask; **arp** stands for matched arp packet **src-ip-addr** stands for source ip address

	dst-ip-addr stands for the destination IP address **ethertype** stands for type of the matched Ethernet packet **cos value** stands for packet header marking.
exit	Log out from the MAC list configuration mode and enter the global configuration mode again.
exit	Goes back to the EXEC mode.
write	Saves the settings.

MAC list configuration example

```
Switch_config#mac access-list 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.

Applying MAC Access-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.

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

Command	Purpose
config	Enters the global configuration mode.
interface g0/1	Enters the to-be-configured port.
[**no**] **mac access-group** *name*	Apply the created MAC list to the port or delete the applied MAC list from the port. NameMAC: 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.

12. 802.1x Configuration

802.1x Configuration Task List

Configuring 802.1x port authentication

Configuring 802.1x multiple port authentication

Configuring 802.1x re-authentication

Configuring 802.1x re-authentication times

Configuring 802.1x transmission frequency

Configuring 802.1x user binding

Configuring authentication method for 802.1x port

Selecting authentication type for 802.1x port

Configuring port mab authentication

Configuring 802.1x accounting

Configuring 802.1x guest-vlan

Forbidding Supplicant with multiple network cards

Resuming default 802.1x configuration

Monitoring 802.1x authentication configuration and state

802.1x Configuration Task

Configuring 802.1x Port Authentication

802.1x defines three control methods for the port: mandatory authentication approval, mandatory authentication disapproval and 802.1x authentication startup.

Mandatory authentication approval means the port has already passed authentication. The port does not need any authentication any more, and all users can perform dara access control through the port. The authentication method is defaulted by the port. Mandatory authentication disapproval means the port authentication does not get passed no matter what kind of method is applied. No user can perform the data access control through the port.

802.1x authentication startup means the port is to run 802.1x authentication protocol. 802.1x authentication will be applied to users who access the port. Only users who pass the authentication can perform data access control through the port. After the 802.1x authentication is started up, the AAA authentication method must be configured.

Run the following command to enable the 802.1x function before configuring 802.1x:

Command	Purpose
dot1x enable	Enable the 802.1x function.

Run the following command to start up the 802.1x authentication:

Command	Purpose
dot1x port-control auto	Configure the 802.1x protocol control method on the port.
aaa authentication dot1x {default |list name} method1 [method2...]	Configure the AAA authentication of 802.1x.

Run one of the following commands in port configuration mode to select 802.1x control method:

Command	Purpose
dot1x port-control auto	Enables the 802.1x authentication method on the port.
dot1x port-control force-authorized	Approve the mandatory port authentication.
dot1x port-control force-unauthorized	Disapprove the mandatory port authentication.
dot1x port-control misc-mab	Enables 802.1x hybrid authentication.

Configuring 802.1x Multiple Port Authentication

802.1x authentication is for the authentication of single host user. In this case, the switch allows only one user to perform authentication and access control. Other users cannot be authenticated and access unless the previous user exits authentication and access. In the case the port connects multiple hosts through switch devices, such as 1108 switch, that do not support 802.1x, you can start up the multiple port access function to make sure that all host users can access.

The multi-auth has two modes: one is multiple-host mode and the other is multiple-auth mode. In **multiple-hosts** mode, the port will be set to **up** if one of the users passes the authentication. Thus, other users can access the device by the port without authentication. In **multiple-auth** mode, the swich will authenticate each user separately. The port will be set to **up** if one user has been successfully authenticated. The port is set to down if all users are failed to authenticate. Thus, the failure of one user will not affect other users' access to the device.

Note: **Multi-auth** mode cannot be configured simultaneously with **guest vlan** or **mab authentication**. If an interface is in multi-auth mode, all users on the interface will be authenticated again.

Run the following command in interface configuration mode to activate 802.1x multiple host authentication:

Command	Purpose
dot1x authentication multiple-hosts	Set the 802.1x multiple port authentication. The port is set to **up** only if one user passes the authentication.
dot1x authentication multiple-auth	Set the 802.1x multiple port authentication. Each user is non-related in authentication.

Configuring 802.1x Re-authentication

After the authentication is passed, the authentication to the client will still be conducted every interval to ensure the legality of the client's authentication.

In this case, you need to enable the re-authentication function. After the re-authentication is started, the authentication request will be periodically sent to the host.

Run the following commands to configure the re-authentication function.

Command	To
dot1x re-authentication	Enables the re-authentication function.
dot1x timeout re-authperiod *time*	Configures the period of the re-authentication function.

Configuring 802.1x Re-authentication times

After the authentication fails, the switch will re-send request/ID packet to enable the authentication. When the re-authentication times exceeds the certain number and there is still no respond, the authentication will be suspended.

Run the following command in interface configuration command to set the maximum times for of re- authentication:

Command	Purpose
dot1x reauth-max *time*	Set the maximum times of re- authentication.

Configuring 802.1x Transmission Frequency

In the process of 802.1x authentication, data texts will be sent to the host. The data transmission can be adjusted by controlling 802.1x transmission frequency so that the host response is successful.

Run the following command to configure the transmission frequency:

Command	Purpose
dot1x timeout tx-period *time*	Set the message transmission frequency of 802.1x.

Configuring 802.1x User Binding

When 802.1x authentication is performed, you can bind a user to a certain port to ensure the security of port access. Run the following command in interface configuration mode to start up 802.1x user binding.

Command	Purpose
dot1x user-permit *xxxz*	Configure a user that is bound to a port.

Configuring Authentication Method for 802.1x Port

The 802.1x authentication can be performed in different methods at different ports. In the default configuration, the 802.1x authentication adopts the **default** method.

Run the following command in interface configuration mode to configure the method of the 802.1x authentication:

Command	Purpose
dot1x authentication method *yyy*	Configure the method of the 802.1x authentication.

Selecting Authentication Type for 802.1x Port

You can select the type for the 802.1x authentication. The 802.1x authentication type determines whether AAA uses Chap authentication or Eap authentication. Eap authentication supports the md5-challenge mode and the eap-tls mode. Challenge required by MD5 is generated locally when the Chap authentication is adopted, while challenge is generated at the authentication server when the eap authentication is adopted. Each port adopts only one authentication type. The authentication type of global configuration is adopted by default. Once a port is set to an authentication type, the port will use the authentication type unless you run the **No** command to resume the default value.

Eap-tls takes the electronic certificate as the authentication warrant and complies with the handshake rules in Translation Layer Security (tls). Therefore, high security is guaranteed.

Run the following command in global configuration mode to configure the authentication type:

Command	Purpose
dot1x authen-type {**chap**|**eap**}	Select chap or eap.

Also run the following command in interface configuration mode:

Command	Purpose
dot1x authentication type {**chap**|**eap**}	Select chap or eap or the configured authentication type in global mode.

Configuring MAB Authentication on the Port

When a peer device cannot run the 802.1x client software, the switch will adopt the MAB authentication mode and then the MAC address of the peer device will be sent as both the username and password to the radius server for authentication.

Note: You can run the dot1x mabformat command on a switch to specify the accounting ID and the password's format so that you make it sure that they are same with those on the radius server.

When MAB is enabled and the peer device, however, neither sends the eapol_start packet nor responds to the request_identity packet and exceeds the timeout threshold, the switch regards the peer device not to support the 802.1x authentication client and then turns to the MAB authentication.

Note: The MAB authentication mode cannot coexist with the multi-auth mode.

When the MAB authentication is enabled, you can set the format of the MAC address to the Radius server through this command.

Command	Purpose
dot1x mab	Enables the MAB authentication on a port.

To set the format of the MAC address, you can run the following command in global configuration mode:

Command	Purpose
dot1x mabformat{1|2|3|4|5|6}	Chooses one MAC address' format from six formats from format 1 to format 6. The default format is 1.

Configuring 802.1x Accounting

The 802.1x authentication and 802.1x accounting can be performed at the same time. It working mechanism is: after the dot1x authentication is approved, judge whether the accounting function is enabled on the authentication interface; if the accounting function is enabled, send the accounting request through the AAA interface; when the AAA module returns successful request response message, the AAA interface can forward texts.

The accounting can adopt various accounting methods configured in the AAA module. For details, refer to AAA configuration.

After the beginning of accounting, dot1x periodically sends **update** message to the server through the AAA interface for obtaining correct accounting information. According to different AAA configuration, the AAA module decides whether to send the **update** message.

At the same time, You are required to enable the dot1x re-authentication function so that the switch can know when supplicant is abnormal.

Run the following commands in interface configuration mode to enable the dot1x accounting and to configure the accounting method:

Command	Purpose
dot1x accounting enable	Enable the dot1x accounting.
dot1x accounting method {*method name***}**	Configure the accounting method. Its default value is **default**.

Configuring 802.1x guest-vlan

Guest-vlan gives releavant ports some access rights (such as downloading client software) when the client does not respond. Guest-vlan can be any configured vlan in the system. If the configured guest-vlan does not meet the conditions, ports cannot run in the guest-vlan.

Note: There is no access right if the authentication fails.

Run the following command in the global mode to enable the guest-vlan:

Command	Purpose

Dot1x guest-vlan	Enable the guest-vlan at all ports.

When there is no **guest-vlan id** originally configured at each port, guest-vlan cannot function even if guest-vlan is enabled in global mode. Only when **guest-vlan id** is configured in port configuration mode, guest-vlan can function.

Run the following command in port configuration mode to configure **guest-vlan id**:

Command	Purpose
Dot1x guest-vlan {id(1-4094)}	Enable the vlan id of guest-vlan at all ports.

Forbidding Supplicant With Multiple Network Cards

Forbid the Supplicant with multiple network adapters to prevent agents. Run the following command in port configuration mode:

Command	Purpose
dot1x forbid multi-network-adapter	Forbid the Supplicant with multiple network adapters.

Resuming Default 802.1x Configuration

Run the following command to resume all global configuration to default configuration:

Command	Purpose
dot1x default	Resume all global configuration to default configuration.

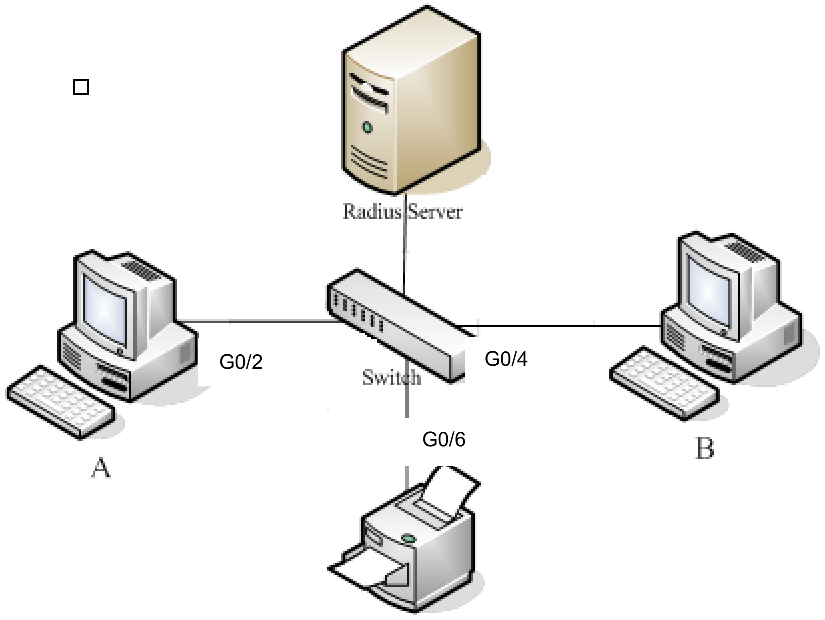
Monitoring 802.1x Authentication Configuration and State

To monitor the configuration and state of 802.1x Authentication and decide which 802.1x parameter needs to be adjusted, run the following command in management mode:

Command	Purpose
show dot1x { *interface*|*statistics*|*misc-mab-db* }	Monitor the configuration and state of 802.1x authentication.

802.1x Configuration Example

□



Host A connects port G0/2 of the switch. Host B connects port G0/4. Host C connects with port G0/6. The IP address of the radius-server host is 192.168.20.2. The key of radius is TST. Port G0/2 adopts remote radius authentication, user binding and re-authentication. Port G0/4 adopts local authentication of eap type, and enables multi-host and guest-vlan. Port G0/6 adopts mab authentication and the mac address format is AA:BB:CC:DD:EE:FF.

Global configuration

```
username switch password 0 TST
username TST password 0 TST
aaa authentication dot1x TST-G0/2 group radius
aaa authentication dot1x TST-G0/4 local
aaa authentication dot1x TST-G0/6 group radius
aaa accounting network dot1x_acc start-stop group radius
dot1x enable
dot1x re-authentication
dot1x timeout re-authperiod 10
dot1x mabformat 2
dot1x guest-vlan
interface VLAN1
ip address 192.168.20.24 255.255.255.0
!
vlan 1-2
radius-server host 192.168.20.2 auth-port 1812 acct-port 1813
radius-server key TST
```

Configuring port G0/2

```
interface GigaEthernet0/2
 dot1x port-control auto
 dot1x authentication method TST-G0/2
 dot1x user-permit radius-TST
                        dot1x accounting enable
```

```
                    dot1x accounting method dot1x_acc
```

Configuring port G0/4

```
Interface GigaEthernet0/4
 dot1x authentication multiple-hosts
 dot1x port-control auto
 dot1x authentication method TST-G0/4
 dot1x guest-vlan 2
```

Configuring port G0/6

```
interface GigaEthernet0/6
dot1x mab
dot1x authentication method TST-G0/6
```

13. GVRP Configuration

Configuring GVRP

Overview

GVRP (GARP VLAN Registration Protocol GARP VLAN) is a GARP (GARP VLAN Registration Protocol GARP VLAN) application that provides IEEE 802.1Q-compliant VLAN pruning and dynamic VLAN creation on 802.1Q trunk ports. With GVRP, the switch can exchange the VLAN configuration information with the other GVRP switches, prune the unnecessary broadcast and unknown unicast traffic, and dynamically create and manage the VLANs on the switches that are connected through the 802.1Q trunk ports.

Configuring Task List

GVRP Configuration Task List

Enabling/Disabling GVRP Globally

Enabling/Disabling GVRP on the Interface

Monitoring and Maintenance of GVRP

GVRP Configuration Task

Enabling/Disabling GVRP Globally

Perform the following configuration in global configuration mode.

Command	Description
[no] gvrp	Enables/disables GVRP globally.

It is disabled by default.

Dynamic VLAN to Validate only on a Registered Port

Run the following commands in global configuration mode:

Command	Description
[no] gvrp dynamic-vlan-pruning	Enable/disable VLAN to validate only on a registered port.

After this function is enabled, dynamic VLAN takes effect only on the ports on which this dynamic VLAN is registered. After this command is enabled and if a port has not registered a dynamic VLAN, this port will not belong to the dynamic VLAN even though this port is a trunk port and it allows the dynamic VLAN to pass through.

The function is disabled by default.

Enabling/Disabling GVRP on the Interface

Perform the following configuration in interface configuration mode:

Command	Description
[no] gvrp	Enables/disables interface GVRP.

In order for the port to become an active GVRP participant, you must enable GVRP globally first and the port must be an 802.1Q trunk port,

It is enabled by default.

Monitoring and Maintenance of GVRP

Perform the following operations in EXEC mode:

Command	Description
show gvrp statistics [**interface** port_list]	Displays GVRP statistics.
show gvrp status	Displays GVRP global state information.
[**no**] **debug gvrp** [**packet** | **event**]	Enables/disables GVRP data packet and event debug switches. All debug switches will be enabled/disabled if not specified the concrete switch.

Display GVRP statistics:

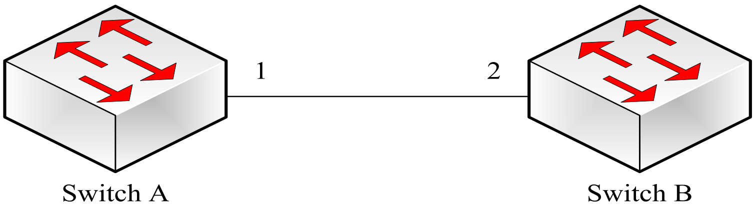
```
switch#show gvrp statistics interface Tthernet0/1
GVRP statistics on port Ethernet0/1
GVRP Status: Enabled
GVRP Failed Registrations: 0
GVRP Last Pdu Origin: 0000.0000.0000
GVRP Registration Type: Normal
```

Display GVRP global state information:

```
Switch#show gvrp status
GVRP is enabled
```

Configuration Example

The network connection is as follows. In order to make the VLAN configuration information of Switch A and Switch B identical, you can enable GVRP on Switch A and Switch B. The configuration is as follows:



Configure the interface 1 that Switch A connects to Switch B to trunk:

```
Switch_config_g0/1# switchport mode trunk
```

Enable global GVRP of switch A:

```
Switch_config#gvrp
```

Enable GVRP of interface 1 of Switch A:

```
Switch_config_g0/1#gvrp
```

Configure VLAN 10, Vlan 20 and Vlan30 on Switch A

```
Switch_config#vlan 10,20,30
```

Configure the interface 2 that Switch A connects to Switch B to trunk:

```
Switch_config_g0/2# switchport mode trunk
```

Enable global GVRP of switch B:

```
Switch_config#gvrp
```

Enable GVRP of interface 2 of Switch B

```
Switch_config_g0/2#gvrp
```

Configure VLAN 40, Vlan 50 and Vlan60 on Switch B

```
Switch_config#vlan 40,50,60
```

After completing the configuration, the VLAN configuration information will be displayed respectively on Switch A and Switch B, that is, VLAN10, VLAN20,VLAN30, VLAN40, VLAN50 and VLAN60 on both switches.

14. VLAN ConfigurationVLAN Configuration

VLAN Introduction

VLAN(Virtual Local Area Network) 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.

VLAN can be classified based on MAC address, IP subnetwork, the protocol and the port.

Dot1Q Tunnel Overview

Preface

Dot1Q Tunnel is a lively name of the tunnel protocol based on 802.1Q encapsulation, which is defined in IEEE 802.1ad. Its core idea is to encapsulate the VLAN tag of the private network to that of the public network, and the packets with two layers of tags traverse the backbone network of ISP and finally a relatively simple L2 VPN tunnel is provided to users. The Dot1Q Tunnel protocol is a simple and manageable protocol, which is realized through static configuration without signaling support and widely applied to enterprise networks, which mainly consist of OLTs, or small-scale MAN.

The Dot1Q Tunnel attribute of XXCOM switches just meets this requirement. As a cheap and compact L2 VPN solution, it is increasingly popular among more and more small-scale users when VPN network is required. At the inside of carrier's network, P device need not support the Dot1Q Tunnel function. That is, traditional L3 switches can meet the requirements fully and protect the investment of the carrier greatly.

Enables Dot1Q Tunnel globally.

Supports the inter-translation between customer VLAN and SPVLAN on the downlink port, including translation in Flat mode and in QinQ mode.

Supports the configuration of the uplink port.

Dot1Q Tunnel Realization Mode

There are two modes to realize Dot1Q Tunnel: port-based Dot1Q Tunnel and Dot1Q Tunnel based on inner CVLAN tag classification.

Port-based Dot1Q Tunnel:

When a port of this device receives packets, no matter whether packets have the VLAN tag, the switch will add the VLAN tag of the default VLAN on this port to these packets. Thus, if a received packet has a VLAN tag, the packet become a packet with double tags; if a received packet is untagged, this packet will be added a default VLAN tag of this port. Thus, if a received packet has a VLAN tag, the packet become a packet with double tags; if a received packet is untagged, this packet will be added a default VLAN tag of this port.

The packet with a single VLAN tag has the following structure, as shown in table 1:

DA (6B)	SA (6B)	ETYPE(8100) (2B)	VLAN TAG (2B)	ETYPE (2B)	DATA (0~1500B)	FCS (4B)

Table 1 The packet with a single VLAN tag

The packet with double VLAN tags has the following structure, as shown in table 2:

DA (6B)	SA (6B)	**ETYPE(8100)** **(2B)**	**SPVLAN** **Tag** **(2B)**	ETYPE (8100) (2B)	CVLAN Tag (2B)	ETYPE (2B)	DATA (0~1500B)	FCS (4B)

Table 2 Packet with double VLAN tags

Dot1Q Tunnel based on the inner CVLAN Tag:

The service is distributed according to the CVLAN ID zone of the inner CVLAN tag of Dot1Q Tunnel. The CVLAN zone can be translated into SPVLAN ID and there are two translation modes: Flat VLAN translation and QinQ VLAN translation. In QinQ VLAN translation mode, when a same user uses different services by using different CVLAN IDs, the services can be distributed according to CVLAN ID. For example, the CVLAN ID of bandwidth service ranges between 101 and 200. The CVLAN ID of VOIP service ranges between 201 and 300. The CVLAN ID of IPTV service ranges between 301 and 400. According to the CVLAN ID range, when the PE device receives the user data, add SPVLAN Tag whose SPVLAN ID is 1000 to the bandwidth service and whose SPVLAN ID is 3000 to the IPTV service. The difference between Flat VLAN translation mode and QinQ VLAN translation mode is SPVLAN Tag in the Flat VLAN translation mode is not add to the outside layer of CVLAN Tag, but replace CVLAN Tag directly.

VLAN Configuration Task List

Adding/Deleting VLAN

Configuring switch port

Creating/Deleting VLAN interface

Monitoring configuration and state of VLAN

Enabling/disabling global Dot1Q Tunnel

VLAN Configuration Task

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

Command	Purpose
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.

Configuring Switch Port

The switch's port supports the following modes: the access mode, the relay mode, the VLAN tunnel mode, the VLAN translating tunnel mode and the VLAN tunnel uplink mode.

The access mode indicates that this port is only subordinate to one vlan and only sends and receives untagged ethernet frame.

The relay mode indicates that the port connects other switches and the tagged Ethernet frame can be transmitted and received.

The VLAN translating tunnel mode is a sub mode based on the relay mode. The port looks up the VLAN translation table according to the VLAN tag of received packets to obtain corresponding SPVLAN, and then the switching chip replaces the original tag with SPVLAN or adds the SPVLAN tag to the outside layer of the original tag. When the packets is forwarded out of the port, the SPVLAN will be replaced by the original tag or the SPVLAN tag will be removed mandatorily. Hence, the switch omits different VLAN partitions that access the network, and then passes them without change to the other subnet that connects the other port of the same client, realizing transparent transmission.

The VLAN tunnel uplink mode is a sub mode based on the relay mode. The SPVLAN should be set when packets are forwarded out of the port. The SPVLAN should be set when packets are forwarded out of the port. If the packets are in the untagged range, all these packets are forwarded out without any change. When the packets are received by the port, their TPIDs will be checked. If difference occurs or they are untagged packets, the SPVLAN tag which contains their own TPID will be added to them as their outer-layer tag.

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-translating-tunnel | dot1q-tunnel-uplink }	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.

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.

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* **| dot1q-tunnel [interface** *intf***]|mac-vlan | subnet |protocol-vlan |dot1q-translating-tunnel]**	Display configuration and state of VLAN or Dot1Q Tunnel.
show interface vlan *x*	Display the states of vlan ports or supervlan port.

Enabling/disabling global Dot1Q Tunnel

After Dot1Q Tunnel is enabled globally, their ports can be defaulted as the downlink ports of Dot1Q Tunnel, and the SPVLAN tag will be added to incoming packets.

The command to enable dot1q-tunnel is shown in the following table:

Run…	To…
dot1q-tunnel	Configures the global dot1q-tunnel on a switch.

Dot1Q Tunnel Configuration Examples

Dot1Q Tunnel configuration examples

The following typical solutions show how to apply Dot1Q tunnel.

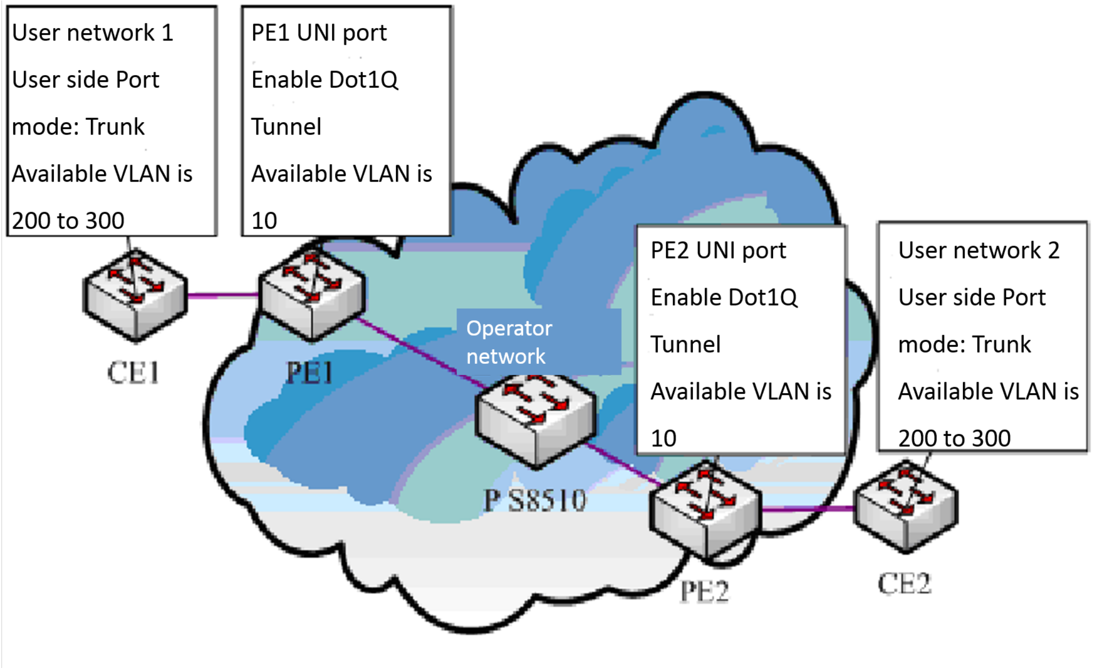


Figure 3 Configuration of Dot1Q Tunnel

As shown in the figure above, port F0/1 of CE1 connects port F0/1 (or port G0/1) of PE1; PE1 connects S8510 on port F0/2 (or port G0/2); PE2 connects S8510 on port F0/2 (or port G0/2); and port F0/1 (or port G0/1) of PE2 connects port F0/1 of CE1.

The ports of PE are set to be the access port of VLAN 10 and on them Dot1Q Tunnel is enabled. However, the ports of CE still need Trunk VLAN 200-300, enabling the link between CE and PE to be an asymmetrical link. In this case, the public network only needs to distribute users a VLAN ID, 10. No matter how many VLAN IDs of private network are planned in the user's network, the newly distributed VLAN ID of the public network will be mandatorily inserted into the tagged packets when these packets enter the backbone network of ISP. These packets then pass through the backbone network through the VLAN ID of the public network, reach the other side of the backbone network, that is, the PE devices, get rid of the VLAN tag of the public network, resume the user's packets and at last are transmitted to the CE devices of the users. Therefore, the packets that are forwarded in the backbone network have two layers of 802.1Q tag headers, one being the tag of the public network and the other being the tag of the private network. The detailed flow of packet forwarding is shown as follows:

Because the egress port of CE1 is a Trunk port, all the packets that are transmitted by users to PE1 have carried the VLAN tag of the private network (ranging from 200 to 300). One of these packets is shown in figure 4.

DA	SA	ETYPE(8100)	VLAN TAG	ETYPE	DATA	FCS

(6B)	(6B)	(2B)	(2B)	(2B)	(0~1500B)	(4B)

Figure 4 Structure of a packet from CE1

After the packets enter PE1, PE1, for the ingress port is the access port of Dot1Q tunnel, ignores the VLAN tag of the private network but inserts the default VLAN 10's tag into these packets, as shown in figure 5.

DA (6B)	SA (6B)	ETYPE(8100) (2B)	SPVLAN Tag (2B)	ETYPE (8100) (2B)	CVLAN Tag (2B)	ETYPE (2B)	DATA (0~1500B)	FCS (4B)

Figure 5 Structure of a packet going into PE1

In the backbone network, packets are transmitted along the port of trunk VLAN 10. The tag of the private network is kept in transparent state until these packets reach PE2.

PE2 discovers that the port where it connects CE2 is the access port of VLAN 10, removes the tag header of VLAN 10 according to 802.1Q, resumes the initial packets of users, and transmit the initial packets to CE2, as shown in figure 6.

DA (6B)	SA (6B)	ETYPE(8100) (2B)	VLAN TAG (2B)	ETYPE (2B)	DATA (0~1500B)	FCS (4B)

Figure 6 Structure of a packet from PE2

Seen from the forwarding flow, Dot1Q Tunnel is very concise for the signaling is not required to maintain the establishment of the tunnel, which can be realized through static configuration.

As to the typical configuration figure of Dot1Q Tunnel, XXCOM's products of different models are configured as follows when they run as PE (PE1 has the same configuration as PE2).

Dot1Q Tunnel Configuration of the switch:

```
Switch_config#dot1q-tunnel
Switch_config_g0/1#switchport pvid 10
Switch_config_g0/2#switchport mode trunk
Switch_config_g0/2#switchport trunk vlan-untagged 1-9,11-4094
```

Appendix Abbreviations

English abbreviation	English full name
VPN	Virtual Private Network
TPID	Tag Protocol Identifier
QoS	Quality of Service

P	provider bridged network core
PE	provider bridged network edge
CE	customer network edge
UNI	user-network interface
NNI	network-network interface
CVLAN	Customer VLAN
SPVLAN	Service provider VLAN

15. Private VLAN Setting

Overview of Private VLAN

Private VLAN has settled the VLAN application problems facing ISPs: If ISP provides each user with a VLAN, the support by each device of 4094 VLANs will restrict the total of ISP-supported users.

Private VLAN Type and Port Type in Private VLAN

Private VLAN subdivides the L2 broadcast domain of a VLAN into multiple sub-domains, each of which consists of a private VLAN pair: a primary VLAN and a secondary VLAN. One private VLAN domain may have multiple private VLAN pairs and each private VLAN pair stands for a sub-domain. There is only one primary VLAN in a private VLAN domain and all private VLAN pairs share the same primary VLAN. The IDs of secondary VLANs in each sub-domain differ with each other.

Having One Primary VLAN Type

Primary VLAN: It is relevant to a promiscuous port and only one primary VLAN exists in the private VLAN. Each port in the primary VLAN is a member in the primary VLAN.

Having Two Secondary VLAN Types

Isolated VLAN: No layer-2 communication can be conducted between two ports in the same isolated VLAN. Also, there is only one isolated VLAN in a private VLAN. The isolated VLAN must be related with the primary VLAN.

Community VLAN: Layer-2 communication can be conducted between two ports in the same VLAN, but they have no communication with the ports in another community VLAN. One private VLAN may contain multiple community VLANs. The community VLAN must be related with the primary VLAN.

Port Types Under the Private VLAN Port

Promiscuous port: it belongs to the primary VLAN. It can communicate with all other ports, including the isolated port and community port of a secondary VLAN in the same private VLAN.

Isolated port: It is the host port in the isolated VLAN. In the same private VLAN, the isolated port is totally L2 isolated from other ports except the promiscuous port, so the flows received from the isolated port can only be forwarded to the promiscuous port.

Community port: It is the host port in the community VLAN. In a private VLAN, the community ports of the same community VLAN can conduct L2 communication each other or with the promiscuous port, but not with the community port of other VLANs and the isolated ports in the isolated VLANs.

Modifying the Fields in VLAN TAG

This functionality supports to modify the VLAN ID and priority in VLAN tag and decides whether the egress packets of private VLAN carry the tag or not.

Private VLAN Configuration Task List

Configuring Private VLAN

Configuring the association of private VLAN domains

Configuring the L2 port of private VLAN to be the host port

Configuring the L2 port of private VLAN to be the promiscuous port

Modifying related fields of egress packets in private VLAN

Displaying the configuration information of private VLAN

Private VLAN Configuration Tasks

The conditions for a private VLAN peer to take effect are listed below:

Having the primary VLAN

Having the secondary VLAN

Having the association between primary VLAN and secondary VLAN

Having the promiscuous port in primary VLAN

Configuring Private VLAN

Use the following commands to set VLAN to be a private VLAN.

Command	Purpose
vlan *vlan-id*	Enters the VLAN mode.
private-vlan {primary|community|isolated}	Configures the features of private VLAN.
no private-vlan {primary|community|isolated}	Deletes the features of private VLAN.
show vlan private-vlan	Displays the configuration of private VLAN.
exit	Exits from Vlan configuration mode.

Configuring the Association of Private VLAN Domains

Run the following commands to associate the primary VLAN and the secondary VLAN.

Command	Purpose
vlan *vlan-id*	Enters the primary VLAN configuration mode.
private-vlan association {*svlist* | **add** *svlist* | **remove** *svlist*}	Sets the to-be-associated secondary VLAN.

no private-vlan association	Clears all associations between the current primary VLAN and all secondary VLANs.
exit	Exits the VLAN configuration mode.

Configuring the L2 Port of Private VLAN to Be the Host Port

Run the following commands to set the L2 port of private VLAN to be the host port:

Command	Purpose
Interface *interface*	Enters the interface configuration mode.
switchport mode private-vlan host	Sets the layer-2 port to be in host's port mode.
no switchport mode	Deletes the private VLAN mode configuration of L2 port.
switchport private-vlan host-association *p_vid s_vid*	Associates the L2 host port with private VLAN.
no switchport private-vlan host-association	Deletes the association between L2 host port and private VLAN.
exit	Exits from the interface configuration mode.

Configuring the L2 Port of Private VLAN to Be the Promiscuous Port

Run the following commands to set the L2 port of private VLAN to be the promiscuous port:

Command	Purpose
Interface *interface*	Enters the interface configuration mode.
switchport mode private-vlan promiscuous	Sets the layer-2 port to be in promiscuous port mode.
no switchport mode	Deletes the private VLAN mode configuration of L2 port.
switchport private-vlan mapping *p_vid{svlist* | *add svlist* | **remove** *svlist}*	Associates the L2 promiscuous port with private VLAN.
no switchport private-vlan mapping	Deletes the association between L2 promiscuous port and private VLAN.
exit	Exits from the interface configuration mode.

Modifying Related Fields of Egress Packets in Private VLAN

Run the following commands to modify related fields of the egress packets in private VLAN:

Command	Purpose
Interface *interface*	Enters the interface configuration mode.

switchport private-vlan tag-pvid *vlan-id*	Sets the VLAN ID field in the tag of egress packet.
switchport private-vlan tag-pri *pri*	Sets the priority field in the tag of egress packet.
[no] switchport private-vlan untagged	Sets whether the egress packets have the tag or not.
exit	Exits from interface configuration mode.

Displaying the Configuration Information of Private VLAN

Run the following commands in global, interface or VLAN configuration mode to display the private VLAN configuration information of private VLAN and L2 port:

Command	Purpose
show vlan private-vlan	Displays the configuration of private VLAN.
show vlan private-vlan interface *interface*	Displays the configuration of the L2 port in the private VLAN.

Configuration Example

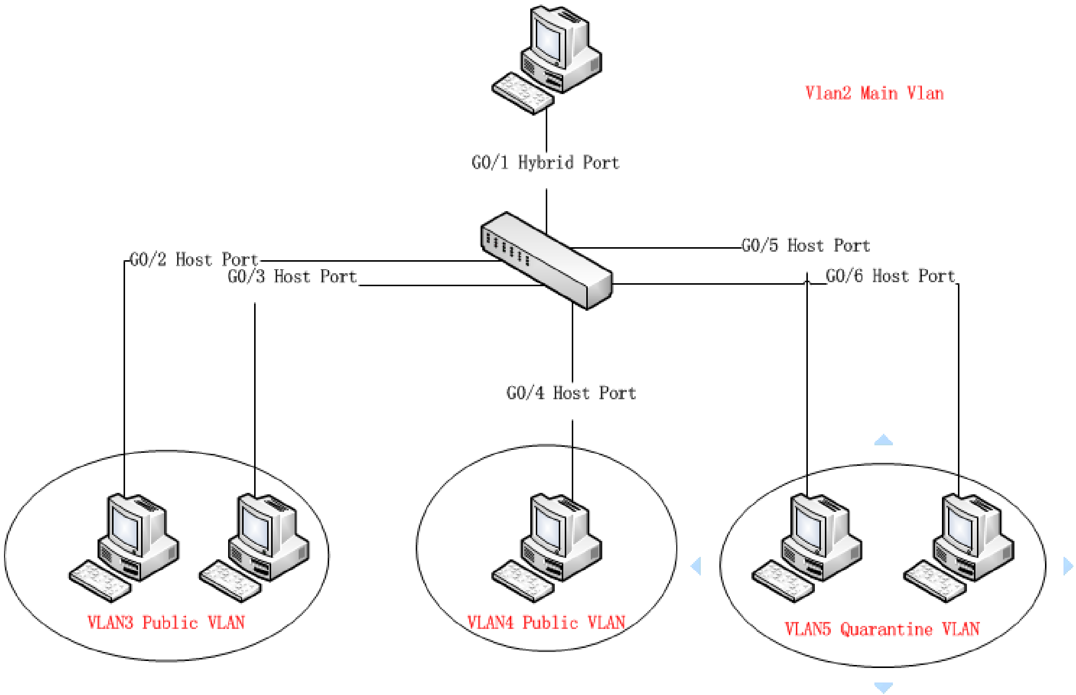


Figure 1: Typical Configuration of Private VLAN

As shown in figure 1, port G0/1 is the promiscuous port in primary VLAN 2 and ports G0/2-G0/6 are host ports, among which ports G0/2 and G0/3 are host ports (public ports) of Community VLAN 3, port G0/4 is that of Community VLAN 4, and ports G0/5 and G0/6 are host ports of Isolated VLAN 5.

According to the definition of private VLAN, L2 communication can be conducted between promiscuous port G0/1 and host ports of all sub-VLAN domains, so it is between host ports G0/2 and G0/3 of community VLAN 3, but they cannot conduct L2 communication with other host ports of secondary VLANs. L2 communication cannot go on between ports G0/5 and G0/6 in Isolated VLAN 5, but the two ports can conduct L2 communication with promiscuous port G0/1.

The commands requiring to be entered in a switch are shown below:

```
Switch_config#interface GigaEthernet0/1
Switch_config_g0/1#switchport mode private-vlan promiscuous
Switch_config_g0/1#switchport private-vlan mapping 2 3-5
Switch_config_g0/1#switchport pvid 2

 Switch_config#interface GigaEthernet0/2
 Switch_config_g0/2#switchport mode private-vlan host
 Switch_config_g0/2#switchport private-vlan host-association 2 3
 Switch_config_g0/2#switchport pvid 3

 Switch_config#interface GigaEthernet0/3
 Switch_config_g0/3#switchport mode private-vlan host
 Switch_config_g0/3#switchport private-vlan host-association 2 3
 Switch_config_g0/3#switchport pvid 3

 Switch_config#interface GigaEthernet0/4
 Switch_config_g0/4#switchport mode private-vlan host
 Switch_config_g0/4#switchport private-vlan host-association 2 4
 Switch_config_g0/4# switchport pvid 4

 Switch_config#interface GigaEthernet0/5
 Switch_config_g0/5#switchport mode private-vlan host
 Switch_config_g0/5#switchport private-vlan host-association 2 5
 Switch_config_g0/5#switchport pvid 5

 Switch_config#interface GigaEthernet0/6
 Switch_config_g0/5#switchport mode private-vlan host
 Switch_config_g0/5#switchport private-vlan host-association 2 5
 Switch_config_g0/5#switchport pvid 5

 Switch_config#vlan 2
 Switch_config_vlan2#private-vlan primary
 Switch_config_vlan2#private-vlan association 3-5
```

```
Switch_config#vlan 3
Switch_config_vlan3#private-vlan community

Switch_config#vlan 4
Switch_config_vlan4#private-vlan community

Switch_config#vlan 5
Switch_config_vlan5#private-vlan isolated



Switch_config#show vlan private-vlan
Primary     Secondary   Type                Ports
-----------     ---------------    ------------------- -----------------------------------------
2             3                community       g0/1, g0/2, g0/3
2             4                community       g0/1, g0/4
2             5                isolated            g0/1, g0/5, g0/6
```

16. STP Configuration

STP Introduction

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 ‘ Configuring RSTP’ 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.

SSTP Configuration Task List

Selecting STP Mode

Disabling/Enabling STP

Forbidding/Enable Port's STP

Configuring the Switch Priority

Configuring the Hello Time

Configuring the Max-Age Time

Configuring the Forward Delay Time

Configuring the Port Priority

Configuring the Path Cost

Monitoring STP State

Configuring SNMP Trap

SSTP Configuration Task

Selecting STP Mode

Run the following command to configure the STP mode:

command	purpose
spanning-tree mode {sstp | pvst | rstp | mstp}	Select the STP configuration.

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 | pvst** | **rstp | mstp**}	Enables a certain mode STP.

Forbidding/Enable Port's STP

Under default circumstances, STP protocol operates on all switching ports (physical ports and aggregation ports). STP operation is forbidden under port configuration mode by the following command:

command	purpose
no spanning-tree	Forbidding port to operate STP.

After STP operation is forbidden on port, port would keep assigning ports and forwarding status, and would not send BPDU. But all STP mode would still do type checking and counting on BPDU received by port. Boundary information and topology information would also be updated.

Notice:
When processing “no spanning-tree”, if port has already have roles like “RootPort”, “AlternatePort”, “MasterPort” or “BackupPort, under RSTP/MSTP mode, protocol information received by port would be aged and turned into “DesignatedPort”. Under SSTP/PVST mode, port would stay as the former role for some time, and information would be aging after timer is over time.

Notice:
Every STP mode supports BpduGuard function on "no spanning-tree" port.

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).

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 (2s).

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).

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

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).

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.

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.

Configuring SNMP Trap

You can monitor the change of STP in a switch remotely from the network management software of the host by configuring the trap function of STP.

STP protocols support two types of traps: newRoot and topologyChange. When the switch changes from the non-root type to the newRoot type, the switch sends newRoot Trap message; when the switch detects the topology change, such as a non-edge port changes from the state of non-forward to forward, the switch sends topologyChange Trap message.

Notice:

It needs to use network management software which supports Trap to receive STP trap. Network management software need to be import Bridge-MIB set, and OID is 1.3.6.1.2.1.17.

Use the following commands to intiate STP Trap under global configuration mode:

Command	Purpose
spanning-tree management trap **[newroot | topologychange]**	Initiating STP Trap. If Trap type is not defined, two kinds of TRAP would be initiated at the mean time.
no spanning-tree management trap	Shut down STP Trap.

Configuring VLAN spanning-tree

Overview

In SSTP mode, there is only one spanning tree instance for the entire network, and the state of the switch port in the spanning tree determines its state in VLAN. In the case of multiple vlans in the network, the isolation between the single spanning tree protocol and the VLAN topology may cause the normal communication of part of the network to be blocked.

The switch supports running independent SSTP on a certain number of vlans, ensuring that ports can have different states in different vlans. At the same time, the traffic balance between VLANs can be realized.

It is important to note that the number of VLANs that can run the spanning tree protocol independently depends on the actual version, and other VLAN topologies that exceed the number limit will not be controlled by STP.

VLAN STP Configuration Task

Follow these commands to configure the properties of SSTP in the VLAN in the global configuration mode:

Command	Purpose
spanning-tree mode pvst	Start the mode of allocating STP by VLAN.
spanning-tree vlan *vlan-list*	Assign a STP Instance to the specified VLAN. vlan-list: VLAN list (same below).
no spanning-tree vlan *vlan-list*	Remove a spanning-tree Instance from the specified VLAN.
spanning-tree vlan *vlan-list* **priority** *value*	Configure the priority level of the spanning tree in the specified VLAN.
no spanning-tree *vlan-list* **priority**	Reset the spanning tree priority in VLAN to default.
spanning-tree vlan *vlan-list* **forward-time** *value*	Configure the Forward Delay of the specified VLAN.
no spanning-tree vlan *vlan-list* **forward-time**	Reset the Forward Delay of the specified VLAN to default.
spanning-tree vlan *vlan-list* **max-age** *value*	Configure the Max-age of the specified VLAN.
no spanning-tree vlan *vlan-list* **max-age**	Reset the Max-age of the specified VLAN to default.
spanning-tree vlan *vlan-list* **hello-time** *value*	Configure the Hello-time of the specified VLAN.
no spanning-tree vlan *vlan-list* **hello-time**	Reset the Hello-time of the specified VLAN to default.

Follow these commands to configure the properties of the port in the interface configuration mode:

Command	Purpose
spanning-tree vlan *vlan-list* **cost**	Configure the port path cost in the specified VLAN.
no spanning-tree vlan *vlan-list* **cost**	Reset the port path cost in the specified VLAN to default.
spanning-tree vlan *vlan-list* **port-priority**	Configure the port-priority in the specified VLAN.
no spanning-tree vlan *vlan-list* **port-priority**	Reset the port-priority in the specified VLAN to default.

Follow these commands to check the state of spanning-tree at specified VLAN in the management configuration mode:

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

show spanning-tree pvst instance-list	Check the relationship between PVST instance and the VLAN.

Configuring RSTP

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

Configuring edge port

Configuring port's connection type

Restarting the check of protocol conversion

RSTP Configuration Task

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)

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 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.

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.

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.

To be noticed is that too-long Hello Time value would cause network bridge cannot receive Hello message because of link’s packet loss. Therefore network bridge would consider link is broken and recalculate spanning tree. If Hello Time value is too short, it would cause that network bridge sends configuration message frequently and the network bandwidth is occupied. It adds burden on network and CPU. It is suggested that user uses default value.

Note: We recommend user to use the default value.

The default Hello Time is 2 seconds.

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.

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.

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.

Configuring edge port

The edge port means this port connects with terminal device on network. A mandatory edge port would be at forwarding status instantly after being linked up. Use the following command to configure RSTP's edge port under port configuration mode:

Command	Purpose
spanning-tree rstp edge	Configuring port as edge port.

Under automatic detection of protocol mode, if port does not receive BPDU at some time, the port is considered as edge port.

Configuring port's connection type

It the switches which operate RSTP protocol connect with each other by point to point, they could establish topology quickly by handshake mechanism.

Under default condition, the protocol determines whether the port uses point-to-point connection according to port's duplex property. If port works under duplex mode, the protocol would consider its connection is point to point. If port works under half duplex mode, the protocol would consider its connection as shared.

If it is confirmed that the switch connected with port runs on RSTP or MSTP protocol, the port's connection type could be configured as point-to-point to guarantee the processing of quick handshake.

Under port configuration mode, use the following command to configure port's connection type:

Command	Purpose
spanning-tree rstp point-to-point [**force-true** | **force-false** | **auto**]	Configuring point-to-point port. force-true: forcing to point-to-point type. force-false: forcing to none point-to-point type. Auto: protocol automatically detects port's type.

Restarting the check of protocol conversion

RSTP protocol allows switch to cooperatively work with traditional 802.1D STP switch by a protocol conversion mechanism. If switch's one port receives STP's configuration information, this port would change to send STP messages only.

After a port is at STP compatible status, this port would recover to RSTP status even if this port does not receive 802.1D STP BPDU any longer. At the meantime, use command **spanning-tree rstp migration-check** to start port's check of protocol conversion and recover port to RSTP mode.

Use the following command to restart the check of RSTP protocol conversion under global configuration mode:

Command	Purpose
spanning-tree rstp migration-check	Restarting all ports' check process of protocol conversion

Use the following command to do check of port's protocol conversion under switch's port configuration mode:

Command	Purpose
spanning-tree rstp migration-check	Restarting the check of current port's protocol conversion process

Configuring MTSP

MSTP Overview

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.

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.

IST, CST, CIST and MSTI

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

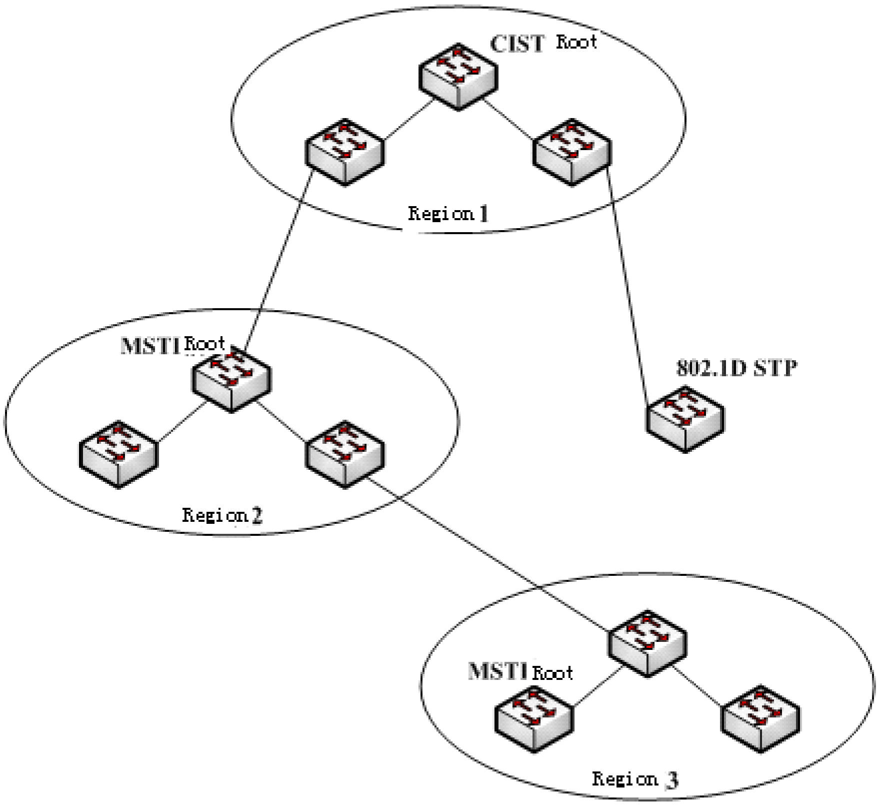


Figure 2.1 MSTP topology

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 selected in each region, which is the shortest path from the heart of the region to CIST root.

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.

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.

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.

Port Role

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

Root port

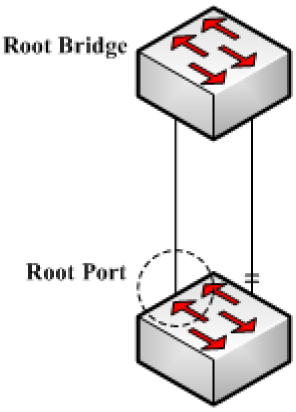


Figure 2.2 Root port

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

Alternate port

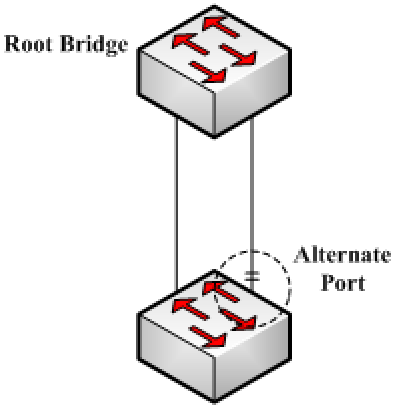


Figure 2.3 Alternate port

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.

Designated port

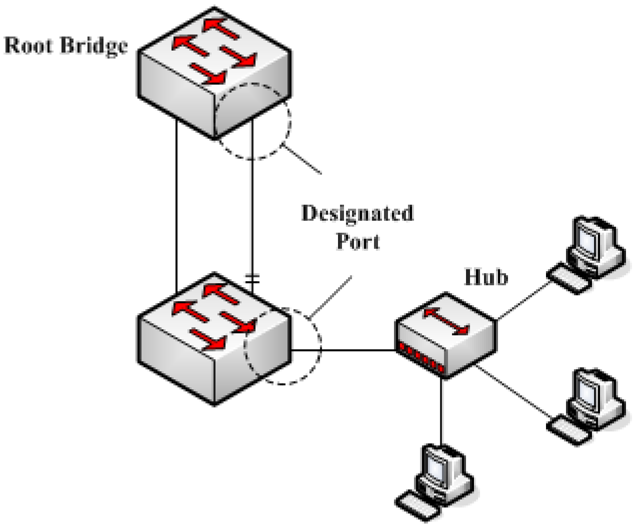


Figure 2.4 Designated port

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

Backup port

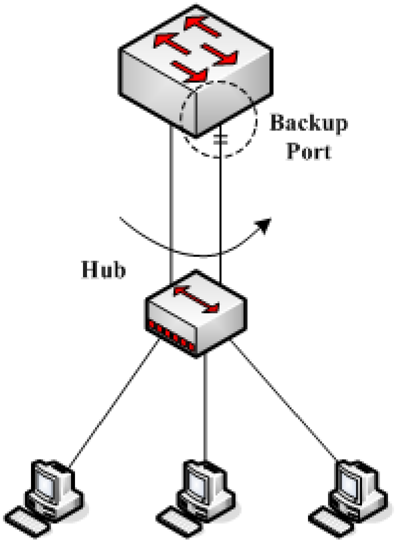


Figure 2.5 Backup port

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 becomes the designated port to continue working.

Master port

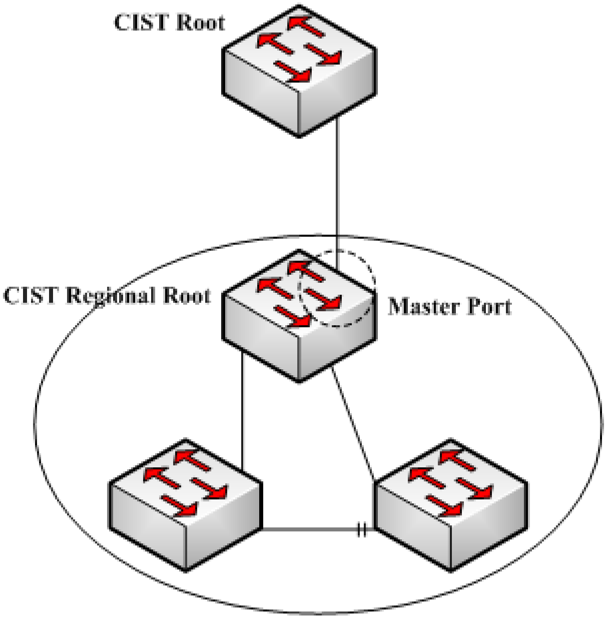


Figure 2.6 Master port

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.

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.

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.

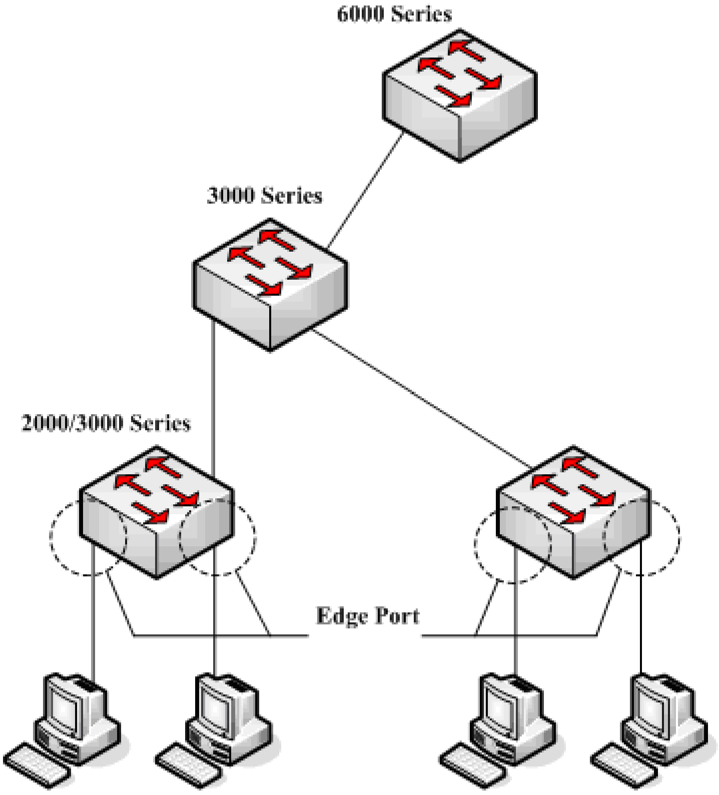


Figure 2.7 Edge port

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.

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

Stable State

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

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

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

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

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

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

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

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

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

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

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

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.

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.

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.

MSTP Configuration Task List

Default MSTP configuration

Enabling and disabling MSTP

Configuring MSTP Area

Configuring Network Root

Configuring Secondary Root

Configuring Bridge Priority

Configuring STP Time Parameters

Configuring Network Diameter

Configuring Maximum Hop Count

Configuring Port Priority

Configuring Path Cost for the Port

Configuring Edge Port

Configuring Port Connection Type

Activating MST-Compatible Mode

Restarting Protocol Conversion Check

Configuring Port’s Role Restriction

Configuring Port’s TCN Restriction

Checking MSTP Information

MSTP Configuration Task

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	1000 Mbps: 20000

MSTI)	100 Mbps: 200000 10 Mbps: 2000000
Hello Time	2 seconds
Forward Delay	15 seconds
Maximum-aging Time	20 seconds
Maximum hop count	20

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.

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.

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.

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.

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.

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

Run the following command to configure the time parameter of the multiple spanning tree protocol:

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.

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.

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.

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.

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.

Configuring Edge Port

Edge port means this port connects with terminal device on network. A mandatory edge port would be at forwarding status instantly after Link Up. Use the following command to configure MSTP's edge port under port configuration mode:

Command	Purpose
spanning-tree mstp edge	Configuring port as edge port
no spanning-tree mstp edge	Recovering the default automatic check edge port

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.

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**.

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.

Configuring Port's Role Restriction

The function of configuring port's role restriction could make the port not be selected as root port.

Use the following command to configure port's role restriction under port configuration mode:

Command	Purpose
spanning-tree mstp restricted-role	Making the port not be selected as root port

Configuring Port's TCN Restriction

The configuration of port's TCN restriction could make port do not spread topology change to other ports.

Use the following command to configure port's TCN restriction under port configuration mode:

Command	Purpose
spanning-tree mstp restricted-tcn	Making port do not spread topology change to other ports.

Checking 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.

17. STP Optional Characteristic ConfigurationConfiguring STP Optional Characteristic

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

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. If Port Fast is configured on a Port connected to a switch, it is possible to create a loop.

The Port Fast feature can be set in either global or Port configuration mode. If configured in global mode, all ports will be considered as Port Fast ports and will quickly enter the Forwarding state. It's also easier to create loops. To prevent network loops from being created by configuring the Port Fast function, you can use the BPDU Guard or BPDU Filter features to protect the ports.

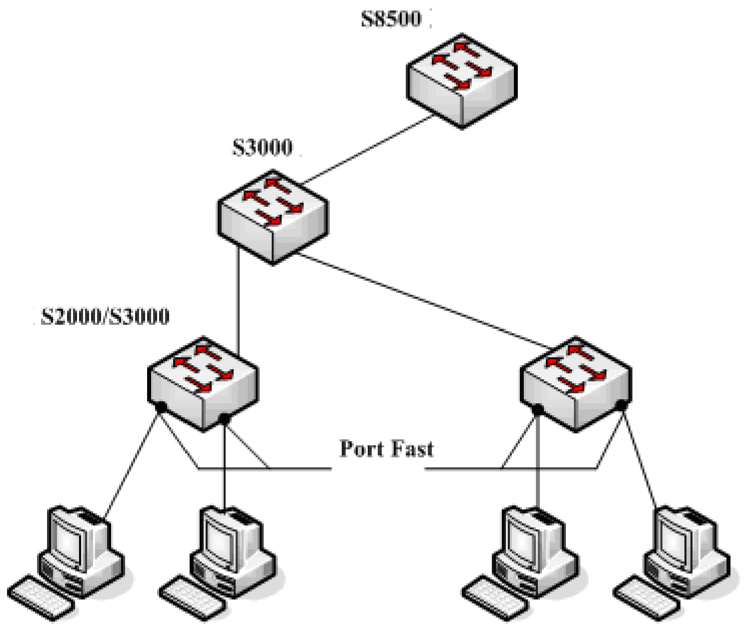


Figure 1.1 Port Fast

Note:

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.

BPDU Guard

If a Port Fast-enabled port receives a BPDU, it can be attributed to a bad network configuration. The BPDU Guard feature passively protects the port after it receives a BPDU.

BPDU Guard behaves differently under different spanning tree protocols. In SSTP/PVST mode, a Port Fast-enabled port that is also configured with the BPDU Guard is forced to shutdown once receiving the BPDU, after which the user can only manually configure it to recover. In RSTP/MSTP mode, a normal port configured with BPDU Guard will be set to a Blocking state for a period of time if it receives a BPDU.

The BPDU Guard feature can be configured independently without Port Fast. In all spanning tree protocol modes, a port configured with the BPDU Guard feature will still send the BPDU, and also receive and process the BPDU. In RSTP/MSTP mode, configuring the BPDU Guard on the port can prevent these devices connected to the switch from receiving BPDU.

The BPDU Guard feature can be configured in global or port mode. In global mode, using the **spanning tree portfast bpduguard** command will not prevent a port from sending BPDU. It is important to note that in a more complex network, improper use of the BPDU Guard function can result in loops.

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 configuration mode, run the command **spanning-tree portfast bpdufilter** to block all ports to send BPDU out. The port, however, can still receive and process BPDU.

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 multiple layers 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.

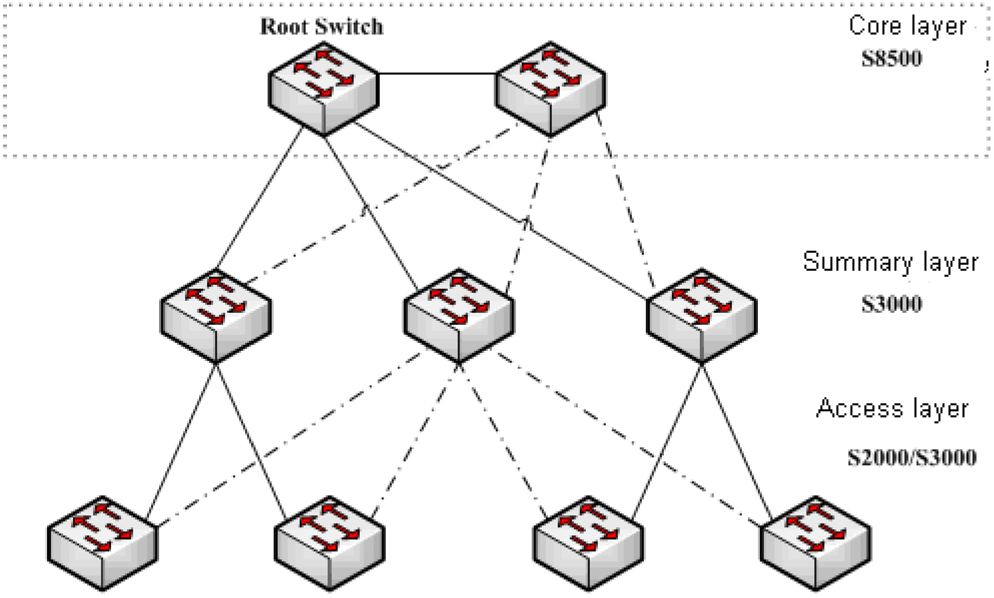


Figure 1.2 Switching network topology

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 starts forwarding.

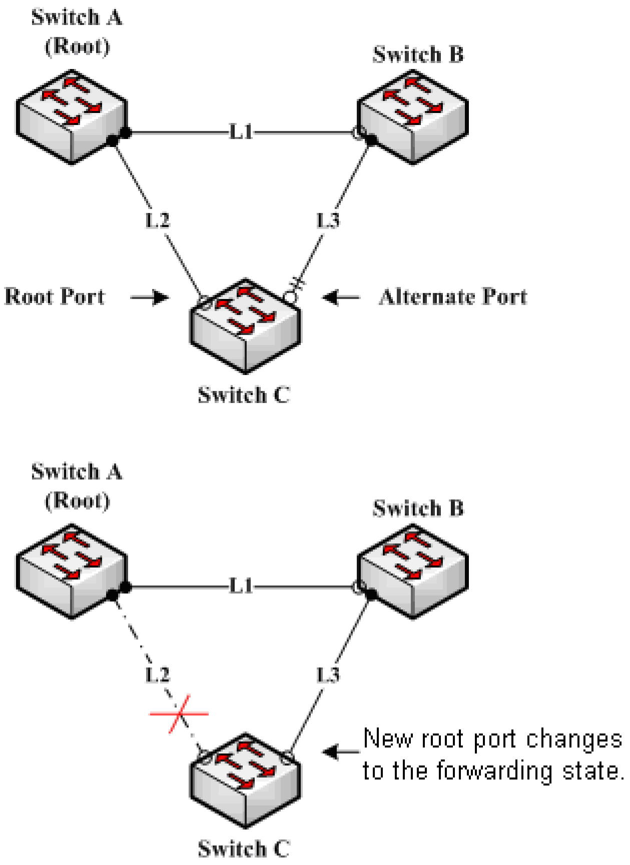


Figure 1.3 Uplink Fast

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.

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.

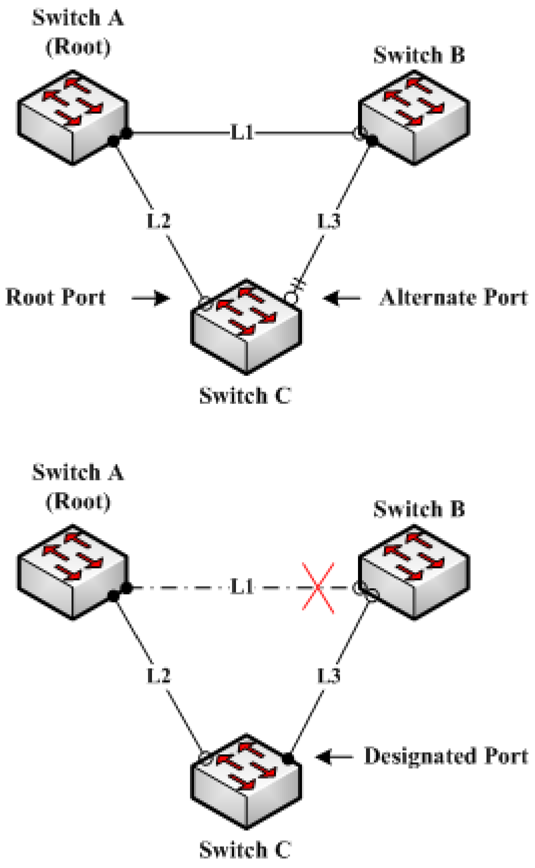


Figure 1.4 Backbone Fast

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.

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.

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.

Configuring STP Optional Characteristic

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

Configuring loop Fast

Configuring Address Table Aging Protection

Configuring FDB-Flush

Configuring BPDU Terminal

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. This function is not valid in other spanning tree modes.

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.

Configuring BPDU Guard

The BPDU Guard feature passively protects the port after it receives a BPDU, and the port still send BPDU.

BPDU Guard behaves differently under different spanning tree protocols. In SSTP/PVST mode, a Port Fast-enabled port that is also configured with the BPDU Guard is forced to shut down once receiving the BPDU, after which the user can only manually configure it to recover. In RSTP/MSTP mode, a normal port configured with BPDU Guard will be set to a Blocking state for a period of time if it receives a BPDU.

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	Disables bpdu guard feature on the interface. It has no effect on the global configuration.

Configuring BPDU Filter

You should enable BPDU filtering in SSTP/PVST mode so that the interface do not send BPDUs, which is also another protection method for the Port Fast port.

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.

Configuring Uplink Fast

The Uplink Fast feature enables the new root port to quickly enter the Forwarding state when the connection between the switch and the network root bridge is interrupted.

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.

Configuring Backbone Fast

Backbone Fast feature is complementary to Uplink Fast technology. Uplink Fast enables redundant lines to start working quickly when the direct connection to the designated switch is interrupted. Backbone Fast can detect non-directly-connected network interruptions in the upper-layer network and speed up port status changes

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.

Configuring Root Guard

Root Guard feature can prevent a port with a high-priority BPDU from becoming a Root port.

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.

Configuring Loop Guard

The Loop Guard feature protects a Root Port or Alternate Port after it becomes a Designated Port. It prevents the port from loops caused by not receiving BPDUs.

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.

Configuring Loop Fast

Notice:
Please use this chapter’s configuration command under the technical engineer’s instruction.

Loop Fast feature is applied to improve network's convergence performance limitedly under special network environment. For example, this feature is enabled on every port which composes the ring network which is made up of dozens of switches.

Use the following command to configure Loop Fast on all ports under global configuration mode:

Command	Purpose
spanning-tree loopfast	Enabling Loop Fast feature for all ports under global configuration mode
no spanning-tree loopfast	Shutting down Loop Fast under global configuration mode

Use the following commands to configure Loop Fast under port configuration mode:

Command	Purpose
spanning-tree loopfast	Enabling port's Loop Fast Feature
no spanning-tree loopfast	Cancelling all port's Loop Fast Configuration. If configuring global Loop Fast, the feature is still valid on ports.
spanning-tree loopfast disable	Disabling port's Loop Fast

Configuring Address Table Aging Protection

Under the condition of network topology's frequent change, configuring address table aging protection could avoid communication impacted because spanning tree protocol updates MAC address table frequently.

Spanning tree protocol with Fast convergence, like RSTP and MSTP, when detects the change of spanning tree's topology, would do elimination operation on switch's MAC address table, which is deleting old MAC address and accelerating MAC address's update to guarantee the communication could recover rapidly. Under default configuration, XXCOM switch finishes elimination operation by the way of MAC address table's fast aging. For most models of switches, address table's fast aging could finish in one second and have rare effect on CPU's function.

After address table's aging protection function is enabled, STP protocol would initiate timer protection after the first aging. Before timer is overtime (default is 15 seconds), aging would not be processed. If network topology changes within 15 seconds, the protocol would operate the second aging after timer is overtime.

Notice:
STP protocol executive address's aging could be disabled completely by the command **no spanning-tree fast-aging.** Before operating this configuration, please confirm network does not have loop. Otherwise, after network topology changes, terminal devices might need 5 minutes or longer time to regain communication with each other.

Use the following commands to configure address table's aging protection function under global configuration mode:

Command	Purpose
spanning-tree fast-aging	Enabling/disabling address table's aging function.
spanning-tree fast-aging protection	Enabling/disabling address table's aging protection function.
spanning-tree fast-aging protection time	Configuring address table's aging protection time. Within the time, spanning tree can only execute one time of address table's aging. The default is 15 seconds.

Adding no on the above commands can disable the relative configuration.

Configuring FDB-Flush

Notice:
Please use this chapter's configuration command under XXCOM technical engineer's instruction.

XXCOM Switch's rapid spanning tree protocol (RSTP and MSTP) eliminates old MAC address by using the address table's fast aging method not FDB-Flush way under default configuration.

Use the following commands to configure FDB-Flush under global configuration mode:

Command	Purpose
spanning-tree fast-aging flush-fdb	Enabling FDB-Flush
no spanning-tree fast-aging flush-fdb	Disabling FDB-Flush

To be noticed is that FDB-Flush is independent with fast aging function. FDB-Flush could be configured when configuring **no spanning-tree fast-aging.** But fast aging protection function is not valid for FDB-Flush.

Configuring BPDU Terminal

By default, XXCOM's switch will forward the BPDU received when no spanning tree is running. The BPDU Terminal function can disable the forwarding of BPDU when no spanning tree is running.

Use the following commands to configure BPDU Terminal under global configuration mode:

Command	Purpose
spanning-tree bpdu-terminal	Enabling BPDU Terminal.
no spanning-tree bpdu-terminal	Disabling BPDU Terminal.

18. Layer-2 Link Aggregation

Configuration Configuring Port Aggregation

The port aggregation configuration task in this chapter describes how to configure port aggregation for the switch.

Overview

Port aggregation means that several physical ports with the same attributes are bound together to form a logical channel. The port aggregation method can be to statically aggregate several physical ports together regardless of whether the ports connected to these physical ports meet the conditions for aggregation. When using LACP for aggregation, after the port aggregation negotiate with the port and the opposite port, the port can be aggregated into a logical channel.

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
  - 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.

Port Aggregation Configuration Task List

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

Port Aggregation Configuration Task

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.

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.

With the LACP protocol, port aggregation must be performed after the peer connected to the port and the port have been negotiated through. 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 provides two aggregation methods, one is Active and the other is Passive. In Active mode, the switch actively initiates the aggregation negotiation process, while In Passive mode, The switch passively accepts the aggregation negotiation process. 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	Description
aggregator-group *agg-id* **mode** { **lacp** | **static** }	Configures aggregation option of the physical port.

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	Description
aggregator-group load-balance	Configures load balance method.

Monitoring the Concrete Conditions of Port Aggregation

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

Command	Description
show aggregator-group [id] {detail|brief|summary}	Displays port aggregation state.

19. LLDP Configuration LLDP Overview

LLDP Overview

The link layer discovery protocol (LLDP) at 802.1AB helps to detect network troubles easily and maintain the network topology. L It enables neighboring devices to send notifications of their status information to other devices, and each port of all devices stores its own defined information. If necessary, it can also send updated information to neighboring devices directly connected to them. The device will store the information in standard SNMP MIBs. The network management system can query the current connection status of the second layer from the MIB. LLDP does not configure or control network elements or traffic, it just reports the configuration of the second layer.

Simply, LLDP is a neighbor discovery protocol. It sets a standard method for the Ethernet network device, such as switches, routers and WAPs. It enables the Ethernet device notify its existence to other nodes and save the discovery information of neighboring devices. For instance, all information including the device configuration and the device identification can be notified through the protocol. Specifically, LLDP defines a universal notification information set, a transmission notification protocol and a method of storing all notification information. The device need to notify the notification information can transmit many notifications in a LAN data packet. The transmission type is TLV.

TLV has three compulsory types: Chassis ID TLV, Port ID TLV and Time To Live TLV; five optional types: Port Description, System Name, System Description, System Capabilities and Management Address; and three extension TLVs: DOT1 (Port Vlan ID, Protocol Vlan ID, Vlan Name, Protocol Identity); DOT3 (MAC/PHY Configuration/Status, Power Via MDI, Link Aggregation, Max Frame Size); MED (MED Capability, Network Policy, Location Identification, Extended Power-via-MDI, Inventory (Hardware Revision, Firmware Revision, Software Revision, Serial Number, Manufacturer Name, Mode Name, Assert ID).

LLDP is a unidirectional protocol. One LLDP agent transmits its state information and functions through its connected MSAP, or receives the current state information or function information about the neighbor. However, the LLDP agent cannot request any information from the peer through the protocol. During message exchange, message transmission and reception do not affect each other. You can configure only message transmission or reception or both.

Initializing the Protocol

LLDP can work under three modes: transmit-only, receive-only and transmit-and-receive. The default mode is transmit-and-receive.

Initializing LLDP Transmit Mode

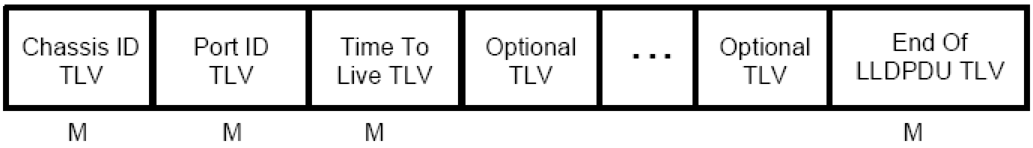
Set LLDP to **transmit-only** in the interface mode. In transmit-only mode, the interface transmits LLDP packets when the state or value of one or more information elements (management object) of the local system change or the transmission timer is timeout. The interface will not transmit LLDP packets when disabling the function.

Initializing LLDP Receive Mode

Set LLDP to **receive-only** in the interface mode. In **receive-only** mode, the interface can receive LLDP packets from the neighbors and save tlv into the remote MIB. The interface will drop LLDP packets when disabling the function.

LLDP PDU Packet Structure Description

In accordance with the order, LLDP PDU includes three compulsory TLVs in the front, one or more optional TLV in the middle and LLDPUD TLV in the end. As shown in figure 1:



M must include TLV.

Figure 1 LLDP PDU Format

Three compulsory TLVs should be listed in sequence at the beginning of LLDP PDU:

Chassis ID TLV

Port ID TLV

Time To Live TLV

Optional TLV selected by the network management can be listed randomly.

Port Description

System Name

System Description

System Capabilities

Management Address

Three extensions (including DOT1):

Port Vlan ID

Protocol Vlan ID

Vlan Name

Protocol Identity

DOT3:

MAC/PHY Configuration/Status

Power Via MDI

Link Aggregation

Max Frame Size

MED (TLV of MED is not transmitted by default. LLDP packets with MED TLV will be transmitted only when LLDP packets with MED TLV are received.)

MED Capability (TLV is compulsory if MED TLV is added.)

Network Policy

Location Identification

Extended Power-via-MDI

Inventory (including Hardware Revision, Firmware Revision, Software Revision, Serial Number, Manufacturer Name, Mode Name or Assert ID)

The end TLV should be the last one in LLDP PDU.

LLDP Configuration Task List

Disabling/enabling LLDP

Configuring Holdtime

Configuring Timer

Configuring Reinit

Configuring the To-Be-Sent TLV

Configuring the Transmission or Reception Mode

Specifying the Management IP Address of a Port

Sending Trap Notification to mib Database

Configuring Show-Relative Commands

Configuring the Deletion Commands

LLDP Configuration Tasks

Disabling/enabling LLDP

When the LLDP is enabled, the local port periodically sends the LLDP frame out to inform the opposite end about the information of the local.

Run the following command in global configuration mode to enable LLDP:

Step	Command	Purpose
Step 1	config	Enters the global configuration mode.
Step 2	lldp run	Enables LLDP

Run the following command to disable LLDP:

Step	Command	Purpose
Step 1	config	Enters the global configuration mode.
Step 2	no lldp run	Disables LLDP

Note:

Only when the LLDP function is enabled can the received LLDP message be processed, otherwise the LLDP frame will be forwarded directly.

Configuring Holdtime

Normally, the remote information stored in the MIB will be updated before aging. But the information in the MIB will also be aging because the update frame may be lost in the process of sending. To prevent this, you can set the TTL value so that update LLDP frames are sent multiple times during the aging time. You can control the timeout time of transmitting the LLDP message through modifying **holdtime**:

Run the following command in global configuration mode to configure **holdtime** of LLDP:

Step	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	lldp holdtime time	Configures the timeout time of LLDP. Range from: 0 to 65535, default 120s.

Run the following command to resume the timeout time to default:

Step	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	no lldp holdtime	Resumes the default timeout time, that is, 120 seconds.

Note:

To ensure the former neighbor information is not lost owing to aging when receiving next LLDP frame, the timeout time should be longer than the LLDP packet transmit interval.

Configuring Timer

You can control the interval of the switch to transmit message by configuring the timer of LLDP.

Run the following command in global configuration mode to configure **timer** of LLDP:

Step	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	lldp timer time	Configures the interval of message transmission of LLDP. The value ranges from 5 to 65534. The default time is 30 seconds.

Run the following command to resume the default interval:

Step	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	no lldp timer	Resumes the default interval, that is, 30 seconds.

Configuring Reinit

LLDP information is automatically sent when the status or value of one or more information elements (managed objects) in the local system changes and the transmission timer expires. Since a single information change requires the transmission of LLDP frames, a continuous series of information changes may trigger the transmission of many LLDP frames. Because only one change is reported in each frame. To avoid this situation, network management defines waiting time between two consecutive transmissions of LLDP frames. You can control the interval of the switch to continuously transmit two messages by configuring reinit of LLDP.

Run the following command in global configuration mode to configure reinit of LLDP:

Step	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	lldp reinit time	Resumes the default interval of continuously transmitting message. The value ranges from 2 to 5. The default interval value is two seconds.

Run the following command to resume the default reinit:

Step	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	no lldp reinit	Resumes the default interval of continuously transmit message, that is, 2 seconds.

Configuring the To-Be-Sent TLV

You can choose TLV which requires to be sent by configuring tlv-select of LLDP. By default, all TLVs are transmitted.

Run the following commands in global configuration mode to add or delete tlv of LLDP:

Step	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	lldp tlv-select management-address	Optional. Transmits the management address tlv. The management address is usually layer-3 IP address which should be easy to use.
Step3	lldp tlv-select port-description	Optional. Transmits the port description tlv. The port description uses number or letters for description.
Step4	lldp tlv-select system-capabilities	Optional. Transmits the system performance tlv. The system performance refers to the system of

		transmitting packets such as the switch or router.
Step5	lldp tlv-select system-description	Optional. Transmits system description tlv. The system description is consist of texts including numbers and letters. The system description should include the full name of the system, the hardware version, the software system and the network software.
Step6	lldp tlv-select system-name	Optional. Transmits system name tlv. The name of the system should be the name of the system manager, i.e. the name of the switch.

Run the following command to delete the to be transmitted tlv in the global configuration mode:

Step	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	no lldp tlv-select management-address	Optional. Transmits the management address tlv. The management address is usually layer-3 IP address which should be easy to use.
Step3	no lldp tlv-select port-description	Optional. Transmits the port description tlv. The port description uses number or letters for description.
Step4	no lldp tlv-select system-capabilities	Optional. Transmits the system performance tlv. The system performance refers to the system of transmitting packets such as the switch or router.
Step5	no lldp tlv-select system-description	Optional. Transmits the port description tlv. The port description uses number or letters for description.
Step6	no lldp tlv-select system-name	Optional. Transmits system name tlv. The name of the system should be the name of the system manager, i.e. the name of the switch.

Specifying the Port's Configuration and Selecting the To-Be-Sent Expanded TLV

Through the configuration of dot1-tlv-select/ dot3-tlv-select/ med-tlv-select of LLDP on a port, you can select expanded TLV to be sent. By default, TLV of both DOT1 and DOT3 will be transmitted while TLV of MED will not be transmitted.

Run the following commands in port configuration mode to add the to-be-sent TLV:

Step	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	interface intf-type intf-id	Enters the interface configuration mode.
Step3	lldp dot1-tlv-select port-vlan-id	Optional. Sends the 802.1-defined TLV and notifies the PVID of a port.

Step4	lldp dot1-tlv-select protocol-vlan-id	Optional. Sends the 802.1-defined TLV and notifies the PPVID of a port.
Step5	lldp dot1-tlv-select vlan-name	Optional. Sends the 802.1-defined TLV and notifies the VLAN name of a port.
Step6	Lldp dot3-tlv-select macphy-confg	Optional. Sends the 802.3-defined TLV: a) The bit rate and the communication mode (duplex) on the physical layer; b) Current duplex and the set bit rate; c) Showing whether the setting is the results of auto-negotiation in the initial connection phase or is a compulsory manual behavior;
Step7	lldp dot3-tlv-select power	Optional. Sends the 802.3-defined TLV and shows the interface allows the power supply connecting to the non-power system through the link.
Step8	lldp dot3-tlv-select link-aggregation	Optional. Sends the 802.3-defined TLV and specifies a port to identify the aggregation if the link can be aggregated.
Step9	lldp dot3-tlv-select max-frame-size	Optional. Sends the 802.3-defined TLV and specifies the size of the maximum frame on a port.
Step10	lldp med-tlv-select network-policy	Optional. Sends the MED-defined TLV and the interface can effectively discover and diagnose VLAN configured error-matching flow and the attribute of layer-2 and layer-3.
Step11	lldp med-tlv-select location	Optional. Sends the MED-defined TLV and specifies the address: a) coordinate-based LCI, which is defined in IETF 3825[6]; b) city's address LCI, which is defined in IETF (refer to Annex B); c) ELIN code of the urgency call service;
Step12	lldp med-tlv-select power-management	Optional. Sends the MED-defined TLV and shows the information of power supply.
Step13	lldp med-tlv-select inventory	Optional. Sends the MED-defined TLV and shows the attribute of detailed inventory.
Step14	lldp dot1-tlv-select protocol-identity	Optional. Sends the 802.1-defined TLV and notifies the Protocol-identity of a port.

Run the following commands in global configuration mode to delete to-be-sent TLV:

Step	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	interface intf-type intf-id	Enters the interface configuration mode.

Step3	no lldp dot1-tlv-select port-vlan-id	Optional. Sends the 802.1-defined TLV and notifies the PVID of a port.
Step4	no lldp dot1-tlv-select protocol-vlan-id	Optional. Sends the 802.1-defined TLV and notifies the PPVID of a port.
Step5	no lldp dot1-tlv-select vlan-name	Optional. Sends the 802.1-defined TLV and notifies the vlan name of a port.
Step6	no lldp dot3-tlv-select macphy-confg	Optional. Sends the 802.3-defined TLV: a) The bit rate and the communication mode (duplex) on the physical layer; b) Current duplex and the set bit rate; c) Showing whether the setting is the results of auto-negotiation in the initial connection phase or is a compulsory manual behavior;
Step7	no lldp dot3-tlv-select power	Optional. Sends the 802.3-defined TLV and shows the interface allows the power supply connecting to the non-power system through the link.
Step8	No lldp dot3-tlv-select link-aggregation	Optional. Sends the 802.3-defined TLV and specifies a port to identify the aggregation if the link can be aggregated.
Step9	no lldp dot3-tlv-select max-frame-size	Optional. Sends the 802.3-defined TLV and specifies the size of the maximum frame on a port.
Step10	no lldp med-tlv-select network-policy	Optional. Sends the MED-defined TLV and the interface can effectively discover and diagnose VLAN configured error-matching flow and the attribute of layer-2 and layer-3.
Step11	no lldp med-tlv-select location	Optional. Sends the MED-defined TLV and specifies the address: a) coordinate-based LCI, which is defined in IETF 3825[6]; b) city's address LCI, which is defined in IETF (refer to Annex B); c) ELIN code of the urgency call service;
Step12	no lldp med-tlv-select power-management	Optional. Sends the MED-defined TLV and shows the information of power supply.
Step13	no lldp med-tlv-select inventory	Optional. Sends the MED-defined TLV and shows the attribute of detailed inventory.
Step14	no lldp dot1-tlv-select protocol-identity	Optional. Sends the 802.1-defined TLV and cancel to notify the Protocol-identity of a port.

Configuring the Transmission or Reception Mode

LLDP can work under three modes: transmit-only, receive-only and transmit-and-receive.

By default, LLDP works under the transmit-and-receive mode. You can modify the working mode of LLDP through the following commands.

Step	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	interface intf-type intf-id	Enters the interface configuration mode.
Step3	no lldp transmit	Disables the transmit-only mode of the port.
Step4	no lldp receive	Disables the receive-only mode of the port.

Run the following commands in the interface configuration mode and set lldp to the transmit-and-receive mode.

Step	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	interface intf-type intf-id	Enters the interface configuration mode.
Step3	lldp transmit	Enables the transmit mode of the port.
Step4	lldp receive	Enables the receive mode of the port.

Note: Except the above mode, the interface can also be configured to the transmit-only mode or the receive-only mode.

Specifying the Management IP Address of a Port

In port configuration state, you can randomly configure the management address of the port, from which the LLDP packets are transmitted. This management address should be an IP address related with this port, and only in this way the normal communication of this port can be guaranteed.

Run the following commands in port configuration mode to set the management IP address:

Step	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	interface intf-type intf-id	Enters the interface configuration mode.
Step3	lldp management-ip A.B.C.D	Sets the management IP address of a port.

Note: Both the no lldp management-ip command can be used to resume the default management address of the port and the default management address is the IP address of the VLAN interface that corresponds to the PVID port. When the corresponding VLAN interface does not exist, the management address is 0.0.0.0.

Sending Trap Notification to mib Database

Run the following commands in the global configuration mode to sending trap notification to lldp mib database or ptopo mib database.

Step	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	lldp trap-send lldp-mib	Sends trap notification to lldp mib database.
Step3	lldp trap-send ptopo-mib	Sends trap notification to ptopo mib database.

Note: Both the no lldp command and the management-ip command can be used to resume the default management address of the port and the default management address is the IP address of the VLAN interface that corresponds to the PVID port. When the corresponding VLAN interface does not exist, the management address is 0.0.0.0.

Configuring the Location Information

The location configuration is used to determine the address of the local machine.

Run the following commands in global configuration mode to configure the location information:

Step	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	location elin identifier id WORD	Sets the location elin information, in which id is the elin identifier number and WORD stands for the elin information, which ranges from 10 to 25 bytes.
Step3	location civic identifier id	Enters the location configuration mode.
Step4	language WORD	Sets the language
Step5	state WORD	Sets the state's (provincial) name, such as shanghai.
Step6	county WORD	Sets the name of a county.
Step7	city WORD	Sets the name of a city.
Step8	division WORD	Sets the name of a division.
Step9	neighborhood WORD	Sets the name of neighborhood.
Step10	street WORD	Sets the name of a street.
Step11	leading-street-dir WORD	Sets the direction of a main street, such as N (north).
Step12	trailing-street-suffix WORD	Sets the suffix of a small street, such as SW.
Step13	street-suffix WORD	Sets the suffix of a street, such as platz.
Step14	number WORD	Sets the street number, such as number 123.

Step15	street-number-suffix WORD	Sets the suffix of the street number, such as number 1/2 of A road.
Step16	landmark WORD	Sets the landmark, such as Colombia University.
Step17	additional-location WORD	Sets the additional location.
Step18	name WORD	Sets the information about a resident, such as Joe’s haircut shop.
Step19	postal-code WORD	Sets the postal code.
Step20	building WORD	Sets the information about a building.
Step21	unit WORD	Sets the information about a unit.
Step22	floor WORD	Sets the information about a floor.
Step23	room WORD	Sets the information about a room.
Step24	type-of-place WORD	Sets the type of a place, such as office.
Step25	postal-community WORD	Sets the name of a postal office.
Step26	post-office-box WORD	Sets the name of a postal box, such as 12345.
Step27	additional-code WORD	Sets the additional code.
Step28	country WORD	Sets the name of a country.
Step29	script WORD	Sets the script.

Run the following commands in global configuration mode to delete the location information:

Step	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	no location elin identifier id	Deletes the location enlin information of elin identifier.
Step3	no location civic identifier id	Deletes the location enlin information of id, which is the number of civic identifier.
Step4	location civic identifier id	Enters the location configuration mode.
Step5	no language	Deletes the language.
Step6	no state	Deletes the state’s (provincial) name, such as shanghai.
Step7	no county	Deletes the name of a county.
Step8	no city	Deletes the name of a city.
Step9	no division	Deletes the name of a division.
Step10	no neighborhood	Deletes the name of neighborhood.
Step11	no street	Deletes the name of a street.
Step12	no leading-street-dir	Deletes the direction of a main street, such as N (north).
Step13	no trailing-street-suffix	Deletes the suffix of a small street, such as SW.

Step14	no street-suffix	Deletes the suffix of a street, such as platz.
Step15	no number	Deletes the street number, such as number 123.
Step16	no street-number-suffix	Deletes the suffix of the street number, such as number 1/2 of A road.
Step17	no landmark	Deletes the landmark, such as Colombia University.
Step18	no additional-location	Deletes the additional location.
Step19	no name	Deletes the information about a resident, such as Joe's haircut shop.
Step20	no postal-code	Deletes the name of a postal office.
Step21	no building	Deletes the information about a building.
Step22	no unit	Deletes the information about a unit.
Step23	no floor	Deletes the information about a floor.
Step24	no room	Deletes the information about a room.
Step25	no type-of-place	Deletes the type of a place, such as office.
Step26	no postal-community	Deletes the name of a postal office.
Step27	no post-office-box	Deletes the name of a postal box, such as 12345.
Step28	no additional-code	Deletes the additional code.
Step29	no country	Deletes the name of a country.
Step30	no script	Deletes the script.

Specifying a Port to Set the Location Information

The following commands can be used to set the location information for a port and bear the location information in TLV.

Run the following commands in port configuration mode to set the location information:

Step	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	interface intf-type intf-id	Enters the interface configuration mode.
Step3	location civic id	Sets the location information of civic id.
Step4	location elin id	Sets the location information of elin id.

Run the following commands in port configuration mode to delete the location information:

Step	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	interface intf-type intf-id	Enters the interface configuration mode.
Step3	no location civic	Deletes the location information of civic id.
Step4	no location elin	Deletes the location information of elin id.

Configuring Show-Relative Commands

You can observe the information about the neighbor, statistics or port state received by the LLDP module by running show-relative commands.

Run the following commands in EXEC or global configuration mode:

Command	Purpose
Show lldp errors	Displays the error information about the LLDP module.
Show lldp interface *interface-name*	Displays the information about port state, that is, the transmission mode and the reception mode.
Show lldp neighbors	Displays the abstract information about the neighbor.
Show lldp neighbors detail	Displays the detailed information about the neighbor.
Show lldp traffic	Displays all received and transmitted statistics information.
Show location elin	Displays the information of location elin.
Show location civic	Displays the information of location civic.

Configuring the Deletion Commands

You can delete the received neighbor lists and all statistics information by running the following command in EXEC mode.

Run the following commands in EXEC mode:

Command	Purpose
clear lldp counters	Deletes all statistics data.
clear lldp table	Deletes all received neighbor information.

Configuration Examples

Network Environment Requirements

Configure LLDP protocol on the port connecting two switches.

Network Topology

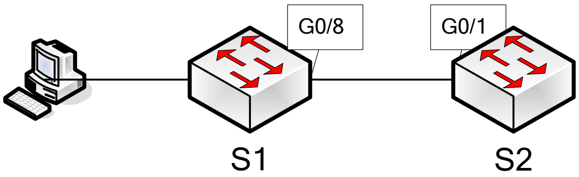


Figure 2 Network Topology

Configuration Steps

Basic Configuration

Configuring switch S1:

```
Switch_config#lldp run
Switch_config#
```

Configuring switch S2:

```
Switch_config#lldp run
Switch_config#
```

The information of Neighbor B will be displayed on Switch A about 1 minute later. MED-TLV information is not sent by default.

S1:

```
Switch_config#show lldp neighbors
Capability Codes:
        (R)Router,(B)Bridge,(C)DOCSIS Cable Device,(T)Telephone
        (W)WLAN Access Point, (P)Repeater,(S)Station,(O)Other

Device-ID         Local-Intf       Hldtme        Port-ID      Capability
Switch            Gig0/8            99             Gig0/1        B

Total entries displayed: 1
Switch_config#show lldp neighbors detail

chassis id: 00e0.0fac.32ff
port id: Gig0/1
port description: GigaEthernet0/1
system name: Switch

system description: SWITCH Software, Version 4.1.0B
Serial: S24090103
Compiled: 2011-9-21 9:24:8 by WRL

Time remaining: 96
system capabilities: R B
enabled capabilities: B
```

```
Management Address:
   IP: 90.0.0.21

Port VLAN ID: 1
PPVID: 1
VLAN 1 name: Default
Auto Negotiation: supported,enabled
Physical media capabilities:
   1000baseX(FD)
   1000baseX(HD)
   100baseTX(FD)
   100baseTX(HD)
Operational MAU type: 2 pair category 5 UTP, full duplex mode(16)

Power Via MDI:
  MDI power support --
    PSE MDI power support: support
    Port class: PSE
    PSE MDI power state: enabled
    PSE pairs selection control ability: can not be controlled
  PSE power pair: signal
  Power Classification: Class 0
Link Aggregation:
        Aggregation capability: capable of being aggregated
        Aggregation status: not currently in aggregation
Maximum frame size: 1500
-----------------------------------------



Total entries displayed: 1
```

TLV Configuration

Configuring Switch S1:

```
Switch_config#lldp run
Switch_config#
```

Configuring Switch S2:

```
Switch_config#lldp run
Switch_config# no lldp tlv-select system-name
Switch_config#int g0/8
Switch_config_g0/8#no lldp dot1-tlv-select port-vlan-id
Switch_config_g0/8#no lldp dot3-tlv-select max-frame-size
Switch_config_g0/8#
```

The information of Neighbor B will be displayed on Switch A about 1 minute later, which is highlighted in red. To differentiate, the information displayed in the basic configuration of 1.4.3.1 is highlighted in blue.

S1:

```
Switch_config#show lldp neighbors
Capability Codes:
        (R)Router,(B)Bridge,(C)DOCSIS Cable Device,(T)Telephone
        (W)WLAN Access Point, (P)Repeater,(S)Station,(O)Other

Device-ID         Local-Intf       Hldtme        Port-ID        Capability
Switch            Gas0/8             92         Gig0/1         R B

Total entries displayed: 1
Switch_config#show lldp neighbors detail

chassis id: 00e0.0fac.32ff
port id: Gig0/1
port description: GigaEthernet0/1
system name: -- not advertised

system description: XXCOM(tm) SWITCH Software, Version 4.1.0B
Serial: S24090103
Copyright by Shanghai Baud Data Communication CO. LTD.
Compiled: 2011-9-21 9:24:8 by WRL

Time remaining: 95
system capabilities: R B
enabled capabilities: B
```

```
Management Address:
   IP: 90.0.0.21

Port VLAN ID -- not advertised
PPVID: 1
VLAN 1 name: Default
Auto Negotiation: supported,enabled
Physical media capabilities:
   1000baseX(FD)
   1000baseX(HD)
   100baseTX(FD)
   100baseTX(HD)
Operational MAU type: 2 pair category 5 UTP, full duplex mode(16)

Power Via MDI:
  MDI power support --
    PSE MDI power support: support
    Port class: PSE
    PSE MDI power state: enabled
    PSE pairs selection control ability: can not be controlled
  PSE power pair: signal
  Power Classification: Class 0
Link Aggregation:
        Aggregation capability: capable of being aggregated
        Aggregation status: not currently in aggregation
-----------------------------------------


Total entries displayed: 1
```

Location Configuration

Configuring switch S1:

```
Switch_config#lldp run
Switch_config#
```

Configuring switch S2:

```
Switch_config#lldp run
Switch_config#location elin identifier 1 1234567890      // Configure elin information
Switch_config#location civic identifier 1                // Enter location configuration mode
Switch_config_civic#language English
Switch_config_civic#city Shanghai
Switch_config_civic#street Curie
Switch_config_civic#script EN              // Above configuring civic information
Switch_config_civic#quit
Switch_config#int g0/8
Switch_config_g0/8#location elin 1             //Specify elin id for the port
Switch_config_g0/8#location civic 1            // Specify civic id for the port
  Switch_config_g0/8#show location elin       //Display elin configuration information
elin information:
   elin 1: 1234567890
total: 1
Switch_config_g0/8#show location civic     // Display civic configuration information
civic address information:
   identifier: 1
   City: Shanghai
   Language: English
   Script: EN
   Street: Curie
------------------------------------
total: 1
Switch_config_g0/8#
```

The information of Neighbor B will be displayed on Switch A about 1 minute later. S1:

```
Switch_config#show lldp neighbors
Capability Codes:
          (R)Router,(B)Bridge,(C)DOCSIS Cable Device,(T)Telephone
          (W)WLAN Access Point, (P)Repeater,(S)Station,(O)Other

Device-ID          Local-Intf         Hldtme           Port-ID         Capability
Switch             Gig0/8               115              Gig0/1            B

Total entries displayed: 1
```

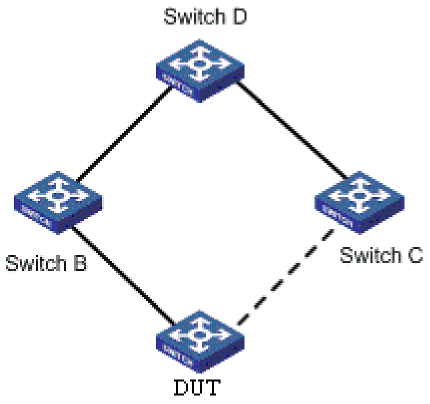
```
Switch_config#show lldp neighbors detail

chassis id: 00e0.0fac.32ff
port id: Gig0/1
port description: GigaEthernet0/1
system name: Switch

system description: SWITCH Software, Version 4.1.0B
Serial: S24090103
Compiled: 2011-9-21 9:24:8 by WRL

Time remaining: 109
system capabilities: R B
enabled capabilities: B
Management Address:
    IP: 90.0.0.21

Port VLAN ID: 1
Auto Negotiation: supported,enabled
Physical media capabilities:
    1000baseX(FD)
    1000baseX(HD)
    100baseTX(FD)
    100baseTX(HD)
Operational MAU type: 2 pair category 5 UTP, full duplex mode(16)

Power Via MDI:
  MDI power support --
     PSE MDI power support: support
     Port class: PSE
     PSE MDI power state: enabled
     PSE pairs selection control ability: can not be controlled
  PSE power pair: signal
  Power Classification: Class 0
MED Information:
    MED Codes:
            (CA)Capabilities, (NP)Network Policy, (LI)Location Identification
            (PS)Power via MDI ¨CPSE, (PD)Power via MDI ¨CPD, (IN)Inventory

    Hardware Revision: 0.4.0
    Software Revision: 4.1.0B
    Serial Number: S24090103
    Manufacturer Name:
    Model Name: SWITCH
    Asset ID: S24090103
    Capabilities: CA,NP,LI,PS,IN
    Device type: Network Connectivity
    Network Policy: Voice
        Policy: Unknown
    Power requirements:
        Type: PSE Device
        Source: Unknown
        Priority: Low
        Value: 150(0.1 Watts)
    Civic address location:
        Language: English
        City: Shanghai
        Street: Curie
        Script: EN
    ELIN location:
        ELIN: 1234567890
------------------------------------------


Total entries displayed: 1
Switch_config#
```

20. BackupLink Configuration

Chapter 1 Introduction of Backup Link

Overview

Dual-uplink networking is a common form of networking. As is shown below, DUT goes upstream to Switch D dually through Switch B and Switch C.



Dual-Uplink Networking

Although the dual-uplink networking can provide link backup, the loops in the network will cause the broadcast storms; therefore, it is necessary to take measures to avoid loops. In general, the loops can be eliminated by STP; but as the STP convergence consumes longer time, more traffic will be lost. So, STP does not apply to networking environment with higher demands for convergence time.

BackupLink provides link backup through a pair of link-layer interfaces while solving the STP problem of slow convergence. In one group of BackupLink ports, one is configured as primary port and the other as the alternate port. These ports can be exchange ports or aggregate ports. In the case that the user does not use STP protocol, BackupLink can ensure the redundancy and backup of link.

BackupLink Port Backup

Configuring Backup Port

For BackupLink, its basic function is to configure another switch port for one switch port as the backup; meanwhile, in two backup ports, only one port is in the forwarding state. Two backup ports can be connected with the same device or different devices.

Note:
1. Two ports which can backup each other may be two physical ports, two aggregate ports or one physical port and one aggregate port;
2. The backup port cannot be configured on the ports which have been configured with link aggregation, port security or EAPS or other network protections;

3. If one port has already been configured with backup, it can no longer become the backup of other ports;
4. The port which has been configured with backup cannot be configured with link aggregation, port security or EAPS or other network protection;
5. On the port which has been configured with BackupLink, the link status detection optimization of the physical layer can be enabled in order to improve the convergence performance.

Status Control of the Port

The ports which are configured with backup function must deleted from STP module; BackupLink is responsible for setting the status of port in all VLANs [1-4094]; these VLANs can belong to different MST (STG).

Port Roles and Status

Configuration commands must be able to specify the default role for two ports which backup each other: Active and Backup.

Note:
1. In the initial case, if the link status of Active and Backup ports is Linkup, the Active port is in the forwarding state, the Backup port is in the blocking state;
2. In the initial case, if one port is in the link status of Linkdown, the other port enters the forwarding state regardless of whether it is the Active role;
3. At one moment, the Backup port is in the forwarding state, the Active port is in the blocking state; if the backup port configuration is repeated on the port, it is necessary to force the Backup port to be in the blocking state and recover the forwarding status of Active port.

Link Status Change Processing

In basic port backup functions, link status changes processing must meet the following requirements:

If the Active port is in the state of Linkdown and the Backup port is in the state of Linkdown, the link breaks, which is unable to forward the data frame;

If the Active port is in the state of Linkdown and the Backup port is in the state of Linkup but not in the forwarding state, the Backup port enters the forwarding state;

If the Active port is in the state of Linkup and the Backup port is in the link status of Linkdown, the Active port enters the forwarding state;

If the Active port is in the state of Linkup and the Backup port is in the state of Linkup and in the forwarding state, the Active port is still in blocking state and the data frame is forwarded from the Backup port without enabling the preemption mode.

If the Active port is in the state of Linkup and the Backup port is in the state of Linkup and in the forwarding state, the forwarded port and blocked port will be decided according to different strategies in the case of enabling the preemption mode. See 1.2.5.

Pre-emption of Backup Port

BackupLink needs to support port preemption: A and B are a pair of backup ports; Port A is in the forwarding state, Port B recovers from LinkDown state and is in blocking state; if Port B meets the conditions of preemption, Port B enters the forwarding state instead of Port A.

The port preemption must be enabled through the command; by default, the preemption is disabled.

Port preemption must be configured independently for each pair of backup ports; different backup port groups can use different preemptive modes:

Preemption based on port role. Preemption is based on the roles specified at the time of configuring backup ports; if the Backup port in the forwarding state and the Active port is in the link status of UP, the Backup port is blocked and the Active port is set as the forwarding state.

Preemption based on port bandwidth. Backup ports must support the preemption of the forwarding state based on the bandwidth; the port with small bandwidth is always blocked.

Note:
The preemption configuration on the same group of backup ports must meet the following requirements:
1. The preemption function takes effect after it is configured on any port in the backup group; but if this configuration is deleted, the function is invalid;
2. The preemption function can be configured on two ports in the backup group, but the preemption mode and delay parameters must be consistent;
3. Two ports which are inconsistent in the preemption parameters cannot be configured as the backup ports.

Delay Preemption

For port preemption, the delay-time preemption is required: If Port B can preempt the forwarding state of Port A, the preemption is completed after the delay-time.

The delay-time preemption must be configured through the command; "0" needs to be taken as the legitimate delay-time preemption, indicating immediate preemption.

VLAN Load Balancing

BackupLink VLAN load balancing enables two ports on the BackupLink port group to simultaneously forward traffic for different VLANs. For example, the BackupLink port group is configured with the forwarding traffic of VLAN 1 ~ 100, where one port forwards the traffic of VLAN1 ~ VLAN50 while the other port forwards the traffic of VLAN51 ~ VLAN100. If one port is in the state of Linkdown, then the other port will forward all the traffic.

Configuration of Load balancing

VLAN load balancing is only configured on the backup port; the user specifies a set of VLAN through the command, and the backup port has the priority to enter the forwarding state in this VLAN group. Therefore, VLAN traffic sharing takes effect only after the backup function is configured on the port.

Note:
For different BackupLink groups, the same group VLAN can be configured, or they have overlapping VLAN segments. But for the overlapping VLAN segments, the system will assign them to different MSTs (STG); therefore, when the port of some group is operated, its states in all MSTs (STG) will take change. So, typically, when the load balancing VLAN group is configured, it is better to select the VLAN group without overlapping.

Port status Control in Traffic Sharing

Create the new MST (STG) for the designated VLAN

In order to achieve the differentiated setting of port status in different VLANs, it is necessary to assign the VLAN specified by the user in the traffic sharing command to a new MST (STG).

BackupLink must check the user-specified VLAN through the interface provided by L2 module; if the specified VLAN has already been used by other protocol modules (for example, in MSTP, it is assigned to some MST, or it is configured as control VLAN of EAPS), this VLAN can no longer be used as VLAN traffic sharing. Such case needs to be handled as the user configuration error.

The same VLAN is used by multiple backup port groups.

BackupLink must be able to handle the case that different backup port groups are configured with the same VLAN. For example: P1 and P2 are mutually backuped, and the VLAN v traffic sharing is configured on P2; P3 and P4 are mutually backuped, and VLAN v is configured on P4. At this time:

1. In the process of loading the configuration, only need to make a distribution operation of the MST in the VLAN v;

2. After the VLAN v traffic sharing is deleted from all the backup port groups, VLAN v needs to be restored to the default MST.

Refresh port status after MST is created

The modification of the MST of VLAN may cause incorrect status of some ports in the system STG table; at this time:

1. L2 is responsible for notifying the protocol module except BackupLink of refreshing port status setting;

2. For each set of backup ports in BackupLink module, the module actively refreshes their status in all VLANs.

Port status setting

After configuring the VLAN traffic sharing, the status setting of backup ports must comply with the following rules:

1. If two ports which are mutually backuped are in the link status of DOWN, their status in all VLANs [1-4094] is set as Blocking;

2. If only one of two ports is in the state of UP, the status of this port in all VLANs is set as Forwarding;

3. If two ports are both in the state of UP, the port which is selected as Active role is set as the Blocking state in traffic sharing VLAN and the Forwarding state in other VLANs; the port which is selected as Backup role is set as the Forwarding state in traffic sharing VLAN and the Blocking state in other VLANs.

MAC Address Aging Operation

BackupLink must support the topology change notifications for the uplink to deal with the case that loops exist in the uplink network, as is shown below:

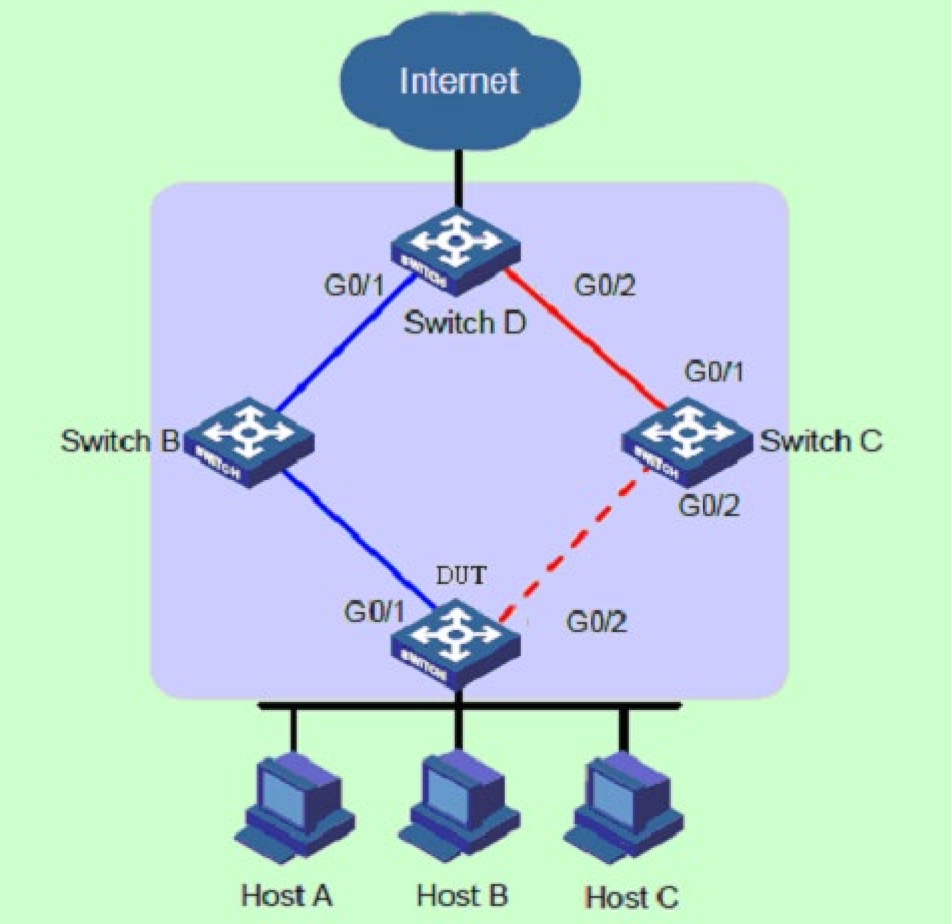


Diagram of BackupLink Address Aging Mechanism

Normal Work Mechanism of the Link

As is shown above, DUT port “GigaEthernet0/1” is the primary; Port “GigaEthernet0/2” is a backup port. When dual uplinks are in normal work condition, the primary port is in the forwarding state and its link is the primary link; the secondary port is blocked and its link is the secondary link. The data are transmitted along the link represented by blue line; no loop exists in the network to avoid broadcast storm.

Downlink Fault Handling Mechanism

When the DUT's primary link fails, the primary port “GigaEthernet0/1” is switched to the standby state, the secondary port “GigaEthernet0/2” is switched to the forwarding state. At this time, MAC address forwarding table entries and ARP table entries on the devices in the network may have been wrong, so it is necessary to provide a mechanism for MAC and ARP updating to complete the quick switch of traffic, avoiding traffic loss. Currently, there are two kinds of updating mechanism:

Notify the device of updating table entries through the link updating packet MMU.

In this way, the upstream device (such as Switch D, Switch B and Switch C (optional) in the above figure) can support the MMU function of BackupLink and identify the situation of MMU packet. To achieve fast link switch, it is necessary to enable the MMU packet sending function on the DUT and enable MMU packet receiving and processing function on the port of upstream device on the dual uplink network.

After the DUT link switch occurs, the MMU packet will be sent from new primary link, that is, from Port “MMU GigaEthernet0/2”. When the upstream device receives the MMU packet, it will judge whether the sending control VLAN of this MMU packet is in the receiving control VLAN list configured by the port receiving the packet. If it is not in the receiving control VLAN list, the device will directly forward the MMU packet without processing; if it is in the receiving control VLAN list, the device will extract the VLAN Bitmap data in the MMU packet and the MAC and ARP entries learned by the device in these VLANs are deleted.

Thereafter, if Switch D receives the data packet of DUT as the destination device, for the packet requiring the layer-2 forwarding, Switch D will forward it in the way of Layer-2 broadcasting; for the packet requiring the layer-3 forwarding, the device will first update ARP entries through using the ARP detection method and then forward the packet out. Thus, the data traffic can be transmitted correctly.

Automatically update entries through traffic

This approach applies to the case of butting with the devices not supporting BackupLink (including other vendors’ devices) under the premise that the upstream traffic is triggered.

If there is no upstream traffic from the DUT to trigger the updating of MAC and ARP entries of Switch D, when Switch D receives the data packet of DUT as the destination device, it will still forward it via the port “GigaEthernet0/1”; but the packet cannot reach the DUT, the traffic breaks until its MAC or ARP entries age automatically.

In the case that the DUT has upstream traffic to send, because MAC and ARP entries of the DUT are also wrong, the traffic will not be sent out until their entries automatically age and re-learn. When the upstream traffic reaches the device “Switch D” through the port “GigaEthernet0/2”, Switch D will update its own MAC and ARP entries; then when Switch D receives the data packet of the DUT as the destination device again, Switch D will forward it out through Port “GigaEthernet0/2”, and the packet can reach DUT via Switch C.

Note:
For the updating of the mechanism which notifies the device of updating through MMU packet, there is no need to wait until the entries age; the time of entry updating can be dramatically reduced.

Uplink Fault Handling Mechanism

In the networking environment shown in the above figure, the BackupLink function is used for the link redundancy backup on the DUT; GigaEthernet0/1 is the primary port; GigaEthernet0/2 is the secondary port. When the primary link where the port “GigaEthernet0/1” is faulty, the traffic is switched to the the secondary link where the port “GigaEthernet0/2” is in the period of milliseconds, achieving the efficient and reliable link backup and fast convergence performance.

However, when the link where the uplink port “GigaEthernet0/1” of Switch B is fails, for the device “DUT” configuring the BackupLink group, as the link where its primary port GigaEthernet0/1 is is not faulty, the link switch in the BackupLink group will not occur at this time. But in fact, the traffic on the DUT cannot uplink to Switch D through the link of the port “GigaEthernet0/1”, so the traffic is interrupted. To solve this problem, BackupLink must support the “MonitorLink” mechanism which changes the local link based on the uplink topology changes. “MonitorLink” is used to monitor the uplink to achieve the purpose of making the downlink synchronize with the uplink, improving the backup role of BackupLink.

Introduction of MonitorLink Concepts

MonitorLink group is composed of one or more upstream and downstream ports. The status of downstream port varies with the change of uplink port status.

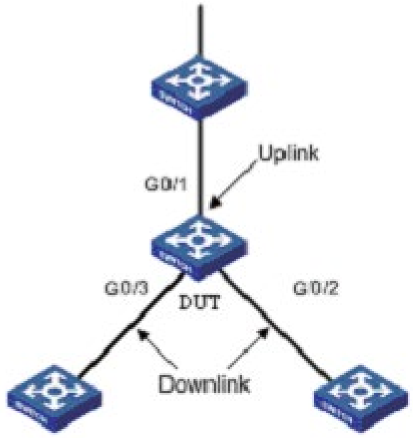


Diagram of MonitorLink Group Concepts Introduction

As is shown above, three ports of DUT (GigaEthernet0/1, GigaEthernet0/2 and GigaEthernet0/3) form a MonitorLink group.

“Uplink Port” is a monitored object in MonitorLink group, which is a port role of the MonitorLink group specified through the command line. The Uplink port of MonitorLink group can be an Ethernet port (electrical or optical), or aggregate interface. As is shown in Figure 3.3, GigaEthernet 1/ 1, a port of the DUT, is the uplink port of MonitorLink group configured on the device. When the uplink port of MonitorLink group fails, the MonitorLink group is in the status of DOWN and all the downlink ports will be closed. When the uplink port of MonitorLink group is not specified, then it is considered that the uplink port fails and that all the downlink ports will be closed.

“Downlink Port” is a monitor in MonitorLink group, which is another port role of the MonitorLink group specified through the command line. The downlink port of MonitorLink group can be an Ethernet port (electrical or optical), or aggregate interface. As is shown in the above figure, two ports of the DUT, GigaEthernet0/2 and GigaEthernet0/3, are two downlink ports of MonitorLink group configured on the device.

MonitorLink operating mechanism

In the networking environment shown below, BackupLink group is configured on the DUT in order to achieve reliable access to the Internet from the host. GigaEthernet0/1 as the primary port is in the forwarding state; GigaEthernet0/2 is the secondary port.

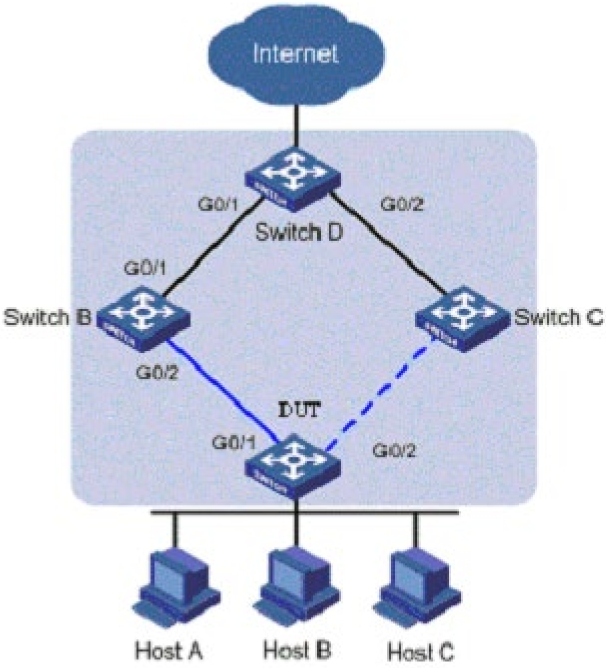


Diagram of MonitorLink operating mechanism

In order to prevent the phenomenon that DUT traffic cannot uplink because of the failure of the link where the port of Switch B, "GigaEthernet 1/ 1", is, MonitorLink group is configured on Switch B, and the port "GigaEthernet0/1" is specified as the uplink port and "GigaEthernet0/2" is specified as downlink port.

When the link where the uplink port of Switch B, GigaEthernet0/1, is fails, MonitorLink group will forcibly shut down this group's downlink port "GigaEthernet0/2", triggering the link switch of BackupLink group on the DUT.

When the link where the uplink port of Switch B, GigaEthernet0/1, is recovers from the failure, the downlink port "GigaEthernet0/2" will also be enabled; if BackupLink group on the DUT is configured as role preemption mode, similarly, the link switch of BackupLink group on the DUT will be triggered; otherwise, it is necessary to wait for the next link switch. Thus, the combination of MonitorLink technology with BackupLink technology enables efficient and reliable link backup and fast convergence performance.

Link Recovery Processing Mechanism

BackupLink group supports two modes: non-role preemption mode and role preemption mode. Link recovery mechanism is different in different modes. For the non-role preemption mode, please see 1.2.4; for the role preemption mode, please see 1.2.5.

BackupLink Configuration

Guidance Notes for BackupLink Configuration

Before configuring BackupLink protocol, please read the following guidance notes:

Primary port (Ethernet port or aggregate port) can be configured with a BackupLink backup port; moreover, this backup port and primary port cannot be the same port;

A port can only belong to one BackupLink group; a backup port can only taken as the backup port of one primary port; one primary port can not belong to other BackupLink groups;

Any port within the BackupLink group cannot be a member of the aggregate ports. Aggregate port and physical port, physical port and physical ports, aggregate port and aggregate port can become the members of BackupLink group.

BackupLink primary port and backup port may be different in type; they may be Fast Ethernet ports, Gigabit ports or aggregate ports, but both must have similar features. Thus, When the primary port fails, the backup port can forward its data traffic in similar way;

VLAN load balancing and BackupLink preemption functions cannot be used simultaneously.

BackupLink Configuration Tasks

Configuring BackupLink group

Configuring the preemption feature for BackupLink group

Configuring load balancing for VLAN

Configuring the MMU feature for BackupLink group

Configuring MonitorLink group

BackupLink Configuration

Configuring BackupLink Group

Configure BackupLink group according to the following steps.

Command	Purpose
Switch#**config**	Enter switch configuration mode.
Switch_config#**backup-link-group** *id*	Configure backuplink group. *Id*: backuplink group instance number.
Switch_config#**interface** *interface-type interface-number*	Enter port configuration mode
Switch_config_g1/1#**backup-link-group** *id* **active[backup]**	Configure backuplink group port role. *Id*: backuplink group instance number.
Switch_config_g1/1#**exit**	Exit from the port configuration mode.
Switch_config#	

Note:
Use the "no backup-link-group id" command to delete backuplink group configuration and backuplink group port configuration.

Note:
If the backuplink group is directly configured for the port in the case that it is not established, the system will automatically create the backuplink group.

Configuring the Preemption Feature for BackupLink Group

Configure the preemption feature for BackupLink group according to the following steps.

Command	**Purpose**
Switch#config	Enter switch configuration mode.
Switch_config#**backup-link-group** *id* {**preemption-mode [forced | bandwidth]** {**delay** *value*}}	Configure the preemption feature for BackupLink group. *Id*: backuplink group instance number; *value*: delay-time.
Switch_config#	

Note:
Use the "backup-link-group id {preemption-mode [forced | bandwidth] {delay value}}" command to directly create BackupLink group.

Configuring Load Balancing for VLAN

Configure load balancing for VLAN according to the following steps.

Command	Purpose
Switch#**config**	Enter switch configuration mode.
Switch_config#**interface** *interface-type interface-number*	Enter port configuration mode
Switch_config_g1/2#**share-load vlan** *vlanmap*	Configure load balancing for VLAN. *Vlanmap*: vlan value
Switch_config_g1/2#**exit**	Exit from the port configuration mode.
Switch_config#	

Note:
The "share-load vlan vlanmap" command is only used for backup port, that is, before the vlan load balancing, the port must be configured as a backup port.

Note:
For different BackupLink groups, the same group VLAN can be configured, or they have overlapping VLAN segments. But after the overlapping VLAN segments are configured, the system will assign them to different MSTs (STG); therefore, when the port of some group is operated, its status in all MSTs (STG) will take change. So, typically, when the

load balancing VLAN group is configured, it is better to select the VLAN group without overlapping.

Configuring the MMU Feature for BackupLink Group

Configure the MMU feature for BackupLink group according to the following steps.

Command	Purpose
Switch#**config**	Enter switch configuration mode.
Switch_config#**interface** *interface-type interface-number*	Enter port configuration mode
Switch_config_g1/2#**backup-link-group mmu transmit [receive]**	Configure MMU sending (receiving) function.
Switch_config_g1/2#**exit**	Exit from the port configuration mode.
Switch_config#	

Note:
The port configured as “transmit” must be the port of backuplink group, that is, it must be first configured as “active” or “backup”. In the case of configuring the port with “receive” function, it is not necessary to configure the port for backuplink group.

Configuring MonitorLink Group

Configure MonitorLink group according to the following steps.

Command	Purpose
Switch#**config**	Enter switch configuration mode.
Switch_config#**monitor-link-group** *id*	Configure MonitorLink group. *Id*: MonitorLink group instance number.
Switch_config#**interface** *interface-type interface-number*	Enter port configuration mode
Switch_config_g1/1#**monitor-link-group** *id* **uplink[downlink]**	Configure MonitorLink group port role. *Id*: MonitorLink group instance number.
Switch_config_g1/1#**exit**	Exit from the port configuration mode.
Switch_config#	

Note:
Use the "no monitor-link-group id" command to delete MonitorLink group configuration and MonitorLink group port configuration.

Note:

If the MonitorLink group port role is directly configured for the port in the case that the MonitorLink group is not established, the system will automatically create the MonitorLink group .

21. EAPS Configuration

Introduction of Fast Ethernet Ring Protection

Overview

MY COMPANYEthernet 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 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.

Remark:
EAPS supports to set a switch to be a node of multiple physical ring to construct complicated topology.

Related Concepts of Fast Ether-Ring Protection

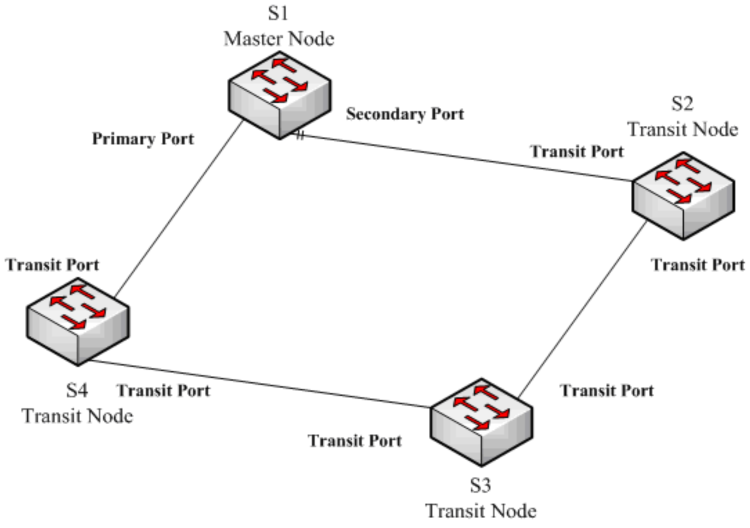


Figure 1.1 EAPS Ethernet ring

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.

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 will open the secondary port to forwarding the data packets.

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.

Remark:
To configure a same switch to belong to multiple rings, the switch must connect different rings through different physical ports.

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.

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.

Aging of the MAC Address Table

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.

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.

Types of EAPS Packets

The EAPS packets can be classified into the following types, as shown in table 1.1.

Table 1.1 Types of EAPS packets

Type of the packet	Remarks
Loopback detection (HEALTH)	It is transmitted by the master node to detect whether the topology of the ring network is complete.
LINK-DOWN	Indicates that link interruption happens in the ring. This kinds of packets are transmitted by the transit node.
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.

Fast Ethernet Ring Protection Mechanism

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.

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.

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.

Fast Ethernet Ring Protection Configuration

Default EAPS Settings

> Note:
> The fast Ethernet protection protocol cannot be set together with STP.
> After STP is disabled, you are recommended to run **spanning-tree bpdu-terminal** to keep the ring node from forwarding BPDU, which leads to the storm.

See the following table:

Table 2.1 Default settings of the Ethernet ring protection protocol and STP.

Spanning tree protocol	**spanning-tree mode rstp**
Fast Ethernet Ring Protection	There is no configuration.

Requisites before Configuration

Before configuring MEAPS, please read the following items carefully:

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. If the ring network is connected in the case that the configuration is not finished, the broadcast storm may easily occur.

EAPS is well compatible with STP, but the port under the control of EAPS is not subject to STP.

The ring protection protocol supports a switch to configure multiple ring networks.

Configuring ring control VLAN will lead to the automatic establishment of corresponding system VLAN.

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.

The physical interface, the fast-Ethernet interface, the gigabit-Ethernet interface and the aggregation interface can all be set to be the ring's interfaces. If link aggregation, 802.1X or port security has been already configured on a physical interface, the physical interface cannot be set to be a ring’s interface any more. Note: The versions of MY COMPANY switch software prior to version 2.0.1L and the versions of hi-end switch software prior to version 4.0.0M do not support the configuration of the converged port.

MEAPS Configuration Tasks

Configuring the Master Node

Configuring the Transit Node

Configuring the Ring Port

Browsing the State of the Ring Protection Protocol

Fast Ethernet Ring Protection Configuration

Configuring the Master Node

Configure a switch to be the master node of a ring network according to the following steps:

Command	**Purpose**
Switch#**config**	Enters the switch configuration mode.
Switch_config#**ether-ring** *id*	Sets a node and enters the node configuration mode. id: Instance ID
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#**exit**	Saves the current settings and exits the node configuration mode.

Remark:

The **no ether-ring *id*** command is used to delete the node settings and port settings of the Ethernet ring.

Configuring the Transit Node

Configure a switch to be the transit node of a ring network according to the following steps:

Command	**Purpose**
Switch#**config**	Enters the switch configuration mode.
Switch_config#**ether-ring** *id*	Sets a node and enters the node configuration mode. id: Instance ID
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.

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**	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 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.

Browsing the State of the Ring Protection Protocol

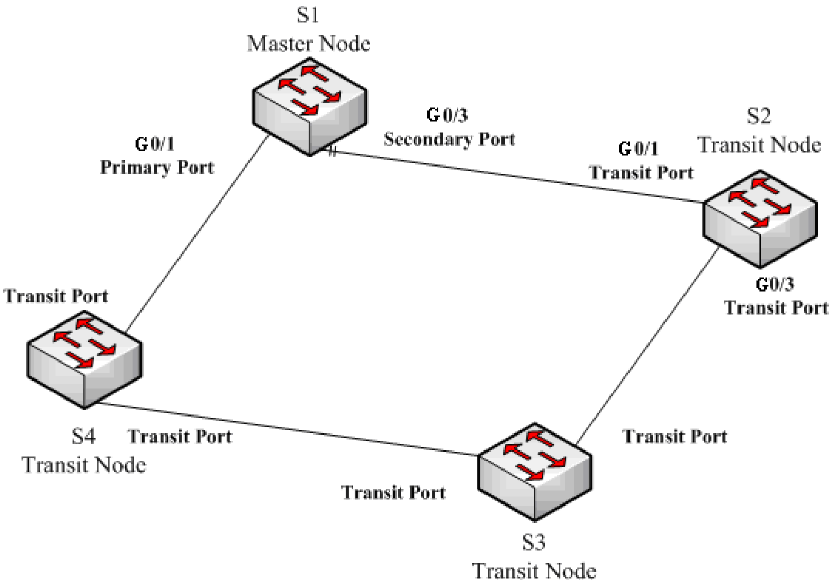
Run the following command to browse the state of the ring protection protocol:

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.

MEAPS configuration

Configuration Example



MEAPS configuration

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
```

The following commands are used to set 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 gigaEthernet 0/1
S1_config_g0/1#ether-ring 1 primary-port
S1_config_g0/1#exit
S1_config#interface gigaEthernet 0/3
S1_config_g0/3#ether-ring 1 secondary-port
S1_config_g0/3#exit
```

Establishes the control VLAN:

```
S1_config#vlan 2
S1_config_vlan2#exit
S1_config#interface range g0/1 , 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 gigaEthernet 0/1
S1_config_g0/1#ether-ring 1 transit-port
S1_config_g0/1#exit
S1_config#interface gigaEthernet 0/3
S1_config_g0/3#ether-ring 1 transit-port
S1_config_g0/3#exit
S1_config#vlan 2
S1_config_vlan2#exit
S1_config#interface range gigaEthernet 0/1 , 3
S1_config_if_range#switchport mode trunk
S1_config_if_range#exit
```

22. MEAPS Configuration

MEAPS Overview

EAPS is a protocol specially applied on the link layer of the Ethernet ring. When the Ethernet ring is complete, you should prevent the broadcast storm from occurring on the data loopback. But when a link of an Ethernet ring is broken, you should enable the backup link rapidly to resume the communication of different nodes in the ring. The role of switch is specified by you through configuration.

MEAPS, an expansion on the basis of EAPS, can support not only the single ring but also the level-2 multi-ring structure. The later structure consists of the aggregation layer in the middle, constructed by aggregation equipment through the Ethernet ring for fast switching, and the access layer at the outside, connected by the access equipment. Different levels of rings are connected through the tangency or intersection mode. See the specific topology in the following figure:

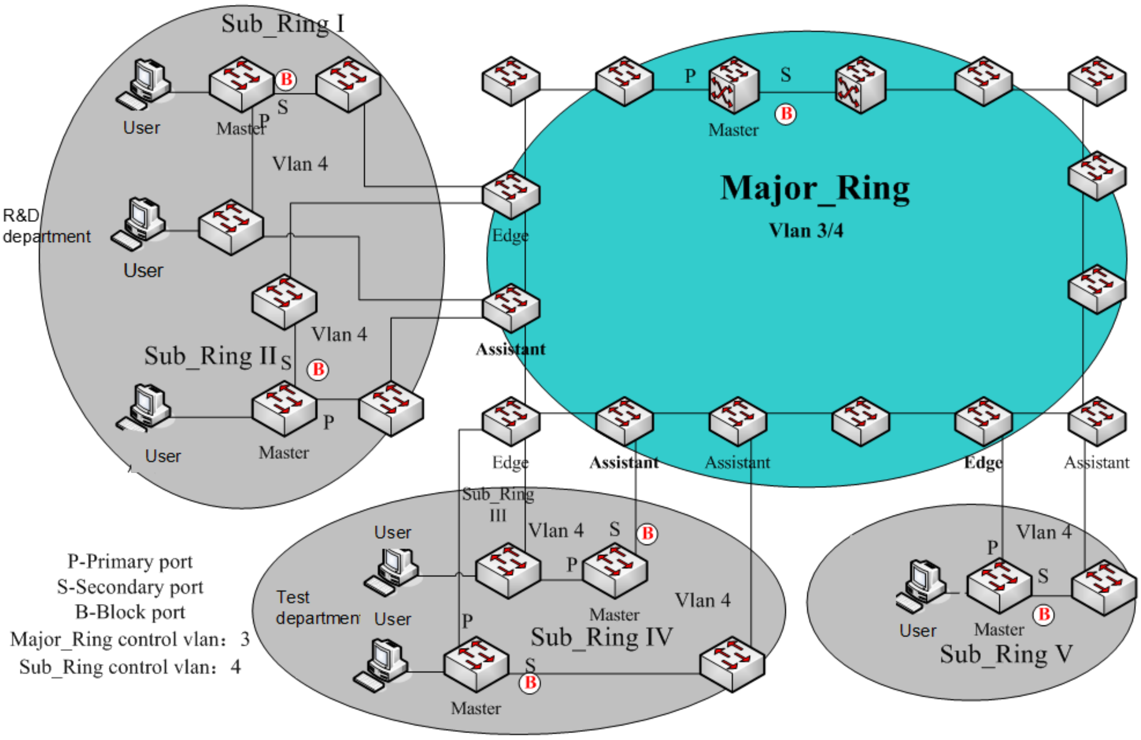


Figure 1 MEAPS Structure

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.

Basic Concepts of MEAPS

Domain

The domain specifies the protection range of the Ethernet loopback protection protocol and is marked by ID, which consists of integers; A group of switches that support the same protection data and have the same control VLAN can form a domain after they are connected with each other. One domain may include only one ring or multiple rings that intersect each other. See Figure-2.

One MEAPS domain has the following factors: MEAPS ring, control VLAN, master node, transit node, edge node and assistant edge node.

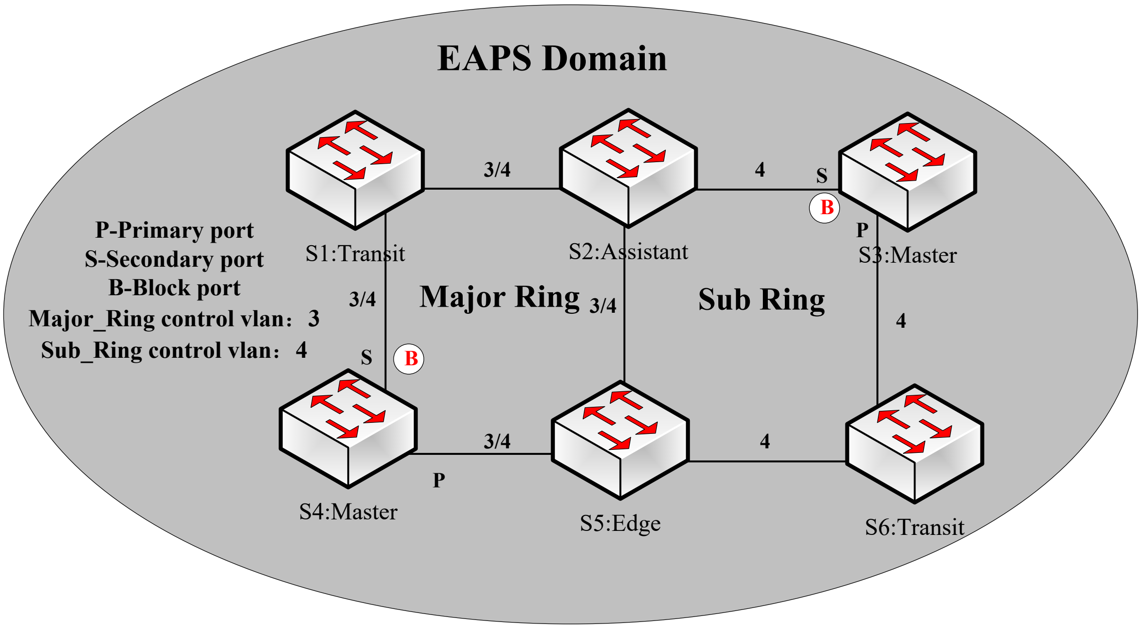


Figure-2 Simple MEAPS model

Ring

One ring corresponds to a ring Ethernet topology physically, which is a group of switches that are connected each other into a ring. One MEAPS domain may include only one MEAPS ring or multiple rings that intersect each other.

Major Ring

When a domain includes many rings, the included rings except the major ring are called as sub rings. The primary and secondary ports of each node on the major ring should be added into the main control VLAN and the sub control VLAN at the same time. See Figure-2.

Sub Ring

When a domain includes many rings, you should choose one ring from them as a major ring. The primary and secondary ports of each node on the sub ring should be added into the sub control VLAN. See Figure-2.

Control VLAN

The control VLAN is a concept against the data VLAN, and in MEAPS, the control VLAN is just used to transmit the MEAPS packets. Each MEAPS has two control VLANs, that is, the main control VLAN and the sub control VLAN.

You need to specify the main control VLAN when configuring the major ring or the sub ring. During configuration you just need to specify the main control VLAN and take the VLAN which is 1 more than the ID of the main control VLAN as the sub control VLAN. The major ring will be added to the main control VLAN and the sub control VLAN at the same time, while the sub ring will only be added to the sub control VLAN. See number 3 and number 4 beside each port on the following figure.

The main-ring protocol packets are transmitted in the main control VLAN, while the sub-ring protocol packets are transmitted in the sub control VLAN. The sub control VLAN on the major ring is the data VLAN of the major ring. The ports of a switch that access the Ethernet ring belong to the control VLAN, and only those ports that access the Ethernet ring can be added into the control VLAN.

Note:
The MEAPS port of the major ring should belong to both the main control VLAN and the sub control VLAN; the MEAPS port of the sub ring only belongs to the sub control VLAN. The major ring is regarded as a logical node of the sub ring and the packets of the sub ring are transparently transmitted through the major ring; the packets of the major ring are transmitted only in the major ring.

Data VLAN

Appearing against the control VLAN, the data VLAN is used to transmit data packets. The data VLAN can also include the MEAPS port and the non-MEAPS port. Each domain protects one or multiple data VLANs. The topology that is calculated by the ring protection protocol in a domain is effective only to the data VLAN in this domain.

Whether the data VLAN is created or not has no influence on the work of the ring state machine, where the MEAPS port is controlled by the MEAPS module and the non-MEAPS port is controlled by the STP module.

Note:
The processing methods which are similar to that of the MSTP module can be used, that is, the status of a port in the default STP instance is decided by the link status of the port, no matter what the VLAN configuration of a port is.

Master Node

The master node works as policy making and control of a ring. Each ring must possess only one master node. The master node takes active attitude to know whether the ring's topology is complete, removes loopback, control other switches to update topology information. See the following figure, where S3 is the master node of the sub ring and S4 is the master node of the major ring.

Transit Node

All switches on the Ethernet except the master node can be called as the transit nodes. The transit node only checks the state of the local port of the ring, and notifies the master node of the invalid link. See the following figure, in which S1, S2, S5 and S6 are all transit nodes.

Edge Node and Assistant Node

When the sub ring and the major ring are intersected, there are two intersection points, two switches beside which are called as the edge node for one and the assistant node for the other. The two nodes are both the nodes of the sub ring. There are no special requirements as to which switch will be set to be the edge node or the assistant node if their configurations can distinguish themselves. However, one of them must be set as the edge node and the other must be set as the assistant node. The edge node or the assistant node is a role that a switch takes on the sub ring, but the switch takes a role of the transit node or the master node when it is on the major ring. See the following figure, in which S2 is the assistant node and S5 is the edge node.

Primary Port and Secondary Port

The two ports through which the master node accesses the Ethernet ring are called as the primary port and the secondary port. The roles of the two ports are decided by the clients.

The primary port is in forwarding state when it is up. Its function is to forward the packets of the data VLAN on the master node and to receive and forward the control packets on the control VLAN. The master node will transmit the loopback detection packets from the primary port to the control VLAN. If the link of the primary port is resumed from the invalid status, the master node requires to send the address aging notification to the control VLAN promptly and then starts to transmit the loopback detection packets from the primary port.

The secondary port is in forwarding or blocking state when it is up. 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 will open the secondary port to forwarding the data packets.

Note:
A port can be set as the primary port or the secondary port of a node and it cannot be set to be both the primary port and the secondary port.

Transit Port

The two ports for the transit node to access the Ethernet ring are both transit ports. Users can decide the role of the two ports through configuration.

The transit port is in forwarding or preforwarding state when it is up. A transit port receives the control packets from the control VLAN and at the same time forwards these packets to other ports in the control VLAN. After the transit port resumes from the invalid state, it first enters the pre-forwarding state, receives and forwards only the control packets, and blocks the data VLAN. After the transit node receives the notification of the aging address table, it enters the forwarding state.

Note:
A port can be set as the primary port or the transit port of a node and it cannot be reset.

Common Port and Edge Port

The edge node and the assistant node are the places where the sub ring and the major ring intersect. As to the two ports that access the Ethernet, one is a common port, which is the public port of the sub ring and the major ring; the other is the edge port in the sub ring. The roles of the two ports are decided by users through configuration.

The common port is on the main-ring port and so its state is decided by the state of the main-ring port. The common port itself has no operations or notifications. When the link, connecting the common port, changes, the sub-ring node where the common port lies will not be notified. The existence of the common port just guarantees the completeness of the ring.

The edge port of the edge node is in forwarding or preforwarding state when it is up. Its basic characteristics are consistent with those of the transit port except one function. The exceptional function is that when the edge port is up and its corresponding main-ring port is also up, it will transmit the edge-hello packets from the main-ring port to detect the completeness of the major ring.

The edge port of the assistant node is in forwarding, preforwarding or EdgePreforwarding state when it is up. Besides the same characteristics of the transit port, it also has one more state, the Edge Preforwarding state. If the edge port is in forwarding state and the main-ring port that the edge port corresponds to has not received the edge-hello packets, the state of the edge port is changed into the EdgePreforwarding state, and it only receives and forwards the control packets and blocks the data VLAN until the corresponding main-ring port receives the Edge-hello packets again.

The edge port of the edge node and the assistant node is to help detect the completeness of the major ring. For more details, see the channel status checkup mechanism of the sub-ring protocol packets on the major ring in the following chapter.

Note:
Each port can be set as the only edge port of a node and it cannot be configured again; the common port can be borne only on a port of the major ring and it cannot be configured on a port without a corresponding main-ring port.

Aging of the MAC Address Table (FLUSH MAC FDB)

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.

Complete Flag of Ring

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. 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.

Types of EAPS Packets

Table 1.1 Types of EAPS packets

Type of the packet	Description
Ring Detection (HEALTH)	It is transmitted by the master node to detect whether the topology of the ring network is complete.
link interruption (LINK-DOWN)	Indicates that link interruption happens in the ring. This kinds of packets are transmitted by the transit node.
MAC address aging table of the transit node (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 resume aging address table (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.
Ring completeness detection (EDGE-HELLO)	It is decided by the edge port of the edge node, transmitted by the main-ring port that the edge node corresponds to, and detects whether the major ring is complete.

Fast Ethernet Ring Protection Mechanism

Polling mechanism

The primary port transmits the HEALTH packets to the control VLAN. In normal case, the HEALTH packets will pass through all other nodes of the ring 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.

As shown in the following figure, the master node, S4, transmits the HELLO packets periodically. If the loopback has no troubles, the HELLO packets will arrive at the secondary port of the master node, and the master node will block data forwarding of the data VLAN that the secondary port belongs to, preventing the loopback from happening.

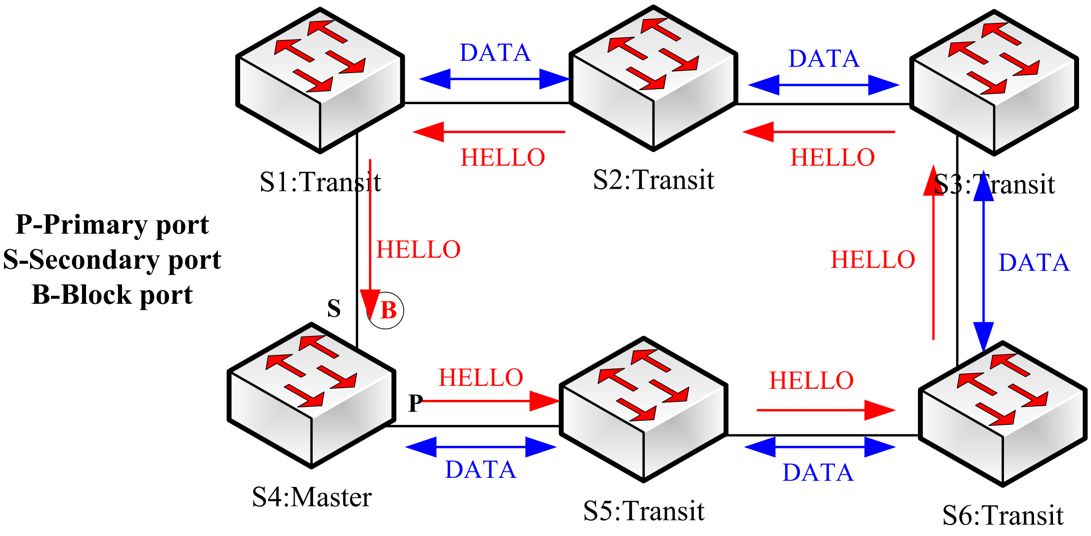


Figure 3 Polling mechanism

Note:
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.

Notification of Invalid Link of Transit Node

The link state change notification mechanism provides a faster processing mechanism for ring network topology changes than the polling mechanism:

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. As shown in the following figure, trouble occurs on the link between node S3 and node S6. After node S3 and node S6 detect that trouble has already occurred on the link, they block the ports that the troubled link corresponds to and transmit the LINK-DOWN packets respectively from the other port; when the master node receives the LINK-DOWN packets, holds that the trouble occurs on the loopback, and decides not to wait for the fail-time any more.

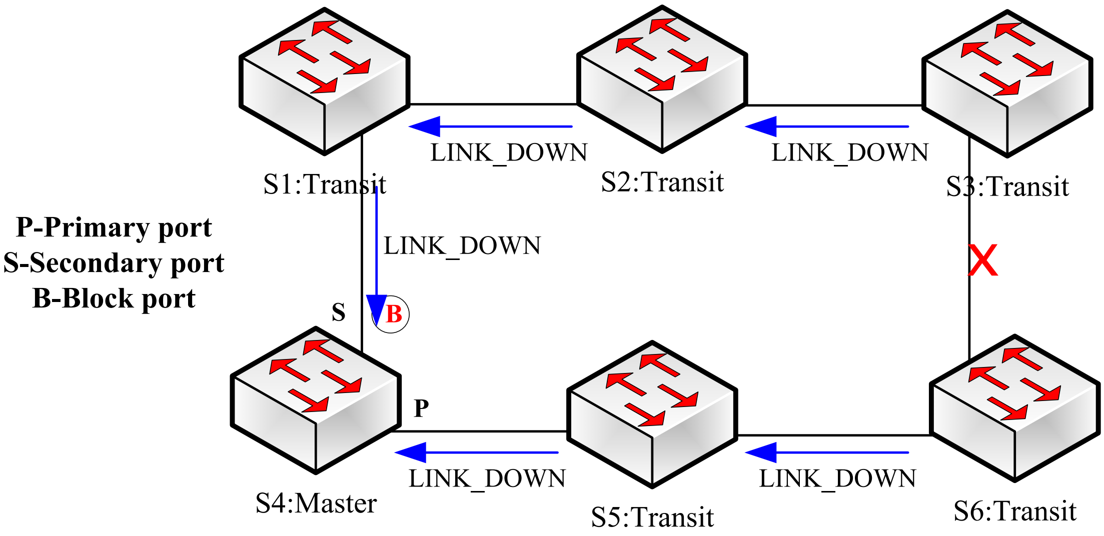


Figure 4 Link status change's notification

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 connecting the master node is already out of effect, and the transit node will automatically set the pre-forwarding port to be a forwarding one.

Note:
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.

Channel Status Checkup Mechanism of the Sub-Ring Protocol Packet on the Major ring

The ports on the major ring are simultaneously added to the control VLAN of the major ring and the control VLAN of the sub ring. Hence, the protocol packets of the sub ring should be broadcast among the edge ports of the edge node and the assistant node through the channel, provided by the major ring. In this case, the whole major ring is just like a node of the sub ring (similar as a virtual transit node), as shown in the following figure:

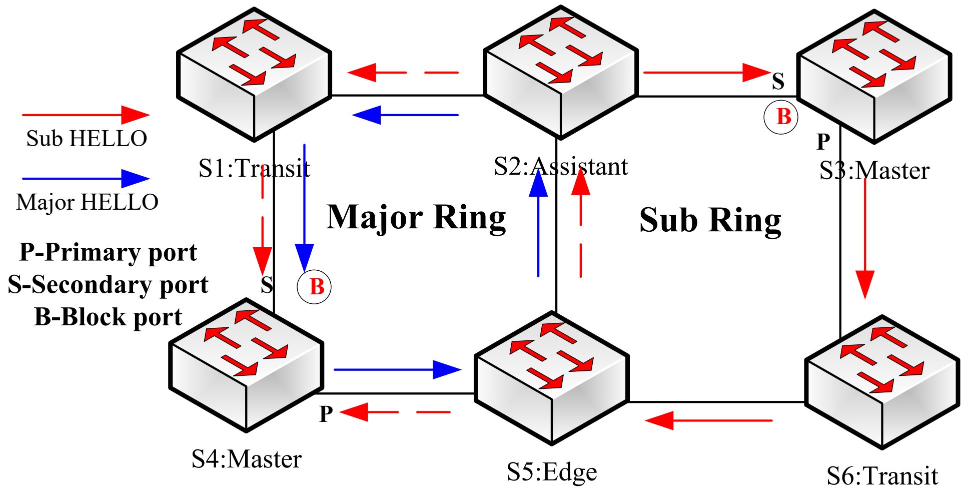


Figure 5 Intersection of the major ring and the sub ring

When trouble occurs on the link of the major ring, and when the channel of the sub-ring protocol packets between the edge node and the assistant node are interrupted, the master node of the sub ring cannot receive the HELLO packets that the master node itself transmits. In this case, the Fail Time times out, and the master node of the sub ring changes to the Failed state and opens its secondary port.

The above-mentioned processes have an effective protection towards general networking, guaranteeing not only the prevention of the broadcast loopback but also the corresponding functions of the backup link. The dual homing networking mode is always used in actual networking, as shown in the following figure. The two sub rings in the dual homing networking, sub ring I and sub ring II, interconnect through the edge node and assistant node, and forms a big ring. When the major ring has troubles, the secondary ports of the master nodes of all sub rings open and forms the broadcast loop (marked by the arrow) in the big ring.

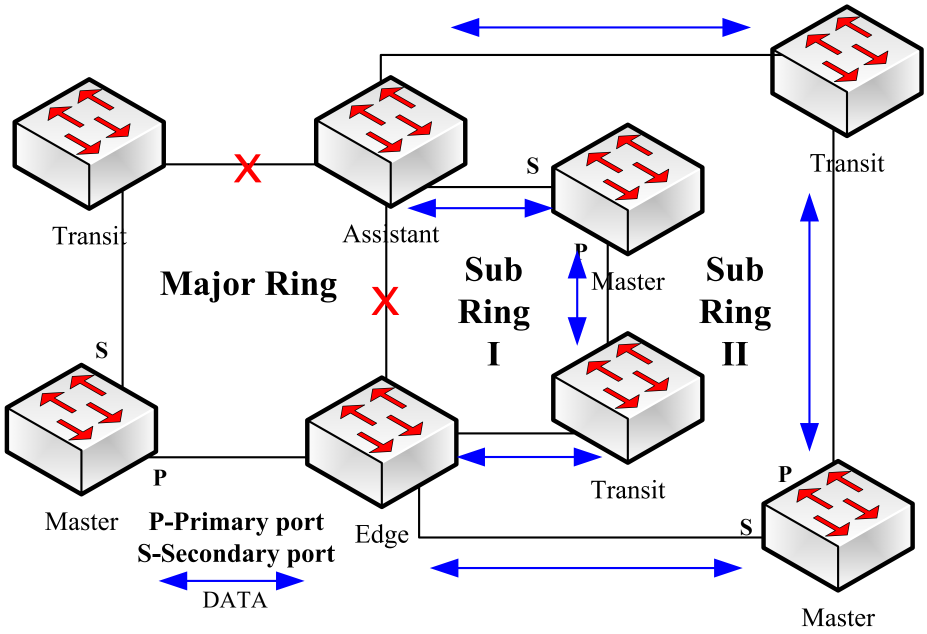


Figure 6 Broadcast storm triggered by the dual homing networking mode

The channel status checkup mechanism of the sub-ring protocol packet on the major ring is introduced to solve the problem about the dual homing ring. This mechanism is to monitor the status of the channel link on the major ring between the edge node and the assistant node, which requires the help of the edge node and the assistant node. The purpose of this mechanism is to keep the data loop from happening by blocking the edge port of the edge node before the secondary port of the master node on the sub ring opens. The edge node is the trigger of the mechanism, while the assistant node is the listener and decider of this mechanism. Once the notification message from the edge node cannot be received, the edge node will instantly be in blocked state until this notification message is received again. The results of the mechanism, which bring about after the troubles on the major ring, are shown in the following figure:

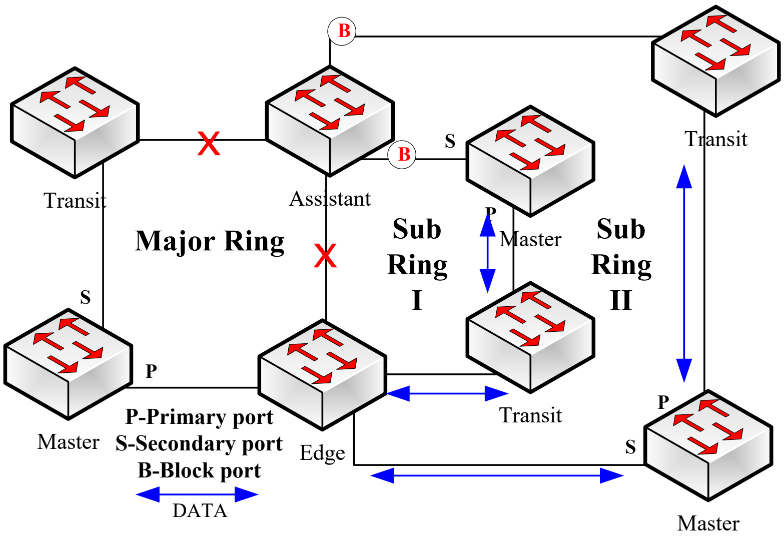


Figure 7 Results of the channel status checkup mechanism

But you should pay special attention to this point that the edge port of the assistant node must be blocked before the secondary port of the master node on the sub ring opens. Otherwise, the broadcast storm will happen.

The whole procedure of this mechanism is described as follows:

1. Check the channel status on the major ring between the edge node and the assistant node.

The edge node of the sub ring periodically transmits the Edge-Hello packets to the major ring through the two ports of the major ring, and these packets pass through all nodes on the major ring in sequence and finally arrive the assistant node, as shown in the following figure. If the assistant node can receive the edge-hello packet in the regulated time, it indicates that the channel of this packet is normal; if not, it indicates that the channel is interrupted. The edge-hello packet is the control packet of the sub ring, but is transmitted and received by the ports on the major ring and is transferred to the sub ring for processing.

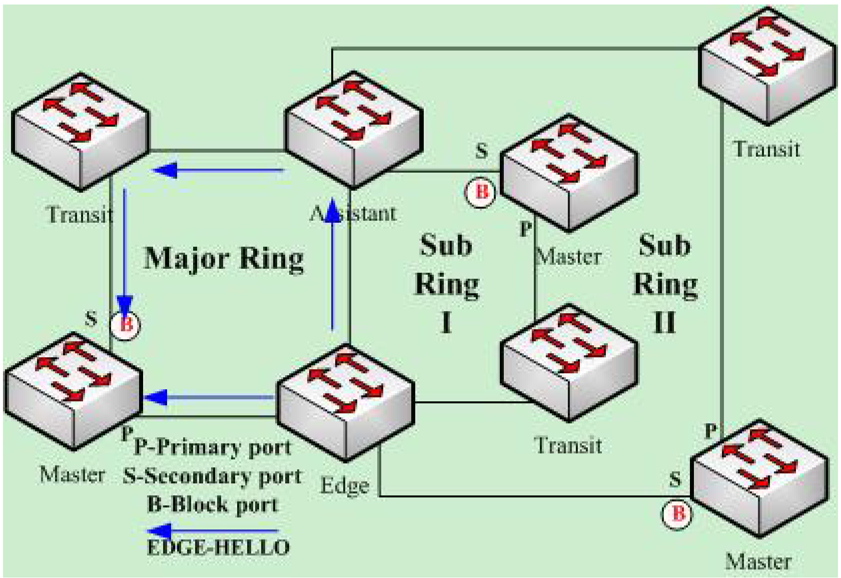


Figure 8 Checking the channel status on the major ring between the edge node and the assistant node

2. The edge node blocks the edge port at the interruption of the channel.

If the assistant node cannot receive the edge-hello packet during Edge Fail Time, the assistant holds that the channel of the sub-ring protocol packet - the edge-hello packet - is interrupted, changes its edge port's status into the Edge-Preforwarding status instantly, blocks the forwarding of the data packets (though still receives and forwards the control packet), and immediately transmits the LINK-DOWN packet to the master node for the master node to open the secondary port to avoid communication interruption among all nodes on the ring.

Note:
In order to guarantee that the edge port first changes into the edge-preforwarding status and then the master node opens the secondary port, you shall be sure that the cycle for the edge node to transmit the edge-hello packet, Edge Hello Time, is smaller than the cycle for the master node to transmit the Hello packet, Hello Time; similarly, the Edge Fail Time of the assistant node should be smaller than Fail Time. At the same time, Fail Time is generally the triple of Hello Time, and Edge Fail Time is also the triple of Edge Hello Time.

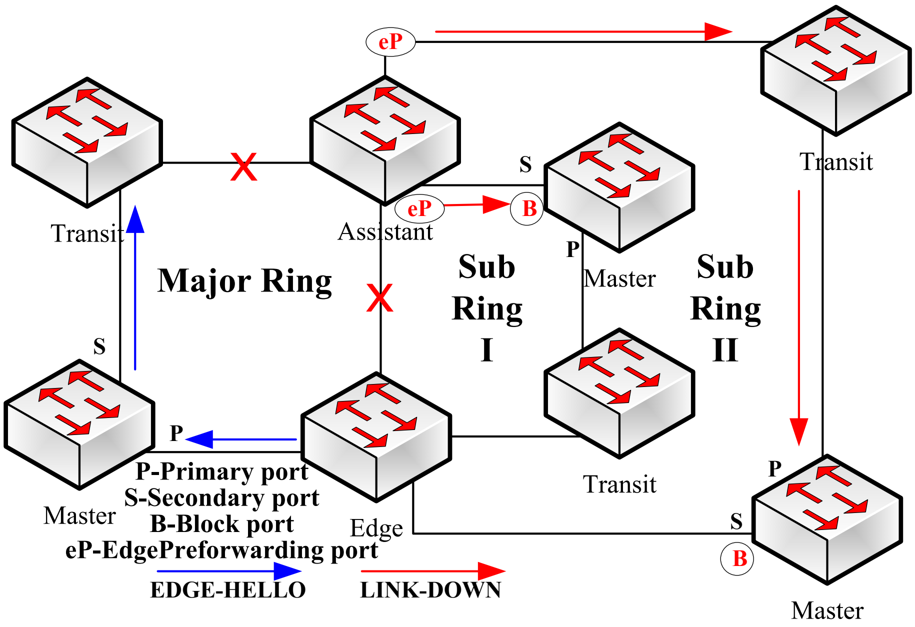


Figure 9 The edge port being blocked by the edge node at the interruption of the channel

3. Channel recovery

When the link of the major ring and the communication between the edge node and the assistant node resumes, the channel of the sub-ring protocol packet resumes to the normal function. In this case, the master node of the sub ring receives the Hello packet again, which is transmitted by the master node itself, and therefore it switches to the Complete status, blocks the secondary port and transmits the RING-UP-FLUSH-FDB packet to the ring. At the same time, the status of the edge port of the assistant node changes from Edge-Preforwarding to Forwarding, guaranteeing a smooth communication among all nodes on the ring. The following figure shows that the channel is resumed and then the communication on the ring is also resumed.

Note:
Before the edge node opens the blocked edge port, the secondary port of the master node on the sub ring should be blocked to prevent the broadcast storm from happening.

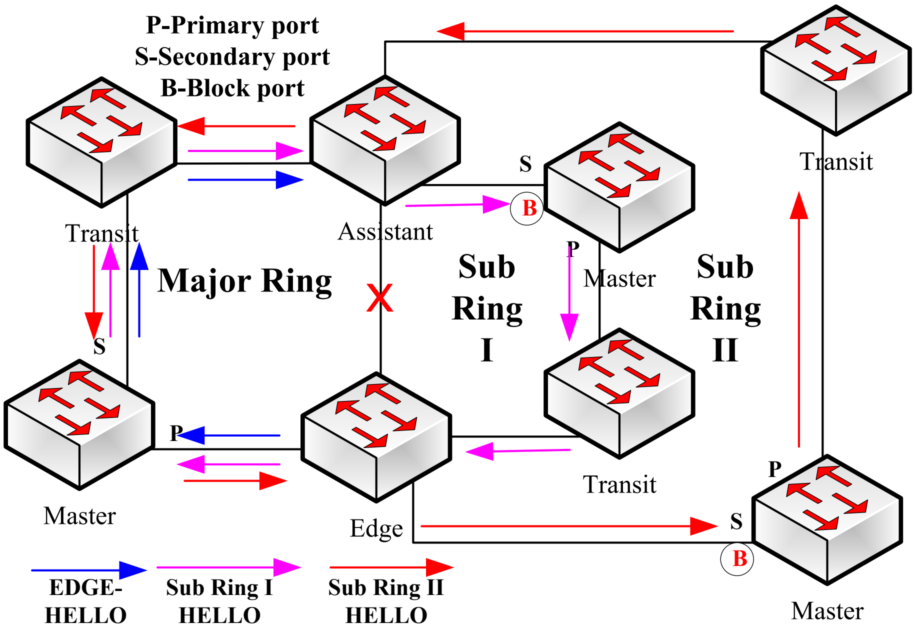


Figure 10 Channel recovery

Fast Ethernet Ring Protection Configuration

Requisites before Configuration

Before configuring MEAPS, please read the following items carefully:

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.

Enable the ring protection protocol to be compatible with the STP of a switch through relative configurations. The users are allowed to set “no spanning-tree”, SSTP, RSTP PVST or MSTP mode.

After an instance of the ring's node is set, users are forbidden to change the basic information of the node (excluding the time parameters) unless the current ring’s node is deleted and then reset.

If you run show to browse the configured node and find its **state** is **init**, it shows that the node’s configuration is unfinished and therefore the node cannot be started. In this case, you are required to change or add basic information to complete the configuration of the node.

The ring protection protocol supports a switch to configure multiple ring networks.

The configuration of the control VLAN of the ring automatically leads to the establishment of the corresponding VLAN without requiring users’ manual configuration.

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.

Users cannot set Edge Hello Time and Edge Fail Time, and their default values are decided by Hello Time and Fail Time respectively for their values are 1/3 of Hello Time and Fail Time respectively.

The physical interface, the fast-Ethernet interface, the gigabit-Ethernet interface and the aggregation interface can all be set to be the ring's interfaces. If link aggregation, 802.1X or port security has been already configured on a physical interface, the physical interface cannot be set to be a ring's interface any more.

This protocol is similar with the original EAPS in functions, but its ring's topology has more expansibility and flexibility. Hence, MEAPS and EAPS are partially compatible, and the intersection configuration can be done on the MEAPS ring and the EAPS ring.

MEAPS Configuration Tasks

Configuring the Master Node

Configuring the Transit Node

Configuring the Edge Node and the Assistant Node

Configuring the Ring Port

Browsing the State of the Ring Protection Protocol

Fast Ethernet Ring Protection Configuration

Configuring the Master Node

Configure a switch to be the master node of a ring network according to the following steps:

Command	Purpose
Switch#**config**	Enters the switch configuration mode.
Switch_config#**mether-ring** *id1* **domain** *id2*	Sets a node and enters the node configuration mode. id1: instance ID of a node id2: instance ID of a domain (omitted when it is 0)
Switch_config_ring1#**master-node**	Compulsory. Configures the node type to be a master node.
Switch_config_ring1#**major-ring[sub-ring]**	Compulsory. Sets the node's level to be one of the major or sub ring node.
Switch_config_ring1#**control-vlan** *vlan-id*	Compulsory. Sets the control VLAN and establishes VLAN "id" and VLAN "id+1". *vlan-id*: control vlan ID

Switch_config_ring1#**hello-time** *value*	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 3 seconds.
Switch_config_ring1#**fail-time** *value*	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 9 seconds.
Switch_config_ring1#**exit**	Saves the current settings and exits the node configuration mode.
Switch_config#	

Note:
The *no mether-ring id domain id2* command is used to delete the node settings and the node's port settings of the ring.

Note:
The major ring and the sub-ring must configure with the same vlan- the major ring control vlan. After configuration, the major ring control vlan and the sub-ring control vlan will be established on the major ring simultaneously. The sub-ring control vlan will be created on the sub-ring and forbid the major ring to control vlan.

Configuring the Transit Node

Configure a switch to be the transit node of a ring network according to the following steps:

Command	Purpose
Switch# config	Enters the switch configuration mode.
Switch_config#**mether-ring** *id1* **domain** *id2*	Sets a node and enters the node configuration mode. *id1*: ID of the node; id2: instance ID of a domain (omitted when it is 0)
Switch_config_ring1# **transit -node**	Compulsory. Configures the node type to be a transit node.
Switch_config_ring1#**major-ring[sub-ring]**	Compulsory. Sets the node's level to be one of the major or sub ring node.
Switch_config_ring1#**control-vlan** *vlan-id*	Compulsory. Sets the control VLAN and establishes VLAN "id" and VLAN "id+1". *vlan-id:* control vlan ID
Switch_config_ring1#**pre-forward-time** *value*	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 9 seconds.
Switch_config_ring#exit	Saves the current settings and exits the node configuration mode.
Switch_config#	

Configuring the Edge Node and the Assistant Node

Configure a switch to be the master node of a ring network according to the following steps:

Command	Purpose
Switch# **config**	Enters the switch configuration mode.
Switch_config#**mether-ring** *id1* **domain** *id2*	Sets a node and enters the node configuration mode. id1: instance ID of a node id2: instance ID of a domain (omitted when it is 0)
Switch_config_ring1#**edge-node[assistant-node]**	Compulsory. Sets the node type to be an edge node.
Switch_config_ring1#**sub-ring**	This step can be omitted. The edge node must be the sub-ring node.
Switch_config_ring1#**control-vlan** *vlan-id*	Compulsory. Sets the control VLAN and establishes VLAN “id” and VLAN “id+1” *vlan-id*: control vlan ID.
Switch_config_ring1#**pre-forward-time** *value*	Optional. Configures the time of maintaining the pre-forwarding state of the edge port. *Value:* It is a time value ranging from 3 to 30 seconds and the default value is 9 seconds.
Switch_config_ring1#**exit**	Saves the current settings and exits the node configuration mode.
Switch_config#	

Configuring Sub-ring Networking Mode

Configure a switch to be the master node of a ring network according to the following steps:

Command	Purpose
Switch# **config**	Enters the switch configuration mode.
Switch_config#**mether-ring** *id1* **domain** *id2*	Sets a node and enters the node configuration mode. id1: instance ID of a node id2: instance ID of a domain (omitted when it is 0)
Switch_config_ring1#**edge-node[assistant-node]**	Compulsory. Sets the node type to be an edge node.
Switch_config_ring1#**sub-ring**	This step can be omitted.The edge node must be the sub-ring node.
Switch_config_ring1#**control-vlan** *vlan-id*	Compulsory. Sets the control VLAN and establishes VLAN “id” and VLAN “id+1”.

	vlan-id: control vlan ID
Switch _config_ring2#**single-subring-mode**	Compulsory. The ring configuration can be finished without configuring the command, but the sub-ring networking mode is not available. In the sub-ring networking mode, the sub-ring protocol packet channel detection mechanism cannot work on the major ring and there must no dual homing networking. The command is effective only for the edge node and the assistant node.
Switch_config_ring1#**pre-forward-time** *value*	Optional. Configures the time of maintaining the pre-forwarding state of the edge port. Value: It is a time value ranging from 3 to 30 seconds and the default value is 9 seconds.
Switch_config_ring1#**exit**	Saves the current settings and exits the node configuration mode.
Switch_config#	

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	Enters the switch configuration mode.
Switch_config#interface *intf-name*	Enters the interface configuration mode.
Switch_config_intf#mether-ring *id1* **domain** *id2* **primary-port [secondary-port | transit-port | common-port | edge-port]**	Configures the type of the port of Ethernet ring. id1: instance ID of a node id2: instance ID of a domain (omitted when it is 0)
Switch_config_intf#exit	Exits from interface configuration mode.

Note:
Run **no mether-ring** *id1* **domain** *id2* **primary-port [secondary-port | transit-port | common-port | edge-port]** to delete the ring port configuration.

Browsing the State of the Ring Protection Protocol

Run the following command to browse the state of the ring protection protocol:

Command	Purpose
show mether-ring	Browses the summary information about the ring protection protocol and the ports of ring.
show mether-ring *id1* **domain** *id2*	Browses the summary information about the designated ring protection protocol and the ports of ring.

	id1: instance ID of a node id2: instance ID of a domain (omitted when it is 0)
show mether-ring *id1* **domain** *id2* **detail**	Browses the detailed information about the designated ring protection protocol and the port of Ethernet ring.
show mether-ring *id1* **domain** *id2* **interface** *intf-name*	Browses the states of the designated ring ports or those of the designated common ports.

Appendix

Working Procedure of MEAPS

MEAPS adopts three protection mechanisms to support the single-ring or level-2 multi-ring structure. The following sections shows, from the complete state to the link-down state, then to recovery and finally to the complete state again, the details of MEAPS running and the change of the MEAPS topology by typical examples.

Complete State

The complete state of the ring, which is advocated for only one ring, is monitored and maintained by the polling mechanism. In complete status, all links on the whole ring are in UP state, which finds expression in the state of the master node. In order to prevent the broadcast storm from occurring, the master node will block its secondary port. At the same time, the master node will periodically transmit the Hello packets from its primary port. These hello packets will pass through the transit node in sequence and finally return to the master node from its secondary port. The ring in complete state is shown in the following figure. The major ring and two sub rings are all in complete state. The hello packet of the major ring is only broadcast in the major ring, while the hello packet of the sub ring can be transparently transmitted through the major ring, then return to the sub ring, and finally get the secondary port of the master node on the sub ring.

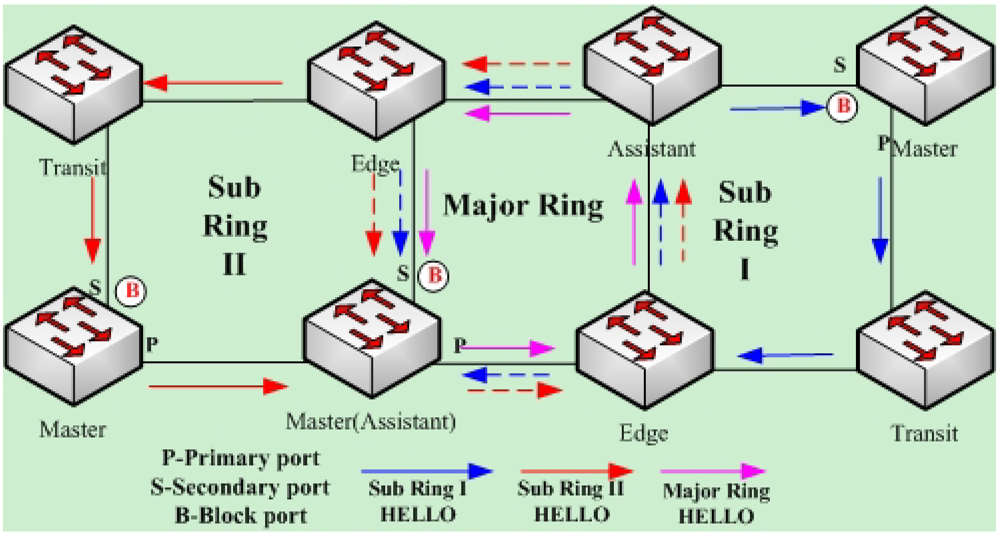


Figure 11 Complete state

Link-Down

The link-down state of the ring is decided by the polling mechanism, the notification of the link state change and the channel status checkup mechanism of the sub-ring protocol packet. Surely the link-down state of the ring is also advocated as to only one ring. When some link in the ring is in link-down state, the ring changes from the compete state to the troubled state, that is, the link-down state.

If link-down occurs on a link, the polling mechanism and the link status change notification mechanism will both function. The transit node, on which link-down occurs, will transmit the link-down packet to the master node through the Up port at its other side; at the same time, the polling mechanism will monitor and change promptly the state of the ring through Fail Time. When a trouble occurs on the sub-ring protocol channel, the trouble will be handled by the channel status checkup mechanism of the sub-ring protocol packet on the major ring. As shown in the following figure, the trouble notification message on the link of the major ring and on the common link is only transmitted on the major ring and finally transmitted to the master node; the trouble notification message on the link of sub ring 2 will be transmitted to the master node of the sub ring, which can be transparently transmitted through the major ring.

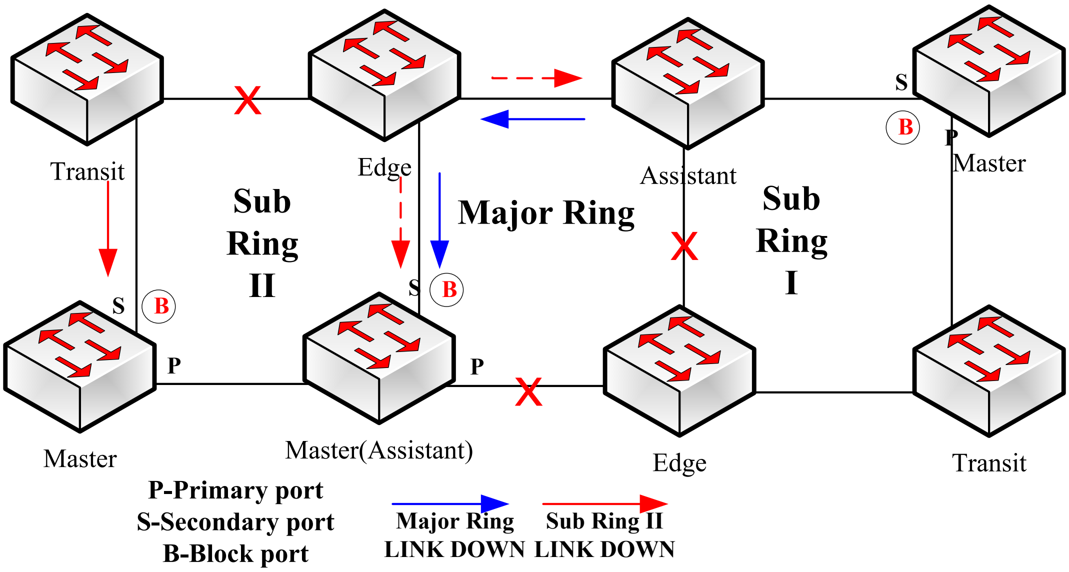


Figure 12 Ring transmitting the trouble and notifying the master node

After the master node receives the link-down packet, its state will be changed to the Failed state and at the same time the secondary port will be opened, the FDB table will be refreshed, and the RING-DOWN-FLUSH-FDB packets will be transmitted from two ports for notifying all nodes. As shown in the following figure, the master node on the major ring notifies the transit node on the major ring of refreshing FDB; sub ring 1 has troubles on its channel, so the edge port of the assistant node will be blocked; the master node of sub ring 2 notifies the transit nodes on the sub ring to refresh FDB and then the transparent transmission will be conducted on the major ring.

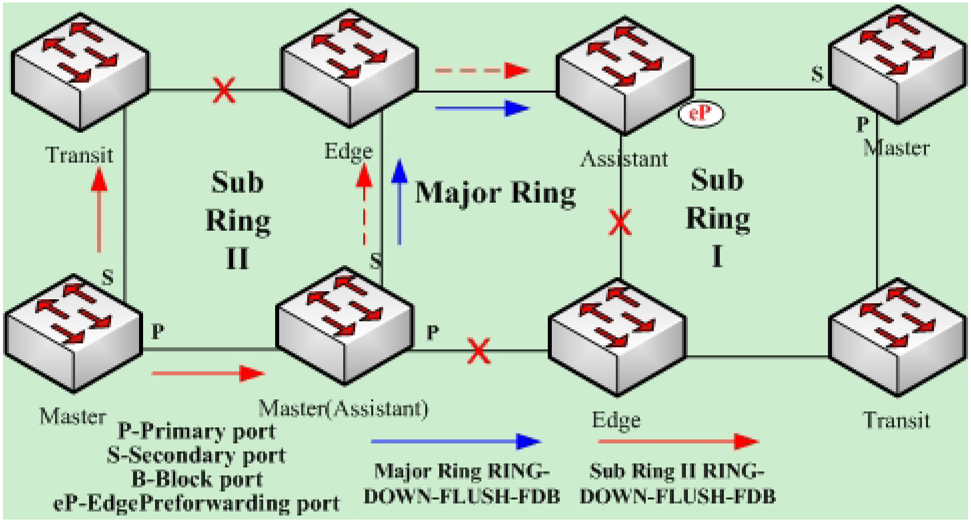


Figure 13 Ring transmitting troubles and refreshing FDB

Recovery

When the port on the transit node is recovered, the transit node will shift to its Preforwarding state. The processing procedure when the port of the transit node is recovered is shown in the following figure. The link of the major ring will recover, while the transit node, which connects the link of the major ring, changes into the Preforwarding state, blocks the data packets but allows the Hello packets of the control packet to pass through; similarly, the transit node on sub ring 2 also changes into the Preforwarding state; when the hello packet on sub ring 1 arrives the edge node, due to the fact that the resumed transit node only allows the control packet of the major to pass through and that the hell packet of sub ring 1 is just like the data packet of the major ring, the hello packet cannot be forwarded.

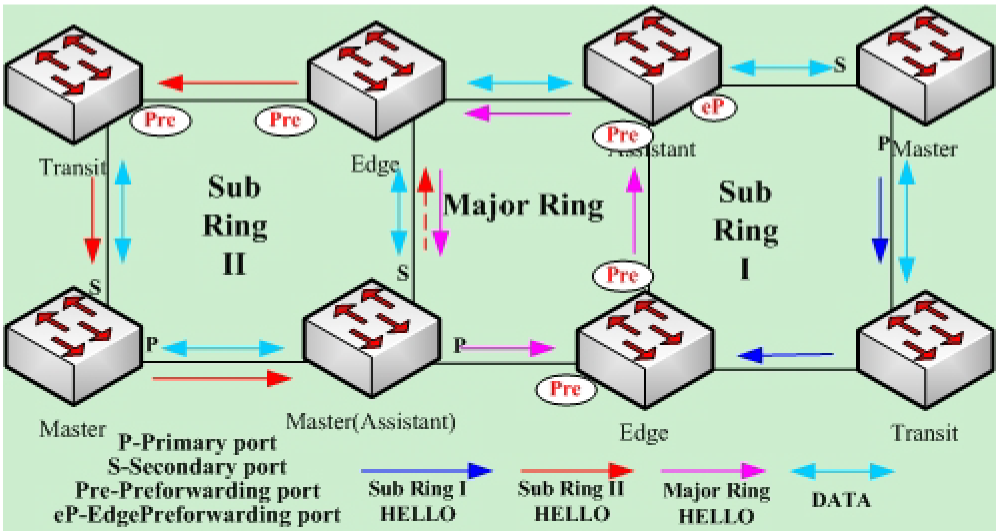


Figure 14 Recovery of the ring's link and the shift of the transit node to preforwarding

The transit port can transmit the control packet in preforwarding state, so the secondary port of the master node can receive the hello packet from the primary port. Hence, the master node shifts its state to Complete, blocks the secondary port and transmits the RING-UP-FLUSH-FDB packet from the primary port. After the transit node receives the RING-UP-FLUSH-FDB packet, the transit node will shift back to the Link-Up state, open the blocked port and refresh the FDB table. The procedure of ring recovery is shown in the following figure. The master node on the major ring changes into the complete state, blocks the secondary port, transmits the RING-UP-FLUSH-FDB packet to all transit nodes on the major ring and makes these transit nodes to shift back to their link-up state, to open the blocked port and to refresh the FDB table; similarly, the transit node and the master node on sub ring 2 also take on the corresponding change; due to the sub-ring protocol packet's channel recovery on sub ring 1, the secondary port of the master node can receive the hello packet from the primary port, and the master node shifts its state back to the complete state, blocks the secondary port, transmits the RING-UP-FLUSH-FDB packet and makes the assistant node open the edge port and sub ring 1 resume to its complete state.

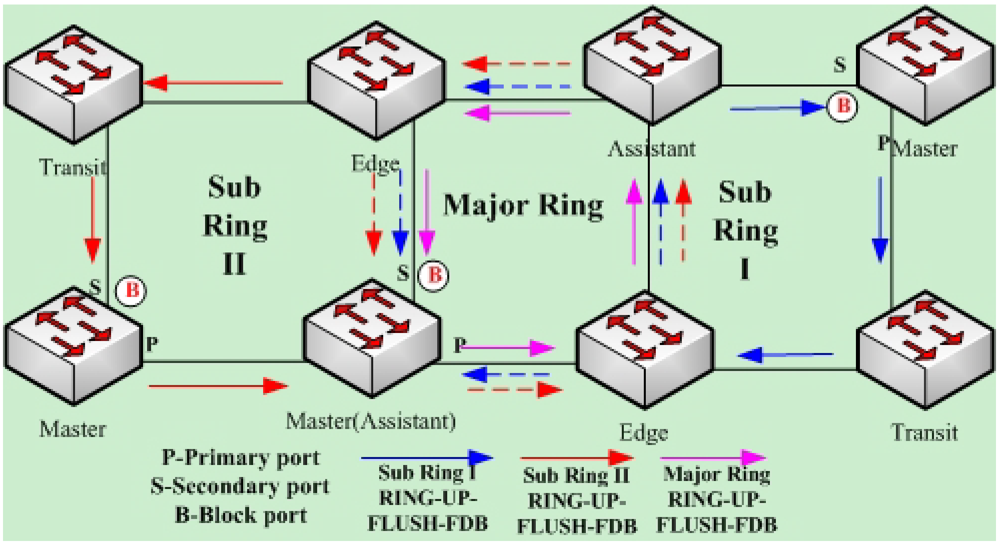


Figure 15 Recovery of the ring

Of course, if the transit node in Preforwarding state does not receive the RING-UP-FLUSH-FDB packet and Fail Time also exceeds, the transit node will open the blocked transit port and resume data communication.

MEAPS Configuration Examples

Configuration Examples

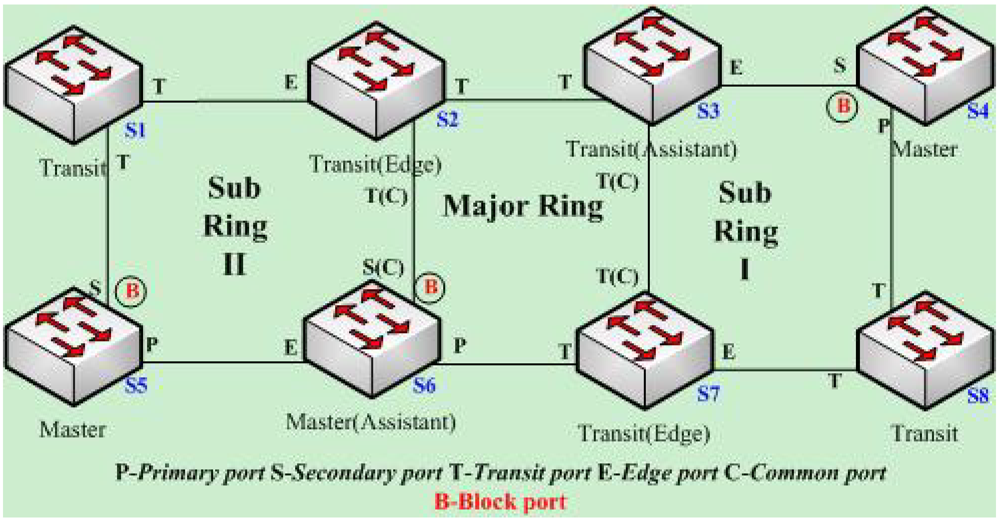


Figure 2.1 MEAPS Configuration Examples

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:

The following commands are used to set the sub-ring transit node, node 2:

```
Switch_config#mether-ring 2 domain 1
Switch_config_ring2#transit-node
Switch_config_ring2#sub-ring
Switch_config_ring2#control-vlan 2
```

The following commands are used to set the time parameter:

```
Switch_config_ring2#pre-forward-time 12
```

Exits from the node configuration mode:

```
Switch_config_ring2#quit
```

The following commands are used to set the transit port of node 2:

```
Switch_config#interface gigaEthernet 0/1
Switch_config_g0/1#mether-ring 2 domain 1 transit-port
Switch_config_g0/1#switchport mode trunk
Switch_config_g0/1#quit
Switch_config#interface gigaEthernet 0/2
Switch_config_g0/2#mether-ring 2 domain 1 transit-port
Switch_config_g0/2#switchport mode trunk
Switch_config_g0/2#quit
```

Configuring switch S2:

The following commands are used to set the major-ring transit node, node 1:

```
Switch_config#mether-ring 1 domain 1
Switch_config_ring1#transit-node
Switch_config_ring1#major-ring
Switch_config_ring1#control-vlan 2
```

The following commands are used to set the time related parameters:

```
Switch_config_ring1#pre-forward-time 12
```

Exits from the node configuration mode:

```
Switch_config_ring1#quit
```

The following commands are used to set the transit port of node 1:

```
Switch_config#interface gigaEthernet 0/1
Switch_config_g0/1#mether-ring 1 domain 1 transit-port
Switch_config_g0/1#switchport mode trunk
Switch_config_g0/1#quit
Switch_config#interface gigaEthernet 0/2
Switch_config_g0/2#mether-ring 1 domain 1 transit-port
Switch_config_g0/2#switchport mode trunk
Switch_config_g0/2#quit
```

The following commands are used to set the sub-ring edge node, node 2:

```
Switch_config#mether-ring 2 domain 1
Switch_config_ring2#edge-node
Switch_config_ring2#sub-ring (This step can be omitted.)
Switch_config_ring2#control-vlan 2
```

The following commands are used to set the time related parameters:

```
Switch_config_ring2#pre-forward-time 12
```

Exits from the node configuration mode:

```
Switch_config_ring2#quit
```

The following commands are used to set the common port and edge port of node 2:

```
Switch_config#interface gigaEthernet 0/2
Switch_config_g0/2#mether-ring 2 domain 1 common-port
Switch_config_g0/2#quit
Switch_config#interface gigaEthernet 0/3
Switch_config_g0/3#mether-ring 2 domain 1 edge-port
Switch_config_g0/3#switchport mode trunk
Switch_config_g0/3#quit
```

Configuring switch S3:

The following commands are used to set the transit port of node 1:

```
Switch_config#mether-ring 1 domain 1
Switch_config_ring1#transit-node
Switch_config_ring1#major-ring
Switch_config_ring1#control-vlan 2
```

The following commands are used to set the time related parameters:

```
Switch_config_ring1#pre-forward-time 12
```

Exits from the node configuration mode:

```
Switch_config_ring1#quit
```

The following commands are used to set the transit port of node 1:

```
Switch_config#interface gigaEthernet 0/1
Switch_config_g0/1#mether-ring 1 domain 1 transit-port
Switch_config_g0/1#switchport mode trunk
Switch_config_g0/1#quit
Switch_config#interface gigaEthernet 0/2
Switch_config_g0/2#mether-ring 1 domain 1 transit-port
Switch_config_g0/2#switchport mode trunk
Switch_config_g0/2#quit
```

The following commands are used to set the sub-ring assistant node, node 4:

```
Switch_config#mether-ring 4 domain 1
Switch_config_ring4#assistant-node
Switch_config_ring4#sub-ring (This step can be omitted.)
Switch_config_ring4#control-vlan 2
```

The following commands are used to set the time related parameters:

```
Switch_config_ring4#pre-forward-time 12
```

Exits from the node configuration mode:

```
Switch_config_ring4#quit
```

The following commands are used to set the common port and edge port of node 2:

```
Switch_config#interface gigaEthernet 0/2
Switch_config_g0/2#mether-ring 4 domain 1 common-port
Switch_config_g0/2#quit
Switch_config#interface gigaEthernet 0/3
Switch_config_g0/3#mether-ring 4 domain 1 edge-port
Switch_config_g0/3#switchport mode trunk
Switch_config_g0/3#quit
```

Configuring switch S4:

The following commands are used to set the sub-ring master node, node 4:

```
Switch_config#mether-ring 4 domain 1
Switch_config_ring4#master-node
Switch_config_ring4#sub-ring
Switch_config_ring4#control-vlan 2
```

The following commands are used to set the time related parameters:

```
Switch_config_ring4#hello-time 4
Switch_config_ring4#fail-time 12
```

Exits from the node configuration mode:

```
Switch_config_ring4#quit
```

The following commands are used to set the primary port and secondary port of node 4:

```
Switch_config#interface gigaEthernet 0/1
Switch_config_g0/1#mether-ring 4 domain 1 primary-port
Switch_config_g0/1#switchport mode trunk
Switch_config_g0/1#quit
Switch_config#interface gigaEthernet 0/2
Switch_config_g0/2#mether-ring 4 domain 1 secondary-port
Switch_config_g0/2#switchport mode trunk
```

```
Switch_config_g0/2#quit
```

Configuring switch S5:

The following commands are used to set the sub-ring master node, node 2:

```
Switch_config#mether-ring 2 domain 1
Switch_config_ring2#master-node
Switch_config_ring2#sub-ring
Switch_config_ring2#control-vlan 2
```

The following commands are used to set the time related parameters:

```
Switch_config_ring2#hello-time 4
Switch_config_ring2#fail-time 12
```

Exits from the node configuration mode:

```
Switch_config_ring2#quit
```

The following commands are used to set the primary port and secondary port of node 2:

```
Switch_config#interface gigaEthernet 0/1
Switch_config_g0/1#mether-ring 2 domain 1 primary-port
Switch_config_g0/1#switchport mode trunk
Switch_config_g0/1#quit
Switch_config#interface gigaEthernet 0/2
Switch_config_g0/2#mether-ring 2 domain 1 secondary-port
Switch_config_g0/2#switchport mode trunk
Switch_config_g0/2#quit
```

Configuring switch S6:

The following commands are used to set the major-ring master node, node 1:

```
Switch_config#mether-ring 1 domain 1
Switch_config_ring1#master-node
Switch_config_ring1#major-ring
Switch_config_ring1#control-vlan 2
```

The following commands are used to set the time related parameters:

```
Switch_config_ring1#hello-time 4
Switch_config_ring1#fail-time 12
```

Exits from the node configuration mode:

```
Switch_config_ring1#quit
```

The following commands are used to set the transit port of node 1:

```
Switch_config#interface gigaEthernet 0/1
Switch_config_g0/1#mether-ring 1 domain 1 primary-port
Switch_config_g0/1#switchport mode trunk
Switch_config_g0/1#quit
Switch_config#interface gigaEthernet 0/2
Switch_config_g0/2#mether-ring 1 domain 1 secondary-port
Switch_config_g0/2#switchport mode trunk
Switch_config_g0/2#quit
```

The following commands are used to set the sub-ring assistant node, node 2:

```
Switch_config#mether-ring 2 domain 1
Switch_config_ring2#assistant-node
Switch_config_ring2#sub-ring (This step can be omitted.)
```

```
Switch_config_ring2#control-vlan 2
```

The following commands are used to set the time related parameters:

```
Switch_config_ring2#pre-forward-time 12
```

Exits from the node configuration mode:

```
Switch_config_ring2#quit
```

The following commands are used to set the common port and edge port of node 2:

```
Switch_config#interface gigaEthernet 0/2
Switch_config_g0/2#mether-ring 2 domain 1 common-port
Switch_config_g0/2#quit
Switch_config#interface gigaEthernet 0/3
Switch_config_g0/3#mether-ring 2 domain 1 edge-port
Switch_config_g0/3#switchport mode trunk
Switch_config_g0/3#quit
```

Configuring switch S7:

The following commands are used to set the major-ring transit node, node 1:

```
Switch_config#mether-ring 1 domain 1
Switch_config_ring1#transit-node
Switch_config_ring1#major-ring
Switch_config_ring1#control-vlan 2
```

The following commands are used to set the time related parameters:

```
Switch_config_ring1#pre-forward-time 12
```

Exits from the node configuration mode:

```
Switch_config_ring1#quit
```

The following commands are used to set the transit port of node 1:

```
Switch_config#interface gigaEthernet 0/1
Switch_config_g0/1#mether-ring 1 domain 1 transit-port
Switch_config_g0/1#switchport mode trunk
Switch_config_g0/1#quit
Switch_config#interface gigaEthernet 0/2
Switch_config_g0/2#mether-ring 1 domain 1 transit-port
Switch_config_g0/2#switchport mode trunk
Switch_config_g0/2#quit
```

The following commands are used to set the secondary port of node 4:

```
Switch_config#mether-ring 4 domain 1
Switch_config_ring4#edge-node
Switch_config_ring4#sub-ring (This step can be omitted.)
Switch_config_ring4#control-vlan 2
```

The following commands are used to set the time related parameters:

```
Switch_config_ring4#pre-forward-time 12
```

Exits from the node configuration mode:

```
Switch_config_ring4#quit
```

The following commands are used to set the common port and edge port of node 2:

```
Switch_config#interface gigaEthernet 0/2
```

```
Switch_config_g0/2#mether-ring 4 domain 1 common-port
Switch_config_g0/2#quit
Switch_config#interface gigaEthernet 0/3
Switch_config_g0/3#mether-ring 4 domain 1 edge-port
Switch_config_g0/3#switchport mode trunk
Switch_config_g0/3#quit
```

Configuring switch S8:

The following commands are used to set the sub-ring transit node, node 4:

```
Switch_config#mether-ring 4 domain 1
Switch_config_ring4# transit -node
Switch_config_ring4#sub-ring
Switch_config_ring4#control-vlan 2
```

The following commands are used to set the time related parameters:

```
Switch_config_ring4#pre-forward-time 12
```

Exits from the node configuration mode:

```
Switch_config_ring4#quit
```

The following commands are used to set the transit port of node 4:

```
Switch_config#interface gigaEthernet 0/1
Switch_config_g0/1#mether-ring 4 domain 1 transit -port
Switch_config_g0/1#switchport mode trunk
Switch_config_g0/1#quit
Switch_config#interface gigaEthernet 0/2
Switch_config_g0/2#mether-ring 4 domain 1 transit -port
Switch_config_g0/2#switchport mode trunk
Switch_config_g0/2#quit
```

Unfinished Configurations (to be continued)

Unfinished basic information configuration: there is one of the ring’s role, the ring’s grade and the control VLAN unset. One exceptional case is that when a node’s role has configured to be the edge node or assistant node, the default ring's grade is sub-ring.

Contradiction of basic information: When a node’s role is edge-node or assistant-node, the default ring's grade is sub-ring; when the ring’s grade is major-ring, prompt information will appear.

Sub ring having no corresponding major-ring node: When a node’s role is edge-node or assistant-node, this node is borne on the major-ring node; if there is no corresponding major-ring node to compulsorily create the sub-ring edge node or sub-ring assistant node, prompt information will appear (in this case, you can use the show command to browse the MEAPS state; if you find the basic information is complete but the state is init, it indicates that the configuration of the ring’s node has not finished).

Conflicts arising during control VLAN configuration: If the control VLAN, which is configured by a node, conflicts with other configured nodes, prompt information will appear (in this case, you can use the show command to browse the MEAPS state; if you find the basic information is complete but the state is init, it indicates that the configuration of the ring’s node has not finished).

When configuring the sub-ring node according to the major ring node, the id of the sub-ring node must be greater than the ID of the major ring node. Otherwise, here pops up a prompt.

23. UDLD Configuration

Unidirectional Link Detection (UDLD)

UDLD Overview

UDLD is a L2 protocol that monitors the physical location of the cable through the devices which are connected by optical cable or twisted-pair, and detects whether the unidirectional link exists. Only when the connected device supports UDLD can the unidirectional link be detected and shut down. The unidirectional link can cause a lot of problems, including the STP topology ring. Hence, when detecting a unidirectional link, UDLD will shut down the affected interface and notify uses.

UDLD works with the physical-layer protocol mechanism to judge the status if the physical link. On the physical layer, the physical signals and incorrect detections are automatically negotiated and processed, while UDLD processes other matters, such as detecting the ID of a neighbor and shutting down the incorrect connection port. If you enable automatic negotiation and UDLD, the detection at layer 1 and layer 2 can prevent physical/logical links and other protocols' problems.

UDLD Mode

UDLD supports two modes, the normal mode (default) and the aggressive mode. In normal mode, UDLD can detect the existence of a unidirectional link according to the unidirectional services of the link. In aggressive mode, UDLD can detect not only the existence of a unidirectional link as in the previous mode but also connection interruption which cannot be detected by L1 detection protocols.

In **normal** mode, if UDLD determines that the connection is gone, UDLD will set the state of the port to **undetermined**, not to **down**. In **aggressive** mode, if UDLD determines that the link is gone and the link cannot be reconnected, it is thought that interrupted communication is a severe network problem and UDLD will set the state of the protocol to **linkdown** and the port is in **errdisable** state. No matter in what mode, if UDLD maintains it is a bidirectional link, the port will be set to **bidirectional**.

In **aggressive** mode, UDLD can detect the following cases of the unidirectional link:

On the optical fiber or the twisted pair, an interface cannot receive or transmit services.

On the optical fiber or the twisted pair, the interface of one terminal is down and the interface of the other terminal is up.

One line in the optical cable is broken, and therefore the data can only be transmitted or only be received.

In previous cases, UDLD will shut down the affected interface.

Running Mechanism

UDLD is a L2 protocol running on the LLC layer, which uses 01-00-0c-cc-cc-cc as its destination MAC address. SNAP HDLC is similar to 0x0111. When it runs with layer-1 FEFI and automatic negotiation, the completeness of a link in the physical layer and the logical link layer can be checked.

UDLD can provide some functions that FEFI and automatic negotiation cannot conduct, such as checking and caching the neighbor information, shutting down any mis-configured port and checking the faults and invalidation on the logical ports except the point-to-point logical ports.

UDLD adopts two basic mechanisms: learn the information about neighbors and save it in the local cache. When a new neighbor is detected or a neighbor applies for synchronizing the cache again, a series of UDLD probe/echo (hello) packets will be transmitted.

UDLD transmits the probe/echo packets on all ports and, when a UDLD echo information is received on the ports, a detection phase and an authentication process are triggered. If all effective conditions are satisfied (port is connected in two directions and the cable is correctly connected), this port will be up. Otherwise, the port will be down.

Once a link is established and labeled as bidirectional, UDLD will transmit a probe/echo message every 15 seconds.

State of the Port

The UDLD interface may be in one of the following states:

Port state	Remark
Detection	Means that the interface is in detection state.
Unknown	Means that the interface is in unknown state, that is, it may be in detection state or it has not conducted detection.
Unidirectional	Means that the unidirectional connection has been detected.
Bidirectional	Means that the bidirectional connection has been detected.

Maintaining the Cache of the Neighbor

UDLD transmits the Probe/Echo packets regularly on each active interface to maintain the completeness of the neighbor’s cache. Once a Hello message is received, it will be saved in the memory temporally and an interval that is defined by hold-time will also be saved. If the hold-time times out, the corresponding cache is fully cleared. If a new Hello message is received in the hold-time, the new Hello message will replace the old one and the timer will be reset to zero.

Once a UDLD-running interface is disabled or the device on the interface is restarted, all the caches on the interface will be removed to maintain the completeness of the UDLD cache. UDLD transmits at least one message to notify the neighbor to remove the corresponding cache items.

Echo Detection

The echo mechanism is the basis of the detection algorithm. Once a UDLD device learns a new neighbor or another synchronization request from an asynchronous neighbor, it will start or restart the detection window of the local terminal and transmit an echo message for full agreement. Because all neighbors are demanded a corresponding action, the echo sender expects an **echos** message. If the checkup window is over before a legal echo is received, this link is thought to be a unidirectional one. In this case, link reconnection will be triggered or the **link down** process on the port is enabled.

UDLD Configuration Task List

Globally Enabling or Disabling UDLD

Enabling or Disabling the UDLD Interface

Setting the Message Interval of the Aggressive Mode

Restarting the Interface Shut Down by UDLD

Displaying the UDLD State

UDLD Configuration Tasks

Globally Enabling or Disabling UDLD

In global configuration mode, run the following command to enable the UDLD function of all interfaces.

Command	Purpose
udld [enable | aggressive]	Enables the UDLD modules of all interfaces in some mode.

In global configuration mode, run the following command to disable the UDLD function of all interfaces.

Command	Purpose
no udld [enable | aggressive]	Shuts down the UDLD modules of all interfaces.

Note: If you enable or disable the UDLD function in global configuration mode, the UDLD function will be performed on all interfaces.

UDLD of the Aggressive mode is a variation of UDLD, which can provide extra benefits. When UDLD is in aggressive mode and the port stops transmitting the UDLD packets, UDLD will try to establish a link with its neighbor again. If the times of tries exceed a certain number, the state of the port is changed into the Error-Disable state and the link of the port is down. When UDLD is running, the ports at both terminals should run in the same mode, or the expecting result cannot be obtained.

Enabling or Disabling the UDLD Interface

In interface configuration mode, run the following command to enable the UDLD function of an interface.

Command	Purpose
udld port [**aggressive**]	Enables the UDLD module of an interfaces in

	some mode. If the **aggressive** parameter is not entered, the UDLD function of the interface is enabled in **normal** mode; if the **aggressive** parameter is entered, the UDLD function of the interface is enabled in **aggressive** mode.

In interface configuration mode, run the following command to disable the UDLD function of an interface.

Command	Purpose
no udld port [**aggressive**]	Disables the UDLD module of the interface by entering the corresponding command in some mode.

Note: When UDLD is running, the ports at both terminals should run in the same mode, or the expecting result cannot be obtained.

Setting the Message Interval of the Aggressive Mode

In global configuration mode, run the following command to set the message interval of the aggressive mode.

Command	Purpose
udld message *time*	Sets the message interval of the aggressive mode.

Restarting the Interface Shut Down by UDLD

In the EXEC mode, run the following command to restart the interface that is shut down by the UDLD module.

Command	Purpose
udld reset	Restarts the interface shut down by UDLD.

Displaying the UDLD State

Run the following command to display the states of the UDLD modules of all current interfaces.

Command	Purpose
show udld	Displays the states of the UDLD modules of all current interfaces.

Run the following command to display the state of the UDLD module of the specified interface.

Command	Purpose

show udld *interface*	Displays the state of the UDLD module of the specified interface.

The UDLD displaying command is used to browse the state and the mode of UDLD, the current detection state, the state of the current link and some information about the neighbors.

It is used to display the running states of the UDLD modules of the current interfaces.

```
Switch#show udld

Interface FastEthernet0/1
---
Port enable administrative configuration setting: Enabled
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisment
Message interval: 15
Time out interval: 5
          Entry 1
          ---
          Expiration time: 42
          Cache Device index: 1
          Device ID: CAT0611Z0L9
          Port ID: FastEthernet0/1
          Neighbor echo 1 device: S35000202
          Neighbor echo 1 port: FastEthernet0/1

          Message interval: 15
          Time out interval: 5
          UDLD Device name: Switch

Interface FastEthernet0/2
---
Port enable administrative configuration setting: Disabled
Port enable operational state: Disabled
Current bidirectional state: Unknown

Interface FastEthernet0/3
---
Port enable administrative configuration setting: Disabled
Port enable operational state: Disabled
Current bidirectional state: Unknown

……………………
```

It is used to display the operational state of the UDLD module of the current interface.

```
Switch#show udld interface f0/1
Interface FastEthernet0/1
---
Port enable administrative configuration setting: Enabled
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisment
Message interval: 15
Time out interval: 5
        Entry 1
        ---
        Expiration time: 42
        Cache Device index: 1
        Device ID: CAT0611Z0L9
        Port ID: FastEthernet0/1
        Neighbor echo 1 device: S35000202
        Neighbor echo 1 port: FastEthernet0/1

        Message interval: 15
        Time out interval: 5
        UDLD Device name: Switch
```

Configuration Example

Network Environment Requirements

Configure the UDLD protocol on the ports that connect two MY COMPANY S3524 switches.

Network Topology

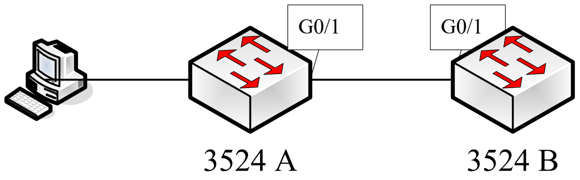


Figure 2 Network topology

Configuration Procedure

Configuring Switch A:

```
Switch_config#udld enable
Switch_config#interface g0/1
Switch_config_g0/1#udld port
Switch_config_g0/1#quit
```

Configuring Switch B:

```
Switch_config#udld enable
Switch_config#interface g0/1
Switch_config_g0/1#udld port
Switch_config_g0/1#quit
```

Entering the **show** command on Switch A:

```
Switch_config#show udld interface g0/1

Interface GigaEthernet0/1
---
Port enable administrative configuration setting: Enabled
Port enable operational state: Enabled
Current bidirectional state: Unknown
Current operational state: Detection
Message interval: 15
Time out interval: 1
        Entry 1
        ---
        Expiration time: 44
        Cache Device index: 1
        Device ID: S35043000
        Port ID: GigaEthernet0/1
        Neighbor echo 1 device: S32030079
        Neighbor echo 1 port: GigaEthernet0/1

        Message interval: 15
        Time out interval: 1
        UDLD Device name: SwitchB
Switch_config#
Switch_config#show udld interface g0/1

Interface GigaEthernet0/1
---
Port enable administrative configuration setting: Enabled
Port enable operational state: Enabled
Current bidirectional state: Unknown
Current operational state: Advertisment
Message interval: 15
Time out interval: 7
        Entry 1
        ---
        Expiration time: 43
        Cache Device index: 1
        Device ID: S35043000
        Port ID: GigaEthernet0/1
        Neighbor echo 1 device: S32030079
        Neighbor echo 1 port: GigaEthernet0/1

        Message interval: 15
        Time out interval: 7
        UDLD Device name: SwitchB
Switch_config#
Switch_config#show udld interface g0/1

Interface GigaEthernet0/1
---
Port enable administrative configuration setting: Enabled
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisment
Message interval: 15
Time out interval: 15
        Entry 1
        ---
        Expiration time: 36
        Cache Device index: 1
        Device ID: S35043000
        Port ID: GigaEthernet0/1
        Neighbor echo 1 device: S32030079
        Neighbor echo 1 port: GigaEthernet0/1

        Message interval: 15
        Time out interval: 15
        UDLD Device name: SwitchB
Switch_config#
```

From the information above, you can find the three phases of the link state which UDLD detects:

Detection phase: In this phase, the UDLD packets are transmitted every other second.

Unknown phase: In this phase, the UDLD packets are transmitted every eight seconds.

Known bidirectional/unidirectional connection phase: Once a link is established and labeled as bidirectional, UDLD will transmit a probe/echo message every 16 seconds.

24. IGMP-SNOOPING Configuration

IGMP-snooping Configuration Task

The task of IGMP-snooping is to maintain the relationships between VLAN and group address and to update simultaneously with the multicast changes, enabling switches to forward data according to the topology structure of the multicast group.

The main functions of IGMP-snooping are shown as follows:

Listening IGMP message;

Maintaining the relationship table between VLAN and group address;

Keeping the IGMP entity of host and the IGMP entity of router in the same state to prevent flooding from occurring.

Note:

Because igmp-snooping realizes the above functions by listening the **query** message and **report** message of igmp, igmp-snooping can function properly only when it works on the multicast router, that is, the switch must periodically receive the igmp **query** information from the router. The **router age** timer of igmp-snooping must be set to a time value that is bigger than the group query period of the multicast router connecting igmp-snooping. You can check the multicast router information in each VLAN by running **show ip igmp-snooping**.

Enabling/Disabling IGMP-snooping of VLAN

Adding/Deleting static multicast address of VLAN

Configuring immediate-leave of VLAN

Configuring Static Routing Interface of VLAN

Configuring IPACL of Generating Multicast Forward Table

Configuring the function to filter multicast message without registered destination address

Configuring the Router Age timer of IGMP-snooping

Configuring the Response Time timer of IGMP-snooping

Configuring IGMP Querier of IGMP-snooping

Configuring IGMP-snooping's Querier Time Timer

Configuring data forwarding of IGMP-snooping's forward-l3-to-mrouter to router port

Configuring sensitive mode and value for IGMP-snooping

Configuring IGMP-snooping's v3-leave-check function

Configuring IGMP-snooping's forward-wrongiif-within-vlan function

Configuring IPACL function at IGMP-snooping's port

Configuring maximum multicast IP address quantity function at IGMP-snooping's port

Monitoring and maintaining IGMP-snooping

IGMP-snooping configuration example

Enabling/Disabling IGMP-Snooping of VLAN

Perform the following configuration in global configuration mode:

Command	Description
ip igmp-snooping [**vlan** *vlan_id*]	Enables IGMP-snooping of VLAN.
no ip igmp-snooping [**vlan** *vlan_id*]	Resumes the default configuration.

If vlan is not specified, all vlans in the system, including vlans created later, can be enabled or disabled.

In the default configuration, IGMP-snooping of all VLANs is enabled, just as the **ip igmp-snooping** command is configured.

Note: IGMP-snooping can run on up to 16 VLANs.

To enable IGMP-snooping on VLAN3, you must first run **no ip IGMP-snooping** to disable IGMP-snooping of all VLANs, then configure **ip IGMP-snooping VLAN 3** and save configuration.

Adding/Deleting Static Multicast Address of VLAN

Hosts that do not support IGMP can receive corresponding multicast message by configuring the static multicast address.

Perform the following configuration in global configuration mode:

Command	Description
ip igmp-snooping vlan *vlan_id* **static** *A.B.C.D* **interface** *intf*	Adds static multicast address of VLAN.
no ip igmp-snooping vlan *vlan_id* **static** *A.B.C.D* **interface** *intf*	Deletes static multicast address of VLAN.

Configuring immediate-leave of VLAN

When the characteristic immediate-leave is configured, the switch can delete the port from the port list of the multicast group after the switch receives the **leave** message. The switch, therefore, does not need to enable the timer to wait for other hosts to join the multicast. If other hosts in the same port belongs to the same group and their users do not want to leave the group, the multicast communication of these users may be affected. In this case, the **immediate-leave** function should not be enabled.

Perform the following configuration in global configuration mode:

Command	Description
ip igmp-snooping vlan *vlan_id* **immediate-leave**	Configures the **immediate-leave** function of the VLAN.

no ip igmp-snooping vlan *vlan_id* **immediate-leave**	Sets immediate-leave of VLAN to its default value.

The **immediate-leave** characteristic of VLAN is disabled by default.

Configuring immediate-leave of port

When the characteristic immediate-leave is configured on a port, the switch can delete the port from the port list of the multicast group after the switch receives the **leave** message. The switch, therefore, does not need to enable the timer to wait for other hosts to join the multicast. If other hosts in the same port belongs to the same group and their users do not want to leave the group, the multicast communication of these users may be affected. In this case, the **immediate-leave** function should not be enabled.

The immediate-leave configuration of the port and the immediate-leave configuration of the VLAN work simultaneously.

Perform the following configuration in interface configuration mode:

Command	Description
ip igmp-snooping immediate-leave	Configures the **immediate-leave** function of the port.
no ip igmp-snooping immediate-leave	Sets immediate-leave of the port to its default value.

By default, the immediate-leave feature of a port is disabled.

Configuring Static Routing Interface of VLAN

Configure the static routing interface and send the multicast packet to the routing port. The switch will send the multicast report packets to all routing ports in vlan.

Run following commands in the global configuration mode:

Command	Purpose
ip igmp-snooping vlan *vlan_id* **mrouter interface** *intf*	Add the static routing port of VLAN.
no ip igmp-snooping vlan *vlan_id* **mrouter interface** *intf*	Delete the static routing port of VLAN.

Configuring IPACL of Generating Multicast Forward Table

Run following commands in global configuration mode to configure IPACl. Thus, The rules and limitations of generating the multicast forwarding table after receiving packets of igmp report can be set.

Command	Purpose

ip igmp-snooping policy *word*	Adds IPACL in generating multicast forwarding table.
no ip igmp-snooping policy	Deletes IPACL in generating multicast forwarding table.

Configuring the Function to Filter Multicast Message Without Registered Destination Addresss

When multicast message target fails to be found (DLF, the destination address is not registered in the switch chip through igmp-snooping), the default process method is to send message on all ports of VLAN.Through configuration, you can change the process method and all multicast messages whose destination addresses are not registered to any port will be dropped.

Command	Description
ip igmp-snooping dlf-drop	Drops multicast message whose destination fails to be found.
no ip igmp-snooping dlf-drop	Resumes the fault configuration (forward).

Note:

The attribute is configured for all VLANs.

The default method for the switch to handle this type of message is forward (message of this type will be broadcasted within VLAN).

Configuring Router Age Timer of IGMP-snooping

The **Router Age** timer is used to monitor whether the IGMP inquirer exists. IGMP inquirers maintains multicast addresses by sending **query** message. IGMP-snooping works through communication between IGMP inquier and host.

Perform the following configuration in global configuration mode:

Command	Description
ip igmp-snooping timer router-age *timer_value*	Configures the value of Router Age of IGMP-snooping.
no ip igmp-snooping timer router-age	Resumes the default value of Router Age of IGMP-snooping.

Note:

For how to configure the timer, refer to the query period setup of IGMP inquirer. The timer cannot be set to be smaller than query period. It is recommended that the timer is set to three times of the query period.

The default value of Router Age of IGMP-snooping is 260 seconds.

Configuring Response Time Timer of IGMP-Snooping.

The **response time** timer is the upper limit time that the host reports the multicast after IGMP inquirer sends the **query** message. If the **report** message is not received after the timer ages, the switch will delete the multicast address.

Perform the following configuration in global configuration mode:

Command	Description
ip igmp-snooping timer response-time timer_value	Configures the value of Response Time of IGMP-snooping.
no ip igmp-snooping timer response-time	Resumes the default value of Response Time of IGMP-snooping.

Note:

The timer value cannot be too small. Otherwise, the multicast communication will be unstable.

The value of Response Time of IGMP-snooping is set to 15 seconds.

Configuring Querier of IGMP-Snooping

If the multicast router does not exist in VLAN where IGMP-snooping is activated, the **querier** function of IGMP-snooping can be used to imitate the multicast router to regularly send IGMP **query** message. (The function is global, that is, it can be enabled or disabled in VLAN where IGMP-snooping is globally enabled)

When the multicast router does not exist in LAN and multicast flow does not need routing, the automatic query function of the switch can be activated through IGMP snooping, enabling IGMP snooping to work properly.

Perform the following configuration in global configuration mode:

Command	Description
[**no**] **ip igmp-snooping querier [address** *[ip_addr*]	Configures the querier of IGMP-snooping. The optional parameter **address** is the source IP address of **query** message.

The **IGMP-snooping querier** function is disabled by default. The source IP address of fake **query** message is 10.0.0.200 by default.

Note:

If the **querier** function is enabled, the function is disabled when the multicast router exists in VLAN; the function can be automatically activated when the multicast router times out.

Configuring IGMP-snooping’s Querier Time Timer

Querier Time Timer is the time interval when switch as local IGMP querier sends messages. Timer broadcasts query message within VLAN after aging.

Configure as following under global configuration mode:

Command	Operation
ip igmp-snooping querier querier-timer *timer_value*	Configuring the value of IGMP-snooping's Querier Time
no ip igmp-snooping querier querier-timer	Recovering IGMP-snooping's Querier Time as default

By default IGMP-snooping querier is shut down. The default time interval of Query messages is 200 seconds.

Notice:

If Querier function is initiated, querier-timer should not be set as too long. In subnet if there are other switches with querier initiated, long querier-timer (longer than other switch's router-age) would lead to the instablization of querier selection in subnet.

Configuring data forwarding of IGMP-snooping's forward-l3-to-mrouter to router port

If L3 multicast feature is initiated and igmp-snooping does not join messages to downstream port, only downstream vlan port can be learnt by multicast route. If forward-l3-to-mrouter function is intiated, all the downstream router ports can be learnt. Data messages could be sent to multicast router pot registered by PIM-SM message not broadcasting messages to all downstream physical port. The command is mainly used under the following conditions.

When multiple switches initiate L3 multicast cascadingly, the upstream device can only learn downstream vlan ports by multicast router protocol. The upstream and downstream devices do not have interactive igmp messages, therefore, the upstream devices' snooping cannot learn the specific physical ports connected with downstream devices. When upstream devices forward multicast flows, they would send them to all physical port in vlan. When this function is initiated, messages could be forwarded to physical ports which connect with downstream devices, and messages would not be broadcasted in downstream vlan.

Configure as following under global configuration mode:

Command	Operation
[**no**] **ip igmp-snooping forward-l3-to-mrouter**	Configuring IGMP-snooping's forward-l3-to-mrouter function.

Under default condition, IGMP-snooping forward-l3-to-mrouter is shut down

Notice:

This command could forward data messages to multicast router port, but switching chip has restraining function on source data port. Therefore, messages would not be forwarded to source data port, but only to downstream router port registered by PIM-SM.

Configuring sensitive mode and value for IGMP-snooping

If IGMP-snooping's sensitive mode is enabled, when port at trunk mode is shut down, set router-age time of mrouter at active status as sensitive value, and send out query message quickly.

Configure as following under global configuration mode:

Command	Operation
[**no**] **ip igmp-snooping sensitive** [value [3-30]]	Configuring IGMP-snooping's sensitive and value could be router-age time of currently active mrouter.

By default IGMP-snooping sensitive is disabled.

Notice:

When it is sensitive mode, sensitive value is used to update router-age aiming at current one time period. Next time, route-age is recovered as configured time router-age time.

Configuring IGMP-snooping's v3-leave-check function

If IGMP-snooping's v3-leave-check feature is enabled, send special query message after receiving v3's leave message. Otherwise, no operation is processed.

Configure as following under global configuration mode:

Command	Operation
[**no**] **ip igmp-snooping v3-leave-check**	Configuring IGMP-snooping's v3-leave-check. Send special query message after receiving v3 leave message.

Configuring IGMP-snooping's forward-wrongiif-within-vlan function

If IGMP-snooping's forward-wrongiif-within-vlan function is enabled, do L2 forwarding of the multicast data message received from wrong vlan interface port within source vlan. Forward messages to the group member ports in the vlan. Otherwise, drop messages.

Configure as following under global configuration mode:

Command	Operation
[**no**] **ip igmp-snooping forward-wrongiif-within-vlan**	Configuring IGMP-snooping's forward-wrongiif-within-vlan and forwarding relative group member ports within the vlan

By default IGMP-snooping forward-wrongiif-within-vlan is enabled.

Notice:

Command ip igmp-snooping forward-wrongiif-within-vlan is only meaningful when L3 multicast is enabled.

Configuring IGMP-snooping’s IPACL function at port

If IGMP-snooping’s IPACL function at port is enabled, use IPACL at port to assign whether messages of some multicast IP address need to be dealt with or ignored.

Configure as following under physical port configuration mode:

Command	Purpose
ip igmp-snooping policy *word*	Adding multicast message’s IPACL which need to be dealt with port.
no ip igmp-snooping policy	Deleteding multicast message’s IPACL which need to be dealt with port.

Configuring IGMP-snooping’s multicast filtering in VLAN

If IGMP-snooping multicast filtering in the VLAN is enabled, only the multicast group report request in the filtering list will be accepted and added to the group in the VLAN, otherwise it will be discarded and no group will be added.

Configure as following in global configuration mode:

Command	Purpose
ip igmp-snooping vlan *value* **filter** *vlanid-list*	Configure IGMP-snooping’s multicast filtering in VLAN. The parameter vlanid-list is VLAN ID list connected with "," and "-". Note that "," and "-" must be followed by at least one space.
ip igmp-snooping vlan *value* **filter** *vlanid-list*	Remove multicast filtering in VLAN

Configuring maximum multicast IP address quantity function at IGMP-snooping’s port

If configuring the maximum multicast IP address quantity at IGMP-snooping port, the quantity of applied groups at the port would be judged whether it is beyond the configured maximum quantity when IGMP-snooping generates forwarding entry. If it is beyond the maximum quantity, the port’s entry would not be generated.

Configure as following under physical port configuration mode:

Command	Operation
[**no**] **ip igmp-snooping limit** [value [1-2048]]	configuring the maximum multicast IP address quantity at IGMP-snooping port

By default the maximum quantity is 2048 at IGMP-snooping.

Configuring IGMP-snooping's report-suppression function

If the report-suppression function of IGMP-snooping is configured, in the same VLAN, regardless of whether the client initiates the request in the initial state or responds to the query, the switch forwards limited number to the mrouter port. The number of forwarding is determined by the parameter after **max-number**, and the range is 1-5. If the max-number keyword is omitted, the number of forwarding is 1 by default.

When the IGMP Snooping function is normal, this configuration can reduce the processing cost of the local switch and the upstream switch, and save the bandwidth for forwarding report packets.

Configure as following in global configuration mode:

Command	Operation
[**no**] **ip igmp-snooping report-suppression** [**max-number** value [1-5]]	Configure the IGMP-snooping report-suppression and its report maximum forwarding number.

By default, IGMP-snooping report-suppression function is disabled

If **ip igmp-snooping report-suppression** is configured without keyword max-number, the number of report forwards is 1 by default.

Configuring IGMP-snooping's proxy-leave function

If the IGMP-snooping proxy-leave function is configured, in the same VLAN, the switch sends the leave message of the multicast group to the upstream device only after all members of a multicast group have truly left the group.

When the IGMP Snooping function is normal, this configuration can reduce the processing cost of the local switch and the upstream switch, and save the bandwidth for forwarding leave packets.

Configure as following in global configuration mode:

Command	Operation
[**no**] **ip igmp-snooping proxy-leave**	Configure IGMP-snooping's proxy-leave function

By default, IGMP-snooping proxy-leave function is disabled.

Monitoring and Maintaining IGMP-Snooping

Perform the following operations in management mode:

Command	Description
show ip igmp-snooping	Displays IGMP-snooping configuration information.
show ip igmp-snooping timer	Displays the clock information of IGMP-snooping.

show ip igmp-snooping group	Displays information about the multicast group of IGMP-snooping.
show ip igmp-snooping group interface	Displays information about the multicast group of IGMP-snooping in port.
show ip igmp-snooping statistics [message|packet|hardware|vlan *vlanid***]**	Displays statistics information about IGMP-snooping.
show ip igmp-snooping vlan	Displays vlan information of IGMP-snooping.
[**no**] **debug ip igmp-snooping** [**packet** | **timer** | **event** | **error**]	Enables and disables packet/clock debug/event/mistake print switch of IGMP-snooping. If the debug switch is not specified, all debug switches will be enabled or disabled.

Display VLAN information about IGMP-snooping running:

```
switch # show ip igmp-snooping
Global IGMP snooping configuration:
----------------------------------
Globally enable          : Enabled
VLAN nodes                   : 1,50,100,200,400,500
Dlf-frames filtering : Disabled
Sensitive                    : Disabled
Querier                        : Enabled
Querier address          : 10.0.0.200
Querier interval        : 140 s
Router age                   : 260 s
Response time              : 15 s

   vlan_id     Immediate-leave     Ports     Router Ports
------------------------------------------------------------
       1             Disabled            5-10        SWITCH(querier);
      50             Disabled            1-4        SWITCH(querier);
     100             Disabled            NULL        SWITCH(querier);G0/1(static);
     200             Disabled            NULL        SWITCH(querier);
     400             Disabled            NULL        SWITCH(querier);
     500             Disabled            NULL        SWITCH(querier);
```

Display information about the multicast group of IGMP-snooping:

```
switch# show ip igmp-snooping group
            The total number of groups            2

 Vlan Group            Type Port(s)
---- -------------- ---- ---------------------------------------------------
 1 226.1.1.1           IGMP G0/1                      G0/3
 1 225.1.1.16          IGMP G0/1                             G0/3
```

Display the IGMP-snooping multicast group information added on the port:

```
Switch#show ip igmp-snooping group interface g0/4

Number of joined groups: 1

Vlan Group              Mode      Source Num
---- -------------- ------- ----------
     2 230.1.1.1          Exclude     0
```

Display IGMP-snooping timer:

```
switch#show ip igmp-snooping timers
vlan 1 router age : 251 Indicating the timeout time of the router age timer
vlan 1 multicast address 0100.5e00.0809 response time : 1    Indicating the period from when the last
  multicast group query message is received to the current time; if no host on the port respond when
  the timer times out, the port will be deleted..
```

Display IGMP-snooping statistics:

```
        Switch_config#show ip igmp-s statistics

        IGMP Snooping Message Statistics
        -----------------------------------
        L2 main messages sent OK         : 75
        L2 main messages sent failed     : 0
        L2 packets received              : 72
        L2 packets sent                  : 72
        L2 packets sent failed           : 0
        L2 link-status messages          : 3
        IGMP Snooping messages received: 79
        IGMP packet messages received    : 72

        IGMP Snooping Packet Statistics
        ----------------------------------------
        Received packets                       : 72
        IGMP packets                            : 29
        M-routing protocol packets             : 0
        Other packets                          : 43
        Received IGMP general queries          : 0
        Received IGMPv2 specific queries       : 0
        Received IGMPv3 g specific queries    : 0
        Received IGMPv3 gs specific queries: 0
        Received IGMPv1 reports                : 0
        Received IGMPv2 reports                : 0
        Received IGMP leaves                    : 0
        Received IGMPv3 reports                : 29
        Flooded queries                        : 0
        Forwarded and proxy-sent reports     : 0
        Forwarded and proxy-sent leaves       : 0

        IGMP Snooping Hardware Operation Statistics
        ------------------------------------------
```

```
      Total                         : 0     Total number of hardware operations
      Succeeded                     : 0     Number of successful hardware operations
      Failed                        : 0     Number of failed hardware operations
      Report/leave processing: 0      Number of hardware operations processing report and leave
      Response timer expiring: 0      Number of hardware operations in response to timer aging
      Group creating/updating: 0    Number of hardware operations resulting from creating and
updating groups
       Group deleting               : 0     Number of hardware operations caused by deleting a group
```

Display VLAN information of IGMP-snooping:

```
Switch_config#show ip igmp-snooping vlan
   vlan_id       Immediate-leave     Ports     Router Ports
----------------------------------------------------------------
        1              Disabled           7-30
        2              Disabled           NULL
```

Debug the message timer of IGMP-snooping:

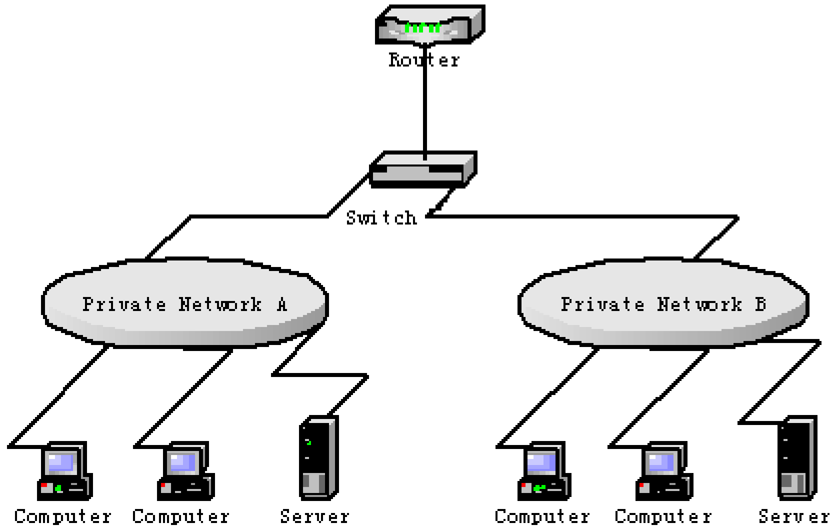
```
switch#debug ip igmp-snooping packet
Jan    1 02:22:28 IGMP-snooping: Receive IGMPv3 report from F0/1, vlan 1:
Jan    1 02:22:28 IGMP-snooping: Flood packet from F0/1 to vlan 1 rc = 0.
Jan    1 02:22:29 IGMP-snooping: Receive IGMPv3 report from F0/1, vlan 1:
Jan    1 02:22:29 IGMP-snooping: Flood packet from F0/1 to vlan 1 rc = 0.
Jan    1 02:22:38 IGMP-snooping: Receive IGMPv3 report from F0/1, vlan 1:
Jan    1 02:22:38 IGMP-snooping: Flood packet from F0/1 to vlan 1 rc = 0.
Jan    1 02:22:39 IGMP-snooping: Receive IGMPv3 report from F0/1, vlan 1:
Jan    1 02:22:39 IGMP-snooping: Flood packet from F0/1 to vlan 1 rc = 0.
Jan    1 02:23:11 IGMP-snooping: Receive IGMPv3 report from F0/1, vlan 1:
Jan    1 02:23:11 IGMP-snooping: Flood packet from F0/1 to vlan 1 rc = 0.
Jan    1 02:23:12 IGMP-snooping: Receive IGMPv3 report from F0/1, vlan 1:
Jan    1 02:23:12 IGMP-snooping: Flood packet from F0/1 to vlan 1 rc = 0.
```

Debug the message timer of IGMP-snooping:

```
switch#debug ip igmp-snooping timer
Jan    1 02:30:36 IGMP-snooping: Vlan 1 router on interface (null) expiry.
Jan    1 02:30:36 IGMP-snooping: Vlan 100 router on interface (null) expiry.
Jan    1 02:30:36 IGMP-snooping: Vlan 200 router on interface (null) expiry.
Jan    1 02:30:36 IGMP-snooping: Vlan 400 router on interface (null) expiry.
Jan    1 02:30:36 IGMP-snooping: Vlan 500 router on interface (null) expiry. Inquerying the
response timer expiry
```

IGMP-Snooping Configuration Example

Figure 1 shows network connection of the example.



Configuring Switch

Enable IGMP-snooping of VLAN 1 connecting Private Network A.

```
Switch_config#ip igmp-snooping vlan 1
```

Enable IGMP-snooping of VLAN 2 connecting Private Network B.

```
Switch_config#ip igmp-snooping vlan 2
```

25. IGMP-PROXY Configuration

IGMP-proxy Configuration Tasks

The IGMP Proxy allows the VLAN where the multicast user is located to receive the multicast source from other VLANs. The IGMP Proxy runs on layer 2 independently without other multicast routing protocols. IGMP proxy will be transmitted by the IGMP 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 packets. IGMP proxy 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.

Although IGMP proxy is based on IGMP snooping, two are independent in application; IGMP Snooping will not be affected when IGMP proxy is enabled or disabled, while IGMP proxy can run only when IGMP Snooping is enabled.

IGMP proxy cannot be used unless the following conditions are met:

L3 switch

Avoiding to enable IP multicast routing at the same time

Preventing a vlan to act as downstream vlan and also upstream vlan

Enabling/Disabling IGMP-Proxy

Adding/deleting VLAN agent relationship

Adding/deleting static multicast source entries

Monitoring and Maintaining IGMP-Proxy

Setting the Example of IGMP Proxy

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 enable	Resumes the default settings.

Note: IGMP-proxy cannot be enabled after IP multicast-routing is enabled. The previously enabled IGMP proxy is automatically shut down if IP multicast routing is enabled. The shutdown of ip multicast-routing will not lead to the automatic enablement of IGMP proxy.

Adding/Deleting VLAN Agent Relationship

Run the following commands in global configuration mode.

Command	Purpose
ip igmp-proxy agent-vlan *avlan_map* **client-vlan map** *cvlan_map*	Adds the agent VLAN (avlan_map) to manage the represented vlan (cvlan_map).
no ip igmp-proxy agent-vlan a*vlan_map* **client-vlan map** *cvlan_map*	Deletes the agent relationship.

Note:

1. The represented VLAN cannot be configured before vlan is designated by avlan_map; also, the agent VLAN cannot be configured before cvlan_map.

2. The represented and agent VLANs must accept the control of IGMP-Snooping.

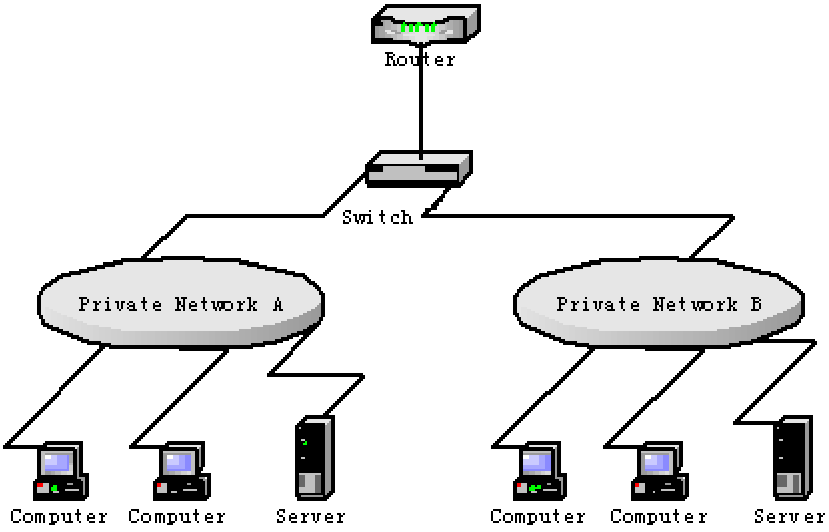
Monitoring and Maintaining IGMP-Proxy

Run the following commands in EXEC mode:

Command	Operation
show ip igmp-proxy	Displays the information about IGMP proxy.
[**no**] **debug ip igmp-proxy** *[error* | *event* | *packet]*	Enables or disables the IGMP-proxy debug switch.

IGMP-Proxy Configuration Example

The network topology is shown in figure 1.



Switch configuration:

Enable IGMP snooping and IGMP proxy.

```
Switch_config#ip igmp-snooping

Switch_config#ip igmp-proxy enable
```

Add VLAN 2 (in Private Network A) as the agent VLAN of the represented VLAN 3 (in Private Network B).

```
Switch_config#ip igmp-proxy agent-vlan 2 client-vlan map 3
```

26. MLD-Snooping Configuration

IPv6 Multicast Overview

The task of MLD snooping is to maintain the forwarding relationship of IPv6 group addresses in VLAN and synchronize with the change of the multicast group, enabling the data to be forwarded according to the topology of the multicast group. Its functions include monitoring MLD-snooping packets, maintaining the table between group address and VLAN, keep the MLD-snooping host the same with the MLD-snooping router and solve the flooding problems.

When a L2 device has not got MLD snooping run, the multicast data will be broadcast at the second layer; when the L2 device gets MLD snooping run, the multicast data of the known multicast group will not be broadcast at the second layer but be sent to the designated receiver, and the unknown multicast data will be dropped.

Note:

Because MLD-snooping solves the above-mentioned problems by monitoring the Query or Report packets of MLD-Snooping, MLD snooping can work normally only when there exists the multicast router, which means the switch must periodically receive the MLD-Snooping query message from the router. Therefore, the router age timer setting of MLD-Snooping must be larger than the group query period of the multicast router connected to it. You can see the multicast router information in each vlan, using the **show ipv6 mdl-snooping** command.

MLD-Snooping Multicast Configuration Tasks

Enabling/Disabling MLD-Snooping

Enabling/Disabling the Solicitation of Hardware Forward of Multicast Group

Adding/Deleting the Static Multicast Address of VLAN

Setting Router Age Timer of MLD-Snooping

Setting Response Time Timer of MLD-Snooping

Setting the Port of the Static Multicast Router

Setting the Immediate Leave Function

Monitoring and Maintaining MLD-Snooping

Enabling/Disabling MLD-Snooping Multicast

Run the following commands in global configuration mode.

Command	Purpose
ipv6 mld-snooping	Enables MLD snooping multicast.
no ipv6 mld-snooping	Disables MLD snooping.

Note:

After MLD-Snooping is enabled and the multicast packets fail to be found, the multicast packets whose destination addresses are not registered are dropped.

Enabling/Disabling the Solicitation of Hardware Forward of Multicast Group

Run the following commands in global configuration mode.

Command	Purpose
ipv6 mld-snooping solicitation	Enables the solicitation of hardware forward of multicast group.
no ipv6 mld-snooping solicitation	Disables the solicitation of hardware forward of multicast group.

Adding/Canceling the Static Multicast Address of VLAN

The static multicast address configuration allows some hosts that do not support the MLD-Snooping protocol to receive the corresponding group packets.

Run the following commands in global configuration mode.

Command	Purpose
ipv6 mld-snooping vlan *vlan_id* **static** *X:X:X:X::X* **interface** *intf_name*	Adds the static multicast address of VLAN.
no ipv6 mld-snooping vlan *vlan_id* **static** *X:X:X:X::X* **interface** *intf_name*	Removes the static multicast address of VLAN.

Setting Router Age Timer of MLD-Snooping

The Router Age timer is used to monitor the existence of an MLD-Snooping querying party. The MLD-Snooping querying party maintains and manages the multicast address by sending query packets. MLD-Snooping relies on the communication between the MLD-Snooping querying party and the host.

Run the following commands in global configuration mode.

Command	Purpose
ipv6 mld-snooping timer router-age *timer_value*	Sets the router age of MLD-Snooping.
no ipv6 mld-snooping timer router-age	Resumes the default router age of MLD-Snooping.

Note:

The settings of this timer shall refer to the query period settings of MLD-Snooping and be larger than the query period. It is recommended to set the router age timer to be triple of the query period.

The default router age of MLD snooping is 260 seconds.

Setting Response Time Timer of MLD-Snooping

Response Time timer is the latest Time for the host to report multicast after the MLD-Snooping interrogator sends the query packet. If the report message has not been received any packet after the timer aging, the switch will delete the multicast address.

Run the following commands in global configuration mode.

Command	Purpose
ipv6 mld-snooping timer response-time *timer_value*	Sets the response time of MLD-Snooping.
no ipv6 mld-snooping timer response-time	Resumes the default response time of MLD-Snooping.

Note:

The value of the timer cannot be set too small, or the multicast communication may be unstable.

The default response time of MLD snooping is 10 seconds.

Setting Querier of MLD-Snooping

If there is no multicast router in enabling VLAN with MLD-snooping, enable Querier of MLD-snooping module (which acts as a virtualized multicast router) to forward IGMP group query packets regularly. (The function can only be enabled or disabled when all VLANs enable MLD-snooping)

When there is no multicast router in the LAN and the multicast flow has no need for routing, run **MLD-snooping querier** command to activate the self-query of the switch.

Run following command in global configuration mode:

Command	Purpose
[**no**] **ipv6 mld-snooping querier [address** *[ip_addr]***]**	Sets Querier of MLD-snooping. Selects the address of the optional parameter as the source IP of the Query packet.

IGMP-snooping querier is disabled by default. The source IP address of the fake Query packet is FE80::3FF:FEFE:FD00:1.

Note:

Enable Querier, if there is a multicast router in the VLAN, the function becomes invalid automatically; if the multicast router is timeout, the function become valid automatically.

Setting the Port of the Static Multicast Router

Once a port is configured as a static multicast router port, all MLD-Snooping report and done messages received are forwarded to that port.

Run the following commands in global configuration mode.

Command	Operation
ipv6 mld-snooping vlan *WORD* **mrouter** interface *inft_name*	Sets the static multicast router's port of MLD snooping in Vlan **word**.
no ipv6 mld-snooping vlan *WORD* **mrouter** interface *inft_name*	Deletes the static multicast router's port of MLD snooping in Vlan **word**.

Enabling/Disabling Immediate Leave

Run the following commands in global configuration mode.

Command	Purpose
ipv6 mld-snooping vlan *WORD* **immediate-leave**	Enables the immediate-leave functionality.
no ipv6 mld-snooping vlan *WORD* **immediate-leave**	Resumes the default settings.

Monitoring and Maintaining MLD-Snooping Multicast

Run the following commands in EXEC mode:

Command	Operation
show ipv6 mld-snooping	Displays the configuration of MLD-Snooping.
show ipv6 mld-snooping timer	Displays the clock of MLD-Snooping.
show ipv6 mld -snooping groups	Displays the multicast group of MLD-Snooping.
show ipv6 mld-snooping statistics	Displays the statistics information of MLD-Snooping.
show ipv6 mld-snooping vlan	Displays the configuration of MLD-Snooping in VLAN.
show ipv6 mld-snooping mac	Displays the multicast MAC addresses recorded by MLD snooping.

The MLD-Snooping information is displayed below:

```
#show ipv6 mld-snooping

Global MLD snooping configuration:
----------------------------------
Globally enable        : Enabled
Querier                : Enabled
Querier address        : FE80::3FF:FEFE:FD00:1
Router age             : 260 s
Response time          : 10 s
```

```
Handle Solicitation    : Disabled

Vlan 1:
----------
       Running
       Routers: SWITCH(querier);
```

The multicast group of MLD-Snooping is displayed blow:

```
#show ipv6 mld--snooping groups

Vlan Group                  Type Port(s)
---- -------------- ---- ------------------------------------
     1 FF02::1:FF32:1B9B MLD    G2/23
     1 FF02::1:FF00:2    MLD    G2/23
     1 FF02::1:FF00:12 MLD    G2/23
     1 FF02::1:FF13:647D MLD    G2/23
     2 FF02::1:FF00:2    MLD    G2/22
     2 FF02::1:FF61:9901 MLD    G2/22
```

The timer of MLD-Snooping is displayed blow:

```
Switch#show ipv6 mld-snooping timer

vlan 1 Querier on port 0 : 251
#
Querier on port 0: 251    meaning the router age timer times out.
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:

```
#show ipv6 mld-snooping statistics
  vlan 1
------------
       v1_packets:0              quantity of v1 packets
       v2_packets:6              quantity of v2 packets
       v3_packets:0              quantity of v3 packets
       general_query_packets:5       Quantity of general query packets
       special_query_packets:0       Quantity of special query packets
       listener_packets:6          Quantity of Report packets
       done_packets:0       Quantity of Leave packets
       err_packets:0         Quantity of error packets
```

The MLD-Snooping proxying is displayed below:

```
  #show ipv6 mld-snooping mac
Vlan Mac                         Ref Flags
---- -------------- ---- ------
     1 3333:0000:0001       1      2
     2 3333:ff61:9901       1      0
              FF02::1:FF61:9901
     1 3333:0000:0002       1      2
     1 3333:ff00:0002       1      0
              FF02::1:FF00:2
```

```
    1 3333:ff00:0012       1     0
         FF02::1:FF00:12
    1 3333:ff13:647d       1     0
         FF02::1:FF13:647D
    1 3333:ff32:1b9b       1     0
         FF02::1:FF32:1B9B
    2 3333:ff00:0002       1     0
         FF02::1:FF00:2
    1 3333:ff00:0001       1     2
    1 3333:ff8e:7000       1     2
```

27. OAM Configuration

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.

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
Period event of error signal	Specifies the signal number *N* as the period. The number of error signals exceeds the defined threshold when *N* signals are received.
Error frame event	The number of error frames exceeds the defined threshold during the unit time.
Period event of error frame	Specifies the frame number *N* as the period. The number of error frames exceeds the defined threshold when *N* frames are received.
Second frame of error frame	Specifies that the number of seconds of the error frame exceeds the defined threshold in the designated *M* second.

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.

Round query of any MIB variables described in chapter 30 of *802.3*.

OAM Mode

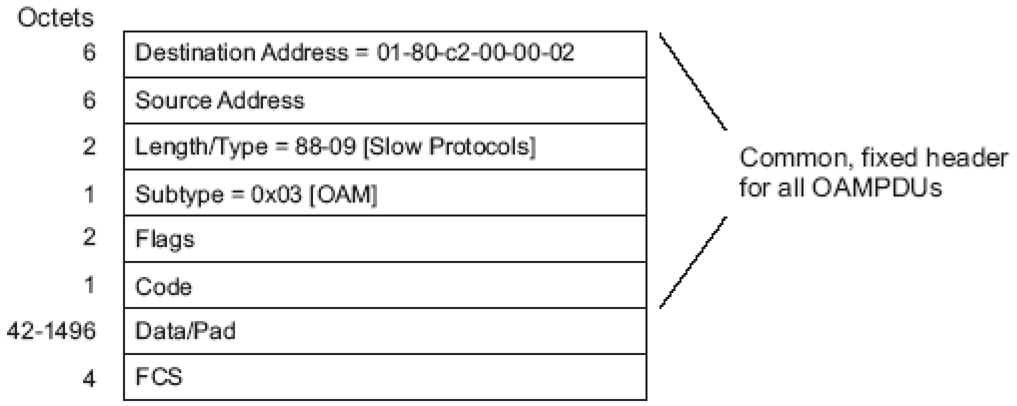
The device can conduct the OAM connection through two modes: active mode and passive mode. The device capacity in different mode is compared in table 2. Only OAM entity in active mode can trigger the connection process, while the OAM entity in passive mode has to wait for the connection request from 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 the peer terminal 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.

Components of the OAM Packet



Octets	
6	Destination Address = 01-80-c2-00-00-02
6	Source Address
2	Length/Type = 88-09 [Slow Protocols]
1	Subtype = 0x03 [OAM]
2	Flags
1	Code
42-1496	Data/Pad
4	FCS

Common, fixed header for all OAMPDUs

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: means the 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.

OAM Configuration Task List

Enabling OAM on an interface

Enabling remote OAM loopback

Configuring OAM link monitoring

Configuring the trouble notification from remote OAM entity

Displaying the information about OAM protocol

OAM Configuration Tasks

Enabling OAM on an Interface

Run the following command to enable OAM:

Procedure	Command	Purpose
Step1	**config**	Enters the global configuration mode.
Step2	**interface** intf-type intf-id	Enters the interface configuration mode.
Step3	**ethernet oam**	Enables Ethernet OAM on an interface.
Step4	**ethernet oam** [**max-rate** oampdus | **min-rate** seconds | **mode** {**active** | **passive**} | **timeout** seconds]	Configures optional OAM parameters: The **max-rate** parameter is used to configure the maximum number of OAMPDUs transmitted per second. It ranges between 1 and 10 and its default value is 10. The **min-rate** parameter is used to configure the minimum transmission rate of OAMPDU. Its unit is second. It ranges between 1 and 10 and its default value is 1. The **mode {active | passive}** parameter is used to set the mode of OAM. The OAM connection can be established between two interfaces only when at least one interface is in active mode. The **timeout** parameter is used to set the timeout time of the OAM connection. It ranges between 1 and 30 seconds and its default value is 1 second.

You can run **no Ethernet oam** to shut down the OAM function.

The remote OAM loopback cannot be enabled on the physical interface that belongs to the aggregation interface.

Configuring OAM Link Monitoring

You can configure the low threshold and the high threshold of OAM link monitoring.

The procedure to configure the OAM link monitoring on an interface is shown in the following table:

Procedure	Command	Purpose
Step1	**config**	Enters the global configuration mode.
Step2	**interface** intf-type intf-id	Enters the interface configuration mode.

Step3	**ethernet oam link-monitor negotiation-supported**	Enables link monitoring on an interface. The link monitoring is supported by default.
Step4	**ethernet oam link-monitor symbol-period {threshold {high {** symbols **|none} | low {**symbols**}} | window** symbols**}**	Sets the high and low threshold of the periodical event of the error signal, which triggers the error link events. The **threshold high** parameter is used to configure the high threshold. Its unit is signal number. It ranges between 1 and 65535 and its default value is **none**. The **threshold high** parameter is used to configure the low threshold. Its unit is signal number. It ranges between 0 and 65535 and its default value is **1**. The **window** parameter is used to configure the window size of the round-query period. The unit of the window size is the number of the 100M signal. The window size ranges between 10 and 600 on a 1000M Ethernet interface and its default value is 10 in this case, while the window size ranges between 1 and 60 on a 100M Ethernet interface and its default value is 1 in this case.
Step5	**ethernet oam link-monitor frame {threshold {high {** symbols **|none} | low {**symbols**}} | window** symbols**}**	Sets the high and low thresholds of the error frame event, which triggers the link events of error frame. The **threshold high** parameter is used to configure the high threshold. Its unit is signal number. It ranges between 1 and 65535 and its default value is **none**. The **threshold high** parameter is used to configure the low threshold. Its unit is signal number. It ranges between 0 and 65535 and its default value is **1**. The **window** parameter is used to configure the window size of the round-query period. Its unit is second. It ranges between 1 and 60 and its default value is 1.
Step6	**ethernet oam link-monitor frame-period {threshold {high {** symbols **|none} | low {**symbols**}} | window** symbols**}**	Sets the high and low thresholds of the period event of error frame, which triggers the link events of error frame period. The **threshold high** parameter is used to configure the high threshold. Its unit is signal number. It ranges between 1 and 65535 and its default value is **none**. The **threshold high** parameter is used to configure the low threshold. Its unit is signal number. It ranges between 0 and 65535 and its default value is **1**. The **window** parameter is used to configure the window size of the round-query period. The unit of the window size is the number of the 14881 frames. The window size ranges between 100 and 6000 on a 1000M Ethernet interface and its default value is 100 in this case, while the window size ranges between 10 and 600 on a 100M Ethernet interface and its default value is 10 in this case.

Step7	**ethernet oam link-monitor frame-seconds {threshold {high {** symbols **|none} | low {**symbols**}} | window** symbols**}**	Sets the high and low thresholds of the second event of error frame, which triggers the link events of error frame's second. The **threshold high** parameter is used to configure the high threshold. Its unit is signal number. It ranges between 1 and 900 and its default value is **none**. The **threshold low** parameter is used to configure the low threshold. Its unit is signal number. It ranges between 0 and 900 and its default value is **1**. The **window** parameter is used to configure the window size of the round-query period. Its unit is second. It ranges between 10 and 900 and its default value is 60.
Step8	**ethernet oam link-monitor receive-crc {threshold {high {** symbols **|none} | low {**symbols**}} | window** symbols**}**	Sets the high and low thresholds of the error CRC frame event, which triggers the link events of CRC checksum error. The **threshold high** parameter is used to configure the high threshold. Its unit is signal number. It ranges between 1 and 65535 and its default value is **none**. The **threshold high** parameter is used to configure the low threshold. Its unit is signal number. It ranges between 0 and 65535 and its default value is **1**. The **window** parameter is used to configure the window size of the round-query period. Its unit is second. It ranges between 1 and 180 and its default value is 10.

Configuring the Trouble Notification from Remote OAM Entity

You can configure an **error-disable** action on an interface. The local interface will enter the **errdisabled** state in the following cases:

1. The high threshold of a normal link event on a local interface is exceeded.
2. The remote interface which connects the local interface enters the **errdisabled** state.
3. The OAM function on the remote interface which connects the local interface is shut down by the administrator.

The procedure to configure the remote OAM trouble indication on an interface is shown in the following table:

Procedure	Command	Purpose
Step1	**config**	Enters the global configuration mode.
Step2	**interface** intf-type intf-id	Enters the interface configuration mode.
Step3	**ethernet oam remote-failure {critical-event | dying-gasp | link-fault} action error-disable-interface**	Configures the trigger action of a remote OAM trouble on an interface: The **critical-event** parameter is used to enable an interface to enter the **errdisabled** state when an undesignated critical event occurs.

		The **dying-gasp** parameter is used to enable the local interface to enter the **errdisabled** state if the high threshold of a normal link event on a local interface is exceeded or if the remote interface which connects the local interface enters the **errdisabled** state or if the OAM function on the remote interface which connects the local interface is shut down by the administrator. The **link-fault** parameter is used to enable an interface to enter the **errdisabled** state when the receiver detects signal loss.

Our switch cannot generate the LINK FAULT packets and the Critical Event packets. However, these packets will be handled if they are received from the remote terminal. Our router can transmit and receive the Dying Gasp packet. When the local port enters the **errdisabled** state or is closed by the administrator or the OAM function of the local port is closed by the manager, the Dying Gasp packet will be transmitted to the remote terminal that connects the local port.

Displaying the Information about OAM Protocol

Table 4 Displaying the information about OAM protocol

Command	Purpose
show ethernet oam discovery interface [intf-type intf-id**]**	Displays the OAM discovery information on all interfaces or a designated interface.
show ethernet oam statistics {pdu | link-monitor | remote-failure} interface [intf-type intf-id**]**	Displays the OAM statistics information on all interfaces or a designated interface. The **pdu** parameter is used to classify and count the OAM packets according to the code-domain value of the OAM packet. The **link-monitor** parameter is used to display the detailed statistics information of normal link events. The **remote-failure** parameter is to display the detailed statistics information about the remote trouble.
show ethernet oam configuration interface [intf-type intf-id**]**	Displays the OAM configuration information on all interfaces or a designated interface.
show ethernet oam runtime interface [intf-type intf-id**]**	Displays the OAM running information on all interfaces or a designated interface.

Configuration Example

Network Environment Requirements

You need configure the OAM protocol on the interface where two switches connect for capturing the information about the switch receiving error frames on user access side.

Network Topology

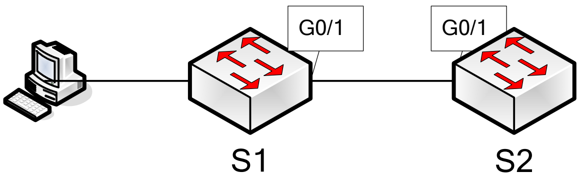


Figure 2 Network topology

Configuration Procedure

Configuring switch S1:

```
Switch_config_g0/1#ethernet oam
Switch_config_g0/1#ethernet oam mode passive
Switch_config_g0/1#ethernet oam link-monitor frame threshold low 10
Switch_config_g0/1#ethernet oam link-monitor frame window 30
Switch_config_g0/1#show ethernet oam configuration int g0/1
GigaEthernet0/1
General
-------
Admin state            : enabled
Mode                     : passive
PDU max rate           : 10 packets/second
PDU min rate           : 1 seconds/packet
Link timeout          : 1 seconds
High threshold action: no action

Remote Failure
--------------
Link fault action      : no action
Dying gasp action      : no action
Critical event action: no action

Remote Loopback
---------------
Is supported           : not supported
Loopback timeout       : 2

Link Monitoring
---------------
Negotiation            : supported
Status                  : on

Errored Symbol Period Event
Window                   : 10 * 100M symbols
Low threshold           : 1 error symbol(s)
High threshold         : none

Errored Frame Event
Window                   : 30 seconds
Low threshold           : 10 error frame(s)
High threshold         : none
```

```
Errored Frame Period Event
Window                      : 100 * 14881 frames
Low threshold            : 1 error frame(s)
High threshold          : none

Errored Frame Seconds Summary Event
Window                      : 60 seconds
Low threshold            : 1 error second(s)
High threshold          : none

Errored CRC Frames Event
Window                      : 1 seconds
Low threshold            : 10 error frame(s)
High threshold          : none
```

Configuring switch S2: Switch_config_g0/1#ethernet oam

```
Switch_config_g0/1#show ethernet oam statistics link-monitor int g0/1
GigaEthernet0/1
Local Link Events:
-------------
Errored Symbol Period Event:
No errored symbol period event happened yet.

Errored Frame Event:
No errored frame event happened yet.

Errored Frame Period Event:
No errored frame period event happened yet.

Errored Frame Seconds Summary Event:
No errored frame seconds summary event happened yet.

Errored CRC Frames Event:
No errored CRC frame event happened yet.

Remote Link Events:
-------------------
Errored Symbol Period Event:
No errored symbol period event happened yet.
```

```
Errored Frame Event:
No errored frame event happened yet.

Errored Frame Period Event:
No errored frame period event happened yet.

Errored Frame Seconds Summary Event:
No errored frame seconds summary event happened yet.

Errored CRC Frames Event:
No errored CRC frame event happened yet.
```

28. DHCP-Snooping Configuration

Chapter 1 DHCP-Snooping Configuration

IGMP-Snooping Configuration Tasks

DHCP-Snooping is to prevent the fake DHCP server from providing the DHCP service by judging the DHCP packets, maintaining the binding relationship between MAC address and IP address. The L2 switch can conduct the DAI function and the IP source guard function according to the binding relationship between MAC address and IP address. The DHCP-snooping is mainly to monitor the DHCP packets and dynamically maintain the MAC-IP binding list. The L2 switch filters the packets, which do not meet the MAC-IP binding relationship, to prevent the network attack from illegal users.

Enabling/Disabling DHCP-snooping function

Enabling DHCP-Snooping in a VLAN

Setting an Interface to a DHCP-Trusting Interface

Enabling DAI in a VLAN

Setting an Interface to an ARP-Trusting Interface

Enabling Source IP Address Monitoring in a VLAN

Setting A Trust Interface for Monitoring Source IP Address

Binding DHCP Snooping to a Standby TFTP Server

Configuring a file name for DHCP-snooping binding backup

Configuring an interval for DHCP-snooping binding backup

Configuring or adding the binding relationship manually

Mointoringandmaintaining DHCP-snooping

DHCP-snooping Example

Enabling/Disabling DHCP-Snooping

Run the following commands in global configuration mode.

Command	Purpose
ip dhcp-relay snooping	Enables DHCP-snooping.
no ip dhcp-relay snooping	Resumes the default settings.

This command is used to enable DHCP snooping in global configuration mode. After this command is run, the switch is to monitor all DHCP packets and form the corresponding binding relationship.

Note: If the client obtains the address of a switch before this command is run, the switch cannot add the corresponding binding relationship.

Enabling DHCP-Snooping in a VLAN

If DHCP snooping is enabled in a VLAN, the DHCP packets which are received from all distrusted physical ports in a VLAN will be legally checked. The DHCP response packets which are received from distrusted physical ports in a VLAN will then be dropped, preventing the faked or mis-configured DHCP server from providing address distribution services. For the DHCP request packet from distrusted ports, if the hardware address field in the DHCP request packet does not match the MAC address of this packet, the DHCP request packet is then thought as a fake packet which is used as the attack packet for DHCP DOS and then the switch will drop it.

Run the following commands in global configuration mode.

Command	Purpose
ip dhcp-relay snooping vlan *vlan_id*	Enables DHCP-snooping in a VLAN.
no ip dhcp-relay snooping vlan *vlan_id*	Disables DHCP-snooping in a VLAN.

Enabling DHCP anti-attack in a VLAN.

To enable attack prevention in a VLAN, you need to configure the allowable maximum DHCP clients in a specific VLAN and conduct the principle of “first come and first serve”. When the number of users in the specific VLAN reaches the maximum number, new clients are not allowed to be distributed.

Run the following commands in global configuration mode.

Command	Purpose
ip dhcp-relay snooping vlan *vlan_id* **max-client** *number*	Enabling DHCP anti-attack in a VLAN.
no ip dhcp-relay snooping vlan *vlan_id* **max-client**	Disables DHCP anti-attack in a VLAN.

Setting an Interface to a DHCP-Trusting Interface

If an interface is set to be a DHCP-trusting interface, the DHCP packets received from this interface will not be checked.

Run the following commands in physical interface configuration mode.

Command	Operation
dhcp snooping trust	Setting an Interface to a DHCP-Trusting Interface
no dhcp snooping trust	Resumes an interface to a DHCP-distrusted interface.

The interface is a distrusted interface by default.

Enabling/Disabling binding table fast update function

This function is disabled by default. When this function is disabled and a port has been bound to client A, the DHCP request of the same MAC address on other ports will be regarded as a fake MAC attack even if client A is off line.

When this function is enabled, the above-mentioned case will not occur.

It is recommended to use this function in case that a client frequently changes its port and address lease, distributed by DHCP server, cannot be modified to a short period of time.

Command	Operation
ip dhcp-relay snooping rapid-refresh-bind	Enables the fast update function of the binding table.
no ip dhcp-relay snooping rapid-refresh-bind	Disables the fast update function of the binding table.

Enabling DAI in a VLAN

When dynamic ARP monitoring is conducted in all physical ports of a VLAN, a received ARP packet will be rejected if the source MAC address and the source IP address of this packet do not match up with the configured MAC-IP binding relationship. The binding relationship on an interface can be dynamically bound by DHCP or configured manually. If no MAC addresses are bound to IP addresses on a physical interface, the switch rejects forwarding all ARP packets.

Command	Operation
ip arp inspection vlan *vlanid*	Enables dynamic ARP monitoring on all distrusted ports in a VLAN.
no ip arp inspection vlan *vlanid*	Disables dynamic ARP monitoring on all distrusted ports in a VLAN.

Setting an Interface to an ARP-Trusting Interface

ARP monitoring is not enabled on those trusted interfaces. The interfaces are distrusted ones by default.

Run the following commands in interface configuration mode.

Command	Operation
arp inspection trust	Setting an Interface to an ARP-Trusting Interface
no arp inspection trust	Resumes an interface to an ARP-distrusting interface.

Enabling Source IP Address Monitoring in a VLAN

After source IP address monitoring is enabled in a VLAN, IP packets received from all physical ports in the VLAN will be rejected if their source MAC addresses and source IP addresses do not match up with the configured MAC-to-IP binding relationship. The binding relationship on an interface can be dynamically bound by DHCP or configured manually. If no MAC addresses are bound to IP addresses on a physical interface, the switch rejects forwarding all IP packets received from the physical interface.

Run the following commands in global configuration mode.

Command	Operation
ip verify source vlan *vlanid*	Enables source IP address checkup on all distrusted interfaces in a VLAN.
no ip verify source vlan *vlanid*	Disables source IP address checkup on all interfaces in a VLAN.

Note: If the DHCP packet (also the IP packet) is received, it will be forwarded because global snooping is configured.

Setting an Interface to the One Which is Trusted by IP Source Address Monitoring

The source address detection function will not be enabled for the IP source address trust interface.

Run the following commands in interface configuration mode.

Command	Operation
ip-source trust	Sets an interface to the one with a trusted source IP address.
no ip-source trust	Resumes an interface to the one with a distrusted source IP address.

Setting DHCP-Snooping Option 82

Option 82 brings the local information to a server and helps the server to distribute addresses to clients.

Run the following commands in global configuration mode.

Command	Operation
ip dhcp-relay snooping information option	Sets that option82, which is in the default format, is carried when DHCP-snooping forwards the DHCP packets.
no ip dhcp-relay snooping information option	Sets that option82 is not carried when DHCP-snooping forwards the DHCP packets.

To specify the format of option82, conduct the following settings in global mode.

Command	Operation
ip dhcp-relay snooping information option format {snmp-ifindex/manual/hn-type / cm-type/[host]/hw-type}	Sets the format of option82 that the DHCP packets carry when they are forwarded by DHCP-Snooping.
no ip dhcp-relay snooping information option format {snmp-ifindex/manual/hn-type /cm-type/[host]/hw-type}	Sets that option82 is not carried when DHCP-snooping forwards the DHCP packets.

If a manual mode is set to enter in option82, conduct the following configurations in interface mode to set the circuit-id:

Command	Operation
dhcp snooping information circuit-id string [STRING]	If option82 is set to be in the manual format, you need to set DHCP-snooping to forward DHCP packets with bearing of option82, whose content is the character string written by STRING. This command is set on the port that connects the client.
dhcp snooping information circuit-id **hex [***xx-xx-xx-xx-xx-xx***]**	If option82 is set to be in the manual format, you need to set DHCP-snooping to forward DHCP packets with bearing of option82, whose content is the Hex system.. This command is set on the port that connects the client.
no dhcp snooping information circuit-id	Deletes the manually configured option82 circuit-id.

If a manual mode is set to enter in option82, conduct the following configurations in interface mode to set the remote-id:

Command	Operation
dhcp snooping information remote-id string [STRING]	If option82 is set to be in the manual format, you need to set DHCP-snooping to forward DHCP packets with bearing of option82, whose content is the character string written by STRING. This command is set on the port that connects the client.
dhcp snooping information remote-id **hex [***xx-xx-xx-xx-xx-xx***]**	If option82 is set to be in the manual format, you need to set DHCP-snooping to forward DHCP packets with bearing of option82, whose content is the Hex system.. This command is set on the port that connects the client.
no dhcp snooping information remote-id	Deletes the manually configured option82 remote-id.

If a manual mode is set to enter in option82, conduct the following configurations in interface mode to set the vendor-specific:

Command	Operation
dhcp snooping information vendor-specific string STRING	If option82 is set to be in the manual format, you need to set DHCP-snooping to forward DHCP packets with bearing of option82, whose content is the character string written by STRING. This command is set on the port that connects the client.
dhcp snooping information vendor-specific hex [*xx-xx-xx-xx-xx-xx***]**	If option82 is set to be in the manual format, you need to set DHCP-snooping to forward DHCP packets with bearing of option82, whose content is the Hex system.. This command is set on the port that connects the client.
no **dhcp snooping information vendor-specific**	Deletes the manually configured option82 vendor-specific.

Setting the Policy of DHCP-Snooping Option82 Packets

You can set the policy for the DHCP request packets, which carry with option82, after these packets are received. The policies include the following ones:

“Drop” policy: Run the following command in port mode to drop the request packets with option82.

Command	Operation
dhcp snooping information drop	Drops the request packets that contain option82.

“Append” policy: Run the following command in port mode to add the request packets with option82.

Command	Operation
dhcp snooping information append	Enables the function to add option82 on a port.
dhcp snooping information append first-subop9-param { hex *xx-xx-xx-xx-xx-xx* **| vlanip | hostname }**	Stands for the first parameter carried by option82 vendor-specific (suboption9).
dhcp snooping information append second-subop9-param { hex *xx-xx-xx-xx-xx-xx* **| vlanip | hostname }**	Stands for the second parameter carried by option82 vendor-specific (suboption9).

Configuring the TFTP Server for Backing up Interface Binding

After the switch configuration is rebooted, the previously-configured interface binding will be lost. In this case, there is no binding relationship on this interface. After source IP address monitoring is enabled, the switch rejected forwarding all IP packets. After the TFTP server is configured for interface binding backup, the binding relationship will be backed up to the server through the TFTP protocol. After the switch is restarted, the switch automatically downloads the binding list from the TFTP server, securing the normal running of the network.

Run the following commands in global configuration mode.

Command	Operation
ip dhcp-relay snooping database-agent *ip-address*	Configures the IP address of the TFTP server which is to back up interface binding.
no ip dhcp-relay snooping database-agent *ip-address*	Cancels the TFTP Server for backing up interface binding.

Configuring a File Name for Interface Binding Backup

When backing up the interface binding relationship, the corresponding file name will be saved on the TFTP server. In this way, different switches can back up their own interface binding relationships to the same TFTP server.

Run the following commands in global configuration mode.

Command	Operation
ip dhcp-relay snooping db-file *name* [timestamp]	Configures a file name for interface binding backup.
no ip dhcp-relay snooping db-file	Cancels a file name for interface binding backup.

Configuring the Interval for Checking Interface Binding Backup

The MAC-to-IP binding relationship on an interface changes dynamically. Hence, you need check whether the binding relationship updates after a certain interval. If the binding relationship updates (adds or deletes binding entries), it need be backed up again. The default time interval is 30mins.

Run the following commands in global configuration mode.

Command	Operation
ip dhcp-relay snooping write-immediately	Configures DHCP Snooping immediate backup when the binding information changes.

	no ip dhcp-relay snooping {write-time | write-immediately} Resumes the interval of checking interface binding backup to the default settings.
ip dhcp-relay snooping write-time *num*	Configures the interval for checking interface binding backup. The unit is min.
no ip dhcp-relay snooping write-time	Resumes the interval of checking interface binding backup to the default settings.

Configuring Interface Binding Manually

If a host does not obtain the address through DHCP, you can add the binding item on an interface of a switch to enable the host to access the network. You can run no ip source binding MAC IP to delete items from the corresponding binding list.

Note that the manually-configured binding items have higher priority than the dynamically-configured binding items. If the manually-configured binding item and the dynamically-configured binding item have the same MAC address, the manually-configured one updates the dynamically-configured one. The interface binding item takes the MAC address as the unique index.

Run the following commands in global configuration mode.

Command	Operation
ip source binding *MAC IP* interface *name vlan-id*	Configures Interface Binding Manually
no ip source binding *MAC IP vlan-id*	Cancels an interface binding item.

Monitoring and Maintaining DHCP-Snooping

Run the following commands in EXEC mode:

Command	Operation
show ip dhcp-relay snooping	Displays the information about DHCP-snooping configuration.
show ip dhcp-relay snooping binding	Displays the effective address binding items on an interface.
show ip dhcp-relay snooping binding all	Displays all binding items which are generated by DHCP snooping.
[**no**] **debug ip dhcp-relay** [snooping | binding | event | all]	Enables or disables the switch of DHCP relay snooping binding or event.

The following shows the information about the DHCP snooping configuration.

```
switch#show ip dhcp-relay snooping
  ip dhcp-relay snooping vlan 3
ip arp inspection vlan 3
DHCP Snooping trust interface:
    GigaEthernet0/1
ARP Inspect interface:
    GigaEthernet0/11
```

The following shows the binding information about dhcp-relay snooping:

```
switch#show ip dhcp-relay snooping binding
Hardware Address      IP Address        remainder time Type              VLAN      interface

00:e0:0f:26:23:89     192.2.2.101       86400       DHCP_SN          3          GigaEthernet0/3
```

The following shows the binding information about dhcp-relay snooping:

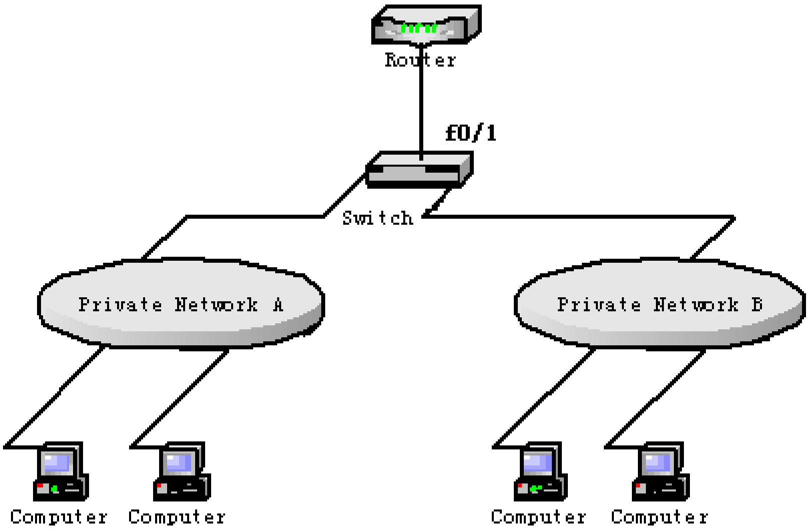
```
switch#show ip dhcp-relay snooping binding all
Hardware Address      IP Address        remainder time Type              VLAN      interface

00:e0:0f:32:1c:59     192.2.2.1         infinite      MANUAL           1          GigaEthernet0/2
00:e0:0f:26:23:89     192.2.2.101       86400       DHCP_SN          3          GigaEthernet0/3
```

The following shows how to debug the information about dhcp-relay snooping.

```
switch#debug ip dhcp-relay all
DHCPR: receive l2 packet from vlan 3, diID: 3
DHCPR: DHCP packet len 277
DHCPR: add binding on interface GigaEthernet0/3
DHCPR: send packet continue
DHCPR: receive l2 packet from vlan 3, diID: 1
DHCPR: DHCP packet len 300
DHCPR: send packet continue
DHCPR: receive l2 packet from vlan 3, diID: 3
DHCPR: DHCP packet len 289
DHCPR: send packet continue
DHCPR: receive l2 packet from vlan 3, diID: 1
DHCPR: DHCP packet len 300
DHCPR: update binding on interface GigaEthernet0/3
DHCPR:    IP address: 192.2.2.101, lease time 86400 seconds
DHCPR: send packet continue
```

DHCP-Snooping Configuration Example

The network topology is shown in figure 1.



Configuring Switch

Enable DHCP snooping in VLAN 1 which connects private network A.

```
Switch_config#ip dhcp-relay snooping
Switch_config#ip dhcp-relay snooping vlan 1
```

Enable DHCP snooping in VLAN 2 which connects private network B.

```
Switch_config#ip dhcp-relay snooping
Switch_config#ip dhcp-relay snooping vlan 2
```

Sets the interface which connects the DHCP server to a DHCP-trusting interface.

```
Switch_config_g0/1#dhcp snooping trust
```

Configure option82 instance manually

```
interface GigaEthernet0/1
  dhcp snooping information circuit-id hex 00-01-00-05
  dhcp snooping information remote-id hex 00-e0-0f-13-1a-50
  dhcp snooping information vendor-specific hex 00-00-0c-f8-0d-01-0b-78-69-61-6f-6d-69-6e-37-31-31-34
  dhcp snooping information append
  dhcp snooping information append first-subop9-param hex 61-62-63-61-62-63
!
interface GigaEthernet0/2
  dhcp snooping trust
  arp inspection trust
  ip-source trust
!
```

```
!
!
ip dhcp-relay snooping
ip dhcp-relay snooping vlan  1-100
ip arp inspection vlan  1
ip verify source vlan  1
ip dhcp-relay snooping information option format manual
```

29. Layer-2 Tunnel Configuration

Overview

The tunnel of layer-2 protocol allows users who connect the two terminals of a switch to transmit the designated layer-2 protocol packets transparently in their own networks through the switch without the affection of the corresponding layer-2 protocol module of this switch. The switch here is just a transparent transmission medium for users.

Layer-2 (L2) Tunnel Protocol Configuration

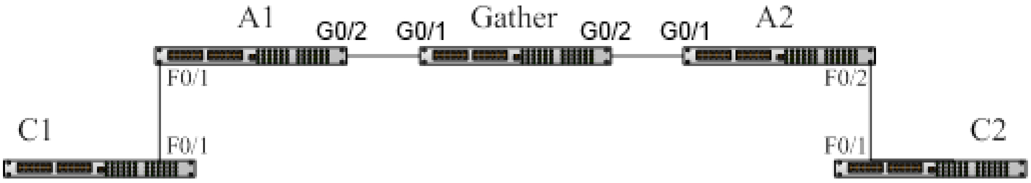
Run the following commands to set the L2 tunnel function on a L2 protocol:

Command	Usage Guidelines
config	Enters the global configuration mode.
interface *<intf_name>*	Enters the interface configuration mode of a switch port. Only the switch ports support the L2 tunnel (including physical ports and aggregation ports)
[**no**] **l2protocol-tunnel** *[stp]*	Sets the L2 protocol, which is used to enable the tunnel function, on this switch port. Currently only the tunnel function of the STP protocol is supported.
no spanning-tree	To disable the STP of a port, run the above-mentioned command.
exit	Goes back to the global mode.
write	Saves the settings.

Note:
This command is used to disable STP on the port on which the tunnel function is enabled, preventing this port from influencing the devices that access the tunnel by sending the STP packets.

L2 Protocol Tunnel Configuration Example

The network topology is shown in the following figure:



A1/A2/Gather belongs to a core network. C1/C2 stands for two switches locating in two branches of a customer. The customer wants the two networks to be managed as an independent network, that is, the core network is just like a transparent transmission channel for this customer. To realize STP transparent transmission, the customer needs to make the following settings on each switch:

- Set port g0/2 of switch A1, port g0/1 of switch Gather and port g0/1 of switch A2 to the trunk mode respectively.
- Set port f0/1 of switch A1 and port f0/2 of switch A2 to access, disable STP, and then enable the tunnel function of the STP protocol on the two ports.

30. QoS Configuration

Chapter 1 QoS Configuration

If you care to use your bandwidth sufficiently and your network resources efficiently, you must pay attention to QoS configuration.

QoS Overview

QoS Concept

In general, the switch works in best-effort served mode in which the switch treats all flows equally and tries its best to deliver all flows. Thus if congestion occurs all flows have the same chance to be discarded. However in a real network different flows have different significances, and the QoS function of the switch can provide different services to different flows based on their own significances, in which the important flows will receive a better service.

As to classify the importance of flows, there are two main ways on the current network:

The tag in the 802.1Q frame header has two bytes and 3 bits are used to present the priority of the packet. There are 8 priorities, among which 0 means the lowest priority and 7 means the highest priority.

The DSCP field in IP header of the IP packet uses the bottom 6 bits in the TOS domain of the IP header.

In real network application the edge switch distributes different priorities to different flows based on their significance and then different services will be provided to different flows based on their priorities, which is the way to realize the terminal-to-terminal QoS.

Additionally, you can also configure a switch in a network, enabling the switch to process those packets with specific attributes (according to the MAC layer or the L3 information of packets) specially. This kind of behaviors are called as the one-leap behaviors.

The QoS function of the switch optimizes the usage of limited network bandwidth so that the entire performance of the network is greatly improved.

Terminal-To-Terminal QoS Model

The service model describes a group of terminal-to-terminal QoS abilities, that is, the abilities for a network to transmit specific network communication services from one terminal to another terminal. The QoS software supports two kinds of service models: Best-Effort service and Differentiated service.

Best-effort service

The best-effort service is a singular service model. In this service model, an application can send any amount of data at any necessary time without application of permits or aforehand network notification. As to the best-effort service, if allowed, the network can transmit data without any guarantee of reliability, delay or throughput. The QoS of the switch on which the best-effort service is realized is in nature this kind of service, that is, first come and first served (FCFS).

Differentiated service

As to the differentiated service, if a special service is to be transmitted in a network, each packet should be specified with a corresponding QoS tag. This designation can be embodied in different modes, such as, use IP priority status setting in IP data packet. The switch uses this QoS rule to conduct classification and complete the intelligent queuing. The QoS of the switch provides Strict Priority (SP), Weighted Round Robin (WRR), Deficit Round Robin (DRR) and First-Come-First-Served (FCFS).

Queue Algorithm of QoS

Each queue algorithm is the important basis to realize QoS. The QoS of the switch provides the following algorithms: Strict Priority (SP), Weighted Round Robin (WRR), Weighted Fair Queuing (WFQ) and First-Come-First-Served (FCFS).

Strict Priority

This algorithm means to first provide service to the flow with the highest priority and after the highest-priority flow comes the service for the next-to-highest flow. This algorithm provides a comparatively good service to those flows with relatively high priority, but its shortage is also explicit that the flows with low priority cannot get service and wait to die.

Weighted Round Robin

Weighted Round Robin (WRR) is an effective solution to the defect of Strict Priority (SP), in which the low-priority queues always die out. WRR is an algorithm that brings each priority queue a certain bandwidth and provides service to each priority queue according to the order from high priority to low priority. After the queue with highest priority has used up all its bandwidth, the system automatically provides service to those queues with next highest priority.

Weighted Fair Queuing

Weighted Fair Queuing (WFQ) classifies the packet according to the priority of the traffic. It sets the egress bandwidth based on the weight of each traffic. The bigger the weight, the greater the bandwidth. Thus, it guarantees the fairness of priority services and embodies the weight of different priority services.

First come first served

The First-Come-First-Served queue algorithm, which is shortened as FCFS, provides service to those packets according to their sequence of arriving at a switch, and the packet that first arrives at the switch will be served first.

Weighted Random Early Detection

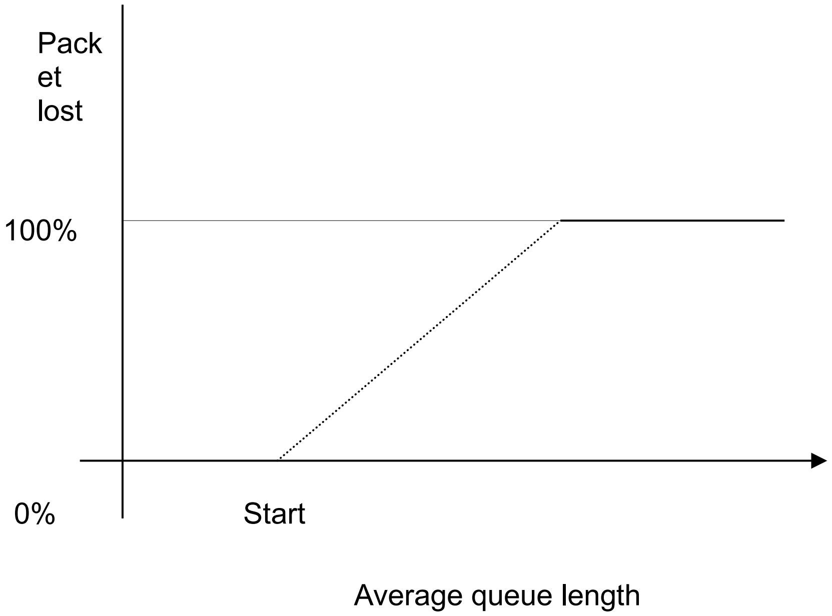
Congestion avoidance and traditional packet loss mechanism

Excessive congestion may inflict damage on network resources, so network congestion should be resolved through some measures. Congestion avoidance is a sort of flow control method of positively dropping packets and regulating network flows to solve network overload via network resource monitoring. The traditional way of resolving network congestion is to drop all incoming packets when the queue length reaches its threshold. But for TCP packets, heavy packet loss may cause TCP timeout and lead to slow TCP startup and congestion avoidance, which is called as TCP global synchronization.

WRED

The WRED algorithm is adopted to prevent TCP global synchronization. WRED helps users to set the queue threshold. When the queue length is less than the configured threshold, the packets will not be dropped; otherwise, the packets will be dropped randomly. Because WRED drops packets randomly, it is avoided for multiple TCP connections to slow down the transmission speed at the same time, which is the reason why TCP global synchronization is avoided. WRED enables other TCP connections to maintain a relatively high transmission speed when the packets of a certain TCP connection begin to be dropped and their transmission speed is slowed down. No matter what time it is, there are always some TCP connections to transmit packets with a high speed, which ensures effective bandwidth usability.

WRED cooperation is conducted when packets enter the outgoing queue and are checked for their size and packets in different ranges get different treatments. The key parameters include **Start**, **Slop** and **Drop priority**.



When the queue length is less than **start**, packets will not be dropped. When the queue length is bigger than **start**, the incoming packets begin to be dropped randomly.The longer the queue is, the higher the dropping rate is.

The rate for packet loss rises along with the increase of the queue length.

QoS Configuration Task List

In general, ONU will try its best to deliver each packet and when congestion occurs all packets have the same chance to be discarded. However, in reality different packets have different importance and the comparatively important packets should get the comparatively good service. QoS is a mechanism to provide different priority services to packets with different importance, in which the network can have its better performance and be used efficiently.

This chapter presents how to set QoS on ONU.

The following are QoS configuration tasks:

Setting the Global cos Priority Queue

Setting the Bandwidth of the cos Priority Queue

Setting the Schedule Policy of the CoS Priority Queue

Setting the Default cos Value of a Port

Setting the cos Priority Queue of a Port

Setting the Bandwidth of the cos Priority Queue of a Port

Setting the Schedule Policy of the cos Priority Queue f a Port

Setting the CoS Priority Queue based on dscp

Establishing the QoS Policy Mapping

Setting the Description of the QoS Policy Mapping

Setting the Matchup Data Flow of the QoS Policy Mapping

Setting the Actions of the Matchup Data Flow of the QoS Policy Mapping

Applying the QoS Policy on a Port

Applying the QoS Policy on a global

Configuring Trust Mode

Displaying the QoS Policy Mapping Table

QoS Configuration Tasks

Setting the Global cos Priority Queue

The task to set the QoS priority queue is to map 8 CoS values, which are defined by IEEE802.1p, to the priority queues in a switch. This series of switch has 8 priority queues. According to different queues, the switch will take different schedule policies to realize QoS.

If a CoS priority queue is set in global mode, the mapping of CoS priority queue on all ports will be affected. When priority queues are set on a L2 port, the priority queues can only work on this L2 port.

Enter the following management mode and run the following commands one by one to set CoS priority queue.

Command	Purpose
config	Enters the global configuration mode.

[**no**] **cos map** *quid cos1..cosn*	Sets the CoS priority queue. quid stands for the ID of a CoS priority queue. cos1…cosn stands for the IEEE802.1p-defined CoS value.
exit	Goes back to the EXEC mode.
write	Saves the settings.

Setting the Bandwidth of the CoS Priority Queue

The bandwidth of priority queue means the bandwidth distribution ratio of each priority queue, which is set when the schedule policy of the CoS priority queue is set to wrr or wfq. This series of switches has 8 priority queues in total.

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/WFQ. This command decides the bandwidth weight value of the CoS priority queue when the WRR/WFQ schedule policy is used.

Run the following commands one by one to set the bandwidth of the CoS priority queue.

Command	Purpose
config	Enters the global configuration mode.
[**no**] **scheduler weight bandwidth** *weight1...weightn*	Sets the bandwidth of the CoS priority queue.. weight1…weightn stand for the weights of 8 CoS priority queues of WRR/DRR.
exit	Goes back to the EXEC mode.
write	Saves the settings.

Setting the Schedule Policy of the CoS Priority Queue

A switch has many output queues on each of its port. This series of switches has 8 priority queues. The output queues can adopt the following four schedule modes:

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 (Weighted Round Robin) is an algorithm that brings each priority queue a certain bandwidth and provides service to each priority queue according to the order from high priority to low priority.

WFQ (Weighted Fair Queuing) is an algorithm that brings each priority queue a certain bandwidth according to the priority of the flow.

The First-Come-First-Served queue algorithm, which is shortened as FCFS, provides service to those packets according to their sequence of arriving at a switch, and the packet that first arrives at the switch will be served first.

Enter the following configuration mode and set the schedule policy of CoS priority queue.

Command	Purpose

config	Enters the global configuration mode.
[**no**] **scheduler policy** { **sp** | **wrr|wfq|fcfs** }	Sets the schedule policy of the CoS priority queue. **sp** means to use the SP schedule policy. **wrr** means to use the WRR schedule policy. wfq means to use the WFQ schedule policy. **fcfs** means to use the FCFS schedule policy.
exit	Goes back to the EXEC mode.
write	Saves the settings.

Setting the Default CoS Value of a Port

If the port of a switch receives a data frame without tag, the switch will add a default CoS priority to it. Setting the default cos value of a port is to set the untagged default CoS value, which is received by the port, to a designated value.

Enter the management mode and run the following commands to set the default CoS value of a port:

Command	Purpose
config	Enters the global configuration mode.
interface g0/1	Enters the to-be-configured port.
[**no**] **cos default** *cos*	Sets the CoS value of the received untagged frames. cos stands for the corresponding CoS value.
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.
write	Saves the settings.

Setting the CoS Priority Queue of a Port

When a priority queue is set on a L2 port, the priority queue will be used by the L2 port; otherwise, you should conduct the configuration of a global CoS priority queue.

Enter the management mode and run the following commands to set the default CoS value of a port:

Command	Purpose
config	Enters the global configuration mode.
interface g0/1	Enters the to-be-configured port.
[**no**] **cos map** *quid cos1..cosn*	Sets the CoS priority queue. quid stands for the ID of a CoS priority queue. cos1…cosn stands for the IEEE802.1p-defined CoS value.

exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.

Setting the Bandwidth of a Port CoS Priority Queue

When a priority queue bandwidth is set on a L2 port, the priority queue bandwidth will be used by the L2 port; otherwise, you should conduct the configuration of a global priority queue bandwidth.

Enter the management mode and run the following commands one by one to set the CoS priority queue bandwidth of a port.

Command	Purpose
config	Enters the global configuration mode.
interface g0/1	Enters the to-be-configured port.
[**no**] **scheduler weight bandwidth** *weight1...weightn*	Sets the bandwidth of the CoS priority queue**.**. **weight1…weightn** stand for the weights of 8 CoS priority queues of WRR/DRR.
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.
write	Saves the settings.

Setting the Schedule Policy of a Port CoS Priority Queue

When a priority queue schedule policy is set on a L2 port, the priority queue schedule policy will be used by the L2 port; otherwise, you should conduct the configuration of a global priority queue schedule policy.

Enter the management mode and run the following commands one by one to set the CoS priority queue schedule policy of a port.

Command	Purpose
config	Enters the global configuration mode.
interface g0/1	Enters the to-be-configured port.
[**no**] **scheduler policy** { **sp** | **wrr|wfq** }	Sets the schedule policy of the CoS priority queue. **sp** means to use the SP schedule policy. **wrr** means to use the WRR schedule policy. **wfq** means to use the WFQ schedule policy. **drr** means to use the DRR schedule policy.
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.

write	Saves the settings.

Setting the CoS Priority Queue Based on DSCP

Based on the DSCP value, the COS queue is mapped again, the DSCP value is modified and the congestion bit is changed.

Enter the management mode and run the following commands to set the default CoS value of a port:

Command	Purpose
config	Enters the global configuration mode.
[**no**]**dscp map** *word* { **cos** *cos-value* } dscp	Word stands for the DSCP range table. Cos-value means to set the mapped priority CoS..
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.

Establishing the QoS Policy Mapping

Flow classification means to identify a class of packets with certain attributes by applying a certain regulation and take designated actions towards to these packets.

Do as follows to set up a QoS policy.

Enter the management mode and then run the following commands to establish a new QoS policy mapping.

Command	Purpose
config	Enters the global configuration mode.
[no]policy-map *name*	Enters the configuration mode of the QoS policy map. name stands for the name of the policy.
exit	Exits from the global configuration mode.
exit	Goes back to the EXEC mode.

Setting the Description of the QoS Policy Mapping

Enter the management mode and run the following commands to set the description of a QoS policy mapping. This settings will replace the previous settings.

Command	Purpose
config	Enters the global configuration mode.
[**no**]**policy-map** *name*	Enters the configuration mode of the QoS

	policy map. name stands for the name of the policy.
description description-text	Sets the description of the QoS policy. description-text stands for the text to describe the policy.
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.

Setting the Matchup Data Flow of the QoS Policy Mapping

The classification rule of the QoS data flow means the filtration rule configured by the administrator according to management requirements. It can be simple, for example, flows with different priorities can be identified by the ToS field of the IP packet's header, or complicated, for example, the packets can be classified according to the related information about the comprehensive link layer, the network layer and the transmission layer, such as the MAC address, the source address of IP, the destination address or the port ID of the application. In general, the classification standard is limited in the header of an encapsulated packet. It is rare to use the content of a packet as the classification standard.

Enter the management configuration mode, set the matchup data flow of policy and replace the previous settings with this data flow according to the following steps:

Command	Purpose
config	Enters the global configuration mode.
[no]policy-map name	Enters the configuration mode of the QoS policy map. name stands for the name of the policy.
description description-text	Sets the description of the QoS policy. description-text stands for the text to describe the policy.

classify {**any** | **cos** *cos* | **icos** *icos* | **vlan** *vlanid* | **ivlan** *ivlanid* | **ethernet-type** *ethernet-type* | **precedence** *precedence-value* | **dscp** *dscp-value* | **tos** *tos-value* | **diffserv** *diffserv-value* | **ip** *ip-access-list* | **ipv6** *ipv6-access-list* | **mac** *mac-access-list* }
no classify { **cos** | **icos** | **vlan** | **ivlan** | **ethernet-type** | **precedence** | **dscp** | **tos** | **diffserv** | **ip** | **ipv6** | **mac** }
	Matches up with any packet.
	Configures the matched COS value which ranges between 0 and 7.
	icos stands for the matched inner COS value which ranges between 0 and 7.
	vlanid stands for the matched VLAN, which ranges from 1 to 4094.
	ivlanid stands for the matched inner VLAN, which ranges from 1 to 4094.

	ethernet-type stands for the matched packet type, which is between 0x0600 and 0xFFFF. **precedence-value** stands for the priority field in tos of IP packet, which ranges from 0 to 7. **dscp-value** stands for the dscp field in tos of IP packet, which ranges from 0 to 63. **tos-value** stands for latency, throughput, reliability and cost fields in tos of IP packet, which ranges from 0 to 15. **diffserv-value** stands for the entire tos field. **Ip-access-list** stands for the name of the matched IP access list. The name has 1 to 20 characters. **Ipv6-access-list** stands for the name of the matched IPv6 access list. The name has 1 to 20 characters. Configures the name of the matched MAC access list. The name has 1 to -20 characters.
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.

Setting the Actions of the Matchup Data Flow of the QoS Policy Mapping

The actions to define the data flow mean to take corresponding actions to a data flow with compliance of the filtration rule, which include bandwidth limit, drop, update, etc.

Enter the management mode and run the following commands to set the action of a policy, matching up the data flow. The action will replace the previous settings.

Command	Purpose
config	Enters the global configuration mode.
[**no**]**policy-map** *name*	Enters the configuration mode of the QoS policy map. name stands for the name of the policy.
action{**bandwidth** *max-band* **|cos** *cos* **| drop | dscp** *dscp-value* **| precedence** *precedence-value* **| forward | icos** *icos* **| ivlanID** { **add** *addivlanid* | *ivlanid*}**| monitor** *session-value* **| quequ** *ququ-*	**max-band** stands for the occupied maximum bandwidth: 1-163840. Unit: 64Kbps Configures policing. **Cos:** Configures the matching flow COS value; the valid range is 0 to 7.

value **| redirect** *interface-id* **| stat-packet | stat-byte | vlanID** { **add** *addvlanid* | *vlanid*} **| copy-to-cpu**}
no action {**bandwidth | cos | drop | dscp | precedence | forward | | icos | ivlanID | monitor | quequ | redirect | stat-packet | stat-byte | vlanID | copy-to-cpu**}
	drop means to drop the matched packets.
	dscp-value: Sets the matched DSCP field to dscp-value 0~63.
	precedence-value stands for the priority field in tos of IP packet (5-7 of tos), which ranges from 0 to 7.
	Forward: Conducts no operations to the matched packets.
	Icos: Sets the matched COS field to cos-value 0-7.
	ivlanID used to replace or add the inner vlan ID, which ranges from 1 to 4094.
	session-value is used to set mirroring, which ranges from 1 to 4.
	queue-value is used to set the mapping queue, which ranges from 1 to 8.
	Interface-id: Redirects the egress port of the matched flow.
	stat-packet stands for the number of packets under statistics.
	stat-byte means the number of bytes under statistics.
	vlanID is used to replace or add the outer vlan ID, which ranges from 1 to 4094.
	copy-to-cpu means to send message to CPU.

exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.

Applying the QoS Policy on a Port

The QoS policy can be applied to a port; multiple QoS policies can be applied to the same port and the same QoS policy can also be applied to multiple ports. On the same port, the priorities of the policies which are earlier applied than those of the policies which are later applied. If a packet is set to have two policies and the actions are contradicted, the actions of the firstly matched policies. After a QoS policy is applied on a port, the switch adds a policy to this port by default to block other data flows, which are not allowed to pass through. When all policies on a port are deleted, the switch will automatically remove the default blockage policy from a port.

Enter the following management mode and run the following commands to apply the QoS policy.

Command	Purpose

config	Enters the global configuration mode.
interface g0/1	Enters the to-be-configured port.
[**no**] **qos policy** *name* { **ingress**|**egress**}	Applies the QoS policy on a port. name stands for the name of QoS policy mapping. ingress means to exert an influence on the ingress. egress means to exert an influence on the egress.
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.

Applying the QoS Policy Globally

Enter the following management mode and run the following commands to apply the QoS policy.

Command	Purpose
config	Enters the global configuration mode.
[**no**] **qos policy** *name* **ingress**	Applies the QoS policy globally. name stands for the name of QoS policy mapping. ingress means to exert an influence on the ingress.
exit	Goes back to the EXEC mode.

Configuring Trust Mode

When configuring the trust mode under the global configuration mode, there are three options: cos, dscp or untrust. The data will be mapped to the queue in the option chosen above. If choosing the option: untrust, the priority of the packet will be mapped to the queque by default.

Configuring the trust mode in EXEC mode as the following steps:

Command	Purpose
config	Enters the global configuration mode.
[**no**] **qos trust** { cos | dscp | untrust }	Configuring the trust mode in the global configuration mode. Untrust stand for not trust any modes.
exit	Goes back to the EXEC mode.

Displaying the QoS Policy Mapping Table

You can run the show command to display all or some designated QoS policy maps.

Run the following command in management mode to display the QoS policy mapping table.

Command	Purpose
show policy-map [*policy-map-name* | *interface* | *global*]	Displays all or some designated QoS policy maps. policy-map-name stands for the name of QoS mapping table. Interface stand for the QoS policy applied on a port. Global stand for the QoS policy for Global application.

QoS Configuration Example

Example for Applying the QoS Policy on a Port

The following example shows how to configure a QoS Policy that meet the IP access list on port g0/2:

```
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 pmap
classify ip ipacl
action drop
interface g0/2
qos policy pmap ingress
```

31. DoS Attack Prevention Configuration

DoS Attack Overview

Concept of DoS Attack

The DoS attack is also called the service rejection attack. Common DoS attacks include network bandwidth attacks and connectivity attacks. DoS attack is a frequent network attack mode triggered by hackers. Its ultimate purpose is to break down networks to stop providing legal users with normal network services.

DoS attack prevention requires a switch to provide many attack prevention methods to stop such attacks as Pingflood, SYNflood, Landattack, Teardrop, and illegal-flags-contained TCP. When a switch is under attack, it needs to judge which attack type it is and handles these attack packets specially, for example, sending them to CPU and drop them.

DoS Attack Type

Hackers will make different types of DoS attack packets to attack the servers. The following are common DoS attack packets:

Ping of Death

Ping of Death is the abnormal Ping packet, which claims its size exceeds the ICMP threshold and causes the breakdown of the TCP/IP stack and finally the breakdown of the receiving host.

Tear Drop

TearDrop uses the information, which is contained in the packet header in the trusted IP fragment in the TCP/IP stack, to realize the attack. IP fragment contains the information that indicates which part of the original packet is contained, and some TCP/IP stacks will break down when they receive the fake fragment that contains the overlapping offset.

SYN Flood

A standard TCP connection needs to experience three hand-shake processes. A client sends the SYN message to a server, the server returns the SYN-ACK message, and the client sends the ACK message to the server after receiving the SYN-ACK message. In this way, a TCP connection is established. SYN flood triggers the DoS attack when the TCP protocol stack initializes the hand-shake procedure between two hosts. After receiving SYN-ACK information, the request party adopts source address cheat causing the service party cannot receive ACK response. Subsequently, the service party will be in the phase of waiting ACK information. If there is continuous connection request from the attacker, TCP connection queue of this server will be blocked and the network bandwidth decreased rapidly, result in the network cannot provide normal service.

Land Attack

The attacker makes a special SYN message (the source address and the destinationaddress are the same service address). The SYN message causes the server to send the SYN-ACK message to the sever itself, hence this address also sends the ACK message and creates a null link. Each of this kinds of links will keep until the timeouttime, so the server will break down. Landattack can be classified into IPland andMACland.

DoS Attack Prevention Configuration Task List

As to global DoS attack prevention configuration, you configure related sub-functions and then the switch drops corresponding DoS attack packets. Hence, the bandwidth of the switch is guaranteed not to be used up.

DoS attack prevention configuration tasks are shown below:

DoSATTACK PREVENTIONconfiguration tasks are shown below:

Configuring DoS Attack Prevention Function

DoS Attack Prevention Configuration Tasks

Configuring Global Dos Attack Prevention

Configuring global DoS attack prevention means configuring DoS attack prevention sub-functions in global mode and each sub-function can prevent a different type of DoS attack packets. The DoS IP sub-function can prevent the LAND attacks, while the DoS ICMP sub-function can prevent Ping of Death. You can set the correspondingsub-function according to actual requirements.

Configure the DoS attack prevention function in EXEC mode.

Command	Purpose
config	Enters the global configuration mode.
[**no**] **dos enable {all | icmp *icmp-value* | ip | l4port | mac | tcpflags | tcpfrag *tcpfrag-value* | tcpsmurf | icmpsmurf | ipsmurf }**	Configures **all** to prevent all types of DoS attack packets. Configures **icmp** to prevent the ICMP packets which is longer than **icmp-value** from PING attack, among which the **icmp-value** meansthe maximum length of the ICMP packet, that is, 0-1023 bytes. Configures **ip** to prevent those IP packets whose source IPs are the same as the destination IPs. Configures **l4port** to prevent those TCP/UDPpackets whose source port IDs are destination port IDs. Configures **mac** to prevent the packet whose source MACs are the same as the destination MACs. Configures **tcpflags** to prevent those TCP packets containing illegal TCP flags. Configures **tcpfrag** to prevent the to-be-detected TCP packets whose minimum TCP header istcpfrag-value. Configures **tcpsmurf** to prevent those TCP

	packets whose destination addresses are boardcast addresses. Configures **icmpsmurf** to prevent those ICMP packets whose destination addresses are boardcast addresses. Configures **ipsmurf** to prevent those IP packets whose destination addresses are boardcast addresses.
exit	Goes back to the EXEC mode.
write	Saves the settings.

Configuring Dos Attack Prevention

You can display the Dos attack prevention configurations through the show command.

Run the following command in EXEC mode to display the configured DoS attackprevention functions.

Command	Purpose
show dos	Displays Dos attack prevention configuration.

DoS Attack Prevention Configuration Example

The following example shows how to configure to prevent the attacks of TCP packets, which have illegal flags, and then displays user's configuration.

```
config
dos enable tcpflags
show dos
```

The following example shows how to prevent the attacks of IP packets whose source IPs are destination IPs in global mode.

```
config
dos enable ip
```

32. Attack Prevention Configuration

Overview of Filter

To guarantee the reasonable usage of network bandwidth, this switch series provides the function to prevent vicious traffic from occupying lots of network bandwidth.

Filter can identify the packets received by the interface of the switch and calculate them according to the packet type. In light of current attack modes, Filter can calculate the number of ARP, IGMP or IP message that a host sends in a time. Once the number exceeds the threshold, the switch will not provide any service to these hosts.

Filter limits the packet from a certain host by blocking the source address. For ARP attack, Filter blocks source MAC address; for IP attacks, such as Ping scan and TCP/UDP scan, Filter blocks source IP address.

The Mode of Filter

The mode of Filter determines how the switch specifies the attack source. There are two modes of Filter.

Source Address Block Time (Raw)

In Raw mode, the switch will drop packets from the attack source in scheduled block-time since the attack source is determined. After block-time, the restriction on the attack source will be removed and a new calculation will be enabled.

In Raw mode, all the packets from the source address will be blocked. For instance, when the MAC address of the attack source is blocked, all packets whose source MAC address are the same with that of the attack source will be dropped, no matter it is ARP, ICMP, DHCP or other types.

Source Address Block Polling (Hybrid)

After blocking the attack source, the switch will continue calculate the packets from the attack source and detect whether the packet number exceeds the threshold before the end of Polling Interval. If the packet number exceeds the threshold, the blocking state keeps. Otherwise, the blocking will be removed. In Hybrid Mode, the packet number when initially determining the attack source and the threshold of the packet number in Polling can be configured independently.

To realize continually calculate the packet, in the hybrid mode the packet type will be matched while the source address is blocked. For instance, if the MAC address of a host is blocked as it triggers ARP attack, IP packets from the host will be sent by the switch continually, unless the host is also identified with the existence of IP attack.

Please select the mode of Filter according to your application environment. If you want to set a strict limit on the attack source and reduce the burden of switch CPU, please use Raw mode; if you want to control the attack source flexibly and resume communication of the host as soon as possible after the end of the attack, please use Hybrid mode. Note that the Filter number a switch can support in Hybrid mode is limited. In condition of inadequate Filter number, Raw mode will be adopted automatically.

32.1 Attack Prevention Configuration

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 filter parameters

Configuring the attack prevention type

Enables the attack prevention function.

Checking the State of Attack Prevention

Attack Prevention Configuration

Configuring the Attack Filter Parameters

In global configuration mode, run the following command to configure the parameters of Filter.

Command	Purpose
Switch# **config**	Enters the global configuration mode.
Switch_config# **filter period** *time*	Sets the attack filter period to time. Its unit is second.
Switch_config# **filter threshold** **[arp | bpdu | dhcp | igmp | ip | icmp | icmpv6]** *value*	Sets the attack filter threshold to value.
Switch_config# **filter block-time** *time*	Sets the out-of-service time (block-time) for the attack source when the attack source is detected. Its unit is second.
Switch_config# **filter polling period** *time*	Sets the filter polling period in Hybrid mode. Its unit is second.
Switch_config# **filter polling threshold** **[arp | bpdu | dhcp | igmp | ip | icmp | icmpv6]** *value*	Sets the filter polling threshod in Hybrid mode.
Switch_config# **filter polling auto-fit**	Sets the corresponding parameters of period and threshold of polling filter which adapts to the attack source filter. The command is efficient by default. The polling period equals with the attack filter period and the polling packet threshold equals to 3/4 of the attack filter packet threshold

Switch_config# **filter shutdown-action**	Shutdown the port when detecting the attack in a raw mode.

Configuring the Attack Prevention Type

In global and interface configuration mode, use the following command to configure the type of attack filter.

Command	Purpose
Switch# **config**	Enters the global configuration mode.
Switch_config# **filter dhcp**	Enables DHCP packet attack filter in the global configuration mode.
Switch_config# **filter icmp**	Enables ICMP packet attack filter.
Switch_config# **filter icmpv6**	Enables ICMPv6 packet attack filter.
Switch_config# **filter igmp**	Enables IGMP packet attack filter.
Switch_config# **filter ip source-ip**	Enables IP attack filter in the global configuration mode.
Switch_config# **interface intf-name**	Enters the interface configuration mode.
Switch_config_intf# **filter arp**	Enables ARP packet attack filter on the interface.
Switch_config_intf# **filter bpdu**	Enables BPDU packet attack filter on the interface.
Switch_config_intf# **filter dhcp**	Enables DHCP packet attack filter on the interface.
Switch_config_intf# **filter icmp**	Enables ICMP packet attack filter on the interface.
Switch_config_intf# **filter icmpv6**	Enables ICMPv6 packet attack filter on the interface.
Switch_config_intf# **filter ip source-ip**	Enables IP packet attack filter on the interface.

Note:

ARP attack takes the combination "the host mac address + the source port" as an attack source. That is to say, packets with the same MAC address but coming from different ports, the count will not be accumulated. Both the IGMP attack and IP attack take the host’s IP address and source port as the attack source.

Note:

The IGMP attack prevention and the IP attack prevention cannot be started up together.

2. IP, ICMP, ICMPv6 and DHCP filter take effect only in global and interface configuration mode.

Enabling the Attack Prevention

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	Purpose
Switch_config# **filter enable**	Enables the attack prevention function.
Switch_config# **filter mode** [**raw** | **hybrid**]	Sets the mode of Filter: Raw or Hybrid.

Use the no filter enable command to disable the attack prevention function and remove the block to all attack sources.

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	Purpose
show filter	After attack prevention is started, you can run the following command to check the state of attack prevention:
show filter summary	Checks the parameter configuration and summary information of Filter.

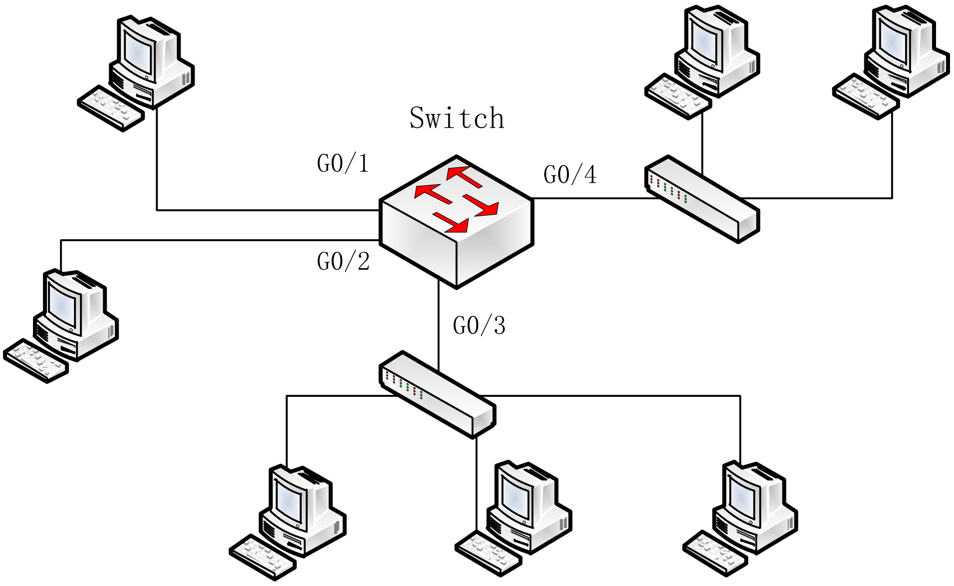
32.2 Attack Prevention Configuration Example

Note:

The examples shown in this chapter is only a reference for Filter configuration. Please configure according to your actual network condition.

Using Filter ARP to Protect the LAN

As shown in the following figure, configure ARP attack Filter on Switch.



Sets the parameter of Filter. A host sending more than 100 ARP messages in 10s will be taken as an attack source.

```
Switch# config
Switch_config# filter period 10
Switch_config# filter threshold arp 100
```

Sets APR attack filter with 4 ports:

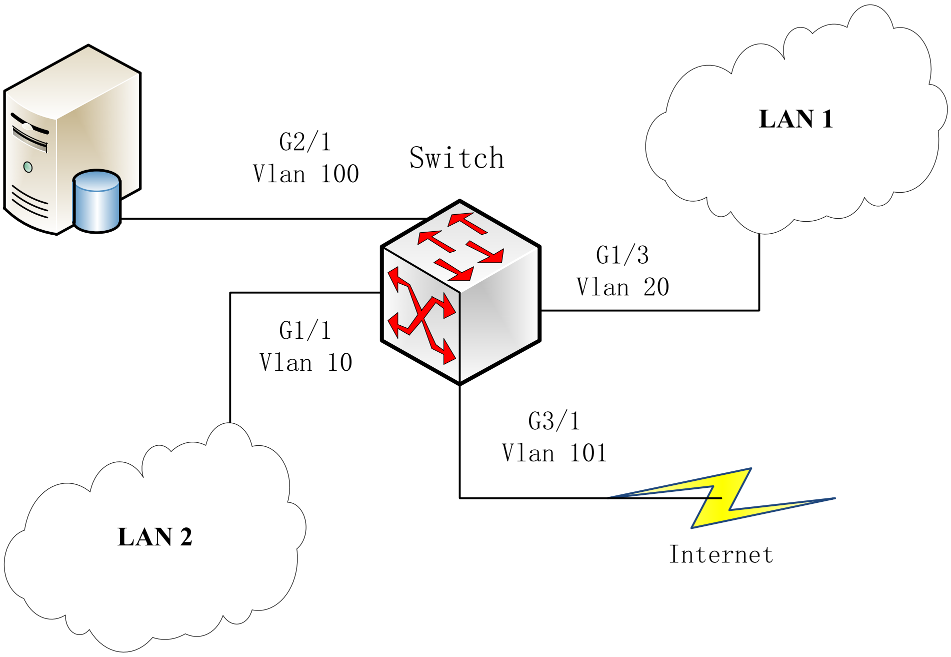
```
Switch_config# interface range g0/1 - 4
Switch_config_intf# filter arp
```

Sets Raw mode and enable Filter:

```
Switch_config_intf# exit
Switch_config# filter mode raw
Switch_config# filter enable
```

Using Filter IP to Protect Layer-3 Network

As shown in the following figure, Switch is connected to multiple LANs, servers and the internet. IP packet attack prevention can block IP scan of cross-subnet and large network connections triggered by BitTorrent in a short time.



Sets the parameter of Filter. A host sending more than 300 ARP messages in 1 minute will be taken as an attack source.

```
Switch# config
Switch_config# filter period 60
Switch_config# filter threshold ip 300
```

Enable IP packet filter in the global configuration mode and the interface mode. Note that the interface connecting the server and the external network is no need to configure:

```
Switch_config# filter ip source-ip
Switch_config# interface g1/1
Switch_config_g1/1# filter ip source-ip
Switch_config_g1/1# interface g1/3
Switch_config_g1/3# filter ip source-ip
Switch_config_g1/3# exit
Switch_config#
```

Enables Filter:

```
Switch_config# filter enable
```

33. Network Protocol Configuration

Configuring IP Addressing

IP Introduction

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 “Configuring IP Addressing.” IP services such as ICMP, HSRP, IP statistics and performance parameters are to be described in “Configuring IP Services.”

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 “IP Addressing Example.”

IP address configuration task list:

Configuring IP address at the network interface

Configuring multiple IP addresses at the network interface

Configuring Address Resolution

Detecting and maintaining IP addressing

Configuring IP Address

Configuring IP Address at the 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 223.255.254.0 223.255.255.0	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:

Command	Purpose
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.

Configuring multiple IP addresses at the 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 IP 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.

Command	Purpose
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.

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 professionals 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 entries if you do not want the ARP entry 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:

Command	Purpose
arp ip-address hardware-address vlan	Globally map an IP address to a MAC address in the ARP cache.
arp ip-address hardware-address vlan **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:

Command	Purpose
arp timeout *seconds*	Set the timeout time of the ARP cache item in the ARP cache.
arp dynamic	Enables arp dynamic learning in the interface

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 entries in the ARP cache.

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:

Command	Usage Guidelines
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.

Sets the maximum retransmissions of the Re-Detect packets.

The ARP entries (to be tagged with G), which the routing entry gateway depends on, require being re-detected at their aging so that the promptness and correctness of the hardware subnet routing can be guaranteed. The greater the retransmission times, the more likely to re-detect.

Command	Usage Guidelines
arp max-gw-retries *number*	Sets the maximum retransmissions of the Re-Detect packets. The default is 3.

Sets re-detection when ARP entry is aging.

By default only ARP depends on routing entry has re-detection when aging. After enable this command, all ARP entries will adopt aging re-detection mechanism.

Command	Usage Guidelines
arp retry-allarp	Sets re-detection when the ARP entry is aging.

2. Mapping host name to IP addres

Any IP address can correspond to a host name. The system has saved a mapping (host name to address) cache which can be telneted or pinged.

To designate a mapping from host name to address, run the following commands in global mode:

Command	Purpose
ip host *name address*	Statically map the host name to the IP address.

Detecting and maintaining IP addressing

To detect and maintain the network, run the following command:

3. 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:

Command	Purpose
clear arp-cache	Clear the IP ARP cache.

4. 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:

Command	Purpose
show arp	Display content in the ARP table.
show hosts	Display the cache table about hostname-to-IP mapping.
show ip interface [*type number*]	Displays the state of a port.
ping {**host | address**}	Test the reachability of the network node.

IP Addressing Example

The following case shows how to configure the IP address on interfaceVLAN11.

```
interface vlan 11
ip address 202.96.2.3 255.255.255.0
```

Chapter 2 Configuring DHCP

Overview

Dynamic Host Configuration Protocol (DHCP) is used to provide some network configuration parameters for the hosts on the Internet which is described in details in RFC 2131. One of the major functions of DHCP is to distribute IPs on an interface. DHCP supports the following three IP distribution mechanism:

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.

DHCP Application

DHCP can be applied at 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.

Advantages of DHCP

In current software version, the DHCP client or the DHCP client on the Ethernet interface is supported. DHCP has the following strong points:

- Fastening the settings;
- Reducing configuration errors;
- Controlling IP addresses of some device ports through the DHCP server

DHCP Terms

DHCP is based on the server/client mode. So the DHCP server and the DHCP client must exist at the same time:

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.

In a word, there exists lease time during the process of dynamic DHCP distribution:

Lease time

It means the effective period of an IP, which starts from the distribution. After the lease time, the DHCP server withdraws the IP. To continue to use this IP, the DHCP client needs to apply it again.

Configuring DHCP Client

Configuration Task List of DHCP Client

- Obtaining an IP address
- Specifying an address for DHCP server
- Configuring DHCP parameters
- Monitoring DHCP

DHCP Client Configuration Tasks

5. Obtaining an IP address

Run the following command on the VLAN interface to obtain an IP address through the DHCP protocol for an interface.

Command	Function
ip address dhcp	Sets the IP address of an Ethernet interface through DHCP.

6. Specifying an address for DHCP server

If knowing the addresses of some DHCP servers, you can specify these servers' addresses on switch so as to reduce the time of protocol processing. You can run the following command in global mode:

Command	Function
ip dhcp-server *ip-address*	Specifies the IP address of the DHCP server.

The command is optional when you perform operations to "obtain an IP address".

7. Configuring DHCP parameters

To adjust the parameters of DHCP communication according to actual requirements, run the following commands in global mode:

Command	Function
ip dhcp client minlease *seconds*	Specifies the acceptable minimum lease time.
ip dhcp client retransmit *count*	Specifies the retransmission times for DHCP packet.
ip dhcp client select *seconds*	Specify the interval for SELECT.
ip dhcp client class_identifier *WORD*	Specify the classification code of the provider.
ip dhcp client client_identifier hrd_ether	Specify the client ID as the Ethernet type
ip dhcp client timeout_shut	Specify client timeout shutdown of the interface

The command is optional when you perform operations to "obtain an IP address".

8. Monitoring DHCP

To browse related information of the DHCP server, which is discovered by the switch currently, run the following command in EXEC mode:

Command	Function
show dhcp server	Displays related information about the DHCP server, which is known by the switch.

To browse which IP address is currently used by the switch, run the following command in EXEC mode:

Command	Function
show dhcp lease	Displays IP resources, which are currently used by the switch, and related information.

Additionally, if you use DHCP to distribute an IP for an Ethernet interface, you can also run show interface to browse whether the IP address required by the Ethernet interface is successfully acquired.

DHCP Client Configuration Example

DHCP Client configuration example is shown below:

9. Obtaining an IP address

The following example shows interface vlan11 obtains an IP address through DHCP.

```
!
interface vlan 11
ip address dhcp
```

Chapter 3 IP Service Configuration

The section is to describe how to configure optional IP service. For the details of the IP service commands, refer to section “IP Service Commands”.

Configuring IP Service

Optional IP service configuration tasks are listed as follows:

Managing IP connection

Configuring performance parameters

Detecting and Maintaining IP Network

The above operations are not mandatory. You can perform the operations according to your requirements.

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:

10. 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.

Command	Purpose
ip unreachables	Enable the function to send an ICMP-unreachable message.

11. 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 canceled.

To enable the function, run the following command in interface configuration mode:

Command	Purpose
ip redirects	Permit sending the ICMP redirection messafge.

12. 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:

Command	Purpose
ip mask-reply	Send the ICMP mask reply message.

13. 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.

14. Setting IP maximum transmission unit (MTU)

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 be 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:

Command	Purpose
ip mtu *bytes*	Set IP MTU of the interface.

15. 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:

Command	Usage Guidelines
ip source-route	Authorizing IP source route.

Configuring performance parameters

Run the following command to adjust IP performance.

16. 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:

Command	Purpose
ip tcp synwait-time *seconds*	Set the wait time for TCP connection.

17. 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:

Command	Purpose
ip tcp window-size *bytes*	Set the size of TCP windows.

Detecting and Maintaining IP Network

To detect and maintain the network, run the following command:

18. Clearing cache, list and database

You can clear all content in a cache, list or database. All incorrect data in a cache, list or database need be cleared.

Run the following command to clear incorrect data:

Command	Purpose
clear tcp statistics	To clear the statistics data about TCP, run the following command:

19. Clearing TCP connection

To disconnect a TCP connection, run the following command:

Command	Purpose
clear tcp {**local** host-name port **remote** host-name port | **tcb** address}	Clear the designated TCP connection. TCB refers to TCP control block.

20. 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 EXEC mode. For details, refer to “IP Service Command”.

Command	Purpose
show ip access-lists *name*	Display the content of one or all access lists.
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	To display the statistics data about TCP, run the following command:
show tcp tcb	Display information about the designated TCP connection state.

21. Displaying debugging information

When problem occurs on the network, you can run debug to display the debugging information.

Run the following command in EXEC mode. For details, refer to “IP Service Command”.

Command	Purpose
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.

Configuring Access List

Filtering IP Packet

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 steps:

Create the access list by designating the access list name and conditions.

Apply the access list to the interface.

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:

Command	Purpose
ip access-list standard *name*	Use a name to define a standard access list.
deny {*source [source-mask]* | **any**}[**log | location**] or **permit** {*source [source-mask]* | **any**}[**log | location**]	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.

Command	Purpose
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*] [**log**][**time-range** time-range] [**location** location] [**donotfragment-set**] [**donotfragment-notset**] [**is-fragment**] [**not-fragment**] [**totallen eq|gt|lt** lentgh] [**ttl eq|gt|lt** time] [**offset-not-zero**] [**offset-zero**] {**deny | permit**} *protocol* **any any** [**precedence** *precedence*] [**tos** *tos*] [**log**][**time-range** time-range] [**location** location] [**donotfragment-set**] [**donotfragment-notset**] [**is-fragment**] [**not-**	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.)

fragment] [**totallen eq|gt|lt** lentgh] [**ttl eq|gt|lt** time] [**offset-not-zero**] [**offset-zero**]	
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 3.2.3 “Applying the Access List to the Interface”.

Apply 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.

Command	Purpose
ip access-group *name* {**in | out**}	Apply the access list to the interface.

The access control list can be used on the incoming or outgoing interface. After a packet is received, the source address of the packet will be checked according to the standard egress interface access control list. For the expanded access control list, the routing switch also checks the destination address. If the access control list permits the destination address, the system will continue handling the packet. However, if the access control list forbids the destination address, the system will drop the packet and then returns an ICMP unreachable packet.

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 control list does not exist, all packets are allowed to pass through.

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.

SMTP connects with TCP port in one end and the arbitrary port number in the other end. 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
```

Configuring IP Access List Based on Physical Port

Filtering IP Packet

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 steps:

Create the access list by designating the access list name and conditions.

Applying ACL on a port

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:

Command	Purpose
ip access-list standard *name*	Use a name to define a standard access list.
deny {*source [source-mask]* | **any**} [**log | location**] or **permit** {*source [source-mask]* | **any**} [**log | location**]	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.

Command	Purpose
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*] [**log**] [**time-range** time-range] [**location** location] [**donotfragment-set**] [**donotfragment-notset**] [**is-fragment**] [**not-fragment**] [**totallen eq|gt|lt** lentgh] [**ttl eq|gt|lt** time] [**offset-not-zero**] [**offset-zero**] {**deny | permit**} *protocol* **any any** [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** time-range] [**location** location] [**donotfragment-set**] [**donotfragment-notset**] [**is-fragment**] [**not-fragment**] [**totallen eq|gt|lt** lentgh] [**ttl eq|gt|lt** time] [**offset-not-zero**] [**offset-zero**]	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. If protocol is TCP/UDP, designate a single or 14 port number in a certain range. For more details, refer to Access List Configuration Example.
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 ACL is established, it must be applied on the lines or ports. For details, refer to section "Applying the Access List to the Interface".

Applying ACL on Ports

When ACL is established, it will be applied on one or multiple ports, or on the ingress port or egress port.

Run the following command to apply IPv6 ACL on a port:

Command	Purpose
ip access-group *name*	Applying ACL on a port

After a packet is received, the source address of the packet will be checked according to the standard egress interface access control list. For the expanded access control list, the routing switch also checks the destination address. If the access control list permits the destination address, the system will continue handling the packet. If not permit, the system will discard the packet and returns an ICMP packet that host can reach.

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

Extensible Access List Example

22. 1. Port-based IP access list supporting TCP/UDP port filtration

The format is 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*]

If you configure the access list by defining the port range, pay attention to the following:

(1) 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.

(2) 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.

23. 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   g0/1
ip access-group aaa
```

34. IP ACL Application Configuration

IP ACL Application Configuration

Applying the IP Access Control List

Applying ACL on Ports

After an ACL is established, it can be applied on one or many slots or globally.

Run the following command in port configuration mode:

Command	Purpose
config	Enters the global configuration mode.
interface g0/1	Enters the to-be-configured port.
[**no**] **{ip | ipv6} access-group** *name*	Applies the established IP access list to an interface or cancels the applied IP on the interface. Name IP: 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.

Run the following command in global configuration mode:

Command	Purpose
config	Enters the global configuration mode.
[**no**] **{ip | ipv6} access-group** *name* **[vlan {***word* **| add** *word* **| remove** *word***}]**	Applies the established IP access list on the global mode or cancels the applied IP on the global. **Egress** means that the ACL is applied in an outbound direction. **Vlan** means that the ACL is applied in an inbound VLAN. **Word** stands for the VLAN range table. **Add** means to add the VLAN range table. **Remove** means to delete the VLAN range table.
exit	Goes back to the EXEC mode.
write	Saves the settings.

Note: IP access list can be applied to VLAN in the global mode, but not to VLAN in port configuration mode.

35. IPv6 Configuration

IPv6 Protocol Configuration

IPv6 Protocol Configuration

The configuration of the IPv6 address of the router only takes effect on the VLAN interface, not on the physical interface.

The IPv6 protocol is disabled in default state. If the IPv6 protocol need be used on a VLAN interface, this protocol should be first enabled in VLAN interface configuration mode. To enable the IPv6 protocol, users have to set the IPv6 address. If on a VLAN interface at least one IPv6 address is set, the VLAN interface can handle the IPv6 packets and communicates with other IPv6 devices.

To enable the IPv6 protocol, users should finish the following task:

Setting at least one IPv6 address in VLAN interface configuration mode

Enabling IPv6

Setting the IPv6 Address

The IPv6 address is used to determine the destination address to which the IPv6 packets can be sent. There are three kinds of IPv6 addresses.

Kind	Referred Format	Remarks
Unicast address	2001:0:0:0:0DB8:800:200C:417A/64	**2001:0:0:0:0DB8:800:200C:417A** stands for a unicast address, while **64** stands for the length of the prefix of this address.
Multicast address	FF01:0:0:0:0:0:0:101	All multicast addresses begin with FF.
Any address	2002:0:0:0:0DB8:800:200C:417A/64	The format of this address is the same as that of the unicast address. Different VLAN interfaces can be set to have the same address, no matter it is a unicast/broadcast/multicast address.

For the further details of the IPv6 address, see RFC 4291.

In order to enable IPv6, users must set a unicast address in VLAN interface configuration mode. The set unicast address must be one or multiple addresses of the following type:

IPv6 link-local address

Global IPv6 address

To set an IPv6 link-local address in VLAN interface configuration mode, run the following commands.

Command	Purpose
ipv6 enable	Sets a link-local address automatically.
ipv6 address fe80::x link-local	Sets a link-local address manually.

Note:

The link-local address must begin with fe80. The default length of the prefix is 64 bit. At manual settings only the values at the last 64 bits can be designated.

On a VLAN interface can only one link-local address be set.

After IPv6 is enabled through the configuration of the link-local address, IPv6 only takes effect on the local link.

Setting the IPv6 Services

Setting the IPv6 Services

After IPv6 is enabled, all services provided by IPv6 can be set. The configurable IPv6 service is shown below:

- Managing the IPv6 Link

Managing the IPv6 Link

IPv6 provides a series of services to control and manage the IPv6 link. This series of services includes:

- Setting the MTU of IPv6
- Setting the transmission frequency of the ICMPv6 packet
- Setting IPv6 destination unreachablity
- Setting IPv6 ACL

Setting the MTU of IPv6

All interfaces have a default IPv6 MTU. If the length of an IPv6 packet exceeds MTU, the router will fragment this IPv6 packet.

To set IPv6 MTU on a specific interface, run the following command in interface configuration mode:

Command	Purpose
ipv6 mtu bytes	Sets IPv6 MTU on an interface.

Setting IPv6 redirection

Sometimes, the route selected by the host is not the best one. In this case, when a switch receives a packet from this route, the switch will transmit, according to the routing table, the packet from the interface where the packet is received, and forward it to another router which belongs to the same network segment with the host. Under this condition, the switch will notify the source host of sending the packets with the same destination address to another router directly, not by way of the switch itself. The redirection packet demands the source host to replace the original route with the more direct route contained in the redirection packet. The operating system of many hosts will add a host route to the routing table. However, the switch more trusts the information getting from the routing protocol and so the host route will not be added according to this information.

IPv6 redirection is opened by default. However, if a hot standby router protocol is configured on an interface, IPv6 redirection is automatically closed. If the hot standby router protocol is canceled, this function will not automatically opened.

To open IPv6 redirection, run the following command:

Command	Purpose
ipv6 redirects	Allows IPv6 to transmit the redirection packets.

3. Setting IPv6 destination unreachablity

In many cases, the system will automatically transmit the destination-unreachable packets. Users can close this function. If this function is closed, the system will not transmit the ICMP unreachable packets.

To enable this function, run the following command:

Command	Purpose
ipv6 unreachables	Allows IPv6 to transmit the destination unreachable packets.

4. Setting IPv6 ACL

Users can use ACL to control the reception and transmission of packets on a VLAN interface. If you introduce ACL on a VLAN interface in global configuration mode and designate the filtration's direction, the IPv6 packets will be filtered on this VLAN interface.

To filter the IPv6 packets, run the following command in interface configuration mode.

Command	Purpose
ipv6 access-group *WORD* { in | out }	Filters the IPv6 packets in the reception direction on a VLAN interface.

36. ND Configuration

ND Configuration

1. ND Overview

A node (host and router) uses ND (Neighbor Discovery protocol) to determine the link-layer addresses of the connected neighbors and to delete invalid cache rapidly. The host also uses the neighbor to discover the packet-forwarding neighboring routers. Additionally, the node uses the ND mechanism to positively trace which neighbors are reachable or unreachable and to test the changed link-layer address. When a router or the path to a router has trouble, the host positively looks for another working router or another path.

IPv6 ND corresponds to IPv4 ARP, ICMP router discovery and ICMP redirect. There is no corresponding neighbor unreachablity detection mechanism and protocol in IPv4.

ND supports the following link types: P2P, multicast, NBMA, shared media, changeable MTU and asymmetric reachability. The ND mechanism has the following functions:

(1) To discover routers: how the host to locate the routers on the connected links.

(2) To discover prefixes: how the host to find a group of address prefixes, defining which destinations are on-link on the connected links.

(3) To discover parameters: how the node to know the link-related or network-related parameters of the transmission interface.

(4) To automatically set addresses: how the node to set the address of an interface automatically.

(5) Address solution: When the IP of a destination is given, how a node determines the link-layer address of the on-link destination.

(6) To determine the next hop: it is an algorithm to map the IP address of a destination to the neighboring IP. The next hop can be a router or destination.

(7) To test unreachable neighbors: how a node to determine unreachable neighbors; if neighbor is a router, the default router can be used.

(8) To test repeated address: how a node to determine whether a to-be-used address is not used by another node.

(9) Redirect: how a router to notify the host of the best next hop.

i. Address Resolution

Address resolution is a procedure of resolving the link-layer address through node’s IP. Packet exchange is realized through ND request and ND notification.

- Configuring a static ND cache

  In most cases, dynamic address resolution is used and static ND cache configuration is not needed. If necessary, you can set static ND cache in global mode and the system will use it to translate IP into the link-layer address. The following table shows how to set a static-IP-to-link-layer-address mapping.

  Run the following relative command in global mode:

Command	Purpose
ipv6 neighbor ipv6address **vlan** vlanid hardware-address	Sets a static ND cache and translates IPv6 address into a link-layer address.

37. NTP ConfigurationTable of Contents

Stipulation

Format Stipulation in the Command Line

Syntax	Meaning
Bold	Stands for the keyword in the command line, which stays unchanged and must be entered without any modification. It is presented as a bold in the command line.
{italic}	Stands for the parameter in the command line, which must be replaced by the actual value. It must be presented by the italic in the brace.
<*italic*>	Stands for the parameter in the command line, which must be replaced by the actual value. It must be presented by the italic in the point bracket.
[ ]	Stands for the optional parameter, which is in the square bracket.
{ x | y | ... }	Means that you can choose one option from two or more options.
[x | y | ...]	Means that you can choose one option or none from two or more options.
{ x | y | ... } *	Means that you has to choose at least one option from two or more options, or even choose all options.
[x | y | ...] *	Means that you can choose multiple options or none from two or more options.
&<1-n>	Means that the parameter before the "&" symbol can be entered 1~n times.
#	Means that the line starting with the "#" symbol is an explanation line.

NTP Configuration

Overview

Network Time Protocol (NTP) is a type of computer time synchronization protocol which can be used for time synchronization between distributed time servers and clients. It has highly accurate time correction function and can prevent malicious protocol attacks through encrypted authentication. Clients and servers communicate through the User Datagram Protocol (UDP), and the port number is 123.

NTP Configuration

Configuring the Equipment As an NTP Server

Configuration mode: Global

Command	Purpose
ntp master primary	In the event that the equipment does not have an upper-level NTP server, configure the equipment as the original NTP server (stratum = 1).
ntp master secondary	In the event that the equipment has an upper-level NTP server, configure the equipment as the secondary NTP server. (In other words, the equipment cannot provide time synchronization service for NTP clients unless the "ntp server" command is configured and time synchronization is achieved in designated servers.)

Configuring NTP Authentication Function

Configuration mode: Global

Command	Purpose
ntp authentication enable	Enable the authentication function (disabled by default).
ntp authentication key *keyid* **md5** *password*	Configure NTP md5 authentication keyid and corresponding keys.
ntp authentication trusted-key *keyid*	Configure the keyid corresponding key as the trusted key.

Configuring NTP Association

Configuration mode: Global

Command	Purpose
ntp server *ip-address* [**version** *number* | **key** *keyid*]*	Configure the IP address of NTP server; the version number, key number.
ntp peer *ip-address* [**version** *number* | **key** *keyid*]*	Configure the IP address of equipment NTP peer; the version number, key number.

Usage Guidelines:

1. Equipment can provide time services for NTP clients provided that the equipment has achieved time synchronization; otherwise the client device that employs the equipment as its server cannot achieve time synchronization.

2. To conduct NTP authentication, both parties must open the NTP authentication function simultaneously, configure the same keyid and key, and designate the keyid as trusted; otherwise time synchronization would fail.

38. IPv6 ACL Configuration

IPv6 ACL Configuration

IPv6 ACL Configuration

Filtering IPv6 Packets

Filtering IPv6 packets helps the control packet run in the network. Such control can limit network transmission and network running by a certain user or device. For enabling or disabling packets from the cross designated port, we provide with ACL. You can use IPv6 ACL as follows:

Limit of packet transmission on the port

Limit of virtual terminal line access

Limit of the route update

This chapter summarizes how to set up IPv6 ACL and how to apply them.

IPv6 ACL is a well-organized set which applies enable/disable of IPv6 address. ROS of the switch will test addresses in ACL accordingly. The first match determines whether the software accept or refuse the address. Because after the first match, the software will stop the match rule, the sequence of the condition is important. If there is no rule to match, the address will be refused.

Steps for using ACL:

Set up ACL by designating ACL name and ACL conditions.

Apply ACL to the port.

Setting up IPv6 ACL

Use a character string to set up IPv6 ACL.

Note:

The standard ACL and the expanded ACL cannot be the same.

In order to set up IPv6 ACL, run the following command in the global configuration mode.

Command	Purpose
IPv6 access-list *name*	Use the name to define an IPv6 ACL.
{**deny** | **permit**} *protocol* {*source-ipv6-prefixlprefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**routing**] [**sequence** *value*] [**time-range** *name*]	In the configuration mode of IPv6 ACL, designate one or multiple enable/disable conditions. This determines whether to pass the packet or not. (dscp is used for matching IPv6 grouping header Traffic Class domain, flow-label is used for matching Flow Label tag domain of IPv6 grouping header, fragments is used for matching fragment grouping when the grouping expansion header includes none-0 offset; log means whether to record

	log, routing is used for the source grouping of the route expansion header of IPv6 grouping header, time-range is used for limit the time range of ACL.)
Exit	Exit from the configuration mode of ACL.

After setting up ACL, any additional parts will be affiliated to the end of the ACL if no sequence is added to the rule deny or permit. In other words, add [**sequence** value] in the front or back of the rule deny/permit, you can add ACL commands in any position of the designated ACL.

Likewise, you can use “no permit” and “no deny” to delete an item in ACL or “no sequence” to delete the rule in a certain position directly.

Note:

When setting up ACL, please remember the end sentence of ACL by default covers the sentence of **deny ipv6 any any.**

The ACL must be applied to the line or port after being set up. Refer to the description of “Apply the ACL to the port”.

Applying ACL to the Ports

ACL can be applied to one or multiple ports or the ingress.

Run this command in the configuration mode.

Command	Purpose
IPv6 access-group *name*	Apply ACL to the port.

For the standard ingress ACL, check the source address of the packet after receiving it. For the expanded ACL, the routing switch also checks the objective address. If the ACL enables the address, the software continues to handle the packet. If ACL does not allow the address, the software will drop the packet and returns one ICMP host unreachable packets.

If there is no designated ACL, all packets will be allowed to pass.

Examples of IPv6 ACL

In the following example, please first enable to connect with the individual destination host of the host A:B:C:D::E and disable the new TCP to connect with SMTP port whose host IPv6 source prefix 255:255:255::/48. The next rule sequence of the final ACL comes before the former rule.

```
Switch_config#ipv6 access-list   xxcom
Switch_config_ipv6acl#permit any host A:B:C:D::E sequence 20
Switch_config_ipv6acl#deny tcp any 255:255:255::/48 eq 25 sequence 10
Switch_config_ipv6acl#ex
Switch_config#show ipv6 access-lists xxcom
ipv6 access-list xxcom
   deny tcp any 255:255:255::/48 eq smtp sequence 10
   permit ipv6 any host A:B:C:D::E sequence 20
```

39. IP-Attack Prevention Configuration

IP-Attack Prevention Configuration

Overview

To ensure the reasonable use of network bandwidth, the company's switches provide the IP-Attack Prevention function to prevent malicious IP traffic from occupying the network bandwidth. For the common attacks at present, communication restrictions are imposed on hosts that send a large number of ICMP, IGMP or IP packets over a period of time, and no network services are provided to these hosts. This configuration can prevent the problem of network congestion caused by malicious packets occupying a large amount of network bandwidth.

IP-Attack Prevention Configuration Task List

When the number of IGMP, ICMP, or IP packets sent by a host within any specified time interval exceeds the threshold, we assume that an attack occurs on the network.

You can choose the anti-attack types (ICMP, IGMP or IP), the application ports and attack detection parameters. The configuration tasks inlclude:

Configure IP-Attack Prevention type

Configure IP attack detection parameters

IP-Attack Prevention Configuration

Configuring IP attack detection parameters

Command	Purpose
ip verify log-enable	Enable/disable attack detection system log
ip verify filter *time*	When the attack source is identified, stop service for them. The adjustment unit is seconds, the default time is 180 seconds

Configuring the IP attack detection type

Command	Purpose
ip verify icmp ping-flood *value*	Limit ping packet reception. **value** means the detection threshold.
ip verify icmp ping-sweep *time*	Limit ping scanning. **time** means detection period, unit is second.
ip verify tcp syn-flood *value*	Restrict tcp syn packet reception. **value** means the detection threshold.

ip verify tcp syn-sweep *time*	Limit tcp syn port scanning. **time** means detection period, unit is second.
ip verify tcp fin-scan *time*	Limit tcp stealth fin scanning. **time** means detection period, unit is second.
ip verify tcp rst-flood *value*	Limit tcp rst packet reception. **value** means the detection threshold.
ip verify udp udp-flood *value*	Limit udp packet reception. **value** means the detection threshold.
ip verify udp udp-sweep *time*	Limit udp scanning. **time** means detection period, unit is second.
ip verify attack Xmas-Tree *time*	Filter Xmas-Tree scanning attacks. **time** means detection period, unit is second.
ip verify attack Null-scan *time*	Filter Null scanning attacks. **time** means detection period, unit is second.
ip verify attack Land	Filter Land attacks.
ip verify attack Smurf	Filter Smurf attacks.
ip verify attack WinNuke	Filter WinNuke attacks.
ip verify attack TearDrop	Filter TearDrop attacks.
ip verify attack Fraggle	Filter Fraggle attacks.

Enabling IP-Attack Prevention function

When all the parameters for anti-attack are configured, the anti-attack function can be activated. It should be noted that the attack prevention function takes up a small amount of processor space.

Command	Purpose
ip verify enable	Enable/disable attack detection.

With no form of this command is used, the attack detection is disabled, and all blocked attack sources are unblocked.

Examples of IP-Attack Prevention Configuration

To enable the port scanning anti-attack, you can configure as follows. When any host scans the port more than one scanning unit in any 15 seconds, it is considered as an attack and block network service for 10 minutes.

```
ip verify icmp ping-sweep 15
ip verify tcp syn-sweep 15
ip verify udp udp-sweep 15
ip verify enable
ip verify log-enable
ip verify filter 600
```

IP Attacks Prevention against Direct Network Segment Scanning

Overview

To prevent malicious attacks from sending a large number of scan packets to the directly connected route, the switch creates a software cache for unreachable addresses of the directly connected route to increase CPU utilization. The function of IP attacks prevention against direct network segment scanning can deal with attacks to reduce the CPU utilization.

Configuration task list of IP Attacks Prevention against Direct Network Segment Scanning

When the number of incomplete arps on a switch vlan exceeds a certain number, we think the switch has received an attack from direct network segment scanning.

When the number of unreachable IP packets within any specified time interval exceeds the threshold, we assume that an attack occurs, then record and print to prompt the user.

The user can select the function mode and attack detection parameters of the anti-direct network segment scanning attack. The configuration tasks include:

Configure detection parameters of IP attacks prevention against direct network segment scanning

Configure detection types of IP anti-direct network segment scanning detection types

Note:

The **ip verify ip-sweep action rate-limit-attacker** command will override the **ip verify ip-sweep action rate-limit** command, otherwise you need to configure **no ip verify ip-sweep action rate-limit-attacker** first to configure **ip verify ip-sweep action rate-limit**. Time and packet parameters are inherited when overwriting.

Configuring IP Attacks Prevention against Direct Network Segment Scanning

Configuring detection parameters of IP attacks prevention against direct network segment scanning

Command	Purpose
ip verify filter *time*	When the attack source is identified, stop service for the attack source. The adjustment unit is seconds, the default time is 180 seconds.

Configure detection types of IP anti-direct network segment scanning detection types

Command	Purpose
ip verify ip-sweep action rate-limit	Limit the number of IP packets
ip verify ip-sweep action rate-limit *time packets*	Limit the number of ip packets, configure the limited time period and the maximum number of ip packets allowed in this period.
ip verify ip-sweep action rate-limit-attacker	Only limit the number of packets defined as attacker's ip packets.
ip verify ip-sweep action rate-limit-attacker *time packets*	Limit the number of packets defined as attacker's ip packets. Configure the limited time period and the maximum number of ip packets allowed for the source address in the period.
ip verify ip-sweep action no-cache	Prohibit the creation of cache for unknown hosts directly connected to the network segment.

Enable IP Attacks Prevention against Direct Network Segment Scanning

When all the parameters are configured, you can enable the IP attacks prevention against direct network segment scanning. It should be noted that the attack prevention function takes up a small amount of processor space.

Command	Purpose
ip verify ip-sweep detect unknown-host	Enable/disable the anti-attack function for IP scanning of unknown hosts on the directly connected network.

With no form of this command is used, the attack detection is disabled, and all blocked attack sources are unblocked.

Examples of IP Attacks Prevention against Direct Network Segment Scanning

To enable the IP attacks prevention against direct network segment scanning, you can configure as follows. That is, the detected attacker is only allowed to forward 200 IP packets every two seconds and the cache of unknown direct network segment hosts is prevented. In addition, the entire test result is reset every 10 minutes,

```
ip verify filter 600

ip verify ip-sweep detect unknown-host

ip verify ip-sweep action no-cache

ip verify ip-sweep action rate-limit 2 200
```

Detection Results of IP Attacks Prevention against Direct Network Segment Scanning

```
Jan    1 00:07:14 Unknown-host (connected network sweep) attack detected
Jan  1 00:07:14 Action rate-limit-attacker is being used.
Jan  1 00:07:14 Action no-cache is being used.
Jan  1 00:07:14 Connected network sweep attacker 100.1.1.2 detected, VLAN 100, port g2/1
Jan  1 00:07:14 [SLOT 2]Connected network sweep attacker 100.1.1.2 detected, VLAN 100, port g2/1
```

When the anti-direct network segment scanning attack and rate-limit-attacker and action no-cache defense methods are enabled, an attacker’s IP network segment scanning attack with port vlan 100, physical port g2/1, and IP address 100.1.1.2 is received, please deal with it as soon as possible.

40. Cable Diagnostic ConfigurationTable of Contents

Cable Diagnostic Configuration

Enable the Ethernet interface cable diagnostic

To enable cable diagnostic under interface mode, use the following command.

Command	Purpose
cable-diagnostic {**period** | **<cr>**} (TX port)	Set the period of the port cable check. If it is 0, it will be checked only once.
No cable-diagnostic	Restore the default setting without checking the port cable.

Note:

The diagnostic results cannot guarantee the accuracy of the cables produced by all manufacturers. The test results are for reference only.

This command may affect the normal use of the interface's services in a short time. After the execution, you can view the test result with the **show interface** command:

Examples are as follows:

```
show interface g0/4
........................................
 Cable Ok (4 pairs)
     Pair A Ok, length < 1 metres
     Pair B Ok, length < 1 metres
     Pair C Ok, length < 1 metres
     Pair D Ok, length < 1 metres
..........................................
```

Cable status:

l OK: indicates that the wire pair ends normally.

l Open: indicates that the wire pair is open.

l Short: indicates that the wire pair is short circuited.

l Crosstalk (crosstalk): indicates that there is crosstalk between the wire pairs (interference with each other).

l Unknown: Other causes of failure.