



Configuration Preparation

Table of Contents

Chapter 1 Configuration Preparation.....	1
1.1 Switch Port Number.....	1
1.2 Before Starting up Switch.....	1
1.3 Help.....	2
1.4 Command Mode.....	2
1.5 Canceling the Command.....	3
1.6 Saving the Settings.....	3

Chapter 1 Configuration Preparation

This document provides the information that you need when configures your switch for the first time, including the port number, necessary procedures before the switch is started up and introduction of Command-Line interface.

- Switch Port Number
- Before Starting up Switch
- Help
- Command Mode
- Canceling the Command
- Saving the Settings

1.1 Switch Port Number

Switch physical port number are formatted as <type><slot>/<port>, types and names of which are listed in the following comparison table:

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

The expansion slot number in standard configuration is always 0. The others begin at 1 and continue from left to right.

Ports number in the same expansion slot is numbered from bottom to top and from left to right, starting with 1. If only one port exists, it is numbered 1.

Note:

Ports in modules are numbered orderly from bottom to top and from left to right.

1.2 Before Starting up Switch

Before configuring after turning on the switch, please confirm the following steps:

- (1) Setup Switch Hardware following the manual.
- (2) Configure the PC Terminal Emulation procedure.
- (3) Making a IP address planning first as per IP network protocol.

1.3 Help

By a question mark (?) or direction keys, you can obtain the associated information for any command:

- The currently available command list can be presented if you enter a question mark.
Switch> ?
- The currently available commands starting with the known characters in the list can be displayed if you enter the known characters and then a question mark (without space).
Switch> s?
- The parameter list of a command will be obtained if you enter the command, press "Space" and enter the question mark.
Switch# show ?
- The previously entered commands can be presented if you press the "up" arrow key. If you continue press the "up" arrow key, more commands can be shown. If you press the "up" arrow key and then the "down" arrow key, the next command line following the current one can be presented.

1.4 Command Mode

The window for the switch's command line can be in multiple modes: Each command mode allows you to set a different suite on a switch, while the presently available commands are up to your current command mode. Input a question mark to list all commands available for current command mode The following table shows frequent command modes:

Command Mode	Access mode	Window prompt	Logout mode
System Supervision Mode	Type "Ctrl-p" after power on	monitor#	None
User mode	Login	Switch>	Run the "exit" or "quit" command.
EXEC mode	Enter the "enter" or "enable" command in user mode.	Switch#	Run the "exit" or "quit" command.
Global Configuration mode	Enter the "config" command in EXEC mode.	Switch_config#	Run the exit or quit command or just press the "Ctrl-z" composite key to return the EXEC mode.
Port configuration mode	Type the interface command in global Configuration Mode, e.g. interface g0/1	Switch_config_g0/1#	Run the exit or quit command or just press the "Ctrl-z" composite key to return the EXEC mode.

Each command mode will certainly limit you to use a certain command subset. If you have trouble in inputting a command, check the interface prompt and input the question mark (?) for a list of available commands. You might be in the wrong command mode or using incorrect syntax.

In the following example, please pay attention to the change of the window prompt and its new command mode:

```
Switch> enter
Password: <enter password>
Switch# config
Switch_config# interface g0/1
Switch_config_g0/1# quit
Switch_config# quit
Switch#
```

1.5 Canceling the Command

If you want to cancel a command or resume the default attributes, usually add the “no” keyword before most commands.

For example, no ip address.

1.6 Saving the Settings

You may need to save the configuration changes, so that you can recover the original configuration in case of system restarted or power cuts. You can use write command to save configuration in the Administration Mode or Global Configuration Mode.

Basic Configuration

Table of Contents

- Chapter 1 System Management Configuration.....1
 - 1.1 File Management Configuration..... 1
 - 1.1.1 Managing the file system.....1
 - 1.1.2 Commands for the file system..... 1
 - 1.1.3 Starting up from a file manually..... 1
 - 1.1.4 Updating software.....2
 - 1.1.5 Updating configuration..... 3
 - 1.1.6 Using ftp to perform the update of software and configuration..... 3
 - 1.2 Basic System Management Configuration..... 4
 - 1.2.1 Configuring Ethernet IP address..... 4
 - 1.2.2 Setting the default route.....4
 - 1.2.3 Using ping to test network connection state.....5
- Chapter 2 Terminal Configuration.....6
 - 2.1 VTY Configuration Overview..... 6
 - 2.2 Configuration Tasks.....6
 - 2.2.1 Relationship between line and interface..... 6
 - 2.3 Monitor and Maintenance.....6
 - 2.4 VTY Configuration Example.....7
- Chapter 3 SSH Configuration Commands.....8
 - 2.5 SSH Overview..... 8
 - 2.5.1 SSH server.....8
 - 2.5.2 SSH client..... 8
 - 2.5.3 Attribute Realization.....8
 - 2.6 Configuration Tasks.....8
 - 2.6.1 Configuring the Authentication Method List..... 8
 - 2.6.2 Configuring Access List.....8
 - 2.6.3 Configuring the Authentication Timeout Time.....9
 - 2.6.4 Configuring the Authentication Retry Times..... 9
 - 2.6.5 Configuring the Login Silence Period..... 9
 - 2.6.6 Enabling SFTP..... 9
 - 2.6.7 Enabling Encryption Key Saving Function.....10
 - 2.6.8 Enabling SSH Server..... 10
 - 2.7 Configuration Example of SSH Server..... 10
 - 2.7.1 ACL..... 10
 - 2.7.2 Global Configuration..... 10

Chapter 1 System Management Configuration

1.1 File Management Configuration

1.1.1 Managing the file system

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

1.1.2 Commands for the file system

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

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

1.1.3 Starting up from a file manually

```
monitor#boot flash <local_filename>
```

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

Description

Parameters	Description
Flash	A file name stored in the flash memory
<i>local_filename</i>	file name, the user must enter the file name

Example

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

1.1.4 Updating software

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

There are two ways of software update in monitor mode.

Through TFTP protocol

```
monitor#copy tftp flash: [ip_addr]
```

The command 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.

Description

parameters or keywords	Description
flash:	The memory device is flash memory.
ip_addr	Means the IP address of the TFTP server. If this parameter is not designated, you are prompted 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#
```

1.1.5 Updating configuration

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

1. Through TFTP protocol

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

1.1.6 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>|cf<:filename>}  

flash<:filename>|cf<:filename>}{flash<:filename>|cf<:filename>}|ftp:[[[//login-name:  

[login-password]@]location] /directory]/filename} <blksize> <mode> <type>
```

Description

Parameters	Description
login-name	Username of the ftp server. If this parameter is not designated, you are prompted to enter the IP address after the copy command is run.
login-password	Password of the ftp server. If this parameter is not designated, you are prompted to enter the IP address 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 this parameter is not designated, you are prompted to enter the IP address after the copy command is run.
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.

```
switch#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

```
switch#copy ftp://login-nam:login-password@192.168.20.1/main.bin flash:switch.bin
#####
#####
FTP:successfully receive 3377 blocks ,1728902 bytes
config#
```

Note:

- 1) When the ftp server is out of service, the wait time is long. If this problem is caused by the tcp timeout time (the default value is 75s), you can configure the global command ip tcp synwait-time to modify the tcp connection time. However, it is not recommended to use it.
- 2) When you use ftp in some networking conditions, the rate of data transmission might be relatively slow. You can properly adjust the size of the transmission block to obtain the best effect. The default size is 512 characters, which guarantee a relatively high operation rate in most of the networks.

1.2 Basic System Management Configuration

1.2.1 Configuring Ethernet IP address

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

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

Description

Parameters	Description
<i>ip_addr</i>	IP address of the Ethernet
<i>net_mask</i>	Mask of the Ethernet

Example

```
monitor#ip address 192.168.1.1 255.255.255.0
```

1.2.2 Setting the default route.

```
monitor#ip route default <ip_addr>
```

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

Description

Parameters	Description
<i>ip_addr</i>	IP address of the gateway

Example

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

1.2.3 Using ping to test network connection state

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

This command is to test network connection state.

Description

Parameters	Description
<i>ip_address</i>	Stands for the destination IP address

Example

```
monitor#ping 192.168.20.100
PING 192.168.20.100: 56 data bytes
64 bytes from 192.168.20.100: icmp_seq=0. time=0. ms
64 bytes from 192.168.20.100: icmp_seq=1. time=0. ms
64 bytes from 192.168.20.100: icmp_seq=2. time=0. ms
64 bytes from 192.168.20.100: icmp_seq=3. time=0. ms
----192.168.20.100 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 0/0/0
```

Chapter 2 Terminal Configuration

2.1 VTY Configuration Overview

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

2.2 Configuration Tasks

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 0

2.2.1 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) (1) Log in to the line configuration mode.
- (2) (2) Configure the terminal parameters.

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

2.3 Monitor and Maintenance

Run show line to check the VTY configuration.

2.4 VTY Configuration Example

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

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

Chapter 3 SSH Configuration Commands

2.5 SSH Overview

2.5.1 SSH server

SSH client can provide a secure and encrypted communication link through SSH server and other devices. This connection has the same functions as those of Telnet. SSH server supports the following encryption algorithms: des, 3des and blowfish.

2.5.2 SSH client

SSH client runs on the basis of the SSH protocol, providing authentication and encryption. Due to the application of authentication and encryption, SSH client allows to establish secure communication in unsecure network environment between communication devices or between other devices that support SSH server. SSH client supports the following encryption algorithms: des, 3des and blowfish.

2.5.3 Attribute Realization

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

2.6 Configuration Tasks

2.6.1 Configuring the Authentication Method List

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

In global configuration mode, the following command can be used to configure the authentication method list.

Command	Purpose
ip sshd auth-method STRING	Configure the authentication method list. The length of the authentication method's name is no more than 20 characters.

2.6.2 Configuring Access List

In order to control SSH server to access other devices, you can configure ACL for SSH server.

In global configuration mode, the following command can be used to configure the timeout time.

Command	Purpose
ip sshd access-class STRING	Configure ACL. The length of the access list's name is no more than 19 characters.

2.6.3 Configuring the Authentication Timeout Time

After SSH client connects SSH server successfully, the SSH server will close the connection if the authentication cannot be passed during the configured time.

In global configuration mode, the following command can be used to configure the authentication timeout.

Command	Purpose
ip sshd timeout <60-65535>	Configure the authentication timeout time.

2.6.4 Configuring the Authentication Retry Times

If the times for failed authentications exceed the maximum times, SSH server will not allow you to retry authentication and the system enters the silent period. The maximum times for retrying authentication is 6 by default.

In global configuration mode, the following command can be used to configure the authentication retry times.

Command	Purpose
ip sshd auth-retries <0-65535>	Configure the authentication retry times.

2.6.5 Configuring the Login Silence Period

The system enters in the silent period when the authentication retry times exceed the threshold. The silence period is 60s by default.

In global configuration mode, the following command can be used to configure the silence period.

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

2.6.6 Enabling SFTP

The SFTP function refers to the secure file transmission system based on SSH, of which the authentication procedure and data transmission are encrypted. Though it has low transmission efficiency, network security is highly improved.

SftpFUNCTIONis disabled by default. Run following command to enable sftpFUNCTIONin global configuration mode.

Command	Purpose
---------	---------

ip sshd sftp	Enable sftp function.
--------------	-----------------------

2.6.7 Enabling Encryption Key Saving Function

Enable ssh server and the initial encryption key needs to be calculated. The process may take one to two minutes. When enabling the encryption key saving function, the initial encryption key is saved in the flash. When enabling ssh server in a second time, the encryption key will be read first.

sftp function is disabled by default. USE THE FOLLOWING COMMAND to enable sftp FUNCTION IN GLOBAL CONFIGURATION MODE:

Command	Purpose
ip sshd save	Enable encryption key saving function.

2.6.8 Enabling SSH Server

SSH server is disabled by default. When SSH server is enabled, a RSA key pair will be generated and then listens the connection request from SSH client. The whole process probably requires one or two minutes.

The following command can be used in global configuration mode to enable SSH server:

Command	Purpose
ip sshd enable	Enable SSH server. The digit of the password is 1024.

2.7 Configuration Example of SSH Server

The following configuration allows the host whose IP is 192.168.20.40 to access SSH server, while the local user database will be used to authenticate the user.

2.7.1 ACL

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

2.7.2 Global Configuration

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

Network Management Configuration

Table of Contents

Chapter 1 Network Management Configuration	1
1.1 Configuring SNMP.....	1
1.1.1 Overview.....	1
1.1.2 SNMP Configuration Tasks.....	3
1.1.3 Configuration Example.....	10
1.2 RMON Configuration.....	11
1.2.1 RMON Configuration Tasks.....	11

Chapter 1 Network Management Configuration

1.1 Configuring SNMP

1.1.1 Overview

The SNMP system includes the following parts:

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

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

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

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

1. SNMP notification

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

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

Since inform requests are more reliable, they consume more resources of the system and network. The trap will be discarded when it is sent. The "inform request" has to be stored in the memory until the echo is received or the request timeouts. In addition, the trap is sent only once, while the "inform request" can be resent for many times. Resending "inform request" adds to network communications and causes more load on network. Therefore, trap and inform request provide balance between reliability and

resource. If SNMP management side needs receiving every notification greatly, then the "inform request" can be used. If you give priority to the communication amount of the network and there is no need to receive every notification, then trap can be used.

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

2. SNMP Version

System of our company supports the following SNMP versions:

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

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

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

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

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

The security features provided in SNMPv3 are:

- Message integrity — Ensuring that a packet has not been tampered with in-transit.
- Authentication — Determining the message is from a valid source.
- Encryption — Scrambling the contents of a packet prevent it from being seen by an unauthorized source.

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the group in which the user resides. A security level is the permitted level of security within a security model. SNMPv3 supports three security levels based on the user's security model, that is (from high to low), authentication and encryption, authentication and no encryption, no authentication. With MD5 or SHA hash algorithm, the password will not be revealed. With DES encryption, the device will not be wiretapped by a third party. To realize identity authentication of the device, you need to configure user/password pair and the group belongs to the user. To determine the access permission to the management information database, you need to configure group and view. Meanwhile, the group limits the lowest security level of users in the group.

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

3. Supported MIB

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

Our system provides its own MIB extension for each system.

1.1.2 SNMP Configuration Tasks

SNMP Configuration Tasks 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 nocode
- Configuring snmp-server event-id
- Configuring snmp-server getbulk-timeout
- Configuring snmp-server getbulk-delay
- Showing snmp running information
- Showing snmp debug information

1. Configuring SNMP view

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

Network Management Configuration

Command	Usage Guidelines
snmp-server view <i>name oid</i> [excluded included]	Adds the subtree or table of OID-specified MIB to the name of the SNMP view, and specifies the access right of the object identifier in the name of the SNMB view.

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.

2. Creating or modifying the access control for SNMP community

You can use the SNMP community character string to define the relationship between SNMP management side and agent. The community character string is similar to the password that enables the access system to log in to the agent. You can specify one or multiple properties 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] <i>string</i> [view <i>view-name</i>] [ro rw] [<i>word</i>]	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”.

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

sysContact and sysLocation are the management variables in the MIB’s system group, respectively defining the linkman’s identifier and actual location of the controlled node. These information can be accessed through config. files. Run the following commands in global configuration mode:

Command	Purpose
snmp-server contact <i>text</i>	Sets the character string for the linkman of the node.

Network Management Configuration

snmp-server location <i>text</i>	Sets the character string for the node location.
-----------------------------------------	--------------------------------------------------

4. 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. Run the following commands in global configuration mode:

Command	Purpose
snmp-server packet-size <i>byte-count</i>	Sets the maximum length of the data packet.

5. Monitoring SNMP state

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

Command	Purpose
show snmp	Monitoring SNMP state

6. Configuring SNMP local engine

Run the following command in the global mode to configure SNMP local engine.

Command	Purpose
snmp-server engineID local <i>engineID</i>	Configuring SNMP local engine

7. 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 <i>host</i> <i>community-string</i> [<i>trap-type</i>]	Specifies the receiver of the trap message.
snmp-server host hostv6 <i>host</i> [<i>udp-port</i> <i>port-num</i>] [<i>permit deny</i> <i>event-id</i>] {{version [v1 v2c v3] [[informs traps] [auth noauth]]}} <i>community-string/user</i> [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 <i>interface</i>	Specifies the source interface where traps originate and sets the source IP address for the message. The command sets the source IP address for the information.
snmp-server queue-length <i>length</i>	Creates the queue length of the message for each host that has traps. The default value is 10.
snmp-server trap-timeout <i>seconds</i>	Defines the frequency to resend traps in the resending queue. The default value is 30 seconds.

8. 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 <i>ipaddress</i>	Set the source address for the SNMP message.

9. 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 <i>portnum</i>	Set SNMP server udp-port number

10. Configuring SNMPv3 group

Configuring SNMPv3 group

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

11. ConfiguringSNMPv3 user

You can run the following command to configure a local user. When an administrator logs in to a device, he has to use 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 <i>username groupname {v3 [encrypted auth] [md5 sha] auth-password}</i>	Configures a local SNMPv3 user.

12. Configuring snmp-server encryption

To display the configured SNMP community, the SHA encryption password and the MD5 encryption password, run `snmp-server encryption` in global mode. This command is a once-for-all command, which cannot be saved or canceled by its negative form. Format of the command is as follows:

Command	Purpose
snmp-server encryption	This command is used to display the SNMP community, the SHA encryption password and the MD5 encryption password in plain text. In this way, the security of the password is guaranteed.

13. Configuring snmp-server trap-source

To designate an interface to be the source address of all traps, run the following first command in global configuration mode. To cancel this interface, run the following second command.

Command	Purpose
snmp-server trap-source <i>interface</i>	When the SNMP server sends out a SNMP trap on whichever interface, the SNMP trap shall carry a trap address. If you want to use the trap address for tracking, you can use this command.

14. Configuring snmp-server trap-timeout

To set the timeout value of retransmitting traps, run the following first command in global configuration mode.

Command	Purpose
snmp-server trap-timeout <i>seconds</i>	Before switch software tries to send traps, it is used to look for the route of destination address. If no routes exists, traps will be saved in the retransmission queue. The server trap-timeout command decides the retransmission interval.

15. Configuring snmp-server trap-add-hostname

To add the host name to the binding variable when SNMP sends traps, run the first one of the following two commands.

Command	Purpose
snmp-server trap-add-hostname	This command is a great help in some cases when the NMS needs to locate which host sends these traps.

16. Configuring snmp-server trap-logs

To write the trap transmission records into logs, run the first one of the following two commands.

Command	Purpose
snmp-server trap-logs	After this function is enabled, the trap transmission records of a device can be sent to the log server and then you can know more about the running state of the device.

17. Configuring snmp -dos-max retry times

To set the incorrect community login retry times in five minutes on the SNMP server, run the first one of the following two commands.

Command	Purpose
snmp-server set-snmp-dos-max <i>retry times</i>	After this function is enabled, the trap transmission records of a device can be sent to the log server and then you can know more about the running state of the device.

The command must be used with snmp-server host.

18. Configuring keep-alive times

To set the timely sending heartbeat trap, run **snmp-server keep-alive** in global configuration mode. The time interval is times.

Command	Purpose
snmp-server keep-alive <i>times</i>	Send keep-alive times regularly to the trap host.

19. Configuring snmp-server necode

To set the information about the management node (the unique identifier of the device), run `snmp-server necode text`. To delete the identifier information, use the `no` form of this command.

Command	Purpose
snmp-server necode text	The command is corresponding to the snmp private MIB variable.

20. Configuring snmp-server event-id

To create and set event list, run command `snmp-server event-id` in the global configuration mode. To delete the event list, use the `no` form of this command.

Command	Purpose
snmp-server event-id number trap-oid oid	The command is used to forward the filter when sending trap in configuring host.

21. Configuring snmp-server getbulk-timeout

To set the timeout of processing getbulk request, run command `snmp-server getbulk-timeout` in the global configuration mode. If all getbulk requests cannot be processed in timeout, the system will return to the current result directly. To delete the configuration, use the `no` form of this command.

Command	Purpose
snmp-server getbulk-timeout seconds	The command is used to set the timeout of processing getbulk request. If all getbulk requests cannot be processed in timeout, the system will return to the current result directly.

22. Configuring snmp-server getbulk-delay

To set getbulk-delay time to prevent snmp occupying excessive cpu when snmp agent processing getbulk request, run command `snmp-server getbulk-delay` in the global configuration mode. The unit is 0.01 seconds. To delete the configuration, use the `no` form of this command.

Command	Purpose
snmp-server getbulk-delay ticks	The command is used to set getbulk-delay time to prevent snmp from occupying excessive cpu when snmp agent processing getbulk request. The unit is 0.01s.

23. Showing snmp running information

To monitor SNMP input and output statistics, including illegal community character strings, the number of errors and request variables, run command `show snmp`. To show

Network Management Configuration

SNMP engine information, run command `show snmp engineID`. To show SNMP trap host information, run command `show snmp host`. To show SNMP view information, run command **show snmp view**. To show snmp mibs registration information, run command **show snmp mibs**. To show snmp group information, run command `show snmp group`. To show SNMP user information, run command `show snmp user`.

Command	Purpose
<code>show snmp engineID</code>	Shows SNMP engine information.
show snmp host	Shows SNMP trap host information.
<code>show snmp view</code>	Shows SNMP view information.
<code>show snmp mibs</code>	Shows SNMP MIB registration information.
<code>show snmp group</code>	Shows SNMP group information.
<code>show snmp user</code>	Shows SNMP user information.

24. Showing snmp debug information

To show SNMP event, packet sending and receiving process and error information, run command **debug snmp**.

Command	Purpose
<code>debug snmp error</code>	Enable the debug OLT of SNMP error information.
<code>debug snmp event</code>	Enable the debug OLT of SNMP event information.
<code>debug snmp packet</code>	Enable the debug OLT of SNMP input/output packets.

1.1.3 Configuration Example

1. Example 1

```
snmp-server community public RO
snmp-server community private RW
snmp-server host 192.168.10.2 public
```

The above example shows: how to set the community string public that can only read all MIB variables. how to set the community string private that can read and write all MIB variables. The above command specifies the community string public to send traps to 192.168.10.2 when a system requires to send traps. For example, when a port of a system is in the down state, the system will send a linkdown trap information to 192.168.10.2.

2. Example 2

```
snmp-server 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.

1.2 RMON Configuration

1.2.1 RMON Configuration Tasks

RMON configuration tasks include:

- Configuring the rMon alarm function for the switch
- Configuring the rMon event function for the switch
- Configuring the rMon statistics function for the switch
- Configuring the rMon history function for the switch
- Displaying the rMon configuration of the switch

1. Configuring the rMon alarm function for the 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	Enters the global configuration mode.
rmon alarm index variable interval {absolute delta} rising-threshold value [eventnumber] falling-threshold value [eventnumber] [owner string] [repeat]	<p>Add a rMon alarm item.</p> <p>index is the index of the alarm item. Its effective range is from 1 to 65535.</p> <p>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 TimeTicks type can be detected.</p> <p>interval is the time section for sampling. Its unit is second. Its effective value is from 1 to 2147483647.</p> <p>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.</p> <p>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.</p> <p>Owner string is to describe the information about the alarm.</p>

Network Management Configuration

	Repeat is to repeat trigger event.
exit	Goes back to the EXEC mode.
write	Saves the settings.

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

2. Configuring the rMon event function for the switch

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

Procedure	Command	Purpose
1.	config	Enters the global configuration mode.
2.	rmon event index [description string] [log] [owner string] [trap community] [ifctrl <i>interface</i>]	Add a rMon event item. index is the index of the alarm 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	Goes back to the EXEC mode.
4.	write	Saves the settings.

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

3. Configuring the rMon statistics function for the 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:

Network Management Configuration

Procedure	Command	Purpose
1.	config	Enters the global configuration mode.
2.	interface iftype ifid	This command is used to enter the interface configuration 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	Goes back to the global mode.
5.	exit	Goes back to the EXEC mode.
6.	write	Saves the settings.

If you run rmon event many times to configure status 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.

4. Configuring RMON history for switch

The RMON history group is used to collect statistics information of different time sections on a port in a device. The steps to configure the rMon statistics are as follows:

Procedure	Command	Purpose
1.	config	Enters the global configuration mode.
2.	interface iftype ifid	Enters 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. In statistics of all history record control entries, the entry nearest to bucket-number needs to be saved. The user can browse the Ethernet history record to obtain the statistics. The default value is 50 entries. The interval means the time between two data collection, whose default value is 1800s (half hours). owner string is to describe the information about the description information in the history control table.
4.	exit	Goes back to the global mode.
5.	exit	Goes back to the EXEC mode.
6.	write	Saving the Settings

After a rMon history item is added, the device will obtain statistics values from the specified port every second. The statistics value will be added to the history item as a piece of information. If you run rmon collection history index many times to configure history items with the same index, only the last configuration is effective. You can run no rmon history index to cancel history items whose indexes are index. Note: Too much system sources will be occupied in the case the value of bucket-number is too big or the value of interval second is too small.

5. Displaying RMON configuration of switch

Run show to display the RMON configuration of the switch.

Command	Purpose
<p>show rmon [alarm] [event] [statistics] [history]</p>	<p>Displays the rmon configuration information.</p> <p>alarm means to display the configuration of the alarm item.</p> <p>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.</p> <p>statistics means to display the configuration of the statistics item and statistics values that the device collects from the port.</p> <p>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.</p>

Security Configuration

Table of Contents

Chapter 1 AAA Configuration.....	1
1.1 AAA Overview.....	1
1.1.1 AAA Security Service.....	1
1.1.2 Benefits of Using AAA.....	2
1.1.3 AAA Principles.....	2
1.1.4 AAA Method List.....	2
1.1.5 AAA Configuration Process.....	3
1.2 Authentication Configuration.....	4
1.2.1 AAA Authentication Configuration Task List.....	4
1.2.2 AAA Authentication Configuration Task.....	4
1.2.3 AAA Authentication Configuration Example.....	8
1.3 Authorization Configuration.....	9
1.3.1 AAA Authorization Configuration Task List.....	9
1.3.2 AAA Authorization Configuration Task.....	9
1.3.3 AAA Authorization Examples.....	10
1.4 AAA Accounting Configuration.....	11
1.4.1 AAA Accounting Configuration Task List.....	11
1.4.2 AAA Accounting Configuration Task.....	11
1.5 Local Account Policy Configuration.....	14
1.5.1 Local Account Policy Configuration Task List.....	14
1.5.2 Local Account Policy Configuration Task.....	14
1.5.3 Local Account Policy Example.....	16
Chapter 2 Configuring RADIUS.....	17
2.1 Overview.....	17
2.1.1 RADIUS Overview.....	17
2.1.2 RADIUS Operation.....	18
2.2 RADIUS Configuration Steps.....	18
2.3 RADIUS Configuration Task List.....	19
2.4 RADIUS Configuration Task.....	19
2.4.1 Configuring Switch to RADIUS Server Communication.....	19
2.4.2 Configuring Switch to Use Vendor-Specific RADIUS Attributes.....	19
2.4.3 Specifying RADIUS Authentication.....	20
2.4.4 Specifying RADIUS Authorization.....	20
2.4.5 Specifying RADIUS Accounting.....	20
2.5 RADIUS Configuration Examples.....	20
2.5.1 RADIUS Authentication Example.....	20
2.5.2 RADIUS Application in AAA.....	21
Chapter 3 TACACS+ Configuration.....	22

Security Configuration

- 3.1 TACACS+ Overview..... 22
 - 3.1.1 The Operation of TACACS+ Protocol..... 22
- 3.2 TACACS+ Configuration Process..... 23
- 3.3 TACACS+ Configuration Task List..... 24
- 3.4 TACACS+ Configuration Task..... 24
 - 3.4.1 Assigning TACACS+ server..... 24
 - 3.4.2 Setting up TACACS+ encrypted secret key..... 25
 - 3.4.3 Assigning to use TACACS+ for authentication..... 25
 - 3.4.4 Assigning to use TACACS+ for authorization..... 25
 - 3.4.5 Assigning to use TACACS+ for accounting..... 25
- 3.5 TACACS+ Configuration Example..... 25
 - 3.5.1 TACACS+ authentication example..... 25
 - 3.5.2 TACACS+ Authorization Examples..... 26
 - 3.5.3 TACACS+ Accounting Example..... 26

Chapter 1 AAA Configuration

1.1 AAA Overview

Access control is the way to control access to the network and services. Authentication, authorization, and accounting (AAA) network security services provide the primary framework through which you set up access control on your OLT or access server.

1.1.1 AAA Security Service

AAA is an architectural framework for configuring a set of three independent security functions in a consistent manner. AAA provides a modular way of performing the following services:

- **Authentication:** 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 any one 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 switch, 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".

1. 1. 2 Benefits of Using AAA

AAA provides the following benefits:

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

1. 1. 3 AAA Principles

AAA is designed to enable you to dynamically configure the type of authentication and authorization you want on a per-line (per-user) or per-service (for example, IP, IPX, or VPDN) basis. You define the type of authentication and authorization you want by creating method lists, then applying those method lists to specific services or interfaces.

1. 1. 4 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 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 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.

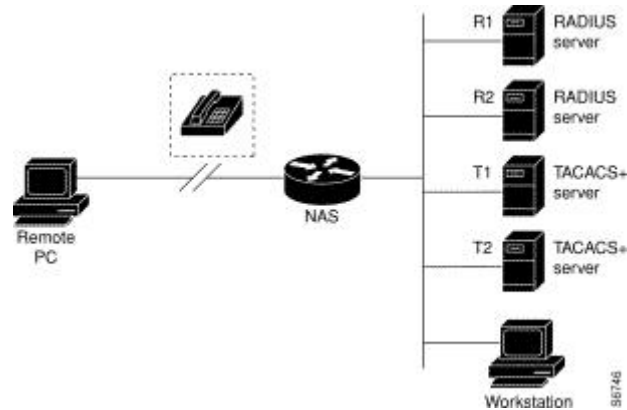


Figure 1-1 Typical AAA Network Configuration

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.

1.1.5 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 switches or access servers, perform the following steps:

- If you decide to use a security server, configure security protocol parameters first, such as RADIUS, TACACS+, or Kerberos.
- Define the method lists for authentication by using an AAA authentication command.
- Apply the method lists to a particular interface or line, if required.

- (Optional) Configure authorization using the aaa authorization command.
- (Optional) Configure accounting using the aaa accounting command.

1.2 Authentication Configuration

1.2.1 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 the Authentication Database with the Local Privilege

1.2.2 AAA Authentication Configuration Task

General configuration process of AAA authentication

To configure AAA authentication, perform the following configuration processes:

- (1) If you decide to use a separate security server, configure security protocol parameters, such as RADIUS, or TACACS+. Refer to the relevant section for the concrete configuration methods.
- (2) Configuring Authentication Method List Using aaa authentication
- (3) If necessary, apply the accounting method list to a specific interface or line.

1.2.2.1 Configuring Login Authentication Using AAA

The AAA security services facilitate a variety of login authentication methods. Use the aaa authentication login command to enable AAA authentication no matter which of the supported login authentication methods you decide to use. With the aaa authentication login command, you create one or more lists of authentication methods that are tried at login. These lists are applied using the login authentication line configuration command. 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 <i>list-name</i> } <i>method1</i> [<i>method2...</i>]	Enables AAA globally.
line [console vty] <i>line-number</i> [<i>ending-line-number</i>]	Enter the configuration mode of a line.

login authentication {default <i>list-name</i> }	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 none keyword 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 <i>name</i>	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) Using the enable password to carry on the login authentication:

To specify the enable password as the user authentication method, run the following command:

```
aaa authentication login default enable
```

(2) Using the line password to login

Use the aaa authentication login command with the line method keyword to specify the line password as the login authentication method. For example, to specify the line password as the method of user authentication at login when no other method list has been defined, enter the following command:

```
aaa authentication login default line
```

Before you can use a line password as the login authentication method, you need to define a line password.

(3) Using the local password to carry on the login authentication:

When you run `aaa authentication login`, you can use the keyword "local" to designate the local database as the login authentication method. For example, if you want to specify the local username database as the user authentication method and not define any other method, run the following command:

```
aaa authentication login default local
```

For information about adding users into the local username database, refer to the section "Establishing Username Authentication" in this chapter.

(4) Login Authentication Using RADIUS

Use the `aaa authentication login` command with the `group radius` method to specify RADIUS as the login authentication method. For example, to specify RADIUS as the method of user authentication at login when no other method list has been defined, enter the following command:

```
aaa authentication login default group radius
```

Before you can use RADIUS as the login authentication method, you need to enable communication with the RADIUS security server. For more information about establishing communication with a RADIUS server, refer to the chapter "Configuring RADIUS."

1. 2. 2. 2 Enabling Password Protection at the Privileged Level

Use the `aaa authentication enable default` command to create a series of authentication methods that are used to determine whether a user can access the privileged EXEC command level. You can specify up to four authentication methods. The additional methods of authentication are used only if the previous method returns an error, not if it fails. To specify that the authentication should succeed even if all methods return an error, specify `none` as the final method in the command line. Use the following command in global configuration mode:

Command	Purpose
aaa authentication enable default <i>method1</i> [<i>method2...</i>]	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:
<code>enable</code>	Uses the enable password for authentication.
<code>group <i>group-name</i></code>	Uses named server group for authentication.
<code>group radius</code>	Uses RADIUS authentication.
<code>group tacacs+</code>	Uses tacacs+ for authentication.
<code>line</code>	Uses the line password for authentication.
<code>none</code>	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 be configured 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.

1. 2. 2. 3 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 <i>text-string delimiter</i>	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 <i>text-string delimiter</i>	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.

1. 2. 2. 4 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 <i>text-string</i>	Modifies the default text of the username input prompt.

1. 2. 2. 5 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 <i>text-string</i>	String of text that will be displayed when the user is prompted to enter a password.

1. 2. 2. 6 Creating the Authentication Database with the Local Privilege

To create the enable password database with the local privilege level, run `enable password { [encryption-type] encrypted-password} [level level]` in global configuration mode. To cancel the enable password database, run `no enable password [level level]`.

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

no enable password [*level level*]

1. 2. 3 AAA Authentication Configuration Example

1. 2. 3. 1 RADIUS Authentication Example

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

```
aaa authentication login radius-login group radius local
aaa authorization network radius-network 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 switch 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.

1.3 Authorization Configuration

1.3.1 AAA Authorization Configuration Task List

- Configuring EXEC authorization through AAA

1.3.2 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.
- (2) Run `aaa authorization` to define the authorization method list. The authorization service is not provided by default.
- (3) If necessary, apply the accounting method list to a specific interface or line.

1.3.2.1 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
<code>aaa authorization exec {default list-name} method1 [method2...]</code>	Creates the global authorization list.
<code>line [console vty] line-number [ending-line-number]</code>	Enter the configuration mode of a line.
<code>login authorization {default list-name}</code>	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 <i>WORD</i>	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.

1. 3. 3 AAA Authorization Examples

1. 3. 3. 1 Example of Local EXECAuthorization

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

```
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.

1.4 AAA Accounting Configuration

1.4.1 AAA Accounting Configuration Task List

- Configuring Connection Accounting using AAA
- Configuring Network Accounting using AAA
- Configuring Accounting Update Through AAA
- Limiting User Accounting WithoutUsername

1.4.2 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.
- (2) Apply the method lists to a particular interface or line, if required. The accounting service is not provided by default.

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

1. 4. 2. 1 Configuring Connection Accounting usingAAA

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 switch, 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
<code>aaa accounting connection {default list-name} {{{start-stop stop-only} group groupname} none}</code>	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 <i>WORD</i>	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.

1. 4. 2. 2 Configuring Network Accounting usingAAA

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
<code>aaa accounting network {default list-name} {{{start-stop stop-only} group groupname} none}</code>	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:

Security Configuration

Keyword	Notes:
group <i>WORD</i>	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.

1. 4. 2. 3 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 <i>number</i>]	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 newinfo` are configured, all currently-registered users will generate temporary accounting records periodically. All new users have accounting records generated according to the `newinfo` algorithm.

1. 4. 2. 4 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**

1.5 Local Account Policy Configuration

1.5.1 Local Account Policy Configuration Task List

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

1.5.2 Local Account Policy Configuration Task

1.5.2.1 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.

1.5.2.2 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.

1.5.2.3 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.

1. 5. 2. 4 Local policy group configuration

To configure local policy group, run *localgroup WORD* in global 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 maxlinks 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.

1. 5. 3 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 `aaa authorization exec default local` 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.

Chapter 2 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.

2.1 Overview

2.1.1 RADIUS Overview

RADIUS is a distributed client/server system that secures networks against unauthorized access. In the implementation, RADIUS clients run on switches and send authentication requests to a central RADIUS server that contains all user authentication and network service access information. RADIUS has been implemented in a variety of network environments that require high levels of security while maintaining network access for remote users.

Use RADIUS in the following network environments that require access security:

- Networks with multiple-vendor access servers, each supporting RADIUS. For example, access servers from several vendors use a single RADIUS server-based security database. In an IP-based network with multiple vendors' access servers, dial-in users are authenticated through a RADIUS server.
- 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

- Switch-to-switch situations. RADIUS does not provide two-way authentication. On the switch 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.

2.1.2 RADIUS Operation

When a user attempts to log in and authenticate to an access server using RADIUS, the following steps occur:

- (1) The user is prompted for and enters a username and password.
- (2) The username and encrypted password are sent over the network to the RADIUS server.
- (3) The user receives one of the following responses from the RADIUS server:

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:

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

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

2.2 RADIUS Configuration Steps

To configure RADIUS on your switch or access server, you must perform the following tasks:

- Use the `aaa authentication global configuration` command to define method lists for RADIUS authentication. For more information about using the `aaa authentication` command, refer to the "Configuring Authentication" chapter.
- Use line and interface commands to enable the defined method lists to be used. For more information, refer to the "Configuring Authentication" chapter.

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 Authorization" 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.

2.3 RADIUS Configuration Task List

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

2.4 RADIUS Configuration Task

2.4.1 Configuring Switch to RADIUS Server Communication

The RADIUS host is normally a multiuser system running RADIUS server software from Livingston, Merit, Microsoft, or another software provider. A RADIUS server and a switch use a shared secret text string to encrypt passwords and exchange responses. To set RADIUS server, run command `radius-server host`; to set the shared key, run command `radius-server key`. Use the following command in global configuration mode:

Command	Purpose
radius-server host <i>ip-address</i> [auth-port <i>port-number</i>][acct-port <i>portnumber</i>]	Specifies the IP address or host name of the remote RADIUS server host and assign authentication and accounting destination port numbers.
radius-server key <i>string</i>	Specifies the shared secret text string used between the switch and a RADIUS server.

To configure global communication settings between the switch and a RADIUS server, use the following `radius-server` commands in global configuration mode:

Command	Purpose
radius-server retransmit <i>retries</i>	Specifies how many times the switch transmits each RADIUS request to the server before giving up (the default is 2).
radius-server timeout <i>seconds</i>	Specifies for how many seconds a switch waits for a reply to a RADIUS request before retransmitting the request.
radius-server deadtime <i>minutes</i>	Specifies for how many minutes a RADIUS server that is not responding to authentication requests is passed over by requests for RADIUS authentication.

2.4.2 Configuring Switch to Use Vendor-Specific RADIUS Attributes

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific information between the network access server and the RADIUS server by using the vendor-specific attribute (attribute 26). Vendor-specific

attributes (VSAs) allow vendors to support their own extended attributes not suitable for general use. For more information about vendor-IDs and VSAs, refer to RFC 2138, Remote Authentication Dial-In User Service (RADIUS). To configure the network access server to recognize and use VSAs, use the following command in global configuration mode:

Command	Purpose
radius-server vsa send [authentication]	Enables the network access server to recognize and use VSAs as defined by RADIUS IETF attribute 26.

2.4.3 Specifying RADIUS Authentication

After you have identified the RADIUS server and defined the RADIUS authentication key, you must define method lists for RADIUS authentication. Because RADIUS authentication is facilitated through AAA, you must enter the `aaa authentication` command, specifying RADIUS as the authentication method. For more information about the two commands, see Authentication Configuration.

2.4.4 Specifying RADIUS Authorization

AAA authorization lets you set parameters that restrict a user's access to the network. Authorization using RADIUS provides one method for remote access control, including one-time authorization or authorization for each service. Because RADIUS authorization is facilitated through AAA, you must issue the `aaa authorization` command, specifying RADIUS as the authorization method. For more information, refer to the chapter "Configuring Authorization."

2.4.5 Specifying RADIUS Accounting

The AAA accounting feature enables you to track the services users are accessing as well as the amount of network resources they are consuming. Because RADIUS accounting is facilitated through AAA, you must issue the `aaa accounting` command, specifying RADIUS as the accounting method. For more information about the two commands, see Authentication Configuration.

2.5 RADIUS Configuration Examples

2.5.1 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 switch 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.

2.5.2 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.

Chapter 3 TACACS+ Configuration

3.1 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.

3.1.1 The Operation of TACACS+ Protocol

3.1.1.1 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.

3.1.1.2 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.

3.2 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+ for 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".

3.3 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

3.4 TACACS+ Configuration Task

3.4.1 Assigning TACACS+ server

Command `tacacs-server` could help to assign the IP address of TACACS+ 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
<code>tacacs-server host ip-address</code> <code>[single-connection multi-connection]</code> <code>[port integer] [timeout integer] [key string]</code>	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.

3. 4. 2 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 <i>keystring</i>	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.

3. 4. 3 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".

3. 4. 4 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".

3. 4. 5 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".

3. 5 TACACS+ Configuration Example

This chapter includes the following TACACS+ configuration example.

3. 5. 1 TACACS+ authentication example

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`.

3. 5. 2 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`.

3. 5. 3 TACACS+ Accounting Example

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 shared encrypted secret key as goaway.

Web Configuration

Table of Contents

Chapter 1 Configuration Preparation.....	1
1.1 HTTP Configuration.....	1
1.1.1 Choosing the Prompt Language.....	1
1.1.2 Setting the HTTP Port.....	1
1.1.3 Enabling the HTTP service.....	1
1.1.4 Setting the HTTP Access Mode.....	1
1.1.5 Setting the maximum number of VLAN entries displayed on a web page.....	2
1.1.6 Setting the Maximum Number of Multicast Entries Displayed on a Web Page.....	2
1.2 HTTPS Configuration.....	2
1.2.1 Setting the HTTP Access Mode.....	2
1.2.2 Setting the HTTPS Port.....	2
Chapter 2 Accessing the Switch through HTTP.....	3
2.1 Accessing the Switch through HTTP.....	4
2.1.1 Initially Accessing the Switch.....	4
2.1.2 Upgrading to the Web-Supported Version.....	4
2.2 Accessing a Switch through Secure Links.....	5
2.3 Introduction of Web Interface.....	5
2.3.1 Top Control Bar.....	5
2.3.2 Navigation Bar.....	6
2.3.3 Configuration Area.....	7
2.3.4 Configuration Area.....	7
Chapter 3 Basic Configuration.....	8
3.1 Hostname Configuration.....	9
3.2 Time Management.....	9
Chapter 4 Configuration of the Physical Interface.....	10
4.1 Configuring Port Description.....	11
4.2 Configuring the Attributes of the Port.....	11
4.3 Rate Limit.....	11
4.4 Port Mirror.....	11
4.5 Keepalive Detection.....	12
4.6 Port security.....	12
4.6.1 IP Binding Configuration.....	12
4.6.2 MAC Binding Configuration.....	12
4.6.3 Setting the Static MAC Filtration Mode.....	12
4.6.4 Static MAC Filtration Entries.....	12
4.6.5 Setting the Dynamic MAC Filtration Mode.....	13
4.7 Storm Control.....	13
4.7.1 Broadcast storm control.....	13
4.7.2 Multicast Storm Control.....	13
4.7.3 Unknown Unicast Storm Control.....	13
4.8 Port Protect Group Configuration.....	14
4.8.1 Port Protect Group List.....	14

Table of Contents

4.8.2 Port Protect Group Interface Configuration.....	14
4.9 POE Management.....	14
4.9.1 POE Global Configuration.....	14
4.9.2 POE Global Realtime Info.....	15
4.9.3 POE Interface List.....	15
4.9.4 POE Port Policy Power.....	15
4.9.5 POE Interface Power List.....	16
4.9.6 POE Port Other Info.....	16
Chapter 5 Layer-2 Configuration.....	17
5.1 VLAN Configuration.....	18
5.1.1 VLAN List.....	18
5.1.2 VLAN Configuration.....	18
5.2 GVRP Configuration.....	19
5.2.1 GVRP Global Attribute Configuration.....	19
5.2.2 GVRP Port Attribute Configuration.....	19
5.3 STP Configuration.....	19
5.3.1 STP Status Information.....	19
5.3.2 Configuring the Attributes of the STP Port.....	20
5.4 IGMP-Snooping Configuration.....	20
5.4.1 IGMP-Snooping Configuration.....	20
5.4.2 IGMP-Snooping VLAN List.....	20
5.4.3 Static Multicast Address.....	21
5.4.4 Multicast List.....	21
5.5 Setting Static ARP.....	22
5.6 Static MAC Configuration.....	22
5.7 LLDP Configuration.....	23
5.7.1 Configuring the Global Attributes of LLDP.....	23
5.7.2 Configuring the Attributes of the LLDP Port.....	23
5.8 DDM Configuration.....	24
5.9 Link Aggregation Configuration.....	24
5.9.1 Port Aggregation Configuration.....	24
5.9.2 Configuring Load Balance of Port Aggregation Group.....	24
5.10 EAPS Ring Protection Configuration.....	25
5.10.1 EAPS Ring List.....	25
5.10.2 EAPS Ring Configuration.....	25
5.11 MEAPS Configuration.....	26
5.11.1 MEAPS Ring Configuration.....	26
5.11.2 MEAPS Ring Configuration.....	26
5.12 Backup Link Protocol Configuration.....	27
5.12.1 Backup Link Protocol Global Configuration.....	27
5.12.2 Backup Link Protocol Interface Configuration.....	28
5.13 MTU Configuration.....	28
5.14 PDP Configuration.....	29
5.14.1 Configuring the Global Attributes of PDP.....	29
5.14.2 Configuring the Attributes of the PDP Port.....	29
Chapter 6 Layer-3 Configuration.....	30

Table of Contents

6.1 Vlan interface configuration.....	31
6.2 Setting the Static Route.....	31
Chapter 7 Advanced Configuration.....	33
7.1 QoS Configuration.....	34
7.1.1 Configuring QoS Port.....	34
7.1.2 Global QoS Configuration.....	34
7.2 IP Access Control List.....	34
7.2.1 Setting the Name of the IP Access Control List.....	34
7.2.2 Setting the Rules of the IP Access Control List.....	35
7.2.3 Applying the IP Access Control List.....	36
7.3 MAC Access Control List.....	36
7.3.1 Setting the Name of the IP Access Control List.....	36
7.3.2 Setting the Rules of the MAC Access Control List.....	37
7.3.3 Applying the MAC Access Control List.....	37
Chapter 8 Network Management Configuration.....	38
8.1 SNMP Configuration.....	39
8.1.1 SNMP Community Management.....	39
8.1.2 SNMP Host Management.....	39
8.2 RMON.....	40
8.2.1 RMON Statistic Information Configuration.....	40
8.2.2 RMON History Information Configuration.....	40
8.2.3 RMON Alarm Information Configuration.....	40
8.2.4 RMON Event Configuration.....	41
Chapter 9 Diagnosis Tools.....	42
9.1 Ping.....	43
9.1.1 Ping.....	43
Chapter 10 System Management.....	44
10.1 User Management.....	45
10.1.1 User List.....	45
10.1.2 Establishing a New User.....	45
10.1.3 User Group Management.....	45
10.1.4 Password Rule Management.....	46
10.1.5 Authentication Rule Management.....	47
10.1.6 Authorization Rule Management.....	47
10.2 Log Management.....	48
10.3 Managing the Configuration Files.....	48
10.3.1 Exporting the Configuration Information.....	48
10.3.2 Importing the Configuration Information.....	49
10.4 Software Management.....	49
10.4.1 Backup System Software.....	49
10.4.2 Update System Software.....	49
10.5 Rebooting the Device.....	50

Chapter 1 Configuration Preparation

1.1 HTTP Configuration

Switch configuration can be conducted not only through command lines and SNMP but also through Web browser. The switches support the HTTP configuration, the abnormal packet timeout configuration, and so on.

1.1.1 Choosing the Prompt Language

Up to now, switches support two languages, that is, English and Chinese, and the two languages can be switched over through the following command.

Command	Purpose
[no] ip http language { english }	Sets the prompt language of Web configuration to English.

1.1.2 Setting the HTTP Port

Generally, the HTTP port is port 80 by default, and users can access a switch by entering the IP address directly; however, switches also support users to change the service port and after the service port is changed you have to use the IP address and the changed port to access switches. For example, if you set the IP address and the service port to 192.168.1.3 and 1234 respectively, the HTTP access address should be changed to http:// 192.168.1.3:1234. You'd better not use other common protocols' ports (such as ftp-20, telnet-23, dns-53, snmp-161) so that access collision should not happen. Because the ports used by a lot of protocols are hard to remember, you'd better use port IDs following port 1024.

Command	Purpose
ip http port { <i>portNumber</i> }	Setting the HTTP Port

1.1.3 Enabling the HTTP service

Switches support to control the HTTP access. Only when the HTTP service is enabled can HTTP exchange happen between switch and PC and, when the HTTP service is closed, HTTP exchange stops.

Command	Purpose
ip http server	Enabling the HTTP service

1.1.4 Setting the HTTP Access Mode

You can access a switch through two access modes: HTTP access and HTTPS access, and you can use the following command to set the access mode to HTTP.

Command	Purpose
---------	---------

ip http http-access enable	Setting the HTTP Access Mode
----------------------------	------------------------------

1.1.5 Setting the maximum number of VLAN entries displayed on a web page

A switch supports at most 4094 VLANs and in most cases Web only displays parts of VLANs, that is, those VLANs users want to see. You can use the following command to set the maximum number of VLANs. The default maximum number of VLANs is 100.

Command	Purpose
ip http web max-vlan { <i>max-vlan</i> }	Sets the maximum number of VLAN entries displayed in a web page.

1.1.6 Setting the Maximum Number of Multicast Entries Displayed on a Web Page

A switch supports at most 100 multicast entries. You can run the following command to set the maximum number of multicast entries and Web then shows these multicast entries. The default maximum number of multicast entries is 15.

Command	Purpose
ip http web igmp-groups { <i>igmp-groups</i> }	Sets the maximum number of multicast entries displayed in a web page.

1.2 HTTPS Configuration

In order to improve the security of communications, switches support not only the HTTP protocol but also the HTTPS protocol. HTTPS is a security-purposed HTTP channel and it is added to the SSL layer under HTTP.

1.2.1 Setting the HTTP Access Mode

You can run the following command to set the access mode to HTTPS.

Command	Purpose
ip http ssl-access enable	Setting the HTTPS access mode

1.2.2 Setting the HTTPS Port

As the HTTP port, HTTPS has its default service port, port 443, and you also can run the following command to change its service port. It is recommended to use those ports following port 1024 so as to avoid collision with other protocols' ports.

Parameters	Notes:
ip http secure-port { <i>portNumber</i> }	Sets the HTTPS port.

Chapter 2 Accessing the Switch through HTTP

2.1 Accessing the Switch through HTTP

When accessing the switch through Web, please make sure that the applied browser complies with the following requirements:

- HTML of version 4.0
- HTTP of version 1.1
- JavaScript™ of version 1.5

What's more, please ensure that the main program file, running on a switch, supports Web access and your computer has already connected the network in which the switch is located.

2.1.1 Initially Accessing the Switch

When the switch is initially used, you can use the Web access without any extra settings:

1. Modify the IP address of the network adapter and subnet mask of your computer to 192.168.0.2 and 255.255.255.0 respectively.
2. Open the Web browser and enter 192.168.0.1 in the address bar. It is noted that 192.168.0.1 is the default management address of the switch.
3. If the Internet Explorer browser is used, you can see the dialog box as below. Both the original username and the password are "admin", which is capital sensitive.



4. After successful authentication, the systematic information about the switch will appear on the IE browser.

2.1.2 Upgrading to the Web-Supported Version

If your switch is upgraded to the Web-supported version during its operation and the switch has already stored its configuration files, the Web visit cannot be directly applied on the switch. Perform the following steps one by one to enable the Web visit on the switch:

1. Connect the console port of the switch with the accessory cable, or telnet to the management address of the switch through the computer.
2. Enter the global configuration mode of the switch through the command line, the DOS prompt of which is similar to "Switch_config#".
3. If the management address of the switch is not configured, please create the VLAN interface and configure the IP address.

4. Enter the command **ip http server**", to enable Web service.
 5. Enter the **username** to set the user name and password of the switch For how to use this command, refer to the "Security Configuration" section in the user manual.
- After the above-mentioned steps are performed, you can enter the address of the switch in the Web browser to access the switch.
6. Enter the command **write**", to save the current configuration to the configuration file.

2.2 Accessing a Switch through Secure Links

The data between the WEB browser and the switch will not be encrypted if you access a switch through common HTTP. To encrypt these data, you can use the secure links, which are based on the secure sockets layer, to access the switch.

To do this, you should follow the following steps:

1. Connect the console port of the switch with the accessory cable, or telnet to the management address of the switch through the computer.
2. Enter the global configuration mode of the switch through the command line, the DOS prompt of which is similar to "Switch_config#".
3. If the management address of the switch is not configured, please create the VLAN interface and configure the IP address.
4. Enter the command **ip http server**", to enable Web service.
5. Enter the **username** to set the user name and password of the switch For how to use this command, refer to the "Security Configuration" section in the user manual.
6. Run **ip http ssl-access enable** to enable the secure link access of the switch.
7. Run **ip http http-access enable** to access the switch through insecure links.
8. Enter the command **write**", to save the current configuration to the configuration file.
9. Open the WEB browser on the PC that the switch connects, enter <https://192.168.0.1> on the address bar (192.168.0.1 stands for the management IP address of the switch)IP address of the switch) and then press the Enter key. Then the switch can be accessed through the secure links.

2.3 Introduction of Web Interface

The whole Web homepage consists of the top control bar, the navigation bar, the configuration area and the bottom control bar.

2.3.1 Top Control Bar

[Save All](#) | [English](#) | [中文](#) | [Logout](#) | [Port Panel](#) | [About](#)

Save All

Write the current settings to the configuration file of the device. It is equivalent to the execution of the **"write"** command.

The configuration that is made through Web will not be promptly written to the configuration file after validation. If you click "Save All", the unsaved

	configuration will be lost after rebooting.
English	The interface will turn into the English version.
Chinese	The interface will turn into the Chinese version.
Logout	Exit from the current login state. After you click "logout", you have to enter the username and the password again if you want to continue the Web function.
Interface panel	Displays the figure of interface panel
About	Displays the manufacturer information and sets auto-refresh.

After you configure the device, the result of the previous step will appear on the left side of the top control bar. If error occurs, please check your configuration and retry it later.

2.3.2 Navigation Bar

Device Status

Device Info

- Interface State
- Interface Flow
- Mac Address Table
- Log Query
- Optic Module Info

Basic Config

Port Config

L2 Config

L3 Config

Advanced Config

Network Mgr.

Diagnostic Tool

System Mgr.

The contents shown in the navigation bar. The contents in the navigation bar are shown in a form of list and are classified according to types. By default, the list is located at "Runtime Info". If a certain item need be configured, please click the group name and then the subitem. For example, to browse the flux of the current port, you have to click "Interface State" and then "Interface Flow".

Note:

The limited user can only browse the state of the device and cannot modify the configuration of the device. If you log on to the Web with limited user's permissions, only "Interface State" will appear.

2.3.3 Configuration Area

System Information	
Device Type	SWITCH
BIOS Version	0.4.5
Firmware Version	3.0.1T Build 37543
Serial No.	E20005050102
MAC Address	8479.733A.2013
IP Address	192.168.1.202
Current Time	1970-1-1 0:5:36
Uptime	0 Day -0 Hour -5 Minute -36 Second
CPU Usage	3%
Memory Usage	26%

[Refresh](#)

The configuration display area shows the state and configuration of the device. The contents of this area can be modified by the clicking of the items in the navigation bar.

2.3.4 Configuration Area

The configuration area is to show the content that is selected in the navigation area. The configuration area always contains one or more buttons, and their functions are listed in the following table:

Refresh	Refresh the content shown in the current configuration area.
Apply	Apply the modified configuration to the device. The application of the configuration does not mean that the configuration is saved in the configuration file. To save the configuration, you have to click "Save All" on the top control bar.
Reset	Means discarding the modification of the sheet. The content of the sheet will be resetted.
New	Creates a list item. For example, you can create a VLAN item or a new user.
Delete	Deletes an item in the list.
Back	Go back to the previous-level configuration page.

Chapter 3 Basic Configuration

Device Status

Basic Config

Hostname

Clock Mgr.

Port Config

L2 Config

L3 Config

Advanced Config

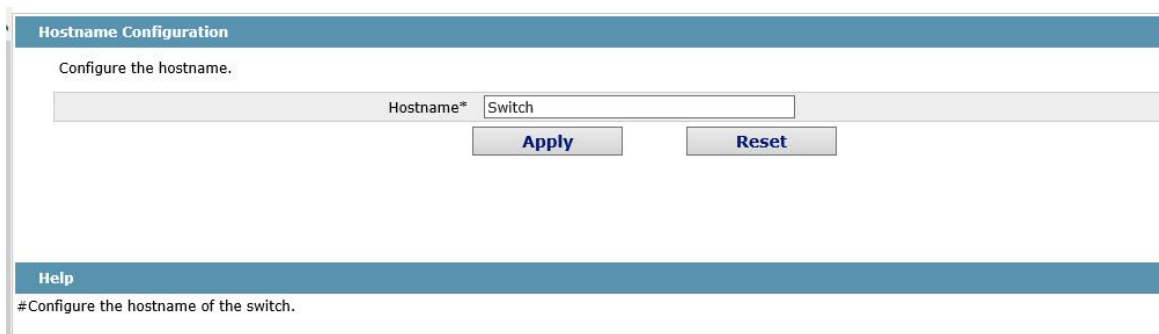
Network Mgr.

Diagnostic Tool

System Mgr.

3.1 Hostname Configuration

If you click **Basic Config -> Hostname** in the navigation bar, the Hostname Configuration page appears, as shown in the following figure.



The hostname will be displayed in the login dialog box.

The default name of the device is “Switch”. You can enter the new hostname in the text box shown in figure 3 and then click “Apply”.

3.2 Time Management

If you click **System Mgr. -> Time Setting**, the Time Setting page appears.



Help

#There are two ways to update the system time, one is to use ntp and the other is to manually set the time.

#Set Time Manually: Select the 'Set Time Manually' option, select the local time zone, enter the current time, and click 'Apply' to save the configuration.

#Network Time Synchronization: Select the 'Network Time Synchronization' option, add no more than three IP addresses of the NTP server.

#Refresh: Click to get the current time of the switch.

To refresh the clock of the displayed device, click “Refresh”.

In the “Select Time-Zone” dropdown box select the time zone where the device is located. When you select “Set Time Manually”, you can set the time of the device manually. When you select “Network Time Synchronization”, you can designate 3 SNTP servers for the device and set the interval of time synchronization.

Chapter 4 Configuration of the Physical Interface

Device Status

Basic Config

Port Config

Port Description

Port Config

Rate Limit

Port Mirror

Keepalive Detection

Port Security

Storm Control

Port Protect Group Config

POE Mgr

L2 Config

L3 Config

Advanced Config

Network Mgr.

Diagnostic Tool

System Mgr.

4.1 Configuring Port Description

If you click **Port Config -> Port Description** in the navigation bar, the Port description Configuration page appears, as shown in the following figure.

Port	Port Description
g0/1	

You can modify the port description on this page and enter up to 120 characters. The description of the VLAN port cannot be set at present.

4.2 Configuring the Attributes of the Port

If you click Port Config-> **Port Config -> Port attribute Config** in the navigation bar, the Port Attribute Configuration page appears, as shown in the following figure.

Port	Status	Speed	Duplex	Flow Control	Medium
g0/1	Enable	Auto	Auto	Off	Auto

You can change the status, speed, duplex mode and flow control of a port on this page.

Note:

2. After the speed or duplex mode of a port is modified, the link state of the port may be switched over and the network communication may be impaired.

4.3 Rate Limit

If you click **Port Config -> Rate Limit** in the navigation bar, the Port rate limit page appears, as shown in figure 4.

Port	Receive Status	Receive Speed Unit	Receive Speed	Send Status	Send Speed Unit	Send Speed
g0/1	Enable	64kbps	(1-16384)	Disable	64kbps	(1-16384)

On this page you can set the reception speed and transmission speed of a port. By default, all ports have no speed limited. The reception speed and transmission speed are configured by a percentage or by the designated unit of the switch.

4.4 Port Mirror

If you click **Port Config-> Port Mirror** in the navigation bar, the Port Mirror Config page appears, as shown in the following figure.

Mirror Port	g0/6		
Filters	Port Type: All	Slot Num: All	Name(s): <input type="text"/> Help
Mirrored Port	Mirror Mode		
<input checked="" type="checkbox"/> g0/1	RX		

Click the dropdown list on the right side of "Mirror Port" and select a port to be the destination port of mirror.

Click a checkbox and select a source port of mirror, that is, a mirrored port.

RX The received packets will be mirrored to the destination port.

TX The transmitted packets will be mirrored to a destination port.

RX & TX The received and transmitted packets will be mirrored simultaneously.

4.5 Keepalive Detection

If you click **Port Config-> Keepalive Detection** in the navigation bar, the Setting the port loopback detection page appears, as shown in Figure 6.

Port	Status	Keepalive Period
g0/1	<input type="button" value="Enable"/>	<input type="text"/> (0-32767)Seconds

You can set the loopback detection cycle on the Loopback Detection page.

4.6 Port security

4.6.1 IP Binding Configuration

If you click **Port Config-> Port Security -> IP Bind** in the navigation bar, the Configure the IP-Binding Info page appears, as shown in figure 7.

Interface Name	Detail
g0/1	Detail

Click “Detail” and then you can conduct the binding of the source IP address for each physical port. In this way, the IP address that is allowed to visit the port will be limited.

	Serial number	Address	Operate
<input type="checkbox"/>	1	192.168.0.2	Edit
<input type="checkbox"/>	2	192.168.0.3	Edit

4.6.2 MAC Binding Configuration

If you click **Port Config-> Port Security -> MAC Bind** in the navigation bar, the Configure the MAC-Binding Info page appears, as shown in figure 10.

Interface Name	Detail
G0/1	Detail

Click “Detail” and then you can conduct the binding of the source MAC address for each physical port. In this way, the MAC address that is allowed to visit the port will be limited.

	Serial number	Address	Operate
<input type="checkbox"/>	1	1234.1234.1234	Edit
<input type="checkbox"/>	2	1234.1234.1235	Edit

4.6.3 Setting the Static MAC Filtration Mode

If you click **Port Config-> Port Security -> Static MAC Filtration Mode** in the navigation bar, the Configure the static MAC filtration mode page appears, as shown in figure 12.

Interface Name	Port Mode	Static MAC Filtration Mode
g0/1	Access	<input type="button" value="Accept"/>

On this page you can set the static MAC filtration mode. By default, the static MAC filter is disabled. Also, the static MAC filter mode cannot be set on ports in trunk mode.

4.6.4 Static MAC Filtration Entries

If you click **Port Config-> Port Security -> Static MAC Filtration Entries** in the navigation bar, the Setting the static MAC filtration entries page appears.

Interface Name	Detail
g0/1	Detail

If you click “Detail”, you can conduct the binding of the source MAC address for each physical port. According to the configured static MAC filtration mode, the MAC address of a port can be limited, allowed or forbidden to visit.

Serial number	Filtration Mode	MAC Address	Operate
<input type="checkbox"/> 1	Disable	0001.0002.0003	Edit

4.6.5 Setting the Dynamic MAC Filtration Mode

If you click **Port Config-> Port Security -> Dynamic MAC Filtration Mode** in the navigation bar, the Configure the dynamic MAC filtration mode page appears, as shown in figure 15.

Interface Name	Dynamic MAC Filtration Mode	Max MAC Address
g0/1	Enable ▼	1 (1-2048)

You can set the dynamic MAC filtration mode and the allowable maximum number of addresses on this page. By default, the dynamic MAC filtration mode is disabled and the maximum number of addresses is 1.

4.7 Storm Control

In the navigation bar, click **Port Config-> Storm Control**. The system then enters the page, on which the broadcast/multicast/unknown unicast storm control can be set.

4.7.1 Broadcast storm control

Port	Status	Threshold
g0/1	Enable ▼	(1-65535) 64Kbps

Through the dropdown boxes in the Status column, you can decide whether to enable broadcast storm control on a port. In the Threshold column you can enter the threshold of the broadcast packets. The legal threshold range for each port is given behind the threshold.

4.7.2 Multicast Storm Control

Port	Status	Threshold
g0/1	Enable ▼	(1-65535) 64Kbps

Through the dropdown boxes in the Status column, you can decide whether to enable multicast storm control on a port. In the Threshold column you can enter the threshold of the multicast packets. The legal threshold range for each port is given behind the threshold.

4.7.3 Unknown Unicast Storm Control

Port	Status	Threshold
g0/1	Enable ▼	(1-65535) 64Kbps

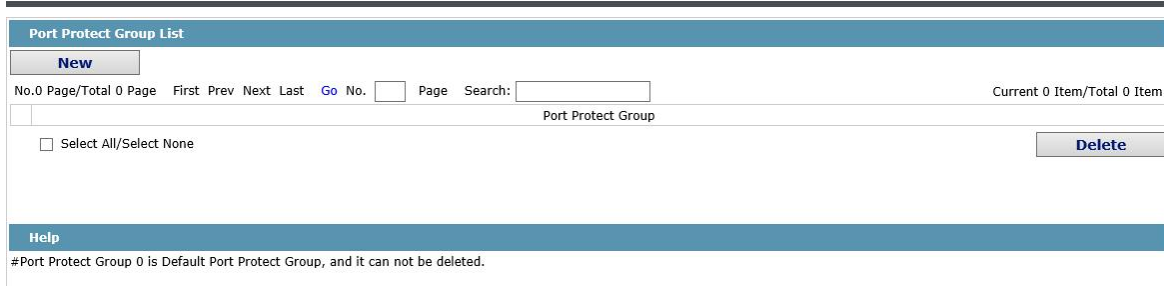
Through the “Status” dropdown box, you can decide whether to enable the unknown unicast storm limit on a port. In the Threshold column you can enter the threshold of the broadcast packets. The legal threshold range for each port is given behind the threshold.

4.8 Port Protect Group Configuration

If you click **Port Config-> Port Protect Group Config -> Port Protect Group List** in the navigation bar, the Port Protect Group List page appears.

4.8.1 Port Protect Group List

If you click **Port Config-> Port Protect Group Config -> Port Protect Group List** in the navigation bar, the Port Protect Group List page appears.



If you click New, a new port protect group will be created, as shown in the following figure.

If you tick a Port Protect Group, you can delete it. The port protect group 0 is by default, which cannot be deleted.



4.8.2 Port Protect Group Interface Configuration

If you click **Port Config-> Port Protect Group Config -> Port Protect Group Interface Config** in the navigation bar, the Port Protect Group Config page appears.

Port	Port Protect Group
g0/1	<input type="text"/>
g0/2	<input type="text"/>

The port protect group must be a created group. If one port has configured the default protect group, others ports can only configure the default groups.

4.9 POE Management

4.9.1 POE Global Configuration

If you click **Port Config -> POE Mgr** in the navigation bar, the POE management configuration page appears, as shown in the following figure.

POE Global Configure

Power Management Mode	Auto	
Low Disable Threshold	18000	(100-30000) mw
Low No Connect Threshold	18000	(100-30000) mw
Duration of POE LED	30	(1-300) s
POE MIB Notification Function	Start	
Threshold of Available Power	100	(1-100)
Power Counter	0	(0-100) s
POE Chip Automatic Protection	Stop	
Power Supply Standard	Max Power Supply	

Help

#Low Disable Threshold means that the lower priority port will be disabled when consumed power

#Low No Connect Threshold means that the lower priority port will not be connected when consumed power

On this page, you can configure the POE power supply management mode, lower priority upgrade preemption threshold, enable/disable POE MIB inform.

4.9.2 POE Global Realtime Info

If you click **Port Config -> POE Mgr->POE Global Realtime Info** in the navigation bar, the POE management configuration page appears, as shown in the following figure.

POE Global Realtime Info

POE Chip	PD69100
POE Port Number	16
PSE Total Power	300000
PSE Usage Threshold	100%
PSE Alarm Power	100
PSE Consumed Power	0
PSE Temperature	38

On this page, you can check POE port number, PSE power and PSE temperature.

4.9.3 POE Interface List

If you click **Port Config -> POE Mgr->POE Interface List** in the navigation bar, the POE management configuration page appears, as shown in the following figure.

POE Interface List

Filters Port Type: Slot Num: Name(s):

Port	Port Max Power	Port Priority	Force Connection	POE Interface Description
g0/1	30000 mw	Low Priority	Disable	
g0/2	30000 mw	Low Priority	Disable	
g0/3	30000 mw	Low Priority	Disable	
g0/4	30000 mw	Low Priority	Disable	
g0/5	30000 mw	Low Priority	Disable	
g0/6	30000 mw	Low Priority	Disable	
g0/7	30000 mw	Low Priority	Disable	

On this page, you can configure the Port Priority, Port Max Power, Force Connection and POE Interface Description.

4.9.4 POE Port Policy Power

If you click **Port Config -> POE Mgr->POE Port Policy Power** in the navigation bar, the POE Port Policy Power configuration page appears, as shown in the following figure.

POE Port Policy Power		
Filters	Port Type: <input type="button" value="All"/>	Slot Num: <input type="button" value="All"/>
		Name(s): <input type="text"/>
Help		
Port	POE Function	Time Range
g0/1	<input type="button" value="Disable"/>	<input type="text" value="POETIME"/>
g0/2	<input type="button" value="Disable"/>	<input type="text"/>
g0/3	<input type="button" value="Enable"/>	<input type="text"/>
g0/4	<input type="button" value="Enable"/>	<input type="text"/>
g0/5	<input type="button" value="Enable"/>	<input type="text"/>
g0/6	<input type="button" value="Enable"/>	<input type="text"/>
g0/7	<input type="button" value="Enable"/>	<input type="text"/>

On this page, you can enable/disable POE Function and Time Range.

4.9.5 POE Interface Power List

If you click **Port Config -> POE Mgr-> POE Port Policy Power** in the navigation bar, the POE Port Policy Power configuration page appears, as shown in the following figure.

POE Interface Power List					
Filters	Port Type: <input type="button" value="All"/>	Slot Num: <input type="button" value="All"/>	Name(s): <input type="text"/>		
Help					
Port	Current Power	Setting Max Power	Average Power	Peak Power	Bottom Power
g0/1	0mw	30000mw	-	-	-
g0/2	0mw	30000mw	-	-	-
g0/3	0mw	30000mw	-	-	-
g0/4	0mw	30000mw	-	-	-
g0/5	0mw	30000mw	-	-	-
g0/6	0mw	30000mw	-	-	-

On this page, you can check Current Power, Setting Max Power, Average Power, Peak Power and Bottom Power.

4.9.6 POE Port Other Info

If you click **Port Config -> POE Mgr-> POE Port Other Info** in the navigation bar, the PPOE Port Other Info configuration page appears, as shown in the following figure.

POE Port Other Info				
Filters	Port Type: <input type="button" value="All"/>	Slot Num: <input type="button" value="All"/>	Name(s): <input type="text"/>	
Help				
Port	POE Port Detection Status	POE Port Power Supply	POE IEEE Class	POE Port Current
g0/1	Searching	Signal	0	0mA
g0/2	Searching	Signal	0	0mA
g0/3	Searching	Signal	0	0mA
g0/4	Searching	Signal	0	0mA
g0/5	Searching	Signal	0	0mA
g0/6	Searching	Signal	0	0mA
g0/7	Searching	Signal	0	0mA

On this page, you can check POE Port Detection Status, POE Port Power Supply, POE IEEE Class, and POE Port Current.

Chapter 5 Layer-2 Configuration

Device Status

Basic Config

Port Config

L2 Config

VLAN Config

GVRP Config

STP Config

IGMP Snooping

Static ARP

Static MAC Config

LLDP Config

DDM Config

Port Channel

Ring Protection

Multiple Ring Protection

BackupLink Config

MTU Config

PDP Config

5.1 VLAN Configuration

5.1.1 VLAN List

If you click **Layer-2 Config -> VLAN Config** in the navigation bar, the VLAN Config page appears, as shown in figure 2.

	VLAN ID	VLAN Name	Operate
<input type="checkbox"/>	1	Default	Edit
<input type="checkbox"/>	2	2	Edit

The VLAN list will display VLAN items that exist in the current device according to the ascending order. In case of lots of items, you can look for the to-be-configured VLAN through the buttons like “Prev”, “Next” and “Search”.

You can click “New” to create a new VLAN.

You can also click “Edit” at the end of a VLAN item to modify the VLAN name and the port’s attributes in the VLAN.

If you select the checkbox before a VLAN and then click “Delete”, the selected VLAN will be deleted.

Note:

By default, a VLAN list can display up to 100 VLAN items. If you want to configure more VLANs through Web, Please log on to the switch through the Console port or Telnet, enter the global configuration mode and then run the “**ip http web max-vlan**” command to modify the maximum number of VLANs that will be displayed.

5.1.2 VLAN Configuration

If you click “New” or “Edit” in the VLAN list, the VLAN configuration page appears, on which new VLANs can be created or the attributes of an existent VLAN can be modified.

Revising VLAN Config

VLAN ID

VLAN Name

Port	Default VLAN	Mode	Untag or not	Allow or not
g0/1	<input style="width: 20px;" type="text" value="1"/> <1-4094>	Access	No	Yes
g0/2	<input style="width: 20px;" type="text" value="1"/> <1-4094>	Access	No	Yes
g0/3	<input style="width: 20px;" type="text" value="1"/> <1-4094>	Access	No	Yes
g0/4	<input style="width: 20px;" type="text" value="1"/> <1-4094>	Access	No	Yes
g0/5	<input style="width: 20px;" type="text" value="1"/> <1-4094>	Access	No	Yes
g0/6	<input style="width: 20px;" type="text" value="1"/> <1-4094>	Access	No	Yes
g0/7	<input style="width: 20px;" type="text" value="1"/> <1-4094>	Access	No	Yes

If you want to create a new VLAN, enter a VLAN ID and a VLAN name; the VLAN name can be null.

Through the port list, you can set for each port the default VLAN , the VLAN mode (Trunk or Access), whether to allow the entrance of current VLAN packets and whether to execute the untagging of the current VLAN when the port works as the egress port.

Note:

When a port in Trunk mode serves as an egress port, it will untag the default VLAN by default.

5.2 GVRP Configuration

5.2.1 GVRP Global Attribute Configuration

Click **L2 Config -> GVRP Config -> GVRP Global Config** in the navigation bar, and enter GVRP global attribute configuration page.

GVRP Global Config	
GVRP Global Config	Disable ▾
Set Dynamic Vlan to Take Effect Only On Registration Ports	Disable ▾
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

You can enable or disable the global GVRP protocol, and set dynamic vlan to take effective or not only in the registered port.

5.2.2 GVRP Port Attribute Configuration

Click **L2 Config -> GVRP Config -> GVRP Interface Config** in the navigation bar and enter GVRP interface attribute configuration page.

Port	GVRP Status
g0/1	Enable ▾

GVRP interface configuration can enable or disable GVRP protocol of the port.

5.3 STP Configuration

5.3.1 STP Status Information

If you click **Advanced Config -> STP Config** in the navigation bar, the STP Config page appears, as shown in figure 10.

Root STP Config	
Spanning Tree Priority	4096
MAC Address	00E0.0F8E.7025
Hello Time	2
Max Age	20
Forward Delay	15

Local STP Config	
Protocol Type	RSTP ▾
Spanning Tree Priority	32768 ▾
MAC Address	8479.733A.2013
Hello Time	<input type="text" value="2"/> (1-10)s
Max Age	<input type="text" value="20"/> (6-40)s
Forward Delay	<input type="text" value="15"/> (4-30)s
BPDU Terminal	Disable ▾
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

The root STP configuration information and the STP port's status are only-read.

Click the dropdown box on the right side of "Protocol" to change the currently running STP mode. The supported modes include STP, RSTP and Disabled STP.

The priority and the time need be configured for different modes.

Note:

The change of the STP mode may lead to the interruption of the network.

5.3.2 Configuring the Attributes of the STP Port

If you click the "Configure RSTP Port" option, the "Configure RSTP Port" page appears.

Port	Protocol Status	Priority(0~240)	Path-Cost(0~200000000)	Edge Port	RSTP Ring
g0/1	Enable	128	0	Disable	Disable

The configuration of the attributes of the port is irrelative of the global STP mode. For example, if the protocol status is set to "Disable" and the STP mode is also changed, the port will not run the protocol in the new mode.

The default value of the path cost of the port is 0, meaning the path cost is automatically calculated according to the speed of the port. If you want to change the path cost, please enter another value.

5.4 IGMP-Snooping Configuration

5.4.1 IGMP-Snooping Configuration

Click **L2 Config -> IGMP Snooping** in the navigation bar, and enter the IGMP-Snooping Configuration page.

IGMP Snooping Config

Multicast Filtration Mode	Transfer Unknown
IGMP Snooping	Disable
Enable Auto Query	Disable

[Apply](#)

On this page you can set whether to make a switch to forward unknown multicasts, whether to enable IGMP snooping, and whether to configure the switch as the querier of IGMP.

5.4.2 IGMP-Snooping VLAN List

In the navigation bar, click **L2 Config -> IGMP Snooping -> IGMP Snooping VLAN list** in the navigation bar, and enter IGMP-Snooping VLAN page.

IGMP Snooping VLAN Config

[New](#)

No.1 Page/Total 1 Page First Prev Next Last Go No. Page Search: Current 1 Item/Total 1 Item

No.	VLAN ID	Status of the IGMP Snooping Vlan	Immediate-leave	Multicast Router Port	Operate
<input type="checkbox"/>	1	Running	Disable	g0/1(static);g0/2(static);	Edit

Select All/Select None [Delete](#)

If you click New, IGMP-snooping VLAN configuration can be done. Through Web up to 8 physical ports can be set on each IGMP snooping VLAN. If you click Cancel, a selected IGMP-Snooping VLAN can be deleted; if you click Edit, you can modify the member port, running status and immediate-leave of IGMP-Snooping VLAN.

Revising the IGMP Snooping VLAN Config

VLAN ID:

Status of the IGMP Snooping Vlan:

Immediate-leave:

Configured Mrouter Port List:

Available Port List:

- g0/1
- g0/2
- g0/3
- g0/4
- g0/5
- g0/6
- g0/7
- g0/8
- g0/9
- g0/10

>> <<

When create new IGMP-Snooping Vlan, VLAN ID can be modified; when modify IGMP-Snooping Vlan, VLAN ID cannot be modified.

You can add or delete the routing port by buttons ">>" or "<<".

5.4.3 Static Multicast Address

Click **L2 Config -> IGMP Snooping > Static Multicast Address List** in the navigation bar, and enter static multicast address configuration page.

Static Multicast Address Config

VLAN ID:

Multicast IP Address:

Assignment Port:

Static Multicast List Info

No.0 Page/Total 0 Page First Prev Next Last Go No. Page Search: Current 0 Item/Total 0 Item

VLAN ID	Group	Port
<input type="checkbox"/> Select All/Select None		

This page displays the static multicast group in current network according to IGMP-Snooping statistics and the port set each member belongs to.

Click "Refresh" to refresh the contents in the list.

5.4.4 Multicast List

Click the Multicast List Info option on the top of the page and the Multicast List Info page appears.

Multicast List Info

No.1 Page/Total 1 Page First Prev Next Last Go No. Page Search: Current 2 Item/Total 2 Item

VLAN ID	Group	Type	Port
1	239.255.255.250	IGMP	g0/9
1	235.80.68.83	IGMP	g0/9

On this page the multicat groups, which are existent in the current network and are in the statistics of IGMP snooping, as well as port sets which members in each group belong to are displayed.

Click "Refresh" to refresh the contents in the list.

Note:

By default, a multicast list can display up to 15 VLAN items. You can modify the number of multicast items by running `ip http web igmp-groups` after you log on to the device through the Console port or Telnet.

5.5 Setting Static ARP

Click **L2 Config** -> **Static ARP** in the navigation bar, and enter the basic ARP configuration page.

Basic ARP Config

No.1 Page/Total 1 Page First Prev Next Last Go No. Page Search: Current 1 Item/Total 1 Item

No.	IP Address	MAC Address	Interface VLAN	Operate
<input type="checkbox"/>	10.0.0.1	22:22:55:55:44:44	1	Edit

Select All/Select None

Help

#MAC: The mac address only supports the unicast address and the following formats:XXXXXXXXXXXX,XXXX.XXXX.XXXX,XX:XX:XX:XX:XX,XX-XX-XX-XX-XX, and X is Hex number

Click “New” to add ARP entry. The VLAN interface needs to be assigned when configuring the ARP entry.

Click “Modify” to modify the current ARP entry.

Click “Delete” to delete the selected ARP entry.

ARP Config

Configure the corresponding MAC address of an IP address

IP Address*

MAC Address*

Interface VLAN*

Help

#MAC: The mac address only supports the unicast address and has the following formats:XXXXXXXXXXXX,XXXX.XXXX.XXXX,XX:XX:XX:XX:XX,XX-XX-XX-XX-XX, and X is Hex number

5.6 Static MAC Configuration

Click **L2 Config** > **Static MAC Config** in the navigation bar, and enter static MAC address configuration page.

Static MAC Address List Info

No.1 Page/Total 1 Page First Prev Next Last Go No. Page Search: Current 1 Item/Total 1 Item

No.	Index	Static MAC Address	VLAN ID	Port	Operate
<input type="checkbox"/>	1	1234.1234.1234	1	G0/3	Edit

Select All/Select None

Click “New” to configure static MAC address and VLAN for the assigned port. The unicast MAC address can only be configured with one port and the multicast MAC address can be configured with multiple ports.

Click “Modify” to modify the configured static MAC address.

Click “Delete” to delete the static MAC address entry.

Static MAC Address Config

Static MAC Address	1234.1234.1234
VLAN ID	2

Configured Port List

g0/4

>>

<<

Available Port List

g0/1
g0/2
g0/3
g0/5
g0/6
g0/7
g0/8
g0/9
g0/10
g0/11

Apply

Reset

Go Back

Help

#Only one port can be configured for a unicast MAC address, while multiple MAC addresses can be configured for a multicast MAC address
#MAC format: XXXX.XXXX.XXXX

5.7 LLDP Configuration

5.7.1 Configuring the Global Attributes of LLDP

If you click **Layer-2 Config -> LLDP Config** in the navigation bar, the Global LLDP Config page appears, as shown in figure 6.

Basic Config of LLDP Protocol

Protocol State	Open the LLDP protocol	
HoldTime Settings	120	(0-65535)s
Reinit Settings	2	(2-5)s
Setting the packet transmission cycle	30	(5-65534)s

Apply

Reset

Help

#HoldTime:Means the TTL(Time to live) of sending LLDP packets. Its default value is 120s.
#Reinit:Means the delay of continuously sending LLDP packets. Its default value is 2s.

You can choose to enable LLDP or disable it. When you choose to disable LLDP, you cannot configure LLDP.

The “HoldTime” parameter means the ttl value of the packet that is transmitted by LLDP, whose default value is 120s.

The “Reinit” parameter means the delay of successive packet transmission of LLDP, whose default value is 2s.

5.7.2 Configuring the Attributes of the LLDP Port

If you click **Layer-2 Config -> LLDP Config-> LLDP Port Config** in the navigation bar, the Setting the attributes of the LLDP port page appears, as shown in figure 7.

Port	Receive LLDP Packet	Send LLDP Packet
g0/1	Enable	Enable

LLDP interface configuration can enable or disable the port transmitting LLDP packets.

5.8 DDM Configuration

Click **L2 Config > DDM Config** in the navigation bar, and enter DDM configuration page.



5.9 Link Aggregation Configuration

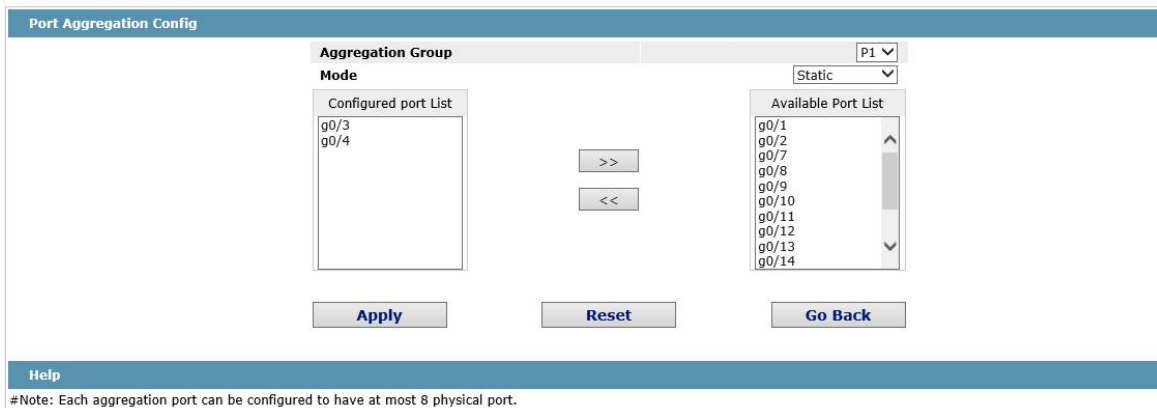
5.9.1 Port Aggregation Configuration

If you click **Advanced Config -> Link Aggregation Config** in the navigation bar, the Link aggregation Config page appears, as shown in figure 22.



Help
#Note: The physical attributes of all the aggregated ports shall be the same, including Speed, Duplex mode and Vlan

If you click **New**, an aggregation group can be created. Up to 32 aggregation groups can be configured through Web and up to 8 physical ports in each group can be aggregated. If you click **Cancel**, you can delete a selected aggregation group; if you click **Modify**, you can modify the member port and the aggregation mode.



Help
#Note: Each aggregation port can be configured to have at most 8 physical port.

An aggregation group is selectable when it is created but is not selectable when it is modified.

When a member port exists on the aggregation port, you can choose the aggregation mode to be Static, LACP Active or LACP Passive.

You can click >> and << to delete and add a member port in the aggregation group.

5.9.2 Configuring Load Balance of Port Aggregation Group

Some models support aggregation group based load balance mode configuration and some not but can be configured in the global configuration mode.

Configuring Load Balance of Port Aggregation Group

Port Channel p1	Loading Balance Mode SRC MAC
--------------------	---------------------------------

You can select link aggregation load balance mode and click "Apply" to apply it.

5.10 EAPS Ring Protection Configuration

5.10.1 EAPS Ring List

If you click **Layer-2 Config -> Ring Protection ->EAPS Config**, the EAPS Ring Config page appears.

ether-ring

No.1 Page/Total 1 Page First Prev Next Last Go No. Page Search: Current 1 Item/Total 1 Item

Ring ID	Node Type	Ring Description	Control VLAN	Status	Hello	Fail	Preforward	Primary Port/Forwarding/Link Status	Secondary Port/Forwarding/Link Status	Operate
0	Master-node		2	RingFail	1	3	3	None/Blocking/Linkdown	None/Blocking/Linkdown	Edit

Select All/Select None

In the list shows the currently configured EAPS ring, including the status of the ring, the forwarding status of the port and the status of the link.

Click "New" to create a new EAPS ring.

Click the "Operate" option to configure the "Time" parameter of the ring.

Note:

1. The system can support 8 EAPS rings.
2. After a ring is configured, its port, node type and control Vlan cannot be modified. If the port of the ring, the node type or the control Vlan need be adjusted, please delete the ring and then establish a new one.

5.10.2 EAPS Ring Configuration

If you click "New" on the EAPS ring list, or "Operate" on the right side of a ring item, the "Configure EAPS" page appears.

ether-ring

Ring ID	0	
Node Type	Master Node	
Ring Description	<input style="width: 95%;" type="text"/>	
Control VLAN	<input style="width: 95%;" type="text"/>	
Hello Time	1	(1-10)s
Fail Time	3	(3-30)s
Preforward Time	3	(3-30)s
Primary Port	None	
Secondary Port	None	

Help

#Ring Description: You can't input 'Enter'.

Note:

25

ANGUSTOS LLC

-INTERNAL USE ONLY-

VERSION 2.5.1A

If you want to modify a ring, on this page the node type, the control VLAN, the primary port and the secondary port cannot be modified.

In the dropdown box on the right of “Ring ID”, select an ID as a ring ID. The ring IDs of all devices on the same ring must be the same.

The dropdown box on the right of “Node Type” is used to select the type of the node. Please note that only one master node can be configured on a ring.

Enter a value between 1 and 4094 in the text box on the right of “Control VLAN” as the control VLAN ID. When a ring is established, the control VLAN will be automatically established too. Please note that if the designated control VLAN is 1 and the VLAN of the control device is also 1 the control device cannot access the control VLAN. Additionally, please do not enter a control VLAN ID that is same as that of another ring.

In the text boxes of “Primary Port” and “Secondary Port”, select a port as the ring port respectively. If "Node Type" is selected as “Transit-Node”, the two ports will be automatically set to transit ports.

Click “Apply” to finish EAPS ring configuration, click “Reset” to resume the initial values of the configuration, or click “Return” to go back to the EAPS list page.

5.11 MEAPS Configuration

5.11.1 MEAPS Ring Configuration

If you click **Layer-2 Config -> Multiple Ring Protection -> Multiple Ring Protection** on the navigation bar, the Multiple Ring Protection Configuration page appears.

Multiple Ring Protection Configuration														
New														
No.1 Page/Total 1 Page	First	Prev	Next	Last	Go	No.	Page	Search:						Current 1 Item/Total 1 Item
Domain ID	Ring ID	Ring Type	Node Type	Control Vlan	Hello Time	Failed Time	Pre Forward Time	Port	Type	Port	Type	Operate		
<input type="checkbox"/>	2	2	Major Ring	Master Node	3	3	9	9	None	Primary-Port	None	Secondary-Port	Edit	
<input type="checkbox"/> Select All/Select None													Delete	

The list shows the current configured MEAPS ring, including Domain ID, Ring ID, Ring type, Node type, Control Vlan, Hello Time, Failed Time, Pre Forward Time, primary port and secondary port.

Click New to create a MEAPS ring.

Click Edit on the right and configure the time parameter and the primary and secondary port of the ring.

Note:

1. The system supports 4 MEAPS (0-3).
2. One domain supports 8 rings (0-7).
3. Once one MEAPS is configured, its Domain ID, ring ID, ring type, node type and control Vlan cannot be modified. If adjustment is needed, please delete the Ethernet ring and reset it.

5.11.2 MEAPS Ring Configuration

If you click New on the Multiple Ring Protection page or click Edit on the right, the New MEAPS Global Config page appears.

Web Configuration

NewMEAPS Global Config

Domain ID*	<input type="text"/>
Ring ID*	<input type="text"/>
Ring Type*	Major Ring ▼
Node Type*	Master Node ▼
Control Vlan*	<input type="text"/>
Hello Time	<input type="text"/>
Failed Time	<input type="text"/>
Pre-Forward Time	<input type="text"/>
Primary-Port	None ▼
Secondary-Port	None ▼

Help

#Your web management may be interrupted as the control VLAN is modified to be the vlan interface that the web browser connects
 #Only the master or transit node can be configured in the major ring
 #The master node, transit node, edge node or assistant node can be configured in the sub ring
 #The master or transit node can be configured in one ring, while the edge node or assistant edge node can be configured in several rings

Note:
 In an existed MEAPS ring, its domain ID, ring ID, ring type, node type and control Vlan cannot be modified.

The primary ring can only be configured with the main node and the Transit node.
 The secondary ring can be configured with the main node, the transit node, the edge node and the assistant edge node.

The primary node and the transit node can only be existed in one ring. The edge node and the assistant edge node can be existed in multiple rings simultaneously.

On the right drop box of “Primary-Port” and “Secondary-Port”, select one port respectively as the ring port or select None.

5.12 Backup Link Protocol Configuration

5.12.1 Backup Link Protocol Global Configuration

If you click **Layer-2 Config ->Backup Link Config ->Backup Link Protocol Global Config** on the navigation bar, the Backup Link Protocol Global Config page appears.

BackupLink Protocol Global Config

No.1 Page/Total 1 Page First Prev Next Last Go No. Page Search: Current 1 Item/Total 1 Item

No.	Group ID	Preemption Mode	Preemption Delay	Operate
<input type="checkbox"/>	2	No Preemption		Edit

Select All/Select None

On the page, the current configured backup link groups are shown, including Preemption Mode and Preemption Delay.

Click New to create a new link backup group.

Click Edit on the right to configure Preemption Mode and Preemption Delay.

BackupLink Protocol Global Config

Group ID	<input type="text"/>
Preemption Mode	No Preemption ▼
Preemption Delay	<input type="text"/>

Note:
 1. The system supports 8 link backup groups.

2. The Preemption mode determines the policy the primary port and the backup port forward packets.

5.12.2 Backup Link Protocol Interface Configuration

If you click **Layer-2 Config -> Backup Link Protocol Config -> Backup Link Protocol Interface Config** on the navigation bar, the Backup Link Protocol Global Config page appears.

BackupLink Protocol Interface Config						
No.1 Page/Total 1 Page	First	Prev	Next	Last	Go No. <input type="text"/>	Page Search: <input type="text"/>
						Current 18 Item/Total 18 Item
Interface Name	Group ID	Interface Attribute	MMU Attribute	Shareload VLAN	Operate	
g0/1					Edit	
g0/2					Edit	
g0/3					Edit	
g0/4					Edit	
g0/5					Edit	
g0/6					Edit	
g0/7					Edit	
g0/8					Edit	

This page shows the backup link group’s member ports, Interface Attribute, MMU Attribute, Shareload Vlan, etc.

Click Edit on the right to configure the Backup Link Protocol.

BackupLink Protocol Interface Config

Interface Name	g0/1		
Group ID	<input type="text"/>		
Interface Attribute	<input type="text"/>		
MMU Attribute	<input type="text"/>		
Shareload VLAN	<input type="text"/>		

Help

#Share Load VLAN can be Only Configured On The Backup Port

The backup link group which has configured the primary port cannot take other ports as its primary port. Likewise, the backup link group which has configured the backup port cannot take other ports as its backup port.

5.13 MTU Configuration

If you click **Layer-2 Config -> MTU Config** on the navigation bar, the MTU Config page appears.

MTU Config

MTU	<input type="text" value="1500"/>		(1500-9216)
-----	-----------------------------------	--	-------------

Help

#Configure the size of the system mtu, whose default value is 1500

You can set the size of the maximum transmission unit (MTU).

5.14 PDP Configuration

5.14.1 Configuring the Global Attributes of PDP

If you click **Layer-2 Config -> PDP Config** in the navigation bar, the Global PDP Config page appears, as shown in figure 4.

Basic Config of PDP Protocol	
Protocol State	Close the PDP protocol ▾
HoldTime Settings	180 (10-255)s
Setting the packet transmission cycle	60 (5-254)s
Protocol Version	Version2 ▾

Help
 #HoldTime:If the other PDP packets are not received, the switch will save the holdtime before clearing the received packets.Its default value is 180s.
 #Cycle of Sending Packets:Its default value is 60s.

You can choose to enable PDP or disable it. When you choose to disable PDP, you cannot configure PDP.

The “HoldTime” parameter means the time to be saved before the router discards the received information if other PDP packets are not received.

5.14.2 Configuring the Attributes of the PDP Port

If you click **Layer-2 Config -> PDP Config-> PDP Port Config** in the navigation bar, the Setting the attributes of the PDP port page appears, as shown in figure 5.

Port	Status
g0/1	Enable PDP ▾

After the PDP port is configured, you can enable or disable PDP on this port.

Chapter 6 Layer-3 Configuration

Device Status

Basic Config

Port Config

L2 Config

L3 Config

VLAN Interfaces and IP Addresses
Static Route

Advanced Config

Network Mgr.

Diagnostic Tool

System Mgr.

6.1 Vlan interface configuration

Click **L3 Config -> VLAN Interfaces and IP Addresses**, and enter the VLAN interface configuration page.

VLAN Interface Config

[New](#)

No.1 Page/Total 1 Page First Prev Next Last Go No. Page Search: Current 1 Item/Total 1 Item

No.	Name of the VLAN Interface	IP Attribute	IP Address	Operate
<input type="checkbox"/>	1	Manual Config	192.168.1.202/16;	Edit

Select All/Select None [Delete](#)

Help
#IP address modification may interrupt your web management

Click **New** to add a new VLAN interface. Click **Cancel** to delete a VLAN interface. Click **Modify** to modify the settings of a corresponding VLAN interface.

When you click **New**, the name of the corresponding VLAN interface can be modified; but if you click **Modify**, the name of the corresponding VLAN interface cannot be modified.

VLAN Interface Config

IP Attribute

VLAN Interface Name*

IP Attribute*

Primary IP Address

IP Address*

MASK address*

Secondary IP Address 1

IP Address*

MASK address*

Secondary IP Address 2

IP Address*

MASK address*

[Apply](#) [Reset](#) [Go Back](#)

Help
The primary IP must be configured for the VLAN interface before the secondary IP is configured

Note:
Before the accessory IP of a VLAN interface is set, you have to set the main IP.

6.2 Setting the Static Route

If you click **Layer-3 Config -> Static Route Config**, the Static route configuration page appears.

Static Routing Protocol Config

[New](#)

No.1 Page/Total 1 Page First Prev Next Last Go No. Page Search: Current 1 Item/Total 1 Item

No.	Default Route	Dest IP Segment	Dest IP Mask	Interface Type	VLAN Interface	Gateway's IP Address	Forwarding Routing Address	Distance metric	Routing Tag	Specify the route description	Operate
<input type="checkbox"/>	false	192.168.0.0	255.255.0.0	gateway		192.168.1.3			2	false	Edit

Select All/Select None [Delete](#)

Help
#Global:The next-hop address is in the global routing table.

Click **Create** to add a static route.

If you click Edit, you can modify the current static route.
 If you click Cancel, you can cancel the chosen static route.

Static Route Config

Configure the static routing protocol

Default Route	<input type="checkbox"/>
Dest IP Segment	<input type="text"/>
Dest IP Mask	<input type="text"/>
Interface Type	<input type="text" value="Interface Null0"/>
Interface Vlan	<input type="text"/>
Gateway's IP Address	<input type="text"/>
Forwarding Routing address	<input type="text"/>
Distance metric	<input type="text"/>
Routing Tag	<input type="text"/>
Specify Route Description	<input type="text"/>

Help

#Global:The next-hop address is in the global routing table.

Chapter 7 Advanced Configuration

Device Status

Basic Config

Port Config

L2 Config

L3 Config

Advanced Config

Qos Config

IP Access List

MAC Access List

Network Mgr.

Diagnostic Tool

System Mgr.

7.1 QoS Configuration

7.1.1 Configuring QoS Port

If you click **Advanced Config -> QoS -> Configure QoS Port**, the Port Priority Config page appears.

Port	COS value
g0/1	▼
g0/2	▼
g0/3	▼
g0/4	▼
g0/5	▼
g0/6	▼
g0/7	▼
g0/8	▼

You can set the CoS value by clicking the dropdown box on the right of each port and selecting a value. The default CoS value of a port is 0, meaning the lowest priority. If the CoS value is 7, it means that the priority is the highest.

7.1.2 Global QoS Configuration

If you click **Advanced Config -> QoS -> Configure QoS Port**, the Port Priority Config page appears.

Queue 1	Queue 2	Queue 3	Queue 4
1 (1-127)	1 (1-127)	1 (0-127)	1 (0-127)
Queue 5	Queue 6	Queue 7	Queue 8
1 (0-127)	1 (0-127)	1 (0-127)	1 (0-127)

COS value	Queue
0	Queue 1 ▼
1	Queue 2 ▼
2	Queue 3 ▼
3	Queue 4 ▼
4	Queue 5 ▼
5	Queue 6 ▼
6	Queue 7 ▼
7	Queue 8 ▼

In WRR mode, you can set the weight ratio of the QoS queue. There are 4 queues in total, among which queue 1 has the lowest priority and queue 4 the highest priority.

7.2 IP Access Control List

7.2.1 Setting the Name of the IP Access Control List

If you click **Advanced Config -> IP Access Control List -> IP Access Control List Config**, the IP ACL configuration page appears.

Web Configuration

IP ACL Config

[New](#)

No.1 Page/Total 1 Page First Prev Next Last Go No. Page Search: Current 2 Item/Total 2 Item

No.	Name of the IP ACL	Attribute of the IP ACL	Operate
<input type="checkbox"/>	MyStandardIPACL	standard	Edit
<input type="checkbox"/>	MyExtendandACL	extended	Edit

Select All/Select None [Delete](#)

Click New to add a name of the IP access control list. Click Cancel to delete an IP access control list.

Creating the IP ACL

Name of the IP ACL*

Attribute

[Apply](#) [Reset](#) [Go Back](#)

If you click Modify, the corresponding IP access control list appears and you can set the corresponding rules for the IP access control list.

7.2.2 Setting the Rules of the IP Access Control List

➤ Standard IP access control list

IP Standard ACLMyStandardIPACL

[New](#)

No.1 Page/Total 1 Page First Prev Next Last Go No. Page Search: Current 1 Item/Total 1 Item

Authority	Src IP	Src IP Mask	Record the log	Operate
<input type="checkbox"/> permit	1.1.1.1	255.255.255.0	log	Edit

Select All/Select None [Go Back](#) [Delete](#)

Click New to add a rule of the IP access control list. Click Cancel to delete a rule of the IP access control list. If you click Modify, the corresponding IP access control list appears and you can set the corresponding rules for the IP access control list.

NewStandard IP ACL Regulation

NewIP Access Control ListMyStandardIPACLItem

Authority

Src IP Type

Src IP*

Src IP Mask

Src IP Range* -

Log

[Apply](#) [Reset](#) [Go Back](#)

➤ Extended IP access control list

Extended IP ACLMyExtendandACL

[New](#)

No.1 Page/Total 1 Page First Prev Next Last Go No. Page Search: Current 1 Item/Total 1 Item

Authority	Mask Type	Protocol Number	Src Address	Src Port	Dst Address	Dst Port	Time-Range	TosPrecedence	Do not fragment the flag	Fragmented Packet	Offset	Length of the IP packet	Time-to-live Value	Record the log	Operate
<input type="checkbox"/> permit	Mask	0	192.168.1.1/255.0.0.0		any										Edit

Select All/Select None [Go Back](#) [Delete](#)

Click New to add a rule of the IP access control list. Click Cancel to delete a rule of the IP access control list. If you click Modify, the corresponding IP access control list appears and you can set the corresponding rules for the IP access control list.

NewExtended IP ACL Regulation

NewIP Access Control ListMyExtendACLItem

Authority	permit
Mask Type	Mask
Protocol Number*	0
Src IP Type	any
Src IP*	
Src IP Mask*	
Src Interface Vlan*	
Src IP Range*	
Src Port	
Src Port Range	
Dst IP Type	any
Dst IP*	
Dst IP Mask*	
Dst Interface Vlan*	
Dst IP Range*	
Dst Port	
Dst Port Range	
Time-Range	
Tos	
Precedence	
Do not fragment	
Fragmented Packet	
Offset	
Length of the IP Packet	
Time-to-live Value	
Log	<input type="checkbox"/>
Location	

Apply Reset Go Back

7.2.3 Applying the IP Access Control List

If you click **Advanced Config -> IP Access Control List -> Applying the IP Access Control List**, the Applying the IP access control list page appears.

Port	Egress ACL	Ingress ACL
G0/1	myacl	
G0/2		acla
G0/3		
G0/4		
G0/5		
G0/6		
G0/7		
G0/8		

7.3 MAC Access Control List

7.3.1 Setting the Name of the IP Access Control List

If you click **Advanced Config -> MAC Access Control List -> MAC Access Control List Config**, the MAC ACL configuration page appears.

MAC ACL Config

New

No.1 Page/Total 1 Page First Prev Next Last Go No. Page Search: Current 1 Item/Total 1 Item

Name of the MAC Access Control List	Operate
MyACL	Edit

Select All/Select None Delete

Click New to add a name of the MAC access control list. Click Cancel to delete an IP access control list.

Creating MAC ACL

Name of the MAC ACL*

Apply Reset Go Back

7.3.2 Setting the Rules of the MAC Access Control List

If you click Modify, the corresponding MAC access control list appears and you can set the corresponding rules for the MAC access control list.

MAC ACLMyACL

No.1	Page/Total 1 Page	First	Prev	Next	Last	Go	No. <input style="width: 20px;" type="text"/>	Page	Search: <input style="width: 50px;" type="text"/>	Current 1 Item/Total 1 Item
<input type="checkbox"/>	Authority	Src MAC Type	Src MAC	Src MAC Mask	Dst MAC Type	Dst MAC	Dst MAC Mask	Operate		
	permit	host	0001.0002.0003		any			Edit		

Select All/Select None

Click New to add a name of the MAC access control list. Click Cancel to delete a rule of the IP access control list. If you click Modify, the corresponding IP access control list appears and you can set the corresponding rules for the MAC access control list.

New MAC ACL Regulation

NewMAC ACLMyACLItem

Authority	<input type="text" value="permit"/>	
Src MAC Type*	<input type="text" value="any"/>	
Src MAC*	<input type="text"/>	
Src MAC Mask*	<input type="text"/>	
Dst MAC Type*	<input type="text" value="any"/>	
Dst MAC*	<input type="text"/>	
Dst MAC Mask*	<input type="text"/>	

Help
 #MAC: the valid mac address can be one of the following formats: XXXXXXXXXXXX, XXXX.XXXX.XXXX, XX:XX:XX:XX:XX:XX, and XX-XX-XX-XX-XX-XX, among which X is a Hex number

7.3.3 Applying the MAC Access Control List

If you click **Advanced Config -> MAC Access Control List -> Applying The MAC Access Control List**, the Applying the MAC access control list page appears.

Port	Egress ACL	Ingress ACL
G0/1	<input type="text"/>	<input type="text"/>
G0/2	<input type="text"/>	<input type="text"/>
G0/3	<input type="text"/>	<input type="text"/>
G0/4	<input type="text"/>	<input type="text"/>
G0/5	<input type="text"/>	<input type="text"/>
G0/6	<input type="text"/>	<input type="text"/>
G0/7	<input type="text"/>	<input type="text"/>

Chapter 8 Network Management Configuration

Device Status

Basic Config

Port Config

L2 Config

L3 Config

Advanced Config

Network Mgr.

SNMP Mgr.

RMON Config

Diagnostic Tool

System Mgr.

8.1 SNMP Configuration

If you click **Network Management Config -> SNMP Management** in the navigation bar, the SNMP management page appears, as shown in figure 2.

8.1.1 SNMP Community Management

The screenshot shows the 'SNMP Community Management' page. At the top, there is a 'New' button. Below it, a table lists the current configuration. The table has columns for 'SNMP Community Name', 'SNMP Community Encryption', 'SNMP Community Attribute', and 'Operate'. The first row shows 'nscrtvEponEocTree', 'False', 'RO', and an 'Edit' link. There are also 'First', 'Prev', 'Next', 'Last', 'Go', 'Page', and 'Search' controls, and a 'Delete' button at the bottom right.

SNMP Community Name	SNMP Community Encryption	SNMP Community Attribute	Operate
nscrtvEponEocTree	False	RO	Edit

On the SNMP community management page, you can know the related configuration information about SNMP community.

You can create, modify or cancel the SNMP community information, and if you click New or Edit, you can switch to the configuration page of SNMP community.

The screenshot shows the configuration form for an SNMP community. It includes fields for 'SNMP Community Name' (with a note 'Input less than 20 characters') and 'SNMP Community Attribute' (set to 'Read Only'). There are 'Apply' and 'Go Back' buttons at the bottom.

On the SNMP community management page you can enter the SNMP community name, select the attributes of SNMP community, which include Read only and Read-Write.

8.1.2 SNMP Host Management

The screenshot shows the 'SNMP Host Management' page. At the top, there is a 'New' button. Below it, a table lists the current configuration. The table has columns for 'SNMP Host IP', 'SNMP Community String', 'SNMP Message Type', 'SNMP Community Version', and 'Operate'. The first row shows '10.1.1.1', 'string', 'Traps', 'v1', and an 'Edit' link. There are also 'First', 'Prev', 'Next', 'Last', 'Go', 'Page', and 'Search' controls, and a 'Delete' button at the bottom right.

SNMP Host IP	SNMP Community String	SNMP Message Type	SNMP Community Version	Operate
10.1.1.1	string	Traps	v1	Edit

On the SNMP community host page, you can know the related configuration information about SNMP host.

You can create, modify or cancel the SNMP host information, and if you click New or Edit, you can switch to the configuration page of SNMP host.

The screenshot shows the configuration form for an SNMP host. It includes fields for 'SNMP Host IP', 'SNMP Community', 'SNMP Message Type' (set to 'Traps' with a note '* Informs is not supported in version v1'), and 'SNMP Community Version' (set to 'v1'). There are 'Apply' and 'Go Back' buttons at the bottom.

On the SNMP host configuration page, you can enter SNMP Host IP, SNMP Community, SNMP Message Type and SNMP Community Version. SNMP Message Type includes Traps and Informs, and as to version 1, SNMP Message Type does not support Informs.

8.2 RMON

8.2.1 RMON Statistic Information Configuration

If you click **Network Management Config -> Rmon -> Rmon Statistics -> New**, the RMON Statistics page appears.

Interface Statistics Config	
Interface	<input type="text" value="g0/1"/>
Index	<input type="text"/> (1-65535)
Owner	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Go Back"/>	

Help
 #It must be configured in interface mode, which is used to enable the interface statistics
 *#The string you totally entered is less than or equal to 255 characters

You need to set a physical port to be the reception terminal of the monitor data.

The index is used to identify a specific interface; if the index is same to that of the previous application interface, it will replace that of the previous application interface.

At present, the monitor statistic information can be obtained through the command line “show rmon statistics”, but the Web does not support this function.

8.2.2 RMON History Information Configuration

If you click **Network Management Config -> RMON -> RMON History -> New**, the RMON history page appears.

Interface History config	
Interface	<input type="text" value="g0/1"/>
Index	<input type="text"/> (1-65535)
Sampling Number	<input type="text" value="50"/> (1-65535)
Sampling Interval	<input type="text" value="1800"/> (1-3600)
Owner	<input type="text" value="config"/> Enter less than 31 characters*
<input type="button" value="Apply"/> <input type="button" value="Go Back"/>	

Help
 #Sampling Number means how many history items must be saved recently

You need to set a physical port to be the reception terminal of the monitor data.

The index is used to identify a specific interface; if the index is same to that of the previous application interface, it will replace that of the previous application interface.

The sampling number means the items that need be reserved, whose default value is 50.

The sampling interval means the time between two data collection, whose default value is 1800s.

At present, the monitor statistic information can be obtained through the command line “show rmon history”, but the Web does not support this function.

8.2.3 RMON Alarm Information Configuration

If you click **Network Management Config -> Rmon -> Rmon Alarm -> New**, the RMON Alarm page appears.

RMON Alarm config	
Index	<input type="text"/> (1-65535)
MIB Node	IfinOctets
OID	1.3.6.1.2.1.2.1.10
Interface	g0/1
Alarm type	absolute
Sampling Interval	<input type="text"/> (1-2147483647)
Rising Threshold	<input type="text"/> (-2147483648 - 2147483647)
Rising Event Index	<input type="text"/> (1-65535)
Falling Threshold	<input type="text"/> (-2147483648 - 2147483647)
Falling Event Index	<input type="text"/> (1-65535)
Owner	<input type="text"/> Enter less than 31 characters*

Help

#The owner can be empty

*#The string you totally entered is limited in 255 characters

The index is used to identify a specific alarm information; if the index is same to the previously applied index, it will replace the previous one.

The MIB node corresponds to OID.

If the alarm type is absolute, the value of the MIB object will be directly monitored; if the alarm type is delta, the change of the value of the MIB object in two sampling will be monitored.

When the monitored MIB object reaches or exceeds the rising threshold, the event corresponding to the index of the rising event will be triggered.

When the monitored MIB object reaches or exceeds the falling threshold, the event corresponding to the index of the falling event will be triggered.

8.2.4 RMON Event Configuration

If you click **Network Management Config -> RMON -> RMON Event -> New**, the RMON event page appears.

RMON Event Config	
Index	<input type="text"/> (1-65535)
Owner	<input type="text"/>
Description	<input type="text"/>
Enable log	<input type="checkbox"/>
Enable trap	<input type="checkbox"/>
Community	<input type="text"/>

Help

#If the log is enabled, the items will be added to the log table at the trigger of the event.

#If the trap is enabled, the trap will be generated with the event community name.

*#The string you totally entered is less than 255 characters

The index corresponds to the rising event index and the falling event index that have already been configured on the RMON alarm config page.

The owner is used to describe the descriptive information of an event.

"Enable log" means to add an item of information in the log table when the event is triggered.

"Enable trap" means a trap will be generated if the event is triggered.

Chapter 9 Diagnosis Tools

Device Status

Basic Config

Port Config

L2 Config

L3 Config

Advanced Config

Network Mgr.

Diagnostic Tool

Ping

System Mgr.

9.1 Ping

9.1.1 Ping

If you click **Diagnosis Tools -> Ping**, the Ping page appears.

RMON Event Config	
Index	<input type="text" value="(1-65535)"/>
Owner	<input type="text"/>
Description	<input type="text"/>
Enable log	<input type="checkbox"/>
Enable trap	<input type="checkbox"/>
Community	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Go Back"/>	
Help	
<p>#If the log is enabled the items will be added to the log table at the trigger of the event.</p> <p>#If the trap is enabled, the trap will be generated with the event community name.</p> <p>*#The string you totally entered is less than 255 characters</p>	

Ping is used to test whether the switch connects other devices.

If a Ping test need be conducted, please enter an IP address in the "Destination address" textbox, such as the IP address of your PC, and then click the "PING" button. If the switch connects your entered address, the device can promptly return a test result to you; if not, the device will take a little more time to return the test result.

"Source IP address" is used to set the source IP address which is carried in the Ping packet.

"Size of the PING packet" is used to set the length of the Ping packet which is transmitted by the device.

Chapter 10 System Management

Device Status

Basic Config

Port Config

L2 Config

L3 Config

Advanced Config

Network Mgr.

Diagnostic Tool

System Mgr.

User Mgr.

Log Mgr.

Startup-config

System Software

Reboot

10.1 User Management

10.1.1 User List

If you click System Mgr.-> User Mgr., the User Management page appears.

User Management

New

No.1 Page/Total 1 Page First Prev Next Last Go No. Page Search: Current 1 Item/Total 1 Item

No.	User name	User permission	Pass-Group	Authen-Group	Author-Group	User Status	Operate
<input type="checkbox"/>	admin	System administrator				Normal	Edit

Select All/Select None

Help

#Note: When only one Admin user exists, You cannot delete the current administrator user. Otherwise, you cannot log on to the switch and configure it.

#Users can be divided into the Admin user and the limited user according to the permission. The Admin user can use all functions of the switch, including browsing, configuring and remote login, while the limited user only has the permission to browse the switch's running state through the WEB page.

#Click the New button to create a new user.

You can click “New” to create a new user.

To modify the permission or the login password, click “Edit” on the right of the user list.

Note:

1. Please make sure that at least one system administrator exists in the system, so that you can manage the devices through Web.
2. The limited user can only browse the status of the device.

10.1.2 Establishing a New User

If you click “New” on the User Management page, the Creating User page appears.

User Management

User name	<input type="text"/>
Password	<input type="password"/>
Confirming password	<input type="password"/>
Pass-Group	<input type="text"/>
Authen-Group	<input type="text"/>
Author-Group	<input type="text"/>

Help

#Click the 'Apply' button to add a user or modify the password and the permission.

#Users can be divided into the Admin user and the limited user according to the permission. The Admin user can use all functions of the switch, including browsing, configuring and remote login, while the limited user only has the permission to browse the switch's running state through the WEB page.

In the “User name” text box, enter a name, which contains letters, numbers and symbols except “?”, “\”, “&”, “#” and the "Space" symbol.

In the “Password” textbox enter a login password, and in the “Confirming password” textbox enter this login password again.

10.1.3 User Group Management

Click the Tab page of user group management and enter user group management page.

User Group Mgr.

[New](#)

No.1 Page/Total 1 Page First Prev Next Last Go No. Page Search: Current 1 Item/Total 1 Item

Serial Number	Group Name	Pass-Group Rule	Authen-Group Rule	Author-Group Rule	Operate	Detail
1	g1			a	Edit	Detail

Select All/Select None [Delete](#)

Click “create new” to create a new user group.

Click “delete” to delete the user group.

User Group Config

User Group Name*

Pass-Group Name

Authen-Group Name

Author-Group Name

[Apply](#) [Reset](#) [Go Back](#)

Help

#The user group mustn't exist.

#Rule must exist.

The new user group name must be not used before. The password rule name, authentication rule name and authorization rule name must have been created, or you cannot create a new user group. Configure the password rule, authentication rule and authorization rule in other 3 tab pages.

10.1.4 Password Rule Management

Click password rule management Tab page to enter password rule management page.

Pass-Group Mgr.

[New](#)

No.1 Page/Total 1 Page First Prev Next Last Go No. Page Search: Current 1 Item/Total 1 Item

Serial Number	Pass-Group Name	Same as the username	Min Length	Validity	Number	Lower-letter	Upper-letter	Special-character	Operate
1	11111	Can be same			Must	Must	Must	Must	Edit

Select All/Select None [Delete](#)

Click “create new” to create new password rule.

Click “delete” to delete password rule.

Pass-Group Config

Pass-Group Name*

Same as Username

Contain Number

Contain Lower-letter

Contain Upper-letter

Contain Special-character

Min Length (1-127)

Validity d h m s

[Apply](#) [Reset](#) [Go Back](#)

Help

#Config Pass-Group

Set some password rules including whether the password can be the same with the user name, whether the password must contain numbers, lowercase, uppercase, special characters, the minimum length and the period of validity.

When the rule is created and applied to the user management, the user password will show invalid if the set password is not complied with the password rule, vice versa.

10.1.5 Authentication Rule Management

Click the Tab page of authentication rule management to enter authentication management page.

Author-Group Mgr.

New

No.1 Page/Total 1 Page First Prev Next Last Go No. Page Search: Current 3 Item/Total 3 Item

	Serial Number	Authen-Group Name	Max try times	Duration for all tries	Operate
<input type="checkbox"/>	1	a	5	3d	Edit
<input type="checkbox"/>	2	b			Edit
<input type="checkbox"/>	3	c			Edit

Select All/Select None **Delete**

Click “create new” to create the new authentication rule.

Click “delete” to delete the authentication rule.

Authen-Group Config

Authen-Group Name*

Max try times (1-9)

Duration for all tries d h m s

Apply **Reset** **Go Back**

Help

#Configure the Authen-Group

♦♦Max Try Times♦♦ and ♦♦Duration for all tries♦♦ must be entered at the same time

You can configure the maximum number of attempts and periods or you don't, but you must configure them simultaneously or neither.

10.1.6 Authorization Rule Management

Click the Tab page of authorization rule and enter the authorization rule management page.

Author-Group Mgr.

New

No.1 Page/Total 1 Page First Prev Next Last Go No. Page Search: Current 3 Item/Total 3 Item

	Serial Number	Author-Group Name	Precedence	Operate
<input type="checkbox"/>	1	a	System administrator	Edit
<input type="checkbox"/>	2	b	System administrator	Edit
<input type="checkbox"/>	3	c	System administrator	Edit

Select All/Select None **Delete**

Click “create new” to create new authorization rule.

Click “delete” to delete the authorization rule.

Author-Group Config

Author-Group Name*

Precedence

Apply **Reset** **Go Back**

Help

#Config Author-Group

The authorization rule determines your permission of the administrator or the limited user. If you are the administrator, you have the administrator right. If you are the limited user, you can only but check the web.

10.2 Log Management

If you click **System Mgr.-> Log Mgr.**, the Log Management page appears.

Enable the log server	<input type="checkbox"/>
Address of the log server	<input type="text"/>
Level of system logs	(6-informational) ▼
Enable the log buffer	<input type="checkbox"/>
Size of the log buffer	4096 (Bytes)
Level of cache logs	(7-debugging) ▼

[Apply](#)

If “Enabling the log server” is selected, the device will transmit the log information to the designated server. In this case, you need enter the address of the server in the “Address of the system log server” textbox and select the log’s grade in the “Grade of the system log information” dropdown box.

If “Enabling the log buffer” is selected, the device will record the log information to the memory. By logging on to the device through the Console port or Telnet, you can run the command “show log” to browse the logs which are saved on the device. The log information which is saved in the memory will be lost after rebooting. Please enter the size of the buffer area in the “Size of the system log buffer” textbox and select the grade of the cached log in the “Grade of the cache log information” dropdown box.

10.3 Managing the Configuration Files

If you click **System Mgr.-> Configuration file**, the Configuration file page appears.

10.3.1 Exporting the Configuration Information

Export the current startup-config

[Export](#)

The current configuration file can be exported, saved in the disk of PC or in the mobile storage device as the backup file.

To export the configuration file, please click the “Export” button and then select the “Save” option in the pop-up download dialog box.

The default name of the configuration file is “startup-config”, but you are suggested to set it to an easily memorable name.

10.3.2 Importing the Configuration Information



You can import the configuration files from PC to the device and replace the configuration file that is currently being used. For example, by importing the backup configuration files, you can resume the device to its configuration of a previous moment.

Note:

1. Please make sure that the imported configuration file has the legal format for the configuration file with illegal format cannot lead to the normal startup of the device.
2. If error occurs during the process of importation, please try it later again, or click the “Save All” button to make the device re-establish the configuration file with the current configuration, avoiding the incomplete file and the abnormality of the device.
3. After the configuration file is imported, if you want to use the imported configuration file immediately, **do not** click “Save All”, but reboot the device directly.

10.4 Software Management

Click **System Mgr. -> Software Update** in the navigation bar, and enter the device software management page.

10.4.1 Backup System Software



The current running software version is displayed in the page. If you need to backup the system, please click “backup system software”, then select “save” in the pop-up file download dialog box and save the system profile to your computer disk, transferable data device or other positions in the network.

Note:

Default name of the system profile is “Switch.bin”. You are suggested to change the default name to a name that easy to identify.

10.4.2 Update System Software

Note:

1. Please ensure your update system profile match with the device type. Otherwise, the system cannot operate normally.
2. The system profile update may need 1 to 2 minutes. After clicking and confirming the “update” button, the profile will be upload to the device. Please be patient.

3. Please do not restart or interrupt the device if errors occur in the update process, or the device cannot start up. Please try update again later.
4. Please save the configuration and restart the device after updating, so that the new system can operate.

The screenshot shows the 'Update System' page with a blue header. A red warning message reads: 'Reboot is required after the update of System software!'. Below this is a checkbox labeled 'Reboot the device automatically after update'. A text input field for 'File name on the server' contains 'switch.bin'. There is a '浏览...' (Browse) button next to the input field. At the bottom is a large 'Upgrade' button.

The update software is usually used for solving the existing problems or improving certain functions. You don't need to update the system software regularly, if your device operates normally.

If your system needs to be update, please enter the full path of the new system profile into the text box right of "update system software" or click "browse" button to select new system profiles and click "update".

10.5 Rebooting the Device

If you click **System Mgr.-> Reboot**, the Rebooting page appears.

The screenshot shows the 'Rebooting' page with a blue header. A large 'Reboot' button is centered on the page. Below the button is a 'Help' section with the text: '#Click the 'Reboot' button to restart the device.'

If the device need be rebooted, please first make sure that the modified configuration of the device has already been saved, and then click the "Reboot" button.

Interface Configuration

Table of Contents

Chapter 1 Overview.....	1
1.1 Supported Interface Types.....	1
1.2 Interface Configuration Introduction.....	1
Chapter 2 Interface Configuration.....	3
2.1 Configuring Interface Common Attribute.....	3
2.1.1 Adding Description.....	3
2.1.2 Configuring Bandwidth.....	3
2.1.3 Configuring Time Delay.....	3
2.2 Monitoring and Maintaining the Interface.....	3
2.2.1 Browsing the state of an interface.....	4
2.2.2 Initializing and deleting the port.....	4
2.2.3 Closing and Restarting the Port.....	4
2.3 Setting the Ethernet Interface.....	4
2.3.1 Choosing an Ethernet Interface.....	4
2.3.2 Setting the Rate.....	5
2.3.3 Setting the Duplex Mode of an Interface.....	5
2.3.4 Setting Flow Control on an Interface.....	5
2.4 Configuring Logical Interface.....	6
2.4.1 Configuring Aggregation Interface.....	6
2.4.2 Configuring VLAN Interface.....	6
Chapter 3 Interface Configuration Example.....	7
3.1 Configuring Public Attribute of Interface.....	7
3.1.1 Example for Interface Description.....	7
3.1.2 Example of Interface Shutdown.....	7

Chapter 1 Overview

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

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

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

1.1 Supported Interface Types

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

Interface type	Task	Reference
Ethernet interface	Configures fast Ethernet interface. Configures gigabit Ethernet interface.	Setting the Ethernet Interface
Logical interface	Aggregation interface VLAN interface	Configuring Logical 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
- Gigabit Ethernet interface

The supported logical interface of our switch include:

- Aggregation interface
- vlan interface

1.2 Interface Configuration Introduction

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

- 1) 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
```

Interface Configuration

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

Transmitted 0 packets, 0 bytes

0 broadcasts, 0 multicasts

0 discard, 0 error, 0 PAUSE

0 sqetest, 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, g 0/2 or g 0/2 is both available.

- (1) You can configure the interface configuration commands in interface configuration mode. Various commands define protocols and application programs to be executed on the interface. These commands will stay until user exits the interface configuration mode or switches to another interface.
- (2) Once the interface configuration has been completed, use the show command in the following chapter 'Monitoring and Maintaining Interface' to test the interface state.

Chapter 2 Interface Configuration

2.1 Configuring Interface Common Attribute

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

2.1.1 Adding Description

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

Command	Purpose
description <i>string</i>	Adds description to the currently-configured interface.

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

2.1.2 Configuring Bandwidth

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

Command	Purpose
bandwidth <i>kilobps</i>	Configures bandwidth for the currently configured interface.

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

2.1.3 Configuring Time Delay

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

Command	Purpose
delay <i>tensofmicroseconds</i>	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.

2.2 Monitoring and Maintaining the Interface

To maintain and monitor the interface, perform the following tasks:

- Browsing the state of an interface
- Initializing and deleting the port

- Closing and restarting the port

2.2.1 Browsing the state of an interface

Our switches support those commands to display interface information, including the version ID of hardware and software, and the interface state. The following table presents you some port monitor commands: For more details, please refer to the "Interface Configuration Command".

Run the following commands:

Command	Purpose
show interface [type [slot port]]	Displays the state of a port.
show running-config	Displays the current settings.
show version	Displays the memory configuration, the software version and the startup mirror.

2.2.2 Initializing and deleting the port

The logic interface can be dynamically created and deleted. So it is with the sub-interface and the channelized interface. The physical interface which cannot be deleted dynamically can return to the default setting of the interface. In global configuration mode, run the following command to initialize and delete an interface:

Command	Purpose
no interface [type [slot port]]	Initializes a physical interface or deletes a virtual interface.

2.2.3 Closing and Restarting the Port

You can disable the interface, so that all functions on this interface can be disabled, and then all monitor commands will label this interface as unavailable. This information can be transmitted to other devices through the dynamic routing protocol. The modification on any route will not affect this port.

Run the following commands in interface configuration mode to shut down an interface and then restart it.

Command	Purpose
shutdown	Disable the interface.
no shutdown	Restarting the interface

To check whether an interface is shut down, you can run show interface and show running-config. After the show interface command is run, a disabled interface will be presented as "administratively down". For more examples, please refer to "Interface Shutdown Example".

2.3 Setting the Ethernet Interface

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

2.3.1 Choosing an Ethernet Interface

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

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

The show interface fastethernet command can be used to show the state of the Ethernet interface, while the show interface gigaethernet command can be used to show the state of the gigabit-Ethernet interface.

2.3.2 Setting the Rate

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

Command	Purpose
Speed {10 100 1000 auto}	Sets the rate of fast Ethernet to 10M, 100M, 1000M or auto-negotiation.
No speed	Resumes the default settings. The rate is auto-negotiation.

Note:

The speed of the optical interface varies with the device. For example, the speed of GE-FX is 1000M, while the speed of FE-FX is 100M. If the speed command for an optical interface has the auto parameter, the optical interface has the automatic negotiation function, or the optical interface is mandatory and cannot be negotiated. The gigabit TX port supports the working mode of 10M, 100M, 1000M. The gigabit TX port must work in auto mode. Do the configuration as the prompt of each port.

2.3.3 Setting the Duplex Mode of an Interface

By default, the Ethernet interface can be auto, half duplex or full duplex. The duplex mode for the gigabit 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.

2.3.4 Setting Flow Control on an Interface

When an interface is in full duplex mode, flow control is realized through the 802.3X-defined PAUSE frame; when an interface is in half duplex mode, flow control is realized through backpressure.

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.

2.4 Configuring Logical Interface

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

Configuring aggregation interface

Configuring VLAN interface

2.4.1 Configuring Aggregation Interface

The aggregator interface is introduced in the background that the bandwidth of a single Ethernet interface is insufficient. It can bind together multiple full-duplex interfaces of the same rate to multiply the bandwidth.

Run the following command to define the aggregation interface:

Command	Function
Interface port-aggregator <i>number</i>	Configuring aggregation interface

2.4.2 Configuring VLAN Interface

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	Purpose
Interface vlan <i>number</i>	Configuring VLAN interface

Chapter 3 Interface Configuration Example

3.1 Configuring Public Attribute of Interface

3.1.1 Example for Interface Description

The following example shows how to add a description for an interface.

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

3.1.2 Example of Interface Shutdown

The following example shows how to disable GigaEthernet interface 0/1.

```
interface GigaEthernet0/1
shutdown
```

The following example shows how to restart the interface.

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

Interface Range Configuration

Table of Contents

Chapter 1 Interface Range Configuration.....	1
1.1 Interface Range Configuration Task.....	1
1.1.1 Understanding Interface Range.....	1
1.1.2 Entering Interface Range Mode.....	1
1.1.3 Configuration Example.....	1

Chapter 1 Interface Range Configuration

1.1 Interface Range Configuration Task

1.1.1 Understanding Interface Range

In the process of configuring interface tasks, there are cases when you have to configure the same attribute on ports of the same type. In order to avoid repeated configuration on each port, we provide the interface range configuration mode. You can configure ports of the same type and slot number with the same configuration parameters. This reduces the workload. Note: when entering the interface range mode, all interfaces included in this mode must have been established.

1.1.2 Entering Interface Range Mode

Run the following command to enter the interface range mode.

Procedure	Command	Purpose
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: <ul style="list-style-type: none"> (1) The slot number is set to slot. (2) The port numbers before/after the hyphen must range between port1 and port2, or equal to port3. (3) Port 2 must be less than port 1 (4) There must be space before/after the hyphen (-) or the comma (,).

1.1.3 Configuration Example

The following example shows how to enter the interface configuration mode of gigabit Ethernet interface 1, 2, 3 or 4 on slot 0.

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

Port Physical Characteristics Configuration

Table of Contents

Chapter 1 Port Physical Characteristics Configuration.....	1
1.1 Setting the Ethernet Interface.....	1
1.1.1 Setting the Rate.....	1
1.1.2 Setting the Duplex Mode of an Interface.....	1
1.1.3 Setting Flow Control on an Interface.....	1

Chapter 1 Port Physical Characteristics Configuration

1.1 Setting the Ethernet Interface

1.1.1 Setting the Rate

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

Command	Function
Speed {10 100 auto} (TX port) speed {100 1000 auto } (Optical port)	Sets the rate of fast Ethernet to 10M, 100M, 1000M or auto-negotiation.
No speed	Resumes the default settings. The rate is auto-negotiation.

Note:

The speed of the optical interface is fixed. 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. The gigabit optical interface enables auto-negotiation function by default. The gigabit combo port does not support configuration of speed 1000 and force full duplex mode simultaneously.

1.1.2 Setting the Duplex Mode of an Interface

By default, the Ethernet interface can be auto, half duplex or full duplex. The gigabit combo port does not support configuration of speed 1000 and force full duplex mode simultaneously.

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

1.1.3 Setting Flow Control on an Interface

When an interface is in full duplex mode, flow control is realized through the 802.3X-defined PAUSE frame; when an interface is in half duplex mode, flow control is realized through backpressure.

Command	Usage Guidelines
flow-control {on off auto}	Configuring Flow Control on the Interface
no flow-control	Resumes the default settings, that is, there is no flow control on an interface.

Note:

The difference between “flow-control auto” and “flow-control on” is in the “auto” mode the device sends flow control frame only when it negotiates successfully with the opposite end as the system is compelled to receive flow control frame in both modes.

Port Additional Characteristics Configuration

Table of Contents

- Chapter 1 Port Additional Characteristics Configuration..... 1
 - 1.1 Port Isolation..... 1
 - 1.2 Storm Control..... 1
 - 1.3 Rate Control..... 2
 - 1.4 Loopback Detection..... 3
 - 1.5 MAC Address Learning.....3
 - 1.6 Port Security..... 3
 - 1.7 Port Binding..... 4
 - 1.8 SVL/IVL..... 5
 - 1.9 Configuring Link scan..... 5
 - 1.9.1 Overview..... 5
 - 1.9.2 Link Scan Configuration Task..... 6
 - 1.9.3 Configuration Example..... 6
 - 1.10 Configuring the Enhanced Link State Detection Command..... 6
 - 1.10.1 Overview..... 6
 - 1.10.2 Configuration Tasks..... 6
 - 1.10.3 Configuration Example..... 6
 - 1.11 Configuring System MTU..... 7
 - 1.11.1 Overview..... 7
 - 1.11.2 Configuration Tasks..... 7
 - 1.11.3 Configuration Example..... 7

Chapter 1 Port Additional Characteristics Configuration

1.1 Port Isolation

Generally, the packets between different ports of a switch can be freely forwarded. In some cases, the data flows between ports need be forbidden and port isolation is then required. Data communication cannot go on between isolated ports, but can do between normal ports or between normal port and isolated port. Data communication cannot go on between the isolated ports within one group, but can do between the isolated port and any arbitrary port outside the group. It is noted that port isolation plays a role in the layer-2 packets. This switch series does not support group-based isolation.

Isolation not based on the group:

Command	Purpose
config	Enters the global configuration mode.
interface g0/1	Enters the to-be-configured port.
[no] switchport protected	Enable or disable Port Isolation
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.

Isolation based on the group:

Command	Purpose
config	Enters the global configuration mode.
[no] port-protected <i>group-id</i>	Creates and enters the isolation group mode, run this command. Sets ID of the isolation group
[no] description <i>word</i>	Describes the group. Word Describes the character string of the group.
exit	Goes back to the global configuration mode.
interface g0/1	Enters the to-be-configured port.
[no] switchport protected <i>group-id</i>	Add/remove the isolation group <i>group-id</i> The isolation group ID
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.

1.2 Storm Control

The port of a switch may bear continuous and abnormal impact from unicast (MAC address fails to be found), multicast or broadcast packets, and therefore gets paralyzed even to the extent that the whole switch breaks down. That's why a mechanism must be provided to limit this phenomena. The storm control enables the OLT to set on the ingress the rates of different kinds of packets.

Port Additional Characteristics Configuration

Command	Purpose
config	Enters the global configuration mode.
interface g0/1	Enters the to-be-configured port.
[no] storm-control { broadcast multicast unicast } threshold <i>count</i>	<p>Sets flow control for a port.</p> <p>unicast means that storm control is conducted to the unicast packets.</p> <p>multicast means that storm control is conducted to the multicast packets.</p> <p>broadcast means that storm control is conducted to the broadcast packets.</p> <p>Count means the threshold of the being configuration</p>
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.

1.3 Rate Control

Rate limit is used to limit the rate of a flow that runs through a port. Enter the privileged mode and run the following commands to limit the rate of a port.

Command	Purpose
config	Enters the global configuration mode.
interface g0/1	Enters the to-be-configured port.
[no] switchport rate-limit { <i>band</i> <i>bandwidth percent</i> } { ingress egress }	<p>Configures the rate limit for a port.</p> <p>Band means to limit the flow rate.</p> <p><i>percent</i> means to limit the flow percentage.</p> <p>ingress means to exert an influence on the ingress.</p> <p>egress means to exert an influence on the egress.</p>
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.

1.4 Loopback Detection

Loopback detection is used to check whether loopback exists on an interface. You can configure the interval for a port to transmit the loop check packets. Enter the privileged mode to run the following commands to set the interval for the port to transmit loopback detection packets.

Command	Purpose
config	Enters the global configuration mode.
Interface g0/1	Enters the to-be-configured port.
[no] keepalive [second]	To configure the interval for a interface to transmit the loop check packets, run keepalive second. To return to the default setting, use the no form of this command. second means the interval of transmitting the packets.
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.

1.5 MAC Address Learning

MAC address learning is used to enable or disable MAC addresss learning on the interface. The configuration method is shown as follows:

Command	Purpose
config	Enters the global configuration mode.
interface g0/1	Enters the to-be-configured port.
[no] switchport disable-learning	Sets MAC address learning on a port. Enables/disables interface MAC address learning.
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.

1.6 Port Security

Port security supports security control on an interface. Port security has four modes: dynamic security mode, static reception mode, static rejection mode and sticky security mode. In dynamic security mode, you can set the threshold of MAC addresses that can be learned by a port. If the learned MAC addresses on a port have reached the threshold in number, the switch will not learn the MAC addresses any more and at the same time drop all DLF packets. In static security mode, you can set the static security MAC address on a port and then you should consider three cases: if it is in static reception mode, only the packets whose destination MACs are security MACs can be allowed to enter this port and other packets will be dropped; if it is in static rejection mode, the packets whose destination MACs are security MACs will be all dropped and other packets will be allowed to pass through this port; if it is in sticky security mode, the mac address of the unknown source unicast packet will be learned to

Port Additional Characteristics Configuration

the sticky mac address. The sticky mac address can be configured manually or dynamically generated. The command "show running-config" can be used to check the sticky mac address. There are two aging modes for the sticky mac address: absolute aging mode and inactivity aging mode. Inactivity, similar to the dynamic aging, is an aging after there is no data traffic. The sticky security mode can set the port allowable learned maximum sticky MAC address number. If the learned MAC addresses on a port have reached the threshold in number, the switch will not learn the MAC addresses any more and at the same time drop all DLF packets.

Command	Purpose
config	Enters the global configuration mode.
interface g0/1	Enters the to-be-configured port.
[no] switchport port-security mode { dynamic static accept { reject sticky }	Setting the Interface Security Mode Dynamic means the dynamic security mode. Static accept means the static reception mode. Static reject means the static rejection mode. Sticky means the sticky security mode.
[no] switchport port-security dynamic maximum num	Sets the maximum number of MAC learning addresses
[no] switchport port-security static mac-address H.H.H	Configures a static security MAC address.
[no] switchport port-security sticky { maximum sticky_number mac-address H.H.H aging-time aging_time absolute-aging inactivity-aging }	Configures the sticky characteristic of MAC address, run this command. maximum sticky_number means the maximum number of sticky mac address mac-address H.H.H means configure the sticky mac address manually aging-time aging_time means configuring the aging time of the sticky mac address absolute-aging means configuring the absolute aging mode(default) inactivity-aging means configuring the aging mode of inactivity
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.

1.7 Port Binding

This type of switches can bind the IP address and the MAC address to a port at the same time, and of course you can bind either one to the port. Port binding is effective to the IP or ARP packets.

Use the following command in interface configuration mode:

Command	Purpose
---------	---------

Port Additional Characteristics Configuration

config	Enters the global configuration mode.
interface g0/1	Enters the to-be-configured port.
[no] switchport port-security bind block {ip arp both-arp-ip A.B.C.D mac H.H.H ipv6 ipv6_addr}	<p>Configures Port Binding</p> <p>bind means that only the packets that comply with the binding requirements can pass while other packets will be dropped; block means that only the packets that comply with the binding requirements will be rejected and other packets will pass.</p> <p>Ip means the relative action, rejection or reception, is effective to the Ip packets that comply with the binding requirements.</p> <p>Arp means the relative action, rejection or reception, is effective to the ARP packets that comply with the binding requirements.</p> <p>both-arp-ip means effective to the IP and ARP packets that comply with the binding requirements.</p>
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.

1.8 SVL/IVL

The switch can configure SVL or IVL mode. It is IVL mode by default. The settings is shown as follows:

Command	Purpose
config	Enters the global configuration mode.
[no]vlan shared-learning	Sets SVL/IVL
exit	Goes back to the EXEC mode.

1.9 Configuring Link scan

1.9.1 Overview

The command is used to scan the time interval on the port. You can fast scan the up/down state on the port.

1.9.2 Link Scan Configuration Task

- Configure the time interval on the port.

1. Set the time interval of port scan

To set the scan interval of an interface, run the following command in the global configuration mode:

Command	Purpose
[no] Link scan [normal fast] interval	Normal means standard link scan mode. Fast means fast link scan mode. Fast mode is mainly used for service protocol requirement, such as rstp. Configure the time interval on the port.

1.9.3 Configuration Example

The following example shows how to set the scan interval to 20ms.

```
link scan normal 20
```

1.10 Configuring the Enhanced Link State Detection Command

1.10.1 Overview

Configuring the enhanced link state detection of the port and fastly checking the link state of the port.

1.10.2 Configuration Tasks

- To enable/disable the enhanced link state detection command, run the following command.

1. To enable/disable the enhanced link state detection command, run the following command.

In port configuration mode, run the following commands respectively to enable or disable the enhanced link state detection:

Command	Purpose
[no] switchport enhanced-link	To enable/disable the enhanced link state detection command, run the following command.

1.10.3 Configuration Example

The following example shows how to enable the enhanced link state detection on interface g0/1:

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

1.11 Configuring System MTU

1.11.1 Overview

Configuring system mtu

1.11.2 Configuration Tasks

- Configuring system mtu

1. Set system mtu.

Run the following command in the global configuration mode:

Command	Purpose
[no] system mtu <i>mtu</i>	To set the value of system mtu, run this command.

1.11.3 Configuration Example

The following example shows how to set system mtu to 2000 bytes.

```
Switch_config#system mtu 2000
```

Port Mirroring Configuration

Table of Contents

Chapter 1 Port Mirroring Configuration.....	1
1.1 Configuring Port Mirroring Task List.....	1
1.2 Configuring Port Mirroring Task.....	1
1.2.1 Configuring port mirroring.....	1
1.2.2 Displaying port mirroring information.....	2
1.3 Remote Mirroring Configuration Example.....	2

Chapter 1 Port Mirroring Configuration

1.1 Configuring Port Mirroring Task List

- Configuring port mirroring
- Displays port mirroring information

1.2 Configuring Port Mirroring Task

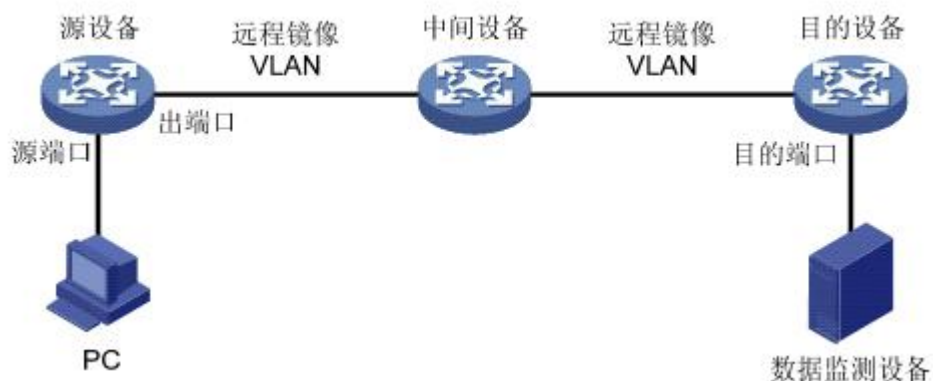
1.2.1 Configuring port mirroring

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

Port Mirroring Configuration

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	Purpose
config	Enters the global configuration mode.
mirror session <i>session_number</i> { destination { interface <i>interface-id</i> } { rspan <i>vid</i> <i>tpid</i> } source { interface <i>interface-id</i> [, -] <i>rx</i> <i>tx</i> <i>both</i> } }	To set port mirror, run this command. session-number is the number of the port mirroring. destination is the destination port of the mirroring. VID is the tag of remote mirroring TPID is the tag of remote mirroring source is the source port of mirroring. rx means the data flow of mirroring. rx means the input data of mirroring. tx means the output data of mirroring, both means both mirroring
exit	Goes back to the EXEC mode.
write	Saves the settings.

1.2.2 Displaying port mirroring information

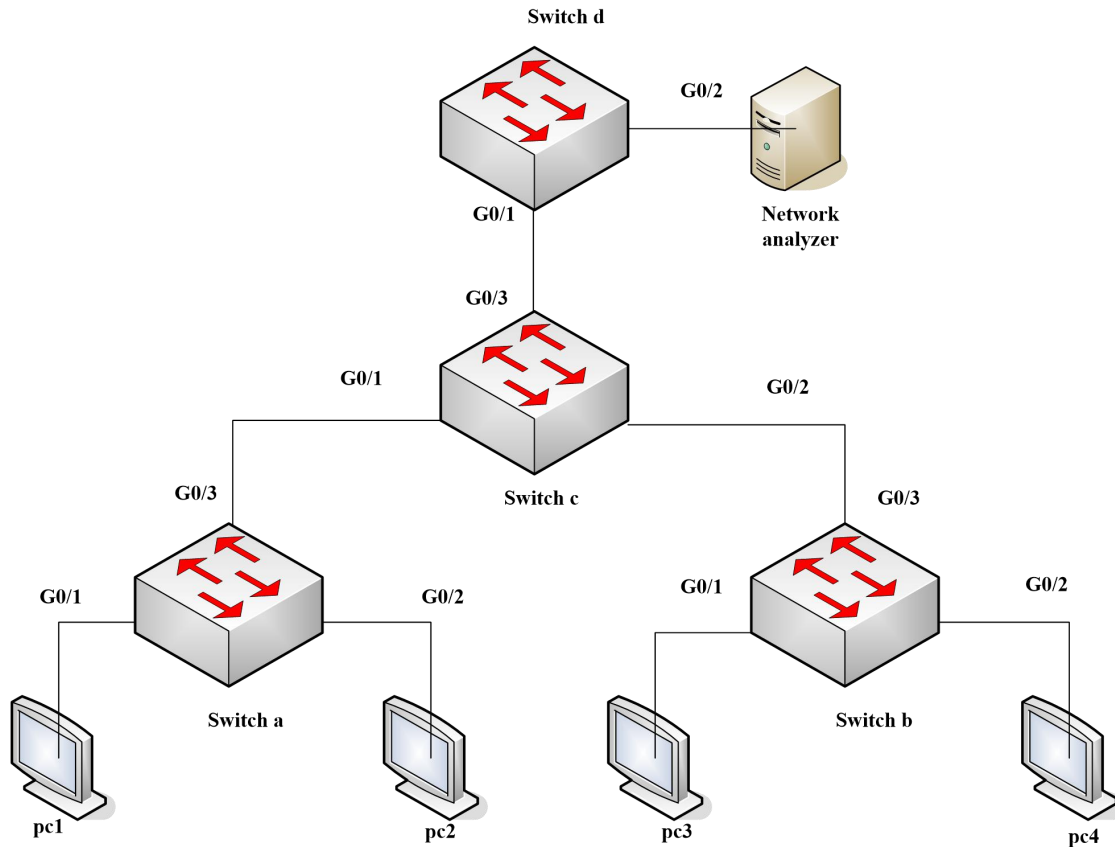
To display the configuration information about port mirroring, run the following command:

Command	Purpose
show mirror [session <i>session_number</i>]	Displays the configuration information about port mirroring session-number means the number of the port mirroring.

1.3 Remote Mirroring Configuration Example

The network topology is shown in the following figure:

Port Mirroring Configuration



You need to monitor the traffic of interface g0/1 on switch a and interface g0/1 on switch b by the network analysis meter.

Configure as follows by the remote mirroring:

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
```

Port Mirroring Configuration

```
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
```

MAC Address Table Configuration

Table of Contents

- Chapter 1 MAC Address Table Configuration..... 1
 - 1.1 MAC Address Configuration Task List..... 1
 - 1.2 MAC Address Configuration Tasks..... 1
 - 1.2.1 Configuring static MAC address..... 1
 - 1.2.2 Configuring MAC address aging time..... 1
 - 1.2.3 Configuring black hole MAC..... 2
 - 1.2.4 Displaying MAC address table..... 2
 - 1.2.5 Removing dynamic MAC address..... 3

Chapter 1 MAC Address Table Configuration

1.1 MAC Address Configuration Task List

This chapter is to describe the functions of configuring MAC address table on the switch as follow:

- Configuring static MAC address
- Configuring MAC address aging time
- Configuring black hole MAC address
- Displaying MAC address table
- Removing dynamic MAC address

1.2 MAC Address Configuration Tasks

1.2.1 Configuring static MAC address

A static MAC address table entry refers to the one that can not be aged by the switch. It only can be deleted manually. Static MAC address can be added or deleted according to the requirements when switches are in use. Enter privilege mode and use the following steps to add or delete a static MAC address.

Command	Purpose
config	Enters the global configuration mode.
[no] mac address-table static mac-addr vlan vlan-id interface interface-id	Add/delete a static MAC address entry. The mac-addr specifies MAC address; vlan-id means VLAN number, the effective range is 1~4094; The interface-id is a port name.
exit	Goes back to the EXEC mode.
write	Saves the settings .

1.2.2 Configuring MAC address aging time

When a dynamic MAC address is not used within a specified aging time, the switch will delete it from MAC address table. The MAC aging time of a switch can be set according to actual needs and the default aging time is 300 seconds.

Enter EXEC mode, use steps as follow to configure the aging time of MAC address.

Command	Purpose
---------	---------

MAC Address Table Configuration

config	Enters the global configuration mode.
mac address-table aging-time [0 10-1000000]	Sets the aging time of the MAC address table. 0 means the address does not age; The range of MAC address aging time is 10 to 1,000,000 seconds.
exit	Goes back to the EXEC mode.
write	Saves the settings .

1.2.3 Configuring black hole MAC

The black hole MAC address entries mean those MAC address entries that cannot communicate but only be removed manually. Black hole MAC address can be added or deleted according to the requirements when switches are in use. Enter EXEC mode and use the following steps to add or delete a static MAC address.

Command	Purpose
config	Enters the global configuration mode.
[no] mac address-table blackhole mac-addr vlan vlan-id	Add/delete a black hole MAC address entry. The mac-addr specifies MAC address; vlan-id means VLAN number, the effective range is 1~4094;
exit	Goes back to the EXEC mode.
write	Saves the settings .

1.2.4 Displaying MAC address table

When using switches, we expect to know the information about MAC address table in need of debugging or management. Use show to display 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, specify the MAC address dynamically learned. The interface-id is the interface name. vlan-id VLAN ID. Value range: 1-4094 Static Static MAC address table Brief Brief information about the MAC address Multicast Multicast MAC address table Interface Interface's MAC address table Vlan Vlan mac address table H.H.H Specific address Blackhole MAC address;

1.2.5 Removing dynamic MAC address

In some cases, it is necessary to clear up the MAC address which switch has learned.

Enter the privileged mode and use the following commands to delete a dynamic MAC address.

Command	Purpose
clear mac address-table dynamic [address <i>mac-addr</i> interface <i>interface-id</i> vlan <i>vlan-id</i>]	<p>Delete a dynamic MAC address entry.</p> <p>dynamic means the MAC address which is learned dynamically.</p> <p>mac-addr means a MAC address.</p> <p>The interface-id is the interface name.</p> <p>The vlan-id is VLANnumber, The value range is 1 to 4094;</p>

MAC Access-List Configuration

Table of Contents

Chapter 1 MAC Access-List Configuration.....	1
1.1 Create MAC access-list.....	1
1.2 Configuring items of MAC access-list.....	1
1.3 Applying MAC access-list.....	2

Chapter 1 MAC Access-List Configuration

Access-list configuration includes:

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

1.1 Create 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 following command. name stands for the name of theMACaccess list.

1.2 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]	To add/delete aMAC 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 destination MAC address; dst-mac-mask stands for destination mac mask;

	<p>arp stands for matched arp packet;</p> <p>src-ip-addr stands for source ip address stands for source ip address</p> <p>dst-ip-addr stands for the destination ip address</p> <p>ethertype stands for type of the matched Ethernet packet</p>
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.

1.3 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	<p>Apply the created MAC list to the port or delete the applied MAC list from the port.name means the name of the MAC list.</p> <p>Name MAC: Name of the MAC access list</p>
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.
write	Saves the settings.

802.1x Configuration

Table of Contents

Chapter 1 802.1x Configuration.....	1
1.1 802.1x Configuration Task List.....	1
1.2 802.1x Configuration Tasks.....	1
1.2.1 Configuring 802.1x Authentication on the Port.....	1
1.2.2 Configuring 802.1x on Multiple Ports Authentication.....	2
1.2.3 Configuring 802.1x Re-Authentication.....	3
1.2.4 Configuring 802.1x Authentication Retry Times.....	3
1.2.5 Configuring 802.1x Transmission Frequency.....	3
1.2.6 Configuring 802.1x User Binding.....	3
1.2.7 Configuring the Authentication Method on the 802.1x Port.....	4
1.2.8 Selecting the Authentication type for the 802.1x Port.....	4
1.2.9 Configuring MAB Authentication on the Port.....	4
1.2.10 Configuring 802.1x Accounting.....	5
1.2.11 Configuring 802.1x guest-vlan.....	5
1.2.12 Forbidding the Multi-NIC Supplicant.....	6
1.2.13 Resuming the Default Settings of 802.1x.....	6
1.2.14 Monitoring the 802.1x Authentication Configuration and State.....	6
1.3 802.1x Configuration Example.....	6

Chapter 1 802.1x Configuration

1.1 802.1x Configuration Task List

- Configuring 802.1x Authentication on the Port
- Configuring 802.1x on Multiple Ports of the Host
- Configuring 802.1x Re-Authentication
- Configuring 802.1x Authentication Retry Times
- Configuring 802.1x transmission frequency
- Configuring 802.1x User Binding
- Configuring the Authentication Method on the 802.1x Port
- Selecting the Authentication Mode for the 802.1x Port
- Configuring MAB Authentication on the Port
- Configuring 802.1x Accounting
- Configuring 802.1x guest-vlan
- Forbidding the Multi-NIC Supplicant
- Resuming the Default Settings of 802.1x
- Monitoring the 802.1x Authentication Configuration and State

1.2 802.1x Configuration Tasks

1.2.1 Configuring 802.1x Authentication on the Port

802.1x has three modes to control the port: force-authorized, force-unauthorized and enable.

Force-authorized means that the port has been authenticated and thus no authentication process is needed. In this mode, all users can conduct the data access control through the port. This mode is the default mode of the port. Force-unauthorized means that port authentication is not passed no matter what kind of authentication method you apply. In this mode, all users cannot conduct the data access control through the port.

Enable means that the 802.1x authentication protocol will be run on the port and the users who access the port will be authenticated by 802.1x. The successfully-authenticated users can conduct the data access control through the port. After enabling 802.1x authentication, you have to configure AAA authentication method.

Before the 802.1x is configured, you have to enable the 802.1x function by running the following commands:

Command	Purpose
dot1x enable	Enables the 802.1x function.

Run the following commands to enable the 802.1x authentication:

Command	Purpose
dot1x port-control auto	Sets the port to the 802.1x control mode.
aaa authentication dot1x {default list name} method	Configures 802.1x AAA authentication.

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

Command	Purpose
dot1x port-control auto	Sets the port to the 802.1x control mode.
dot1x port-control force-authorized	The port authentication is authorized mandatorily.
dot1x port-control force-unauthorized	The port authentication is unauthorized mandatorily.
dot1x port-control misc-mab	The hybrid mode of multi-user and mab authentication

1.2.2 Configuring 802.1x on Multiple Ports Authentication

The 802.1x authentication is mainly for the single host user. At this time, the switch allows only one user to conduct the authentication and the access control. However, sometimes the port may connect multiple hosts through 802.1x-unsupported switching device, such as switch 1108. In order to make these hosts' users access successfully, you can enable the multi-host port access function. Actually, the authentication port may connect with multiple users. To ensure all users can be authenticated and visited, enable multiuser authentication function.

There are two kinds of multi-host authentication: one is the multiple-hosts mode and the other is multiple-auth mode. The multiple-hosts mode is that when one of the hosts passes through the authentication the port will be up and the other hosts (including the previous ones and the following ones) will not need authentication; the multiple-auth mode is that the switch authenticates each host respectively and these authentications do not interfere with each other. When only one user passes its authentication, the interface will be up; only when all users fail in their authentication, in another word, only when no successfully authenticated user exist on the interface, the interface will be down. This mechanism gives guarantee to respective authentication for each user and if a user fails in its authentication, other users still have the normal access rights.

Note: The multi-auth mode cannot coexist with guest vlan or mab. 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 the 802.1x multi-host port authentication:

Command	Purpose
dot1x authentication multiple-hosts	Sets 802.1x multiple-hosts interface access mode. As long as one user passes the

	authentication, the interface is up.
dot1x authentication multiple-auth	Sets 802.1x multiple-hosts interface authentication mode. The authentication for each user is in parallel.

1.2.3 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	Purpose
dot1x re-authentication	Enables the re-authentication function.
dot1x timeout re-authperiod <i>time</i>	Configures the period of the re-authentication function.

1.2.4 Configuring 802.1x Authentication Retry Times

After the authentication is failed, the switch will continue forward request/ID packet to resume the authentication. If the device has no response when the authentication exceeds the max retry times, the authentication will be suspended.

Run the following commands to configure the max re-authentication times:

Command	Purpose
dot1x reauth-max <i>time</i>	Configures the retry times after the re-authentication function fails.

1.2.5 Configuring 802.1x Transmission Frequency

During 802.1x authentication, the packets will be transmitted to the client's host. You can adjust the data transmission to ensure the response of the client's host by controlling the 802.1x transmission frequency.

Run the following command to configure the transmission frequency.

Command	Purpose
dot1x timeout tx-period <i>time</i>	Sets the transmission frequency of the 802.1x packet.

1.2.6 Configuring 802.1x User Binding

You can bind the user to a certain port during 802.1x authentication to ensure the security of the interface access. To enable the 802.1x user binding, run the following command in interface configuration mode:

Command	Purpose
---------	---------

dot1x user-permit xxxz	Configures the user which is bound to the interface.
-------------------------------	------------------------------------------------------

1.2.7 Configuring the Authentication Method on the 802.1x Port

Different ports will be applied with different authentication methods during 802.1x authentication. By default, the 802.1x authentication adopts the default method.

To configure the 802.1x authentication method, run the following command in interface configuration mode:

Command	Purpose
dot1x authentication method yyy	Configures the 802.1x authentication method.

1.2.8 Selecting the Authentication type for the 802.1x Port

The authentication mode can be selected during the 802.1x authentication. The authentication class decides whether AAA uses the CHAP authentication or the EAP authentication. If the CHAP authentication is used, the challenge required by MD5 is locally generated; if the EAP authentication is used, the challenge is generated on the authentication server. Only one authentication mode can be applied to one interface. By default, the authentication mode is applied in global mode. When an authentication mode is configured for an interface, the authentication mode will be always used on the interface unless the negative form of the command is run to resume the default settings.

EAP-TLS adopts the electronic certificate as the evidence of authentication and follows the handshake regulations in TLS so that it is more secure.

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

Command	Purpose
dot1x authen-type {chap eap}	Selects CHAP or EAP.

To configure the authentication mode, you also can run the following command in interface configuration mode:

Command	Purpose
dot1x authentication type {chap eap}	Selects CHAP or EAP, or just uses the configuration class in global mode.

1.2.9 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 the MAB authentication 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 this case as the evidence of not support the 802.1x authentication client on the peer device and then turns to the MAB authentication. When the switch sends the gained MAC address as the username and password to the Radius server for authentication, the authentication will still not succeed until the Radius server has authorized this MAC address.

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

To enable the MAB authentication, you also can run the following command in interface configuration mode:

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 format 1 to format 6. The default format is 1.

1.2.10 Configuring 802.1x Accounting

The time the dot1x authentication is adopted you can conduct accounting. The actual accounting mechanism is that after dot1x authentication a judgment will be made as of whether the accounting is enabled on an authentication interface; if it is yes, the AAA interface will send the accounting request, and after receiving the request response information from the AAA module the authentication interface can allow the packets to pass through.

For the detailed accounting methods, refer to the relevant contents in the document AAA Settings.

For the correctness of the accounting data, the dot1x, after the accounting starts, will periodically use the AAA interface to send the update data to the server, while the AAA module, according to different AAA settings, decides whether to really send the accounting data.

Meanwhile, the dot1x re-authentication shall be enabled so that the switch will know a trouble as soon as it occurs on the supplicant.

To enable dot1x accounting and then set the accounting method, run the following commands in interface configuration mode:

Command	Purpose
dot1x accounting enable	Opens 802.1x accounting.
dot1x accounting method {method name}	Sets the accounting method.

1.2.11 Configuring 802.1x guest-vlan

Guest-vlan is to attribute the corresponding port with a limited access permission when the client does not respond. Guest-VLAN can be any configured VLAN in a system; when the configured guest -VLAN cannot reach the requirements, the port cannot enter the guest VLAN.

Note: If the authentication fails, the port will obtain no access permission.

To enable the guest vlan in global mode, run the following command:

Command	Purpose
dot1x guest-vlan	Opens the guest-VLAN on all ports.

At the initial time when the guest-vlan ID of each port is 0, the guest-vlan takes no effect even if it is enabled in global mode; only when the guest vlan ID is set in port configuration mode can the guest VLAN work.

Run the following command to set guest-vlan ID in port configuration mode:

Command	Purpose
dot1x guest-vlan {id(1-4094)}	Sets the VLAN ID of the guest VLAN on a port.

1.2.12 Forbidding the Multi-NIC Supplicant

This command can be used to forbid the supplicant terminal with multiple network adapters, preventing an agent from being occurred. Run the following command in port configuration mode:

Command	Purpose
dot1x forbid multi-network-adapter	Forbids the supplicant with multiple NICs.

1.2.13 Resuming the Default Settings of 802.1x

This command is used to resume all global configurations to the default settings. To configure the authentication mode, you also can run the following command in interface configuration mode:

Command	Purpose
dot1x default	This command is used to resume all global configurations to the default settings.

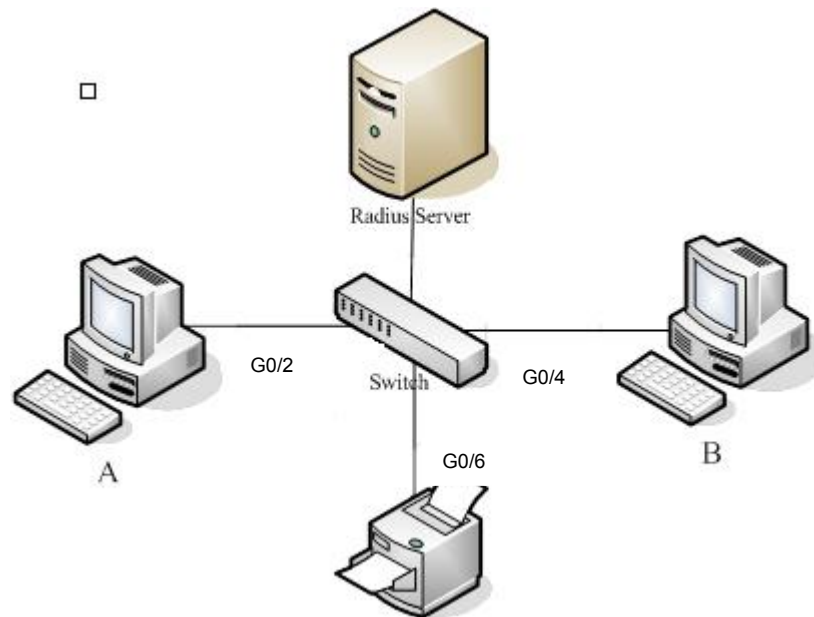
1.2.14 Monitoring the 802.1x Authentication Configuration and State

To monitor the 802.1x authentication configuration and state, run the following commands in EXEC mode:

Command	Purpose
show dot1x { interface statistics misc-mab-db }	Monitoring the 802.1x Authentication Configuration and State

1.3 802.1x Configuration Example

See the following figure:



Host A connects the G0/2 interface of the switch, host B the G0/4 interface, and host C the G0/6 interface; the radius-server host's IP is 192.168.20.2 and its key is TST; on the G0/2 interface the remote radius authentication, user-bind, accounting and re-authentication will be enabled altogether, on the G0/4 interface the local authentication, eap, multi-hosts and guest-vlan are enabled altogether, and on the G0/6 interface the MAB authentication is used and its 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
```

Configuration of interface f0/2

```
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
```

Configuration of interface f0/4

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

Configuration of interface f0/6

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

VLAN Configuration

Table of Contents

Chapter 1 VLAN Configuration.....	1
1.1 VLAN Introduction.....	1
1.2 Dot1Q Tunnel Overview.....	1
1.2.1 Preface.....	1
1.2.2 Dot1Q Tunnel Realization Mode.....	2
1.3 VLANConfiguration Task List.....	2
1.4 VLAN Configuration Task.....	2
1.4.1 Adding/Deleting VLAN.....	2
1.4.2 Configuring the Port of the Switch.....	3
1.4.3 Creating/deleting the VLAN interface.....	4
1.4.4 Monitoring the VLAN Configuration and VLAN State.....	4
1.4.5 Enabling or Disabling Dot1Q Tunnel Globally.....	4
1.5 Configuration Example.....	4
1.5.1 Dot1Q Tunnel Configuration Examples.....	4
Appendix A Abbreviations.....	7

Chapter 1 VLAN Configuration

1.1 VLAN Introduction

The virtual local area network (VLAN) is an exchange network which logically groups the devices in LAN. IEEE issued the IEEE 802.1Q standard in 1999 for realizing the VLAN standard. The VLAN technology can divide a physical LAN logic address into different broadcast domains. Each VLAN has a group of devices which have the same demands but the same attributes with those on the physical LAN. Because it is a logical group, the devices in a same VLAN can be in different physical spaces. The broadcast/unicast flow within a VLAN cannot be forwarded to other VLANs. Such advantages as flow control, low device investment, easy network management and high network security, hence, are obtained.

- Support port-based VLAN
- Support 802.1Q relay mode
- Support the access port

The port-based VLAN is to classify the port into a subset of VLAN supported by the switch. If the VLAN subnet includes only one VLAN, the port is the access port; if the VLAN subnet has multiple VLANs, the port is a trunk port; there is a default VLAN among these VLANs, which is the native VLAN of the port and whose ID is PVID.

- Support VLAN range control

The `vlan-allowed` parameter is used to control the VLAN range; the `vlan-untagged` parameter is used to control the transmission of the untagged VLAN packet from the port to the corresponding VLAN.

VLAN planning modes are various such as based on MAC, IP subnet, protocol, or port.

1.2 Dot1Q Tunnel Overview

1.2.1 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 consisting of L3 switches or small-scale MAN.

The Dot1Q Tunnel attribute of 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.

1.2.2 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.

1) 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.

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 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

2) 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 201~300; and the CVLAN ID of IPTV service ranges between 301~400. When PE device receives the user data, set SPVLAN Tag with ID as 1000 for the bandwidth service; set SPVLAN Tag with ID as 2000 for the VOIP service; set SPVLAN Tag with ID as 3000 for IPTV. The difference of the Flat VLAN translation mode and the QinQ VLAN translation mode is that in the flat VLAN translation mode the SPVLAN tag is not on the out-layer of the CVLAN tag, but replaces the CVLAN tag directly.

1.3 VLANConfiguration Task List

- Adding/Deleting VLAN
- Configuring the Port of the Switch
- Creating/deleting the VLAN interface
- Monitoring the VLAN Configuration and VLAN State
- Enabling or Disabling Dot1Q Tunnel Globally

1.4 VLAN Configuration Task

1.4.1 Adding/Deleting VLAN

VLAN is grouped according to different functions, project groups or different applications, not based on the physical locations of these users. VLAN has the

similar attributes as the physical LAN, but can group terminals in different physical LANs into a same VLAN. One VLAN can have multiple ports, while all unicast/broadcast/multicast packets can be forwarded or diffused to the terminals through a same VLAN. Each VLAN is a logical network; to forward one packet to another VLAN, the routes or bridge must be used to forward it.

Run the following commands to configure VLAN:

Command	Purpose
vlan <i>vlan-id</i>	Enters theVLANconfiguration mode.
name <i>str</i>	Name in theVLANconfiguration mode
Exit	Exits theVLANconfiguration mode and creates theVLAN.
vlan <i>vlan-range</i>	Creates multiple VLANs simultaneously.
no vlan <i>vlan-id vlan-range</i>	Deletes one or multiple VLANs.

You can use the GVRP protocol to dynamically add or delete the VLAN.

1.4.2 Configuring the Port of the Switch

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 the port belongs to just one VLAN; only the untagged Ethernet frame can be transmitted and received.
- 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. 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. 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 a default VLAN and PVID; all VLAN-untagged data received on the port belongs to the packets of the VLAN.

The relay mode can group the port to multiple VLANs; at the same time, you can configure the type of to-be-forwarded packets and the quantity of the corresponding VLANs.

Run the following commands to configure the switch's port:

Command	Purpose
switchport pvid <i>vlan-id</i>	Configures PVID of the switch's interface.
switchport mode { access trunk dot1q-translating-tunnel dot1q-tunnel-uplink }	Configures the interface mode of the switch.
switchport trunk vlan-allowed ...	Configures the VLAN range of the switch's interface.
switchport trunk vlan-untagged ...	Configures the untagged VLAN ranges of the switch's port.

1.4.3 Creating/deleting the VLAN interface

To realize network management or layer-3 routing, you need create a VLAN interface which can be used for designating the IP address and mask of the interface. Run the following command to configure the VLAN interface.

Command	Purpose
[no] interface vlan <i>vlan-id</i>	Creates or deletes a VLAN interface.

1.4.4 Monitoring the VLAN Configuration and VLAN State

To monitor the configuration and state of VLAN and Dot1Q tunnel, run the following commands in EXEC mode:

Command	Purpose
show vlan [id <i>x</i> interface <i>intf</i> dot1q-tunnel [interface <i>intf</i>] mac-vlan subnet protocol-vlan dot1q-translating-tunnel flat-translation-table]	Displays the configuration and state of VLAN or Dot1Q tunnel.
show interface vlan <i>x</i>	Displays the state of the VLAN interface or that of the supervlan interface.

1.4.5 Enabling or Disabling Dot1Q Tunnel Globally

After Qot1Q Tunnel is globally enabled, all ports serve as the downlink ports of Qot1Q Tunnel by default and put the SPVLAN tag on the incoming packets.

The command to enable dot1q-tunnel globally:

Command	Purpose
dot1q-tunnel	The command is used to configure dot1q-tunnel globally.

1.5 Configuration Example

1.5.1 Dot1Q Tunnel Configuration Examples

The following typical solutions show how to apply Dot1Q tunnel.

1. Example 1

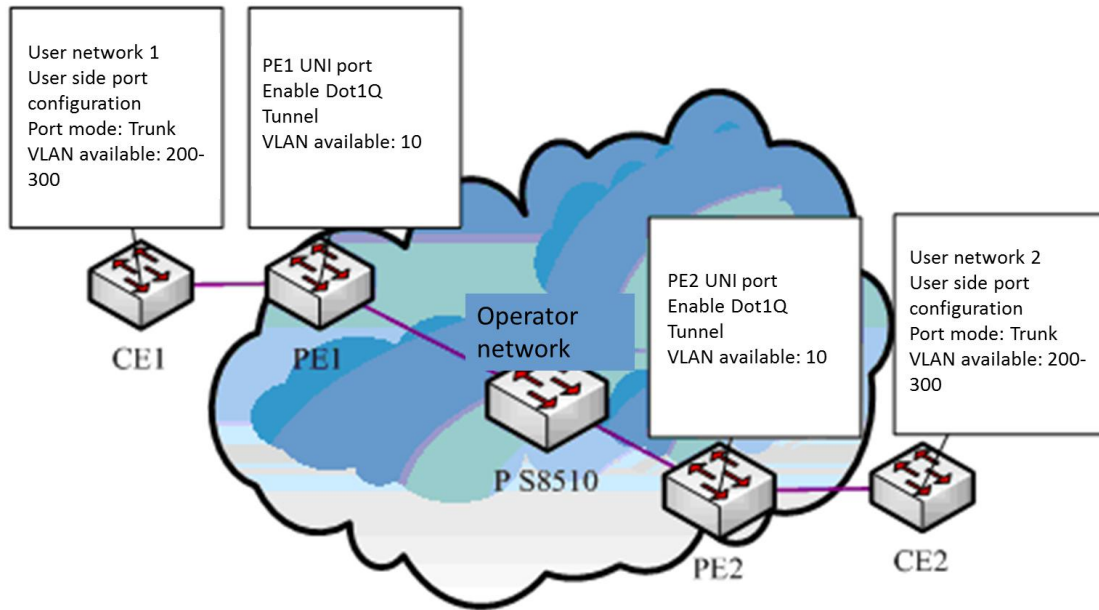


Figure 3 Typical configuration of Dot1Q tunnel

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.

Port G0/1 of PE is 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:

- 1) 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 (6B)	SA (6B)	ETYPE(8100) (2B)	VLAN TAG (2B)	ETYPE (2B)	DATA (0~1500B)	FCS (4B)
------------	------------	---------------------	------------------	---------------	-------------------	-------------

Figure 4 Structure of a packet from CE1

- 2) 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

- 3) 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.
- 4) 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, products of different models are configured as follows when they run as PE (PE1 configuration is same to PE2).

- 1) 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 A Abbreviations

Abbrev.	Full Name	Chinese Name
VPN	Virtual Private Network	Virtual Private Network
TPID	Tag Protocol Identifier	Tag Protocol Identifier
QoS	Quality of Service	QoS
P	provider bridged network core	provider bridged network core
PE	provider bridged network edge	provider bridged network edge
CE	customer network edge	customer network edge
UNI	user-network interface	user-network interface
NNI	network-network interface	network-network interface
CVLAN	Customer VLAN	Customer VLAN
SPVLAN	Service provider VLAN	Service provider VLAN

GVRP Configuration

Table of Contents

Chapter 1 GVRP Configuration.....	1
1.1 Overview.....	1
1.2 Configuring Task List.....	1
1.2.1 GVRP Configuration Task List.....	1
1.3 GVRP Configuration Task.....	1
1.3.1 Enabling/Disabling GVRP Globally.....	1
1.3.2 Setting Dynamic VLAN to Validate only on a Registered Port.....	1
1.3.3 Enabling/Disabling GVRP on the Interface.....	2
1.3.4 Monitoring and Maintenance of GVRP.....	2
1.4 Configuration Example.....	2

Chapter 1 GVRP Configuration

1.1 Overview

GVRP (GARP VLAN Registration Protocol GARP VLAN) is a concrete application of GARP (GARP VLAN Registration Protocol GARP VLAN). All switches that support GVRP can receive other switches' VLAN information and dynamically update the local VLAN registration information, including current VLAN members and the ports through which these VLAN members can be reached. Also, all the switches that support GVRP can broadcast the local VLAN registration information to other switches, making all GVRP-supported devices in the same switching network have the same VLAN information.

1.2 Configuring Task List

1.2.1 GVRP Configuration Task List

- Enabling/Disabling GVRP Globally
- Enabling/Disabling GVRP on the Interface
- Monitoring and Maintenance of GVRP

1.3 GVRP Configuration Task

1.3.1 Enabling/Disabling GVRP Globally

Run the following commands in global configuration mode.

Command	Operation
[no] gvrp	Enabling/Disabling GVRP Globally

GVRP is disabled by default.

1.3.2 Setting Dynamic VLAN to Validate only on a Registered Port

Run the following commands in global configuration mode.

Command	Operation
[no] gvrp dynamic-vlan-pruning	Enables or disables dynamic 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.

This function is not enabled by default.

1.3.3 Enabling/Disabling GVRP on the Interface

Run the following commands in interface configuration mode.

Command	Operation
[no] gvrp	Enable/disable interface GVRP.

Before enabling GVRP, please enable global GVRP first, or the interface GVRP cannot work. Moreover, GVRP function can only be configured on the Trunk interface, or the interface GVRP function cannot work.

By default, the interface GVRP function is enabled.

1.3.4 Monitoring and Maintenance of GVRP

Run the following commands in EXEC mode:

Command	Operation
show gvrp statistics [interface port_list]	This command is used to display the gvrp statistics information.
show gvrp status	This command is used to display the gvrp global state information.
[no] debug gvrp { packet event }	Enable/disable GVRP data packet or event debug switch.

This command is used to display the gvrp statistics information.

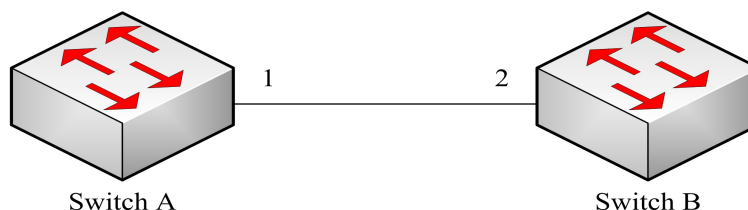
```
switch#show gvrp statistics interface g0/1
GVRP statistics on port g0/1
  GVRP Status:           : Enabled
  GVRP Frames Received   : 0
  GVRP Frames Transmitted : 66
  GVRP Frames Discarded  : 0
  GVRP Last Pdu Origin   : 0000.0000.0000
```

This command is used to display the gvrp global state information.

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

1.4 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:



- (1) Configure the interface 1 that Switch A connects to Switch B to trunk:
Switch_config_g0/1# switchport mode trunk
- (2) Enable global GVRP of switch A
Switch_config#gvrp
- (3) Enable GVRP of interface 1 of Switch A
Switch_config_g0/1#gvrp
- (4) Configure VLAN 10, Vlan 20 and Vlan30 on Switch A
Switch_config#vlan 10,20,30
- (5) Configure the interface 2 that Switch A connects to Switch B to trunk:
Switch_config_g0/2# switchport mode trunk
- (6) Enable global GVRP of switch B
Switch_config#gvrp
- (7) Enable GVRP of interface 2 of Switch B
Switch_config_g0/2#gvrp
- (8) 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.

STP Configuration

Table of Contents

Chapter 1 Configuring STP.....	1
1.1 STP Introduction.....	1
1.2 SSTP Configuration Task List.....	2
1.3 SSTP Configuration Tasks.....	2
1.3.1 Choosing the STP Mode.....	2
1.3.2 Disabling/Enabling STP.....	2
1.3.3 Disabling/Enabling STP on a Port.....	3
1.3.4 Setting the Bridge Priority.....	3
1.3.5 Setting the Hello Time.....	4
1.3.6 Setting the Max Age.....	4
1.3.7 Setting the Forward Delay.....	4
1.3.8 Setting the Port Priority.....	4
1.3.9 Value of the path cost of a port.....	5
1.3.10 Monitoring the STP state.....	5
1.3.11 Setting the SNMP Trap.....	5
1.4 Setting the Spanning Tree of VLAN.....	6
1.4.1 Overview.....	6
1.4.2 VLAN STP Configuration Tasks.....	6
Chapter 2 Configuring RSTP.....	8
2.1 RSTP Configuration Task List.....	8
2.2 RSTP Configuration Tasks.....	8
2.2.1 Enabling/disabling RSTP of the Switch.....	8
2.2.2 Setting the Bridge Priority.....	8
2.2.3 Setting the Forward Time.....	9
2.2.4 Setting the Hello Time.....	9
2.2.5 Setting the Max Age.....	10
2.2.6 Value of the path cost of a port.....	10
2.2.7 Setting the Port Priority.....	10
2.2.8 Setting the Edge Port.....	11
2.2.9 Setting the Port Connection Type.....	11
2.2.10 Restarting the protocol conversion check.....	12
Chapter 3 Configuring MSTP.....	13
3.1 MSTP Introduction.....	13
3.1.1 Overview.....	13
3.1.2 MST Region.....	13
3.1.3 IST, CST, CIST and MSTI.....	13
3.1.4 Port Role.....	15
3.1.5 MSTP BPDU.....	18
3.1.6 Stable State.....	19
3.1.7 Hop Count.....	20
3.1.8 STP Compatibility.....	20
3.2 MSTP Configuration Task List.....	20
3.3 MSTP Configuration Tasks.....	21
3.3.1 Default MSTP Configuration.....	21

Table of Contents

3.3.2 Enabling and disabling MSTP.....	22
3.3.3 Configuring MSTP region.....	22
3.3.4 Configuring network root.....	23
3.3.5 Configuring secondary root.....	24
3.3.6 Configuring Bridge Priority.....	25
3.3.7 Configuring time parameters of STP.....	25
3.3.8 Configuring network diameter.....	26
3.3.9 Configuring maximum hop count.....	27
3.3.10 Setting the Port Priority.....	27
3.3.11 Value of the path cost of a port.....	28
3.3.12 Setting the Edge Port.....	28
3.3.13 Setting the Port Connection Type.....	28
3.3.14 Activating MST-compatible mode.....	29
3.3.15 Restarting the protocol conversion check.....	30
3.3.16 Configuring role restriction of the port.....	30
3.3.17 Configuring TCN restriction of the port.....	30
3.3.18 Check MSTP information.....	31

Chapter 1 Configuring STP

1.1 STP Introduction

The standard Spanning Tree Protocol (STP) is based on the IEEE 802.1D standard. An OLT stack appears as a single spanning-tree node to the rest of the network, and all stack members use the same bridge ID.

The spanning-tree algorithm and the spanning-tree protocol can set any bridge LAN to be a simply connected mobile topology. In the mobile topology, some bridge ports can forward frames, while other ports are blocked and cannot forward data. A port in blocked state can also be contained in the mobile topology. When some network device is out of effect, added or removed, the port in blocked state will enter the forwarding state.

In the spanning-tree topology, a bridge is regarded as a root or a root bridge. Each LAN segment has a bridge port to take in charge of data forwarding from this network segment to the root. This bridge port is regarded as the designated port of this LAN segment, while the bridge where the bridge port locates is regarded as the designated bridge of LAN. The root is the designated bridge of each LAN segment that connects this root. In each bridge port, the port that is nearest to the root bridge is the root port of this bridge and only the root port and the designated port are in forwarding state; another kind of ports are open, but they are not root ports or designated ports but standby ports.

The following parameters decide the structure of the stable mobile topology:

- (1) Each unique bridge identifier
- (2) path cost of each port
- (3) ID of each bridge port

The bridge with the highest priority (the identifier value is the smallest) will be chosen as the root bridge. The ports of each bridge in the network all have root path cost, that is, the root path cost is the smallest value of the path cost sum of all ports between the root bridge and the bridge. The designated port of each LAN segment means the port that connect this LAN segment and has the smallest root path cost; if several ports have the same root path cost, their bridge identifiers will first be compared and then their port identifiers. According to this method, each LAN segment has only one designated port and each bridge has only one root port.

The spanning tree topology makes the loop inexistent in a network, guaranteeing the stability and fault recovery of the network. With the wide spread of Ethernet switch, STP plays a more and more important role. Therefore, STP is provided as a basic function of switches.

Rapid Spanning-Tree Protocol (RSTP) is an important update of 802.1D STP. When faults occur in the bridge, bridge port or LAN segment in a network, RSTP will realize the rapid convergence of the network topology. In this case, the new root port on the bridge will enter the forwarding state promptly, and at the same time the direct

acceptance between bridges can make a designated port to forward data immediately. Please refer to Chapter 2 for RSTP protocol [Configuring RSTP](#).

This chapter describes how to configure the standard STP of the switch.

Note:

802.1D STP and 802.1D RSTP mentioned in this text are simplified as SSTP and RSTP respectively. SSTP here is short for Single Spanning-Tree Protocol.

1.2 SSTP Configuration Task List

- [Choosing the STP Mode](#)
- [Disabling/Enabling STP](#)
- [Disabling/Enabling STP on a Port](#)
- [Setting the Bridge Priority](#)
- [Setting the Hello Time](#)
- [Setting the Max Age](#)
- [Setting the Forward Delay](#)
- [Setting the Port Priority](#)
- [Value of the path cost of a port](#)
- [Monitoring the STP state](#)
- [Setting the SNMP Trap](#)

1.3 SSTP Configuration Tasks

1.3.1 Choosing the STP Mode

Run the following command to set the STP mode:

Command	Purpose
spanning-tree mode {sstp pvst rstp mstp}	Selects the STP mode.

1.3.2 Disabling/Enabling STP

By default, when STP is started, the running mode is RSTP; if STP is not required, you can stop it from running.

Run the following command to disable STP:

Command	Purpose
---------	---------

STP Configuration

no spanning-tree	Disables STP.
-------------------------	---------------

Run the following commands to enable STP:

Command	Purpose
spanning-tree	Enables STP that runs in default mode—RSTP.
spanning-tree mode {sstp pvst rstp mstp}	Selects a mode for the enabled STP.

1.3.3 Disabling/Enabling STP on a Port

By default, STP is running on all switch ports (physical ports and aggregation ports); if you want to disable STP, you can run the following command in port configuration mode.

Command	Purpose
no spanning-tree	Disables STP to run on the ports.

After STP is forbidden to run on a port, this port maintains a designated port and its forwarding state and stops to transmit BPDU again. However, each STP mode still has such operations as type checkup, numbering, edge information update and topology information update towards BPDU that a port receives.

Note:

When no spanning-tree is set and a port has served as a root port, alternate port, master port or backup port, the protocol information that this port receives in RSTP/MSTP mode will age immediately and transfer to be a designated port, while the protocol information that this port receives in SSTP/PVST mode will remain the original role for a certain period and then age after the timer times out.

Note:

Every STP mode supports the BPDU Guard function on the port on which no spanning-tree is set.

1.3.4 Setting the Bridge Priority

You can choose the spanning-tree root of the network topology by changing the bridge priority of a switch.

Run the following commands to set the bridge priority of SSTP:

Command	Purpose
spanning-tree sstp priority <i>value</i>	Modifies the bridge priority of the SSTP mode.
no spanning-tree sstp priority	Resumes the SSTP bridge priority to the default value, 32768.

1.3.5 Setting the Hello Time

You can configure the hello time of the SSTP to decide the packet transmission's interval when the switch works as the root.

Run the following commands to set the SSTP hello time.

Command	Purpose
spanning-tree sstp hello-time <i>value</i>	Modifies the hello time in SSTP mode.
no spanning-tree sstp hello-time	Resumes the Sstp hello time to the default value, 2 seconds.

1.3.6 Setting the Max Age

You can configure the Sstp max age to decide the maximum lifespan of the packet when the switch works as the root.

Run the following commands to configure the Sstp max age.

Command	Purpose
spanning-tree sstp max-age <i>value</i>	Modifies the Max Age of the Sstp mode.
no spanning-tree sstp max-age	Resumes the max age to the default value, 20 seconds.

1.3.7 Setting the Forward Delay

You can configure the forward delay time of the Sstp to decide the state change interval of all switches when these switches works as the root.

Run the following commands to configure the Sstp forward delay.

Command	Purpose
spanning-tree sstp forward-time <i>value</i>	Modifies the forward time of the Sstp mode.
no spanning-tree sstp forward-time	Resumes the default forward time, 15 seconds.

1.3.8 Setting the PortPriority

When a loop generates, STP will change the states of some ports to the blocking state to cut off the loop. You can control whether to block a port by setting the port priority and the port path cost.

Run the following commands to set the port priority of Sstp:

Command	Purpose
spanning-tree port-priority <i>value</i>	Sets the port priority in all modes.
spanning-tree sstp port-priority <i>value</i>	Modifies the port priority of the Sstp mode.
no spanning-tree sstp port-priority	Resumes the port priority to the default value,

	128.
--	------

1.3.9 Value of the path cost of a port

Run the following commands to set the port path cost of SSTP.

Command	Purpose
spanning-tree cost <i>value</i>	Sets the port priority in all modes.
spanning-tree sstp cost <i>value</i>	Modifies the port path cost in SSTP mode.
no spanning-tree sstp cost	Resumes the port path cost to the default value.

1.3.10 Monitoring the STP state

To monitor STP configuration and STP's state, run the following commands in EXEC mode:

Command	Purpose
show spanning-tree	Displays the state of STP in current mode.
show spanning-tree detail	Displays the detailed information about STP in current mode.
show spanning-tree interface	Displays the information about a port in STP in current mode.

1.3.11 Setting the 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 a switch changes from a non-root to a root, the newRoot Trap message will be transmitted; when the topology change is detected, such as a non-edge port is changed from the non-forwarding state to the forwarding state, the topologyChange Trap message will be transmitted.

Note:

The STP trap can be received only when the network management software supports trap reception. The network management need be imported into the bridge MIB and OID is 1.3.6.1.2.1.17.

Run the following commands in global configuration mode to enable the STP trap:

Command	Purpose
spanning-tree management trap	Enables the STP trap.
[newroot topologychange]	If the trap type is not designated, two kinds of traps will be enabled at the same time.
no spanning-tree management trap	Disables the STP trap.

1.4 Setting the Spanning Tree of VLAN

1.4.1 Overview

In SSTP mode, the whole network only has one spanning-tree instance, and the state of a port in the spanning tree decides its state in all VLANs. When multiple VLANs exist in a network, the isolation between SSTP and VLAN topology may lead to the communication block of some network parts.

The switch supports that independent SSTP runs on a certain number of VLANs and guarantees that a port has different states in different VLANs. At the same time the flow balance can be realized between VLANs.

It should be noted that the VLAN number which can independently running STP protocol depends on the actual version. Other VLAN topology exceeding the number limit will not be affected by STP.

1.4.2 VLAN STP Configuration Tasks

Run the following commands to set the features of SSTP in VLAN:

Command	Purpose
spanning-tree mode pvst	Enables STP distribution according to VLAN.
spanning-tree vlan <i>vlan-list</i>	Distributes the STP instance for a designated VLAN. <i>vlan-list</i> means the VLAN list (similarly hereinafter).
no spanning-tree vlan <i>vlan-list</i>	Deletes the spanning-tree instance in a designated VLAN
spanning-tree vlan <i>vlan-list</i> priority <i>value</i>	Sets the spanning-tree priority in a designated VLAN.
no spanning-tree <i>vlan-list</i> priority	Resumes the spanning-tree priority in a VLAN to the default value.
spanning-tree vlan <i>vlan-list</i> forward-time <i>value</i>	Sets the Forward Delay of a designated VLAN.
no spanning-tree vlan <i>vlan-list</i> forward-time	Resumes the Forward Delay of a designated VLAN.
spanning-tree vlan <i>vlan-list</i> max-age <i>value</i>	Sets the max age of a designated VLAN.
no spanning-tree vlan <i>vlan-list</i> max-age	Resumes the Max-Age of a designated VLAN to the default value.
spanning-tree vlan <i>vlan-list</i> hello-time <i>value</i>	Sets the Hello-time of a designated VLAN.
no spanning-tree vlan <i>vlan-list</i> hello-time	Resumes the hello-time of a designated VLAN to the default value.

Run the following commands to set the port's features in switch port configuration mode:

STP Configuration

Command	Purpose
spanning-tree vlan <i>vlan-list</i> cost	Sets the path cost of a port in a designated VLAN.
no spanning-tree vlan <i>vlan-list</i> cost	Resumes the path cost of a port in VLAN to the default value.
spanning-tree vlan <i>vlan-list</i> port-priority	Sets the port priority in VLAN.
no spanning-tree vlan <i>vlan-list</i> port-priority	Resumes the priority of a port in VLAN to the default value.

In monitor or configuration mode, run the following commands to browse the state of the spanning tree in a designated VLAN:

Command	Purpose
show spanning-tree vlan <i>vlan-list</i>	Browns the state of the spanning tree in a VLAN.
show spanning-tree pvst instance-list	To check the corresponding relation between PVST instances and VLAN, run this command.

Chapter 2 Configuring RSTP

2.1 RSTP Configuration Task List

- [Enabling/disabling RSTP of the Switch](#)
- [Setting the Bridge Priority](#)
- [Setting the Forward Time](#)
- [Setting the Hello Time](#)
- [Setting the Max Age](#)
- [Value of the path cost of a port](#)
- [Setting the Port Priority](#)
- [Setting the Edge Port](#)
- [Setting the Port Connection Type](#)
- [Restarting the protocol conversion check](#)

2.2 RSTP Configuration Tasks

2.2.1 Enabling/disabling RSTP of the Switch

Run the following commands in global configuration mode.

Command	Purpose
spanning-tree mode rstp	Enables RSTP.
no spanning-tree mode	Disables stp funciton.

2.2.2 Settingthe Bridge Priority

The bridge priority decides whether this bridge can be chosen as the root bridge of the whole spanning tree. Setting a comparatively low priority can make a bridge to be the root bridge of the spanning tree.

Run the following commands in global configuration mode.

Command	Purpose
spanning-tree rstp priority <i>value</i>	Sets the priority of a bridge.
no spanning-tree rstp priority	Resumes the bridge priority to be the default

	value.
--	--------

It is especially noted that if the priorities of all bridges in an entire OLT network have the same value the bridge with the smallest MAC address will be chosen as the root bridge. In case that RSTP is enabled, if the bridge priority is changed the spanning tree will be calculated again.

In the default settings, the bridge priority is set to 32768.

2.2.3 Setting the Forward Time

Link fault will trigger the recalculation of the spanning-tree structure, but the new configuration information, which is obtained through recalculation, cannot be sent to the whole network immediately; if the newly chosen root port and designated port starts data forwarding immediately, temporary loop may be caused. To solve this problem, RSTP adopts a state removal mechanism. Before the root port and the designated port begin to forward data, an intermediate state must be experienced. The intermediate state changes into the forwarding state after the forward delay that guarantees the new configuration information has spread all over the whole network. The Forward Delay of a bridge depends on the diameter of the OLT network. Generally speaking, the longer the network diameter is, the longer the forward delay should be set to be.

Run the following commands in global configuration mode.

Command	Purpose
spanning-tree rstp forward-time <i>value</i>	Sets the Forward Delay.
no spanning-tree rstp forward-time	Resumes the default forward delay, 15 seconds.

It is especially noted that if Forward Delay is set too small the temporary redundant path may occur in the network, but if Forward Delay is set too big the network may be disconnected for a long time. That's why users are recommended to take the default value.

In the default settings, the forward delay of a bridge is 15 seconds.

2.2.4 Setting the Hello Time

A suitable hello time not only guarantees that a bridge can detect a link fault in a network promptly but also occupies a few network resources.

Run the following commands in global configuration mode.

Command	Purpose
spanning-tree rstp hello-time <i>value</i>	Sets the Hello Time.
no spanning-tree rstp hello-time	Resumes the hello time to the default value.

It takes attention that if a long hello time is set, packet loss in the links may cause a bridge not to receive the hello packets for a long time and the bridge then regards the occurrence of link faults and starts spanning-tree recalculation, but if a too short hello time is set the bridge will frequently send the configuration information and then the network bandwidth will be heavily occupied and the network/CPU load will be increased. That's why users are recommended to take the default value.

In the default settings, the hello time of a bridge is 2 seconds.

2.2.5 Setting the Max Age

The max age is used to judge whether the configuration information expires. Users can set the max age according actual conditions.

Run the following commands in global configuration mode.

Command	Purpose
spanning-tree rstp max-age <i>value</i>	Setting the Max Age
no spanning-tree rstp max-age	Resumes the max age to the default value, 20 seconds.

Link fault, reduces the network auto-adaptivity. 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.

2.2.6 Value of the path cost of a port

The path cost is related with the link rate of the port. If the link rate is required to be high, the path cost should be set to a small value; when the path cost is set to its default value, RSTP can automatically check the link rate of the current Ethernet port and calculate the corresponding path cost.

Run the following commands in interface configuration mode.

Command	Purpose
spanning-tree rstp cost <i>value</i>	Sets the path cost of a port.
no spanning-tree rstp cost	Resumes the path cost of a port to the default value.

It is especially noted that the settings of the path cost will lead to the recalculation of the spanning tree, so users are recommended to take the default value and wait RSTP to calculate the path cost of the current Ethernet port automatically.

By default, the path costs of all Ethernet ports of a bridge are all set to 2000,000 at the 10Mbps port rate, or set to 200,000 at the 100Mbps port rate.

2.2.7 Setting the Port Priority

Port priority settings can be used to designate a specific Ethernet port to be contained in the spanning tree. In general, the smaller the value is, the higher the port priority is, and the Ethernet port has more possibility to be contained in the spanning tree. If all Ethernet ports of a bridge adopt the same priority value, the index number of an Ethernet port decides whether the Ethernet port has a high priority or not.

Run the following commands in interface configuration mode.

STP Configuration

Command	Purpose
spanning-tree rstp port-priority <i>value</i>	Sets the port priority.
no spanning-tree rstp port-priority	Resumes the port priority to the default value.

It should be noted that the change of the priority of an Ethernet port can lead to the recalculation of the spanning tree.

The priority of all Ethernet ports of a bridge is 128 by default.

2.2.8 Setting the Edge Port

The edge port means this port connects terminal devices of a network. A mandatory edge port will enter the forwarding state after link-up. In port configuration mode, run the following command to set the edge port of RSTP:

Command	Purpose
spanning-tree rstp edge	Sets the edge port.

In auto mode, if a port has not received BPDU in a certain time this port is viewed as the edge port.

2.2.9 Setting the Port Connection Type

If switches, on which RSTP is run, are in the point-to-point connection, these switches can establish a topology rapidly through the handshake mechanism. When the port connection type is set, the connection of a port can be set point-to-point.

By default, RSTP will judge whether a port is in the point-to-point connection according to the duplex mode of this port. If this port works in full duplex mode, RSTP regards this port is in a point-to-point connection; if this port works in half duplex mode, RSTP regards this port's connection is shared.

If it is confirmed that RSTP or MSTP is running on the switches connected by a port, you should set this port's connection type to point-to-point so that fast handshake should be conducted.

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

Command	Purpose
spanning-tree rstp point-to-point [force-true force-false auto]	Sets the point to point interface. force-true: Mandatorily sets the connection to point-to-point. force-false: Mandatorily sets the connection to non-point-to-point. auto: Automatically checks the port type.

2.2.10 Restarting the protocol conversion check

RSTP makes a switch to work together with a traditional 802.1D STP switch through a protocol transfer mechanism. If one port of the switch receives the STP configuration message, the port then only transmits the STP message.

After a port enters the STP-compatible state, even if this port does not receive 802.1D STP BPDU again, this port will not resume the RSTP state. In this case, you can run `spanning-tree rstp migration-check` to enable the protocol transfer checkup process and resume this port to the RSTP mode.

In global mode run the following command to restart RSTP transfer checkup:

Command	Purpose
spanning-tree rstp migration-check	Restarts RSTP transfer checkup on all ports.

In switch port configuration mode, run the following command to conduct protocol transfer checkup on this port:

Command	Purpose
spanning-tree rstp migration-check	Restarts RSTP transfer checkup on the current port.

Chapter 3 Configuring MSTP

3.1 MSTP Introduction

3.1.1 Overview

Multiple Spanning Tree Protocol (MSTP) is used to establish a simple and complete topology in the bridge LAN. MSTP is compatible with STP (Spanning Tree Protocol) and RSTP (Rapid Spanning Tree Protocol).

Both STP and RSTP only construct a single spanning tree topology in a network and the packets of all VLANs are forwarded along with this unique topology. STP converges too slowly, while RSTP guarantees the a rapid and stable network topology through handshake.

MSTP keeps the fast handshake of RSTP to guarantee fast topology establishment, and at the same time MSTP allows different VLANs to be classified into different spanning trees to establish multiple tree topologies in the network. In a MSTP-constructing network, frames that belong to different VLANs can be forwarded on different paths to realize the load balance of VLAN data.

Different from PVST (per-VLAN Spanning Tree), MSTP permits multiple VLANs to be classified into the same spanning tree topology, effectively reducing spanning trees that are used to support VLANs.

3.1.2 MST Region

In MSTP, the relationship of VLAN and spanning tree is described through a MSTP. The MST configuration table, along with a configuration name and a configuration edit number, makes up of a MST configuration identifier.

In a network, the bridges that interconnect with others and possess the same MST configuration identifier are regarded that they are in the same MST region. The bridges in the same MST region generally have the same VLAN settings so that the frames of these VLANs can only be running at the inside of this MST region.

3.1.3 IST, CST, CIST and MSTI

Figure 2.1 shows an MSTP network, which consists of 3 MST regions and a switch running 802.1D STP protocol.

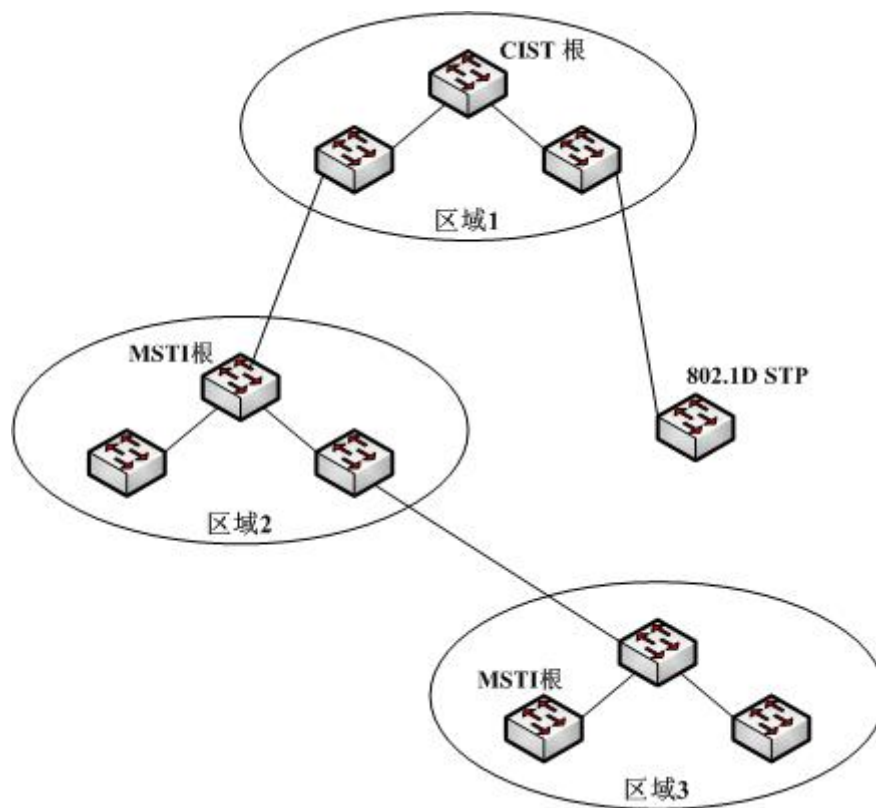


Figure 2.1 MSTP topology

1. CIST

CIST stands for Common and Internal Spanning Tree. 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.

2. CST

CST stands for Common Spanning Tree. If each MST region is viewed as a single switch, CST is then the spanning tree that connects these "single switches". As shown in figure 2.1, regions 1-3 and the STP switch constitute a CST of this network.

3. IST

IST stands for Internal Spanning Tree. IST means a CIST part in a MST region, or be considered that IST and CST constitute CIST.

4. MSTI

MSTI stands for Multiple Spanning Tree Instance. MSTP permits different VLANs to be classified into different spanning trees to establish multiple MSTIs. In general, MSTI 0 means CIST, which can be expanded to the whole network, while other MSTIs are each in a region. Each MSTI can be distributed to multiple VLANs. Originally, all VLANs are distributed in CIST.

All MSTIs in the MST region are independent and they can choose different switches to be their roots. For example, in region 3 of figure 2.1, the root of MSTI01 may be the switch at the left bottom corner, while the root of MSTI00 (CIST) may be the switch in the middle.

3.1.4 Port Role

MSTP, like RSTP, has the similar function to conduct port role distribution.

1. Root Port

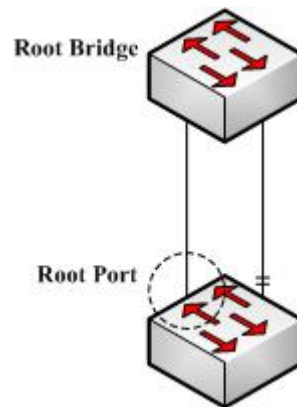


Figure 2.2 Root port

The root port means the path between the current switch to the root bridge. This path has the minimum root path cost.

2. Alternate Port

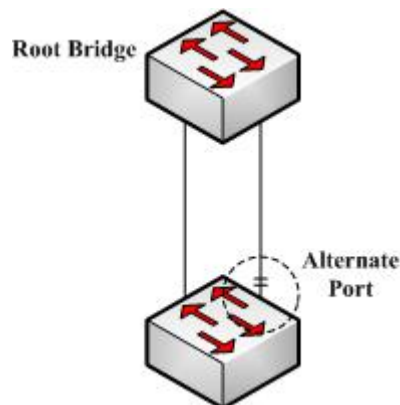


Figure 2.3 Alternate Port

The alternate port serves as path backup between the current switch and the root bridge. When the root port fails to connect, the alternate port can be immediately transferred to be a new root port and start work.

3. Designated Port

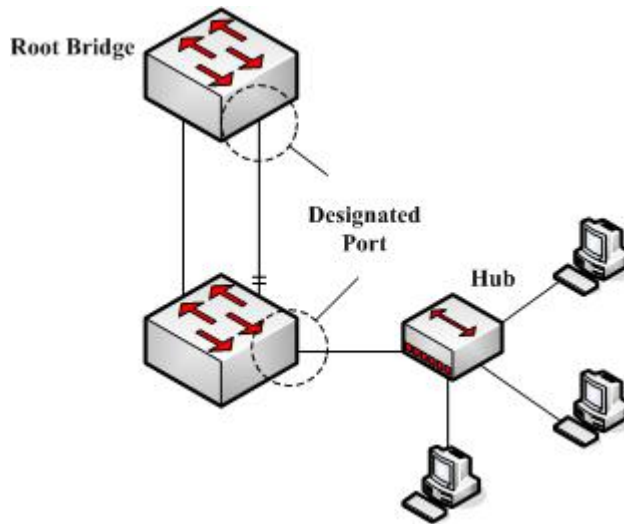


Figure 2.4 Designated port

The designated port can be used to connect the downstream switch or the downstream LAN and then runs as the path between LAN and thr root bridge.

4. Backup Port

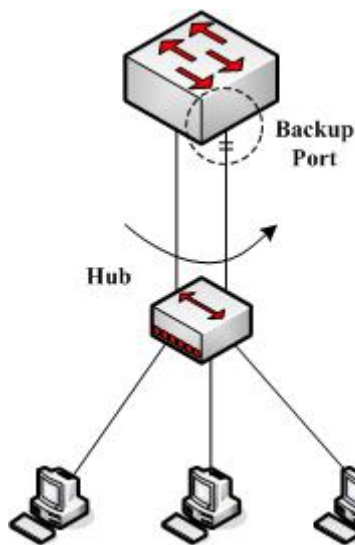


Figure 2.5 Backup port

When two ports of a switch connect directly or connect the same LAN, the port with relatively low priority will run as the backup port and the other port will run as the designated port. If the designated port invalidates, the backup port will serve as the designated port.

5. Master port

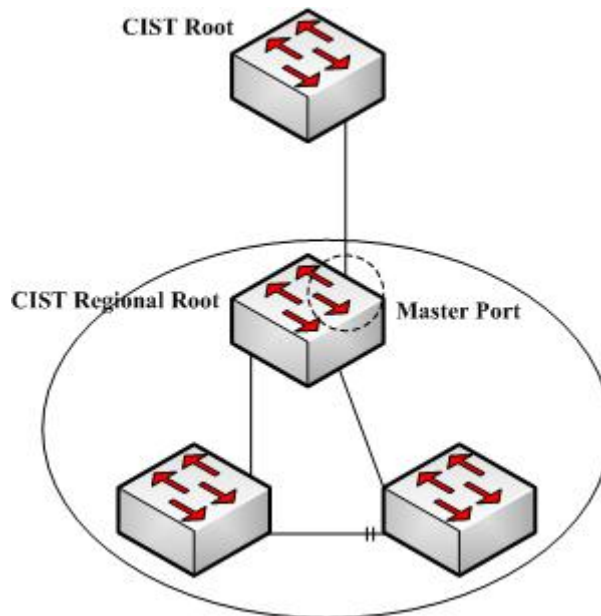


Figure 2.6 Master port

The master port is used as the shortest path between MST region and CIST root bridge. The master port is also the root port of the root bridge in CIST region.

6. Boundary Port

The concept of the boundary port is different from in CIST and in MSTI. In CIST, the boundary port means a port connecting another MST region; while in MSTI, the boundary port means that this spanning tree instance is not extended outside of this port.

7. Edge Port

In RSTP and MSTP, the edge port means a port directly connecting the host, and is capable of entering the forwarding state directly without waiting and loop.

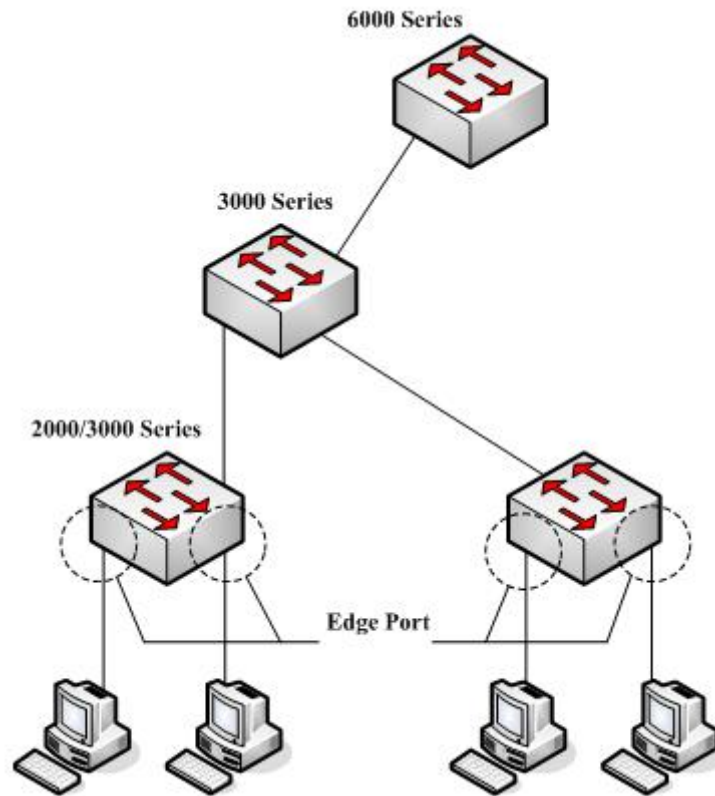


Figure 2.7 Edge port

Originally, MSTP, including RSTP, regards all ports are edge ports and therefore the network topology can be established swiftly. If a port in this case receives BPDU from another switch, the port will resume its edge state from its normal state; if it receives 802.1D STP BPDU, it has to wait for double forward delays and then enters its forwarding state.

3.1.5 MSTP BPDU

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

Table 2.1 MSTP BPDU

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

STP Configuration

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

3.1.6 Stable State

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

- (1) One switch is selected as the CIST root of the whole network.
- (2) Each switch and LAN segment can decide the minimum cost path to the CIST root, ensuring a complete connection and prevent loops.
- (3) Each region has a switch as the CIST regional root. The switch has the minimum cost path to the CIST root.
- (4) Each MSTI can independently choose a switch as the MSTI regional root.

- (5) Each switch in the region and the LAN segment can decide the minimum cost path to the MSTI root.
- (6) The root port of CIST provides the minimum-cost path between the CIST regional root and the CIST root.
- (7) The designated port of the CIST provides its LAN with the minimum-cost path to the CIST root.
- (8) The Alternate port and the Backup port provides connection when the switch, port or the LAN does not work or is removed.
- (9) The MSTI root port provides the minimum cost path to the MSTI regional root.
- (10) The designated port of MSTI provides the minimum cost path to the MSTI regional root.
- (11) A master port provides the connection between the region and the CIST root. In the region, the CIST root port of the CIST regional root functions as the master port of all MSTI in the region.

3.1.7 Hop Count

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

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

3.1.8 STP Compatibility

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

Note:

When a port is in the STP-compatible state, the port will not automatically resume to the MSTP state even if the port does not receive the STP message any more. In this case, you can run `spanning-tree mstpmigration-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.

3.2 MSTP Configuration Task List

- [Default MSTP Configuration](#)

- [Enabling and disabling MSTP](#)
- [Configuring MSTP region](#)
- [Configuring network root](#)
- [Configuring secondary root](#)
- [Configuring bridge priority](#)
- [Configuring time parameters of STP](#)
- [Configuring network diameter](#)
- [Configuring maximum hop count](#)
- [Configuring port priority](#)
- [Configuring path cost for port](#)
- [Configuring the edge port](#)
- [Configuring port connection type](#)
- [Activating MST-compatible mode](#)
- [Restarting the protocol conversion check](#)
- [Configuring role restriction of the port](#)
- [Configuring TCN restriction of the port](#)
- [CheckMSTPinformation](#)

3.3 MSTP Configuration Tasks

3.3.1 Default MSTP Configuration

Attributes	Default Settings
STP mode	RSTP (PVST, SSTP and MSTP is not enabled)
Area name	Its default value is the MAC address of a switch.
Area edit level	0
MST configuration list	All VLANs are mapped to CIST (MST00).
Spanning-tree port priority (CIST and all MSTI)	32768
Spanning-tree port priority (CIST and all MSTI)	128
Path cost of the spanning-tree port (CIST and allMSTI)	1000 Mbps: 20000

STP Configuration

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

3.3.2 Enabling and disabling MSTP

The STP protocol can be started in RSTP 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.

3.3.3 Configuring MSTP region

The MST area where the switch resides is decided by three attributes: configurationname, 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 MACaddress 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 esignated 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 <i>string</i>	Configures the MST configuration name. string means the character string of the configurationname. 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 <i>value</i>	Sets the MST edit number.

STP Configuration

	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 <i>instance-id vlan vlan-list</i>	Maps VLAN to MSTI. Instance ID of the spanning-tree, which stands for an MSTI Value range: 1-15 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 which stands for an STP instance. vlan-list can represent a group of VLANs, such as "1,2,3", "1-5" and "1,2,5-10". "1,2: 5-10"...
no spanning-tree mstp instance <i>instance-id</i>	Cancels the VLAN mapping of MSTI and disables the spanning tree instance. instance-id: Instance ID of the spanning-tree, which stands for a MSTI. Value range: 1-15

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.

3.3.4 Configuring network root

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

MSTP can set the switch to the network root through configuration. You can run the command `Spanning-tree mstp instance-id root` to modify the priority value of the switch in a spanning tree instance from the default value (32768) to a sufficiently small value, ensuring the switch turns to be the root in the spanning tree instance.

In general, after the command to set the primary root is executed, the protocol automatically checks the bridge ID of the current network's root and then sets the priority of the bridge ID to 24576, which guarantees that the current switch serves as the root of the STP instance.

If the priority value of the network root is less than 24576, the protocol will automatically set the STP priority of the current bridge to a value which is 4096 smaller than the priority of the root. It deserves attention that 4096 is the step of the priority value of the bridge.

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

STP Configuration

parameters include 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 <i>instance-id</i> root primary [diameter <i>net-diameter</i> [hello-time <i>seconds</i>]]	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 <i>instance-id</i> root	Cancels the root configuration of the switch in the spanning tree. instance-id represents 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 <i>instance-id</i>]	Checks the MSTP message.

3.3.5 Configuring secondary root

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

Different from primary root configuration, after the command to set the secondary root is executed, the protocol directly set the STP priority of the switch to 28672. In case that the priority value of other switches in the network is 32768 by default, the current switch serves as 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 start functioning.

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

Command	Purpose
spanning-tree mstp <i>instance-id</i> root secondary [diameter <i>net-diameter</i> [hello-time <i>seconds</i>]]	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.

STP Configuration

	<p>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.</p> <p>seconds represents the unit of the hello time, ranging from 1 to 10.</p>
no spanning-tree mstp instance-id root	<p>Cancels the root configuration of the switch in the spanning tree.</p> <p>instance-id represents the number of the spanning tree instance, ranging from 0 to 15.</p>

Run the following command to check the MSTP message:

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

3.3.6 Configuring Bridge Priority

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

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

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

3.3.7 Configuring time parameters of STP

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:

- $2 \times (\text{fwd_delay} - 1.0) \geq \text{max_age}$
- $\text{max_age} \geq (\text{hello_time} + 1) \times 2$

Running the following command to set the time parameter of MSTP:

Command	Purpose
spanning-tree mstp hello-time <i>seconds</i>	Resumes Hello Time to the default value. seconds: value range: 1-10 seconds, Default value: 2 seconds
no spanning-tree mstp hello-time	Resumes the hello time to the default value.
spanning-tree mstp forward-time <i>seconds</i>	Sets the parameter Forward Delay. seconds: value range from 4 to 30 seconds, the default value is 15 seconds.
no spanning-tree mstp forward-time	Resumes Forward Delay to the default value.
spanning-tree mstp max-age <i>seconds</i>	Sets the parameter Max Age. seconds: value range from 6 to 40 seconds, the default value is 20 seconds.
no spanning-tree mstp max-age	Resumes the Max Age to the default value.

It is recommended to modify the time parameter of STP through setting the root or network diameter, ensuring the rationality of the time parameter.

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.

3.3.8 Configuring network diameter

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

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

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

STP Configuration

Command	Purpose
spanning-tree mstp diameter <i>net-diameter</i>	Configure net-diameter. net-diameter: value range: 2-7; default value: 7
no spanning-tree mstp diameter	Resumes net-diameter to the default value.

The net-diameter parameter is not saved as an independent configuration in the switch. Only the time parameter which is modified through network diameter configuration can be saved.

3.3.9 Configuring maximum hop count

Use the following command to configure the max hop-count.

Command	Purpose
spanning-tree mstp max-hops <i>hop-count</i>	Set the maximum hops. hop-count: value range: 6-40 Default value: 20
no spanning-tree mstp max-hops	Resume the maximum hop count to the default value.

3.3.10 Setting the 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 <i>instance-id</i> port-priority <i>priority</i>	Sets the priority of the STP port. instance-id represents 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 <i>value</i>	Sets the port priority in all spanning tree instances. value: value of the port priority, which 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 <i>instance-id</i> 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.

3.3.11 Value of the path cost of a 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 <i>instance-id</i> cost <i>cost</i>	Sets the path cost of the port. instance-id represents 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 <i>value</i>	Sets the path cost of the port in all spanning tree instances. value: Path cost of a port, which ranges between 1 and 200,000,000
no spanning-tree mstp <i>instance-id</i> cost	Resumes the port path cost to the default value.
no spanning-tree cost	Resumes the path cost of the port to the default value.

3.3.12 Setting the Edge Port

The edge port means this port connects terminal devices of a network. A mandatory edge port will enter the forwarding state after link-up. In port configuration mode, run following command to set the edge port of MSTP:

Command	Purpose
spanning-tree mstp edge	Sets the edge port.
no spanning-tree mstp edge	Resume the default setting.

3.3.13 Setting the Port Connection Type

If switches, on which RSTP is run, are in the point-to-point connection, these switches can establish a topology rapidly through the handshake mechanism. When the port connection type is set, the connection of a port can be set point-to-point.

By default, RSTP will judge whether a port is in the point-to-point connection according to the duplex mode of this port. If this port works in full duplex mode, RSTP regards this port is in a point-to-point connection; if this port works in half duplex mode, RSTP regards this port's connection is shared.

If it is confirmed that RSTP or MSTP is running on the switches connected by a port, you should set this port's connection type to point-to-point so that fast handshake should be conducted.

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

Command	Purpose
spanning-tree mstp point-to-point force-true	Sets the port connection mode to point-to-point.
spanning-tree mstp point-to-point force-false	Sets the port connection mode to non-point-to-point.
spanning-tree mstp point-to-point auto	Sets the port connection mode to auto-check (the default mode).
no spanning-tree mstp point-to-point	Resumes the port connection type to the default settings.

3.3.14 Activating MST-compatible mode

The MSTP protocol that our switches support is based on IEEE 802.1Q. 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 MST-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 mstmigration-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 resume to send standard MST BPDU even if the compatible mode is shut down in global configuration mode. In this case, run `migration-check`.

3.3.15 Restarting the 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. Likewise, in MST compatible mode, if one interface receives the compatible BPDU, the interface will also forward compatible BPDU.

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.

3.3.16 Configuring role restriction of the port

The port will not be selected as the root port if the role restriction of the port is enabled.

In the port configuration mode, run the following command to set the role restriction of a port.

Command	Purpose
spanning-tree mstp restricted-role	Sets the port not to be the root port

3.3.17 Configuring TCN restriction of the port

The topology change will not be transferred to other port if TCN restriction of the port is enabled.

In the port configuration mode, run the following command to set the TCN restriction of a port.

Command	Purpose
spanning-tree mstp restricted-tcn	Enable the topology changes on one port cannot

STP Configuration

	be transmitted to other ports.
--	--------------------------------

3.3.18 Check MSTP information

In monitoring mode, global configuration mode or port configuration mode, 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 MSTP information. (Information about SSTP, PVST, RSTP and MSTP can be checked)
show spanning-tree interface <i>interface-id</i>	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 <i>instance-id</i>	Checks information about a MST instance.
show spanning-tree mstp detail	Checks detailed MST information.
show spanning-tree mstp interface <i>interface-id</i>	Checks MST port configuration.
show spanning-tree mstp protocol-migration	Checks the protocol conversion state of the port.

STP Optional Characteristic Configuration

Table of Contents

Chapter 1 Configuring STP Optional Characteristic.....	1
1.1 STP Optional Characteristic Introduction.....	1
1.1.1 Port Fast.....	1
1.1.2 BPDU Guard.....	2
1.1.3 BPDU Filter.....	2
1.1.4 Uplink Fast.....	3
1.1.5 Backbone Fast.....	4
1.1.6 Root Guard.....	6
1.1.7 Loop Guard.....	6
1.2 Configuring STP Optional Characteristic.....	7
1.2.1 STP Optional Characteristic Configuration Task.....	7
1.2.2 Configuring Port Fast.....	7
1.2.3 Configuring BPDU Guard.....	7
1.2.4 Configuring BPDU Filter.....	8
1.2.5 Configuring Uplink Fast.....	9
1.2.6 Configuring Backbone Fast.....	9
1.2.7 Configuring Root Guard.....	9
1.2.8 Configuring Loop Guard.....	9
1.2.9 Configuring Loop Fast.....	10
1.2.10 Configuring Address Table Aging Protection.....	11
1.2.11 Configuring FDB-Flush.....	11
1.2.12 Configuring BPDU Terminal.....	12

Chapter 1 Configuring STP Optional Characteristic

1.1 STP Optional Characteristic Introduction

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

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

1.1.1 Port Fast

Port Fast immediately brings an interface to the forwarding state, bypassing the listening and learning states. In SSTP and PVST mode, you can use Port Fast on interfaces connected to the host or server, to allow those devices to immediately connect to the network.

Port Fast is applicable for connecting ports of the host. As these ports will not receive BPDU and will not affect the network topology, they can enter the forward state without waiting. If the Port Fast function is configured on the interface connecting to the switch, there may cause a loop.

Port Fast Characteristics can be configured in global configuration mode or interface configuration mode. When in global configuration mode, all interfaces will be taken as Port Fast interfaces and fast enter Forwarding state. Thus, it is more likely to cause loop. For avoiding the network loop resulting from Port Fast function, use BPDU Guard or BPDU Filter to protect the interface.

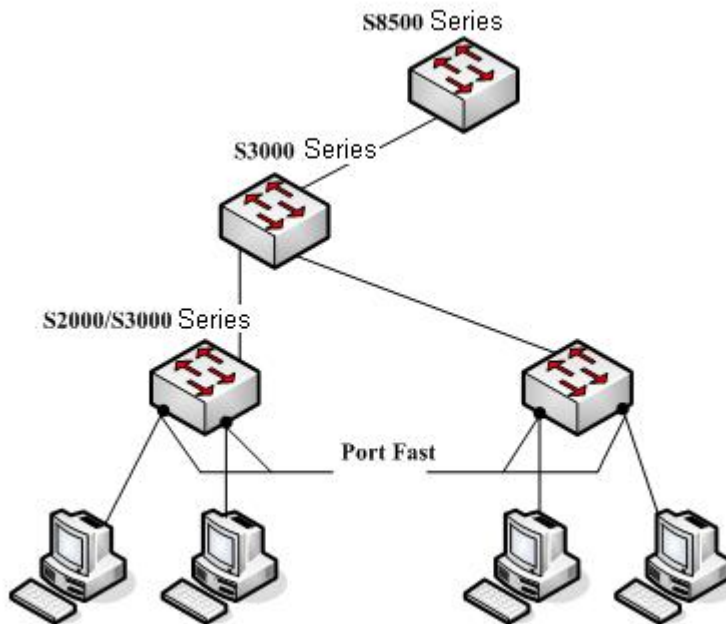


Figure 1.1 Port Fast

Note:

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.

1.1.2 BPDU Guard

If one Port Fast receives BPDU, it may be because of the false network configuration. When one Port Fast receives BPDU, BPDU Guard will protect it passively.

In different STP modes, BPDU Guard acts differently. In SSTP/PVST mode, if a port that has the BPDU Guard function and the Portfast function configured receives BPDU, this port will be mandatorily shut down. You have to configure the port manually to resume this port. In RSTP/MSTP mode, if a BPDU-Guard-configured port receives BPDU, the port will be set to the Blocking state in a period of time.

BPDU Guard characteristics can be configured independent of Port Fast. In all STP modes, the interfaces configured with BPDU Guard will not send BPDU. But the interface can receive BPDU and process it. In RSTP/MSTP mode, you can configure BPDU Guard on the port to ensure the device connected to the switch will not receive BPDU.

BPDU Guard characteristics can be configured in global or interface mode. In global configuration mode, run command `spanning-tree portfast bpduguard` to block all interfaces sending BPDU. Note that inappropriate use of BPDU Guard will cause loop in complicated network.

1.1.3 BPDU Filter

With the BPDU filtering characteristic, the switch will block BPDU to send out in SSTP/PVST mode, and also from a protection of the Port Fast.

In SSTP/PVST mode, if a Port Fast port with BPDU filter configured receives the BPDU, the characteristic 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 same with BPDU Guard, BPDU Filter characteristic can be configured in global configuration mode or in port configuration mode. In global configuration mode, run the command `spanning-tree portfast bpduguard` to block all ports to send BPDU out. The port, however, can still receive and process BPDU.

1.1.4 Uplink Fast

The characteristic 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.

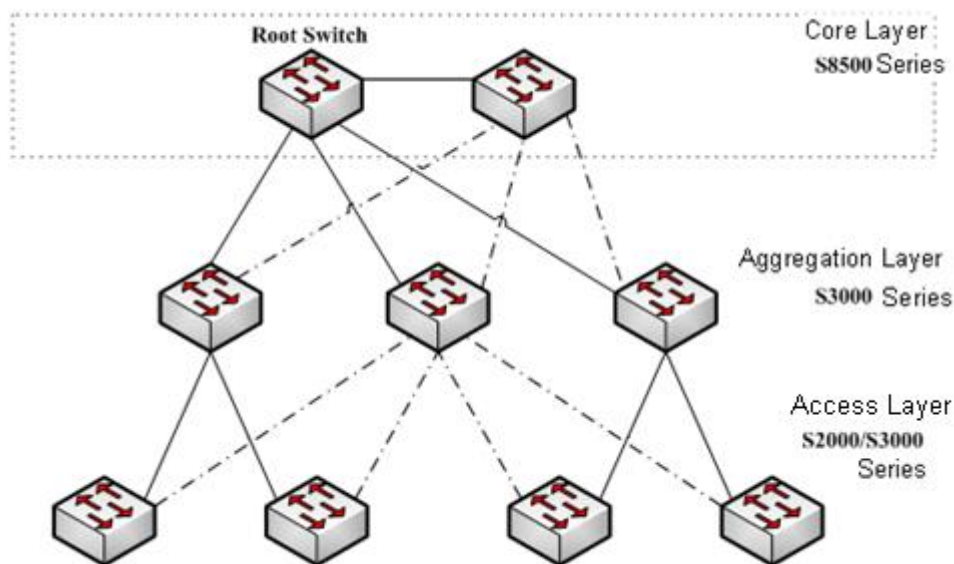


Figure 1.2 Switching network topology

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 device C to connect device B is the standby port when the port is in the original state. When the connection between device C and root device A is disconnected, the previous Alternate port is selected as new root port and immediately starts forwarding.

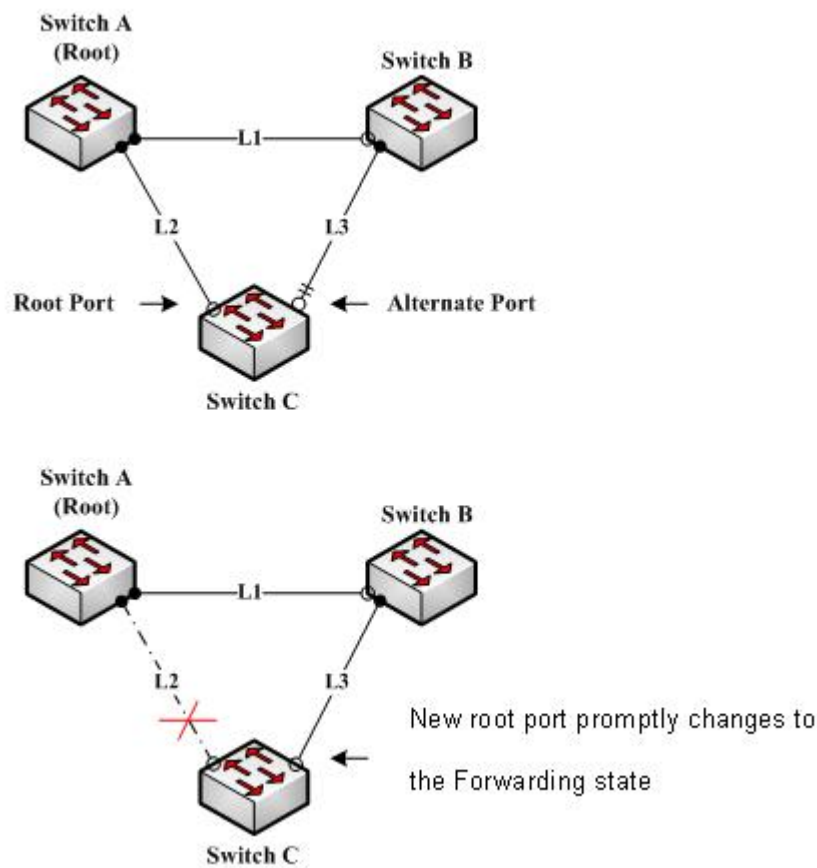


Figure 1.3 Uplink Fast

Note:

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

1.1.5 Backbone Fast

The Backbone Fast characteristic 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 devices A and B is called as the indirect link of device 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.

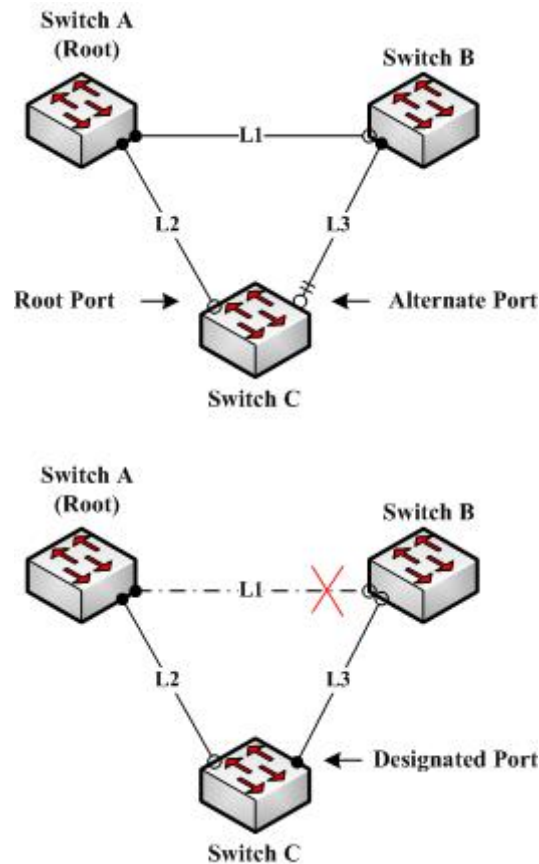


Figure 1.4 Backbone Fast

Suppose the bridge priority of switch C is higher than that of switch B. When L1 is disconnected, device B is selected to send BPDU to device C because the bridge priority is used as root priority. To device C, the information contained by BPDU is not prior to information contained by its own. When Backbone Fast is not enabled, the port between device C and device 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 device C receives a BPDU with lower priority, device C thinks that an indirect-link and root-device-reachable connection on the port is disconnected. Device 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 characteristic is effective in SSTP and

PVST modes.

1.1.6 Root Guard

The Root Guard attribute can prevent a port from serving as a root port after it receives a higher-priority BPDU.

In a complicated layer-2 network, the administrator may hope a switch in the core layer as the root of the network, but it cannot manage all switches in the access layer (That's because the switch in the access layer may belong to other clients.) Thus, the inappropriate configuration of other switches may cause the core switch cannot become the root.

To avoid the root role is occupied by switches outside the management area, you can configure Root Guard function on the boundary switch. If an interface configured Root Guard receives information that a higher BPDU is chosen as Port Port, Root Guard will automatically set the port as the blocking state and resumes it as the designated port.

In PVST and MSTP mode, Root Guard can work independently in each STP. In MSTP mode, if a boundary interface in CIST is blocked because of Root Guard, the interface will be blocked in all MSTI. The boundary interfaces are those connected to the LAN host, STP switch, RSTP switch or MSTP switch outside the region.

In interface configuration mode, run command **spanning-tree guard root** to enable Root Guard characteristic.

Note:

Root Guard characteristic acts differently somehow in SSTP/PVST and RSTP/MSTP. In SSTP/PVST mode, Root port is always blocked by Root Guard.

In RSTP/MSTP mode, Root port won't be blocked until receiving higher level BPDU. A port which formerly plays the Root role will not be blocked.

1.1.7 Loop Guard

The Loop Guard attribute can protect a port after it changes from a root port or an alternate port to a designated port. This function can prevent a port from generating a loop when the port cannot receive BPDU continuously.

You can enable this feature by using the spanning-tree loopguard default global configuration command. After enabled the command, a Root port or Alternate port will change to designated port and set as the block state. If the port receives high priority BODU in a while, it will resumes from Loop Guard automatically.

In PVST and MSTP mode, Loop Guard can work independently in each STP. In MSTP mode, if a boundary interface in CIST is blocked because of Root Guard, the interface will be blocked in all MSTI.

Note:

Root Guard characteristic acts differently somehow in SSTP/PVST and RSTP/MSTP. In SSTP/PVST mode, designated port is always blocked by Loop Guard. In RSTP/MSTP mode, the port will be blocked when it changes to designated port if it cannot receive BPDU. An interface receiving low priority BPDU and is of the designated role will not be blocked by

Loop Guard.

1.2 Configuring STP Optional Characteristic

1.2.1 STP Optional Characteristic Configuration Task

- Configuring Port Fast
- Configuring BPDU Guard
- Configuring BPDU Filter
- Configuring Uplink Fast
- Configuring Backbone Fast
- Configuring Root Guard
- Configuring Loop Guard
- Configuring Loop Fast
- Configuring Address Table Aging Protection
- Configuring FDB-Flush
- Configuring BPDU Terminal

1.2.2 Configuring Port Fast

In SSTP/PVST mode, Port Fast immediately brings an interface to the forwarding state, bypassing the listening and learning states. The function is invalid in other STP mode.

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

Command	Purpose
spanning-tree portfast 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	Disables port fast feature on the interface. It has no effect on the global configuration.
no spanning-tree portfast	Globally disables port fast feature. It has no effect on the interface configuration.

1.2.3 Configuring BPDU Guard

BPDU Guard feature acts when receiving BPDU. The interface configured BPDU Guard feature will not send BPDU.

In different STP modes, BPDU Guard acts differently. In SSTP/PVST mode, if a configured

port that has the BPDU Guard function and the Portfast function receives BPDU, this port will be shut down mandatorily. You have to configure the port manually to resume this port. In RSTP/MSTP mode, if a BPDU-Guard-configured port receives BPDU, the port will be set to the Blocking state in a period of time.

In global configuration mode, run command BPDU Guard:

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.

Note:

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

Use the following command to configure the BPDU Guard feature in the 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.

1.2.4 Configuring BPDU Filter

With the BPDU filtering characteristic, the switch will block BPDU to send out in SSTP/PVST mode, and also from a protection of the Port Fast.

In global configuration mode, run command BPDU Filter:

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.

Note:

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

Use the following command to configure 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 on the interface. It has no effect on the global configuration.

no spanning-tree bpdufilter	Disables BPDU Filter feature on the interface. It has no effect on the global configuration.
------------------------------------	----------------------------------------------------------------------------------------------

1.2.5 Configuring Uplink Fast

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

The Uplink Fast function validates only in SSTP/PVST mode.

In global configuration mode, run command Uplink Fast characteristic:

Command	Purpose
spanning-tree uplinkfast	Enables uplink fast feature.
no spanning-tree uplinkfast	Disables Uplink Fast feature.

1.2.6 Configuring Backbone Fast

The Backbone Fast characteristic 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.

The backbonefast function validates only in SSTP/PVST mode.

In global configuration mode, run command Backbone Fast characteristic:

Command	Purpose
spanning-tree backbonefast	Enables backbone fast feature.
no spanning-tree backbonefast	Disables backbone fast feature.

1.2.7 Configuring Root Guard

The Root Guard attribute can prevent a port from serving as a root port after it receives a higher-priority BPDU.

Root Guard characteristic 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.

Use the following command to configure the Root Guard feature in the interface configuration mode:

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

1.2.8 Configuring Loop Guard

The Loop Guard attribute can protect a port after it changes from a root port or an alternate port to a designated port. This function can prevent a port from generating a loop when the

port cannot receive BPDU continuously.

Root Guard characteristic acts differently somehow in SSTP/PVST and RSTP/MSTP. In SSTP/PVST mode, designated port is always blocked by Loop Guard. In RSTP/MSTP mode, the port will be blocked when it changes to designated port if it cannot receive BPDU. An interface receiving low priority BPDU and is of the designated role will not be blocked by Loop Guard.

In global configuration mode, run command Loop Guard:

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.

Use the following command to configure the Loop Guard feature 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 features on the interface.
spanning-tree guard none	Disables root guard and loop guard features on the interface.

1.2.9 Configuring Loop Fast

Note:

Please configure this command under the guide of technical engineers.

Loop Fast feature is applied to improve the network convergence in a limited range in special network environment. For instance, enable Loop Fast feature for all interfaces in the ring network with a dozen of switches.

Run following commands in global mode to configure Loop Fast feature:

Command	Purpose
spanning-tree loopfast	Globally enables Loop Fast feature. It is valid to all interfaces.
no spanning-tree loopfast	Globally disables Loop Fast.

Use the following command in interface configuration mode to enable Loop Fast:

Command	Purpose
spanning-tree loopfast	Enables loop fast feature on the interface.
no spanning-tree loopfast	Disables Loop Fast feature on the interface. If the global loop fast is configured, the feature on the interface remains effective.
spanning-tree loopfast disable	Disables Loop Fast on the interface.

1.2.10 Configuring Address Table Aging Protection

Under the circumstance of changeable network topology, the configuration of address table aging protection will not affect communication as a result of STP frequently changing the MAC address table.

STPs, such as RSTP and MSTP, will clear the MAC address table of the switch when detecting the STP topology change (delete the old MAC address and update the MAC address), so that the communication can be recovered rapidly. By default, clear action is finished through MAC address table fast aging. Most switches can finish MAC address table fast aging within 1 minute and has little effect on the performance of CPU.

After enabling the address table aging protection function, STP enables protection timer after running the first aging. Before the timeout, another aging will not run. The timer is 15 seconds by default. If the network topology changes within 15 seconds, STP will run a second aging automatically after the timeout.

Note:

The command **no spanning-tree fast-aging** can disable STP running address table aging. Before running the configuration, please ensure the network does not exist loop. Otherwise, the terminal device may need 5 mins or even longer time to resume the communication after the network topology changes

In global configuration mode, run following command to configure the address table aging protection function.

Command	Purpose
spanning-tree fast-aging	Enable/disable address table aging function.
spanning-tree fast-aging protection	Enable/disable address table aging protection function.
spanning-tree fast-aging protection time	Sets the time of address table aging protection. Before the time, STP can only run address table aging once. The default value is 15 second.

Use the no form of this command to resume the default setting

1.2.11 Configuring FDB-Flush

Note:

Please configure this command under the guide of technical engineers.

By default, RSTP and MSTP of the switch clear the old MAC address by way of address table fast aging, rather than FDB-Flush.

In global configuration mode, run the following command to configure FDB-Flush:

Command	Purpose
spanning-tree fast-aging flush-fdb	Enable FDB-Flush.

no spanning-tree fast-aging flush-fdb	Disable FDB-Flush.
----------------------------------------------	--------------------

Note that FDB-Flush is independent of fast aging. FDB-Flush can be configured while no spanning-tree fast-aging is configured. But fast aging protection function has no effect on FDB-Flush.

1.2.12 Configuring BPDU Terminal

By default, the device will forward the received BPDU when there is no STP running. BPDU terminal function can forbid forwarding BPDU when there is no STP running.

In global configuration mode, run the following command to configure BPDU Terminal:

Command	Purpose
spanning-tree bpdu-terminal	Enables BPDU Terminal.
no spanning-tree bpdu-terminal	Disables BPDU Terminal.

Link Aggregation Configuration

Table of Contents

Chapter 1 Configuring Port Aggregation.....	1
1.1 Overview.....	1
1.2 Port Aggregation Configuration Task.....	1
1.3 Port Aggregation Configuration Task.....	1
1.3.1 Configuring Logical Channel Used for Aggregation.....	1
1.3.2 Aggregation of Physical Port.....	1
1.3.3 Selecting the Load Balance Mode after Port Aggregation.....	2
1.3.4 Monitoring the Concrete Condition of Port Aggregation.....	3

Chapter 1 Configuring Port Aggregation

This chapter describes how to set the port aggregation of the switch.

1.1 Overview

Port aggregation is binding the physical ports with the same attribute together, so as to establish a logic channel. 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.

Port aggregation supports the following operation modes and functions:

Static aggregation control

After the settings of physical ports are bound to a logical port, you need not worry whether these physical ports can be bound to a logical port. You must deem that these ports can be bound to a logical port.

Aggregation control of LACP dynamic negotiation

After physical ports are bound to a logical port, only the physical ports under LACP negotiation can be bound to a logical port and other ports cannot be bound to the logical port.

Flow balance of port aggregation is supported.

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

1.2 Port Aggregation Configuration Task

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

1.3 Port Aggregation Configuration Task

1.3.1 Configuring Logical Channel Used for Aggregation

Configuring logical channel used to aggregation

Use the following command to configure the logical channel:

Command	Purpose
interface port-aggregator id	Configures aggregated logical channel.

1.3.2 Aggregation of Physical Port

To aggregate multiple physical ports into a logical channel, you can use static aggregation or LACP protocol for negotiation.

In the case when the static aggregation is used, it is required that the link of the physical port should be up, and the VLAN attribute of aggregation port and physical port should be identical, and then this port will be aggregated to the logical channel, regardless of whether the current

port accords with the conditions of port aggregation and whether the port that connects with the physical port accords with the aggregation conditions.

Use LACP and the ports can be aggregated after the negotiations both in the local end and the opposite end pass. Prerequisites for ports to be aggregated: The link of the port must be up and the port should be negotiated to full-duplex mode. The speed of all physical ports should be same during aggregation process, that is, if there is one physical port that has been aggregated successfully, then the speed of the second physical port must be the same as the first configured one. Also the vlan attributes of all physical ports must be identical to the aggregated port.

LACP packets are exchanged between ports in two modes: Active — Places a port into an active negotiating state, in which the port initiates negotiations with remote ports by sending LACP packets. Passive — Places a port into a passive negotiating state, in which the port responds to LACP packets it receives but does not initiate LACP negotiation. In this mode, the port channel group attaches the interface to the bundle. If both ports use Passive method, then the aggregation fails. This is because both sides will wait for the other side to launch aggregation negotiation process.

VALN attributes: PVID, Trunk attribute, vlan-allowed range and vlan-untagged range.

Use the following command to perform aggregation on the physical ports:

Command	Purpose
aggregator-group <i>agg-id</i> mode { lacp static }	Configures aggregation option of the physical port.

1.3.3 Selecting the Load Balance Mode 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 source and destination IP addresses, that is, the message with same IP address attributes is to get through a physical port.

Use the following command to configure load balance method:

Command	Purpose
aggregator-group load-balance	Configures load balance method.

1.3.4 Monitoring the Concrete Condition of Port Aggregation

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

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

PDP Configuration

Table of Contents

Chapter 1 PDP Overview.....	1
1.1 Overview.....	1
1.2 PDP Configuration Tasks.....	1
1.2.1 Default PDP Configuration.....	1
1.2.2 Setting the PDP Clock and Information Storage.....	1
1.2.3 Setting the PDP Version.....	2
1.2.4 Starting PDP on a Switch.....	2
1.2.5 Starting PDP on a Port.....	2
1.2.6 PDP Monitoring and Management.....	2
1.3 PDP Configuration Example.....	2

Chapter 1 PDP Overview

1.1 Overview

PDP is specially used to discover network equipment, that is, it is used to find all neighbors of a known device. Through PDP, the network management program can use SNMP to query neighboring devices to acquire network topology.

Our company's switches can discover the neighboring devices but they do not accept SNMP queries. Therefore, switches only run at the edge of network, or they cannot acquire a complete network topology.

PDP can be set on all SNAPs (e.g. Ethernet).

1.2 PDP Configuration Tasks

- Default PDP Configuration
- Setting the PDP Clock and Information Storage
- Setting the PDP Version
- Starting PDP on a Switch
- Starting PDP on a Port
- PDP Monitoring and Management

1.2.1 Default PDP Configuration

Purpose	Default Settings
Global configuration mode	This function is not enabled by default.
Interface configuration mode	Enable
PDP clock (packet transmission frequency)	60 seconds
PDP information storage	180 seconds
PDP version	2

1.2.2 Setting the PDP Clock and Information Storage

Setting the PDP Clock and Information Storage

Command	Purpose
---------	---------

pdp timer seconds	Sets the transmission frequency of the PDP packets.
pdp holdtime seconds	Sets the PDP information storage time.

1.2.3 Setting the PDP Version

To set the PDP version, you can run the following command in global configuration mode.

Command	Purpose
pdp version {1 2}	Sets the PDP version.

1.2.4 Starting PDP on a Switch

To enable PDP, you can run the following commands in global configuration mode.

Command	Purpose
pdp run	Starts PDP on a switch.

1.2.5 Starting PDP on a Port

To enable PDP on a port by default, you can run the following command in port configuration mode.

Command	Purpose
pdp enable	Starts PDP on a port of a switch.

1.2.6 PDP Monitoring and Management

To monitor the PDP, run the following commands in EXEC mode:

Command	Purpose
show pdp traffic	Displays the counts of received and transmitted PDP packets.
show pdp neighbor [detail]	Displays neighbors that PDP discovers.

1.3 PDP Configuration Example

Example 1: Starting PDP

```
Switch_config# pdp run
Switch_config# int g0/1
Switch_config_g0/1#pdp enable
```

Example 2: Setting the PDP clock and information storage

```
Switch_config#pdp timer 30
Switch_config#pdp holdtime 90
```

PDP Configuration

Example 3: Setting the PDP version

```
Switch_config#pdp version 1
```

Example 4: Monitoring PDP

```
Switch_config#show pdp neighbor
```

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge

S - Switch, H - Host, I - IGMP, r - Repeater

Device-ID	Local-Intf	Hldtme	Port-ID	Platform	Capability
Switch	Gig0/1	169	Gig0/1	COM, RISC	R S

LLDP Configuration

Table of Contents

Chapter 1 Link Layer-2 Discovery Protocol (LLDP).....	1
1.1 LLDP Overview.....	1
1.1.1 Initializing the Protocol.....	1
1.1.2 Initializing LLDP Transmit Mode.....	1
1.1.3 Initializing LLDP Reception Mode.....	2
1.1.4 LLDP PDU Packet Structure Description.....	2
1.2 LLDP Configuration Task List.....	3
1.3 LLDP Configuration Tasks.....	4
1.3.1 Disabling/enablingLLDP.....	4
1.3.2 Configuringholdtime.....	4
1.3.3 Configuring Timer.....	5
1.3.4 Configuring Reinit.....	5
1.3.5 Configuring the To-Be-SentTLV.....	6
1.3.6 Specifying the Port's Configuration and Selecting the To-Be-Sent Expanded TLV...7	
1.3.7 Configuring the Transmission or Reception Mode.....	9
1.3.8 Specifying the Management IP Address of a Port.....	10
1.3.9 Sending Trap Notification to mib Database.....	10
1.3.10 Configuring the Location Information.....	11
1.3.11 Specifying a Port to Set the Location Information.....	13
1.3.12 Configuring Show-Relative Commands.....	14
1.3.13 Configuring the Deletion Commands.....	14
1.4 Configuration Example.....	14
1.4.1 Network Environment Requirements.....	14
1.4.2 Network Topology.....	15
1.4.3 Configuration Procedure.....	15

Chapter 1 Link Layer-2 Discovery Protocol (LLDP)

1.1 LLDP Overview

802.1AB The link layer discovery protocol (LLDP) at 802.1AB helps to detect network troubles easily and maintain the network topology. It enables the neighboring device to sending out notice of its own state information to other devices and each port of all devices stores information of defining themselves. If necessary, they can also sending update information to the neighboring devices and the neighboring devices will store the information in standard SNMP MIBs. The network management system can inquire the connection of current layer-2 from MIB. LLDP can neither configure nor control the network element or traffic. It only reports configuration of layer-2.

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.

1.1.1 Initializing the Protocol

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

1.1.2 Initializing LLDP Transmit Mode

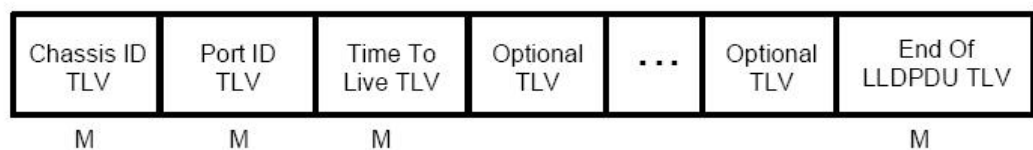
Set LLDP to transmit-only in the interface mode. In transmit-only mode, the interface transmits LLDP packets when the state or value of one or more information elements (management object) of the local system change or the transmission timer is timeout. The interface will not transmit LLDP packets when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

1.1.3 Initializing LLDP Reception 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.

1.1.4 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

- (1) Three compulsory TLVs should be listed in sequence at the beginning of LLDP PDU:

1. Chassis ID TLV
2. Port ID TLV
3. Time To Live TLV

- (2) Optional TLV selected by the network management can be listed randomly.

4. Port Description
5. System Name
6. System Description
7. System Capabilities
8. Management Address

Three extensions (including DOT1):

9. Port Vlan ID
10. Protocol Vlan ID
11. Vlan Name
12. Protocol Identity

DOT3:

13. MAC/PHY Configuration/Status
14. Power Via MDI
15. Link Aggregation
16. 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.)

17. MED Capability (TLV is compulsory if MED TLV is added.)
18. Network Policy
19. Location Identification
20. Extended Power-via-MDI
21. Inventory (包含 Hardware Revision、Firmware Revision、Software Revision、Serial Number、Manufacturer Name、Mode Name、Assert ID)

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

1.2 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

1.3 LLDP Configuration Tasks

1.3.1 Disabling/enablingLLDP

LLDP is disabled by default. You need start up LLDP before it runs. After enabling LLDP, the local port regularly forwards lldp frame to notify the information of the opposite local port.

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

Procedure	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	lldp run	Runs LLDP.

Run the following command to disable LLDP:

Procedure	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	no lldp run	Disables LLDP.

Caution: Only lldp function is enabled can the system process lldp packets. Otherwise, lldp frame will be directly forwarded.

1.3.2 Configuringholdtime

In normal condition, the remote information stored in MIB will update before aging. But the frame may loss in sending and causes the information ages. For avoiding this, you need to set the value of TTL and ensure the update LLDP frame is forwarded time after 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:

Procedure	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	lldp holdtime time	Configures the timeout time of LLDP. The value range from 0 to 65535. The default value is 120s.

Resumes the timeout time to the default value:

Procedure	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	no lldp holdtime	Resumes the timeout time to the default value, 120 seconds.

Caution: 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.

1.3.3 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:

Procedure	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.

Resumes the default interval, that is, 30 seconds.

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

1.3.4 Configuring Reinit

LLDP information will be forwarded automatically in two conditions: first, the status or value of one or more information elements (management objects) change; second, the sending timer timeouts. A single information change cause the LLDP packet is forwarded and a series of information change may cause many LLDP frames forwarded, but a frame can only report one change. For avoiding this, the web management defines the interval of two continuous 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:

Procedure	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	lldp reinit time	Configures the interval of LLDP to continuously transmit message. The value ranges from 2 to 5. The default time is 2 seconds.

Resumes the default value of reinit.

Procedure	Command	Purpose
-----------	---------	---------

LLDP Configuration

Step1	config	Enters the global configuration mode.
Step2	no lldp reinit	Resumes the default interval of continuously transmitting message; the default interval value is two seconds.

1.3.5 Configuring the To-Be-SentTLV

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:

Procedure	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	lldp tlv-select management-address	This step is 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	This step is optional. Transmits the port description tlv. The port description uses number or letters for description.
Step4	lldp tlv-select system-capabilities	This step is 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	This step is 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	This step is optional. Transmits system name tlv. The system name domain is a specified name consisted of numbers and letters. The name of the system should be the name of the system manager. That is the name of the switch.

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

Procedure	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	no lldp tlv-select management-address	This step is optional. Transmits the management address tlv. The management

LLDP Configuration

		address is usually layer-3 IP address which should be easy to use.
Step3	no lldp tlv-select port-description	This step is optional. Transmits the port description tlv. The port description uses number or letters for description.
Step4	no lldp tlv-select system-capabilities	This step is 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	This step is 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	no lldp tlv-select system-name	This step is optional. Transmits system name tlv. The system name domain is a specified name consisted of numbers and letters. The name of the system should be the name of the system manager. That is the name of the switch.

1.3.6 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:

Procedure	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. The following contents are contained: a) The bit rate and the communication mode (duplex) on the physical layer;

LLDP Configuration

		<p>b) Current duplex and the set bit rate;</p> <p>c) Showing whether the setting is the results of auto-negotiation in the initial connection phase or is a compulsory manual behavior;</p>
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(byte) .
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	<p>(Optional) Sends the MED-defined TLV and specifies the address.</p> <p>a) coordinate-based LCI, which is defined in IETF 3825[6];</p> <p>b) city's address LCI, which is defined in IETF (refer to Annex B);</p> <p>c) ELIN code of the urgency call service;</p>
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.

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

Procedure	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. The following contents are contained:

LLDP Configuration

		<p>a) The bit rate and the communication mode (duplex) on the physical layer;</p> <p>b) Current duplex and the set bit rate;</p> <p>c) Showing whether the setting is the results of auto-negotiation in the initial connection phase or is a compulsory manual behavior;</p>
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(byte) .
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	<p>(Optional) Sends the MED-defined TLV and specifies the address.</p> <p>a) coordinate-based LCI, which is defined in IETF 3825[6];</p> <p>b) city's address LCI, which is defined in IETF (refer to Annex B);</p> <p>c) ELIN code of the urgency call service;</p>
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.

1.3.7 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.

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

Procedure	Command	Purpose
Step1	config	Enters the global configuration mode.

LLDP Configuration

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.

Procedure	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.

1.3.8 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:

Procedure	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 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.

1.3.9 Sending Trap Notification to mib Database

Sending Trap Notification to lldp mib database or ptopomib database.

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

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

LLDP Configuration

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.

1.3.10 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:

Procedure	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.

LLDP Configuration

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:

Procedure	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.

LLDP Configuration

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.

1.3.11 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:

Procedure	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:

Procedure	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.

1.3.12 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.

1.3.13 Configuring the Deletion Commands

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

Run the following commands in EXEC mode:

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

1.4 Configuration Example

1.4.1 Network Environment Requirements

Configure LLDP protocol on the port connecting two switches.

1.4.2 Network Topology

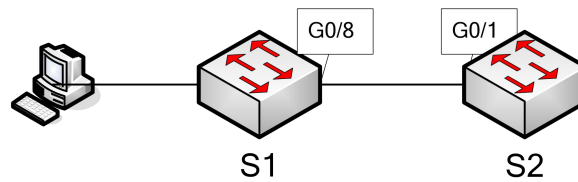


Figure 2 Network Topology

1.4.3 Configuration Procedure

1. Basic Settings

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

2. 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.

LLDP Configuration

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: SWITCH Software, Version 4.1.0B

Serial: S24090103

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

LLDP Configuration

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

3. Location Configuration

Configuring switch S1:

Switch_config#lldp run

Switch_config#

 LLDP Configuration

```

Configuring switch S2:

Switch_config#lldp run

Switch_config#location elin identifier 1 1234567890 //Configuring elin
information

Switch_config#location civic identifier 1 //Entering location
configuration mode

Switch_config_civic#language English

Switch_config_civic#city Shanghai

Switch_config_civic#street Curie

Switch_config_civic#script EN //The above configured is
civic information

Switch_config_civic#quit

Switch_config#int g0/8

Switch_config_g0/8#location elin 1 //Set elin id for the
interface

Switch_config_g0/8#location elin 1 //Set civic id for the
interface

Switch_config_g0/8#show location elin //Display elin configuration
information

elin information:

elin 1: 1234567890

total: 1

Switch_config_g0/8#show location elin //Display civic
configuration information

civic address information:

identifier: 1

City: Shanghai

Language: English

Script: EN

Street: Curie

```

 LLDP Configuration

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:

LLDP Configuration

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:

LLDP Configuration

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#

BackupLink Configuration

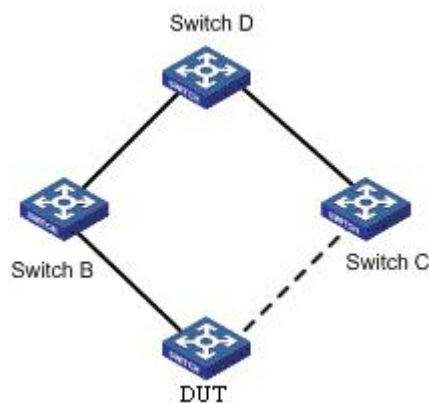
Table of Contents

Chapter 1 Introduction of Backup Link.....	1
1.1 Overview.....	1
1.2 BackupLink Port Backup.....	1
1.2.1 Setting the Backup Port.....	1
1.2.2 Status Control of the Port.....	2
1.2.3 Port Roles and Status.....	2
1.2.4 Link Status Change Processing.....	2
1.2.5 Pre-emption of Backup Port.....	3
1.2.6 Delay Preemption.....	3
1.3 VLANLoad Balancing.....	3
1.3.1 Configuration of Load balancing.....	4
1.3.2 Port Status Control in Traffic Sharing.....	4
1.4 MAC Address Aging Operation.....	5
1.4.1 Normal Work Mechanism of the Link.....	6
1.4.2 Downlink Fault Handling Mechanism.....	6
1.4.3 Uplink Fault Handling Mechanism.....	7
1.4.4 Link Recovery Processing Mechanism.....	9
Chapter 2 BackupLink Configuration.....	10
.....	10
2.1 Guidance for BackupLink Configuration.....	10
2.2 BackupLink Configuration Tasks.....	10
2.3 BackupLink Configuration.....	10
2.3.1 Configuring Backup Link Group.....	10
2.3.2 Configuring the Preemption Feature for Backuplink Group.....	11
2.3.3 Configuring Load Balancing for VLAN.....	11
2.3.4 Configuring the MMU Feature for BackupLink Group.....	12
2.3.5 Configuring MonitorLink Group.....	12

Chapter 1 Introduction of Backup Link

1.1 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.

1.2 BackupLink Port Backup

1.2.1 Setting the 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.
-

1.2.2 Status Control of the Port

The ports which are configured with backup function must be 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).

1.2.3 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.
-

1.2.4 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](#).

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 is 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.
-

1.2.6 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.

1.3 VLANLoad 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.

1.3.1 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. If there are overlapped VLAN segments, the system will classify these VLANs into different MSTs (STGs) and conduct operations toward a group of ports, the statuses of these ports in different MSTs vary. So, typically, when the load balancing VLAN group is configured, it is better to select the VLAN group without overlapping.

1.3.2 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 backed up, and the VLAN v traffic sharing is configured on P2; P3 and P4 are mutually backed up, 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.

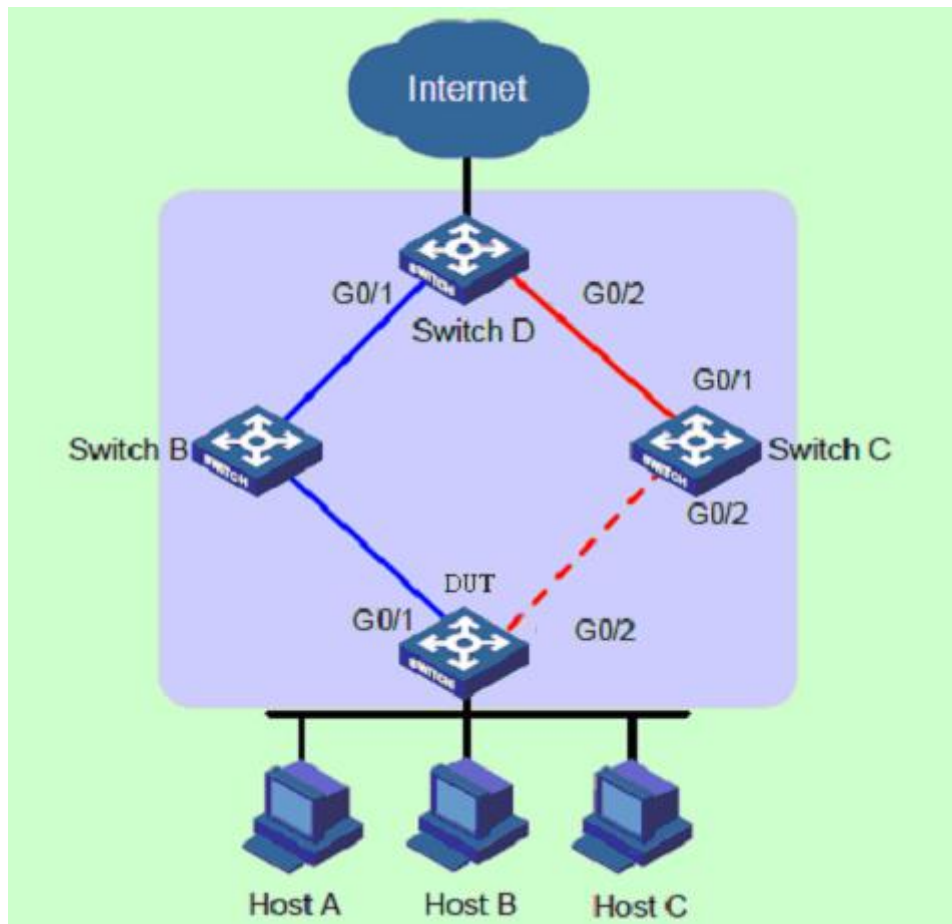
- Port status setting

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 backed up 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.

1.4 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:



BackupLink Address Aging Mechanism

1.4.1 Normal Work Mechanism of the Link

As is shown above, DUT port “GigaEthernet1 / 1” is the primary; Port “GigaEthernet1/ 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.

1.4.2 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.

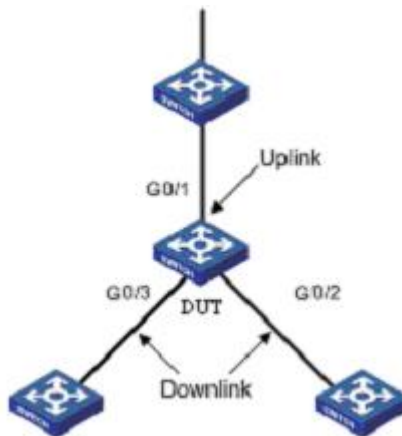
1.4.3 Uplink Fault Handling Mechanism

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 fails, for the device “DUT” configuring the BackupLink group, as the link where its primary port GigaEthernet1/ 1 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 “GigaEthernet1/ 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.



MonitorLink Group Concepts Introduction

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

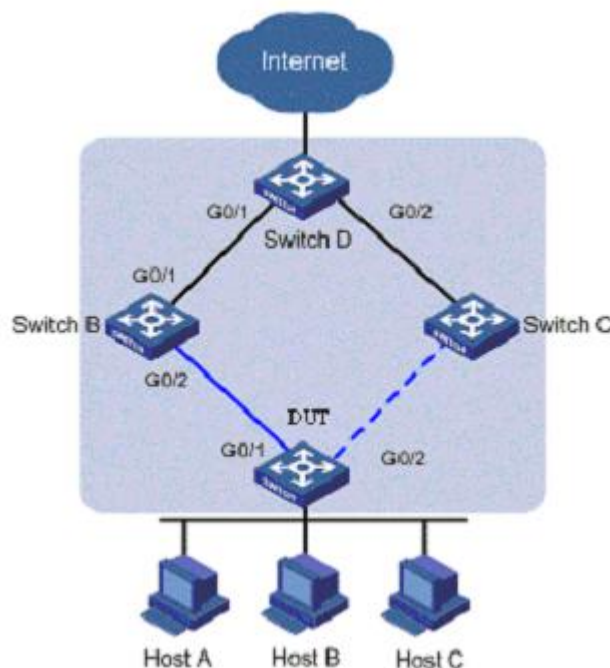
“Uplink Port” is a monitored object in MonitorLink group, which is a port role of the MonitorLink group specified through the command line. The Uplink port of MonitorLink group can be an Ethernet port (electrical or optical), or aggregate interface. As is shown

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 disabled. 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 disabled.

“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, GigaEthernet 0/2 and GigaEthernet 0/3, 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.



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 0/ 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.

1.4.4 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. [1.2.4](#). For the non-role preemption mode, please see 1.2.4; for the role preemption mode, please see [1.2.5](#).

Chapter 2 BackupLink Configuration

2.1 Guidance for BackupLink Configuration

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

- Primary port (Ethernet port or aggregation 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. Aggregation port and physical port, physical port and physical ports, aggregation port and aggregation 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 aggregation 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.

2.2 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](#)

2.3 BackupLink Configuration

2.3.1 Configuring Backup Link Group

Configure BackupLink group according to the following steps.

Command	Purpose
Switch# config	Enters the switch configuration mode.

BackupLink Configuration

Switch_config# backup-link-group <i>id</i>	Configuring backuplink group. <i>id</i> : backuplink group instance number.
Switch_config# interface gigaEthernet <i>intf-name</i>	Enters the interface configuration mode.
Switch_config_g0/1# backup-link-group <i>id</i> active[backup]	Configure backuplink group port role. <i>id</i> : backuplink group instance number.
Switch_config_g0/1# exit	Exits from interface 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 not established, it will be automatically created when you configure the backuplink group on a port directly.

2.3.2 Configuring the Preemption Feature for Backuplink Group

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

Command	Purpose
Switch#config	Enters the switch configuration mode.
Switch_config# backup-link-group <i>id</i> {preemption-mode [forced bandwidth] {delay <i>value</i> }}	Configure the preemption feature for BackupLink group. <i>id</i> : backuplink group instance number; <i>value</i> : delay-time
Switch_config#	

Note:

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

2.3.3 Configuring Load Balancing for VLAN

Configure load balancing for VLAN according to the following steps.

Command	Purpose

BackupLink Configuration

Switch# config	Enters the switch configuration mode.
Switch_config# interface gigaEthernet <i>intf-name</i>	Enters the interface configuration mode.
Switch_config_g0/2# share-load vlan <i>vlanmap</i>	Configure load balancing for VLAN. <i>vlanmap</i> : <i>vlan value</i>
Switch_config_g0/2# exit	Exits from interface configuration mode.
Switch_config#	

Note:

This command can be set only on the backup port, that is, a port must be set to be a backup port before VLAN load balance is set on the 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.

2.3.4 Configuring the MMU Feature for BackupLink Group

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

Command	Purpose
Switch# config	Enters the switch configuration mode.
Switch_config# interface gigaEthernet <i>intf-name</i>	Enters the interface configuration mode.
Switch_config_g0/2# backup-link-group mmu transmit [receive]	Configure MMU sending (receiving) function.
Switch_config_g0/2# exit	Exits from interface configuration mode.
Switch_config#	

Note:

Only the ports of the backuplink group can be set to transmit, that is, the ports must be set to active or backup. The ports that are set to receive are not necessarily the ports of the backuplink group.

2.3.5 Configuring MonitorLink Group

Configure MonitorLink group according to the following steps.

BackupLink Configuration

Command	Purpose
Switch# config	Enters the switch configuration mode.
Switch_config# monitor-link-group <i>id</i>	To set the MonitorLink group, run the following command: <i>id</i> : MonitorLink group instance number.
Switch_config# interface gigaEthernet <i>intf-name</i>	Enters the interface configuration mode.
Switch_config_g0/1# monitor-link-group <i>id</i> uplink[downlink]	Configures MonitorLink group port role. <i>id</i> : MonitorLink group instance number.
Switch_config_g0/1# exit	Exits from interface configuration mode.
Switch_config#	

Note:

Use the "no monitor-link-group *id*" to delete *MonitorLink group port* configuration and *Monitor Link groupport* 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.

Fast Ethernet Ring Protection Configuration

Table of Contents

Chapter 1 Introduction of Fast Ethernet Ring Protection.....	1
1.1 Overview.....	1
1.2 Related Concepts of Fast Ether-Ring Protection.....	1
1.2.1 Roles of Ring's Nodes.....	2
1.2.2 Role of the Ring's Port.....	2
1.2.3 Control VLAN and Data VLAN.....	2
1.2.4 Aging of the MAC Address Table.....	3
1.2.5 Symbol of a Complete Ring Network.....	3
1.3 Types of EAPS Packets.....	3
1.4 Fast Ethernet Ring Protection Mechanism.....	4
1.4.1 Ring Detection and Control of Master Node.....	4
1.4.2 Notification of Invalid Link of Transit Node.....	4
1.4.3 Resuming the Link of the Transit Node.....	4
Chapter 2 Fast Ethernet Ring Protection Configuration.....	6
2.1 Default EAPS Settings.....	6
2.2 Requisites Before Configuration.....	6
2.3 MEAPS Configuration Tasks.....	7
2.4 Fast Ethernet Ring Protection Configuration.....	7
2.4.1 Configuring the Master Node.....	7
2.4.2 The no ether-ring id command is used to delete the node settings and port settings of the Ethernet ring. Configuring the Transit Node.....	8
2.4.3 Configuring the Ring Port.....	8
2.4.4 Browsing the State of the Ring Protection Protocol.....	9
2.5 MEAPS configuration.....	9
2.5.1 Configuration Example.....	9

Chapter 1 Introduction of Fast Ethernet Ring Protection

1.1 Overview

Ethernet ring protection protocol is a special type of link-layer protocol specially designed for constructing the ring Ethernet topology. The Ethernet protection protocol can shut down one link in a complete ring topology, preventing the data loop from forming the broadcast storm. If a link is broken, the protocol immediately resumes the link that is previously shut down. In this way, the nodes among the ring network can communicate with each other.

The ring protection protocol and STP are both used for topology control on the link layer. STP is suitable for all kinds of complicated networks, which transmits the change of network topology hop by hop. The ring protection protocol is used for ring topology and adopts the pervasion mechanism to transmit the change of network topology. Therefore, the convergence of the ring protection protocol in the ring network is better than STP. In a sound network, the ring protection protocol can resume network communication within less than 50ms.

Note:

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

1.2 Related Concepts of Fast Ether-Ring Protection

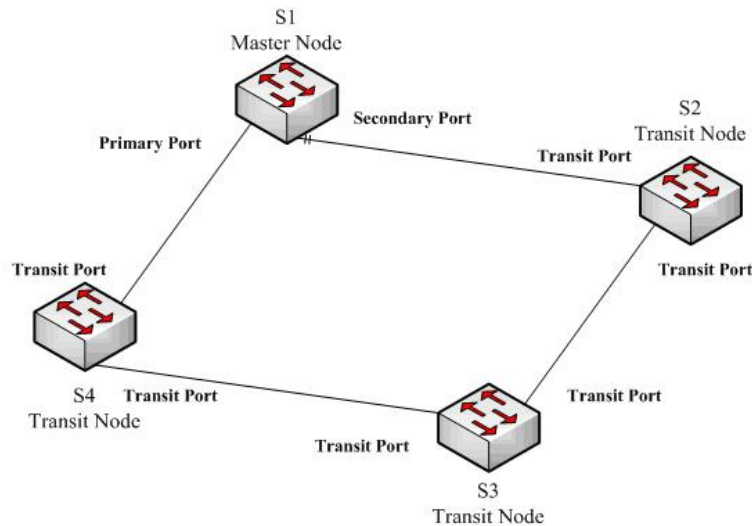


Figure 1.1 EAPS Ethernet ring

1.2.1 Roles of Ring's Nodes

Each switch on an Ethernet ring is a ring node. The ring nodes are classified into master nodes and transit nodes. Only one switch on the Ethernet ring can serve as a mere master node and other switches are worked as transit nodes.

Master node: It positively knows whether the ring's topology is complete, removes loopback, control other switches to update topology information.

Transit node: It only checks the state of the local port of the ring, and notifies the master node of the invalid link.

The role of each node can be specified by user through configuration. The thing is that each switch in the same ring can be set to only one kind of node. In figure 1.1, switch S1 is the master node of ring network, while switches S2, S3 and S4 are transit nodes.

1.2.2 Role of the Ring's Port

EAPS demands each switch has two ports to connect the ring network. Each port of the ring network also needs to be specified through configuration and the protocol supports the following kinds of port roles:

Primary port: the primary port can be configured only on the master node. The master node transmits the ring detection packets through the primary port.

Secondary port: the secondary port can be configured only on the master node. The master node receives the ring detection packets from the secondary port and judges whether the topology of the ring network is complete. In complete topology, the master node blocks the data packets on the secondary port, and prevents loopback from occurring; after a link on the ring network is interrupted, the master node 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.

Note:

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

1.2.3 Control VLAN and Data VLAN

A private control VLAN is used between master node and transit node to transmit protocol packets. This control VLAN is specified by user through configuration and ring's ports are added also by user to the control VLAN, which guarantees that the protocol packets can be normally forwarded. In general, each port of the ring network is in the forwarding state in the control VLAN and the ports which do not belong to the ring network cannot forward the packets of control VLAN.

Note:

You can specify different control VLAN for each ring on a switch. The control VLAN is only used to forward the control packets of the ring network, not for L2/L3 communication. For example, if the VLAN port that corresponds to the control VLAN is established, the IP address of the VLAN port cannot be pinged through other devices.

Other VLANs except the control VLAN are data VLAN, which is used for transitting general service packets or switch managment packets. Whether the Ethernet ring port can transit packets of data vlan is determined by the ring network protection protocol; all the non-Ethernet ring ports can transit data VLAN 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.

1.2.4 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.

1.2.5 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.

1.3 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	Notes:
Loopback detection (HEALTH)	It is transmitted by the master node to detect whether the topology of the ring network is complete.
LINK-DOWN (LINK-DOWN)	Indicates that link interruption happens in the ring. This kinds of packets are transmitted by the transit node.
Ethernet ring interruption aging	It is transmitted by the master node after interruption of the ring

address table (RING-DOWN-FLUSH-FDB)	network is detected and the packets show the MAC address aging table of the transit node.
Ethernet ring recovering 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.

1.4 Fast Ethernet Ring Protection Mechanism

1.4.1 Ring Detection and Control of Master Node

The master node transmits the HEALTH packets to the control VLAN through the primary port in a configurable period. In normal case, the HEALTH packets will pass through all other nodes of the ring network and finally arrive at the secondary port of the master node.

The secondary port blocks all data VLANs in primitive condition. When receiving the HEALTH packets continuously, the secondary port keeps blocking data VLANs and blocking the loop. If the secondary port does not receive the HEALTH packets from the primary port in a certain time (which can be configured), it will regard the ring network is out of effect. Then the master node removes the blocking of data VLANs on the secondary port, ages the local MAC address table, and transmits the RING-DOWN-FLUSH-FDB packets to notify other nodes.

If the master node receives the HEALTH packets at the secondary port that is open to data VLANs, the ring network is resumed. In this case, the master node immediately blocks data VLANs on the secondary port, updates the local topology information and reports other nodes to age the MAC address table through RING-UP-FLUSH-FDB packets.

You can configure related commands on the Hello-time node and the Fail-time node to modify the interval for the primary port to transmit the HEALTH packets and the time limit for the secondary port to wait for the HEALTH packets.

1.4.2 Notification of Invalid Link of Transit Node

After the transit port of the transit node is out of effect, the LINK-DOWN packet will be immediately transmitted by the other transit port to notify other nodes. In normal case, the packet passes through other transit nodes and finally arrives at one port of the master node.

After the master node receives the LINK-DOWN packet, it thinks that the ring network is invalid. In this case, the master node removes the blocking of data VLANs on its secondary port, ages the local MAC address table, transmits the RING-DOWN-FLUSH-FDB packet and notifies other nodes.

1.4.3 Resuming the Link of the Transit Node

After the transit port is resumed, it does not immediately transmit the packets of data VLANs, but enters the Pre-Forwarding state. A transit port in pre-forwarding state only transmits and receives the control packets from the control VLAN.

If there is only one transit port invalid in the ring network and when the port enters the pre-forwarding state, the secondary port of the master node can receive the HEALTH packet from the primary port again. In this case, the master node blocks data VLANs on the secondary port again and transmits the notification of ageing address table outside. After the node with a transit port in pre-forwarding state receives the notification of aging address table, the node will first modify the pre-forwarding port to the forwarding port and then ages the local MAC address table.

If a transit mode does not receives the notification of aging address table from the master node, it thinks that the link to the master node is already out of effect, the transit node will automatically set the pre-forwarding port to be a forwarding one.

You can configure the related commands through the pre-forward-time node to modify the time for the transit port to keep the pre-forwarding state.

Chapter 2 Fast Ethernet Ring Protection Configuration

2.1 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 bpduterminal 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 (STP)	spanning-tree mode rstp
Fast Ethernet Ring Protection	There is no configuration.

2.2 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 instance, after configuring the master node and all transmission nodes, connect network cables for the secondary port the master node. 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 Pre-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 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.

2.3 MEAPS Configuration Tasks

- [Configuring the Master Node](#)
- [Configuring the Transit Node](#)
- [Configuring the Ring Port](#)
- [Browsing the State of the Ring Protection Protocol](#)

2.4 Fast Ethernet Ring Protection Configuration

2.4.1 Configuring the Master Node

Configure a switch to be the master node of a ring network according to the following steps:

Command	Purpose
Switch# 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.

Notes:

The **no ether-ring command** is used to delete the node settings and port settings of the Ethernet ring.

2.4.2 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. Run the following command to configure 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.

2.4.3 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: ID of the node of Ethernet ring
Switch_config_intf# exit	Exits from interface configuration mode.

Note:

The **no ether-ring id {primary-port | secondary-port | transit-port }** command can be used to cancel the port settings of Ethernet ring.

2.4.4 Browsing the State of the Ring Protection Protocol

Run the following command to browse the state of the ring protection protocol:

Command	Purpose
show ether-ring <i>id</i>	Browses the summary information about the ring protection protocol and the port of Ethernet ring. id: ID of Ethernet ring
show ether-ring <i>id</i> detail	Browses the detailed information about the ring protection protocol and the port of Ethernet ring.
show ether-ring <i>id</i> interface <i>intf-name</i>	Browses the state of the Ether-ring port or that of the common port.

2.5 MEAPS configuration

2.5.1 Configuration Example

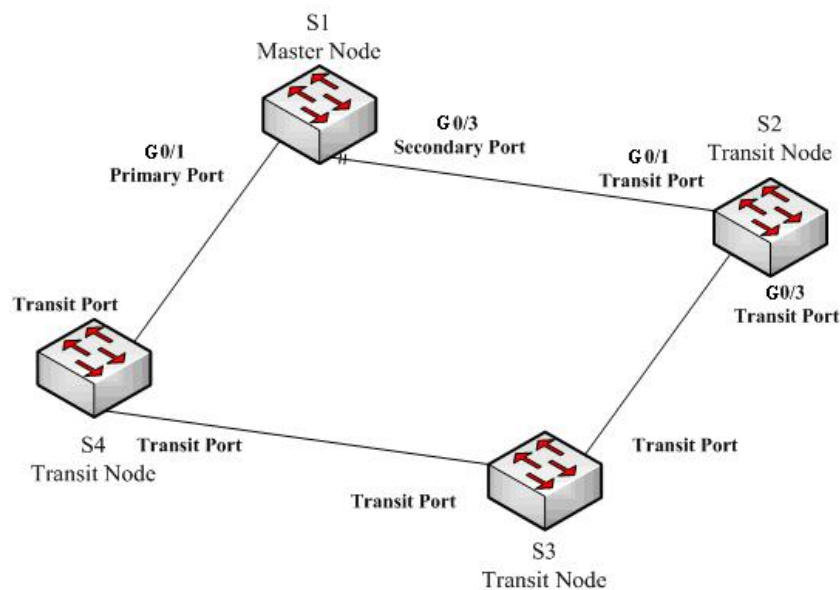


Figure 2.1 Fast Ethernet Ring Protection Configuration Example

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. 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
```

MEAPS Configuration

Table of Contents

Chapter 1 MEAPS Introduction.....	1
1.1 MEAPS Overview.....	1
1.2 Basic Concepts of MEAPS.....	2
1.2.1 Domain.....	2
1.2.2 Ring.....	3
1.2.3 Major Ring.....	3
1.2.4 Sub Ring.....	3
1.2.5 Control VLAN.....	3
1.2.6 Data VLAN.....	4
1.2.7 Master Node.....	4
1.2.8 Transit Node.....	4
1.2.9 Edge Node and Assistant Node.....	5
1.2.10 Primary Port and Secondary Port.....	5
1.2.11 Transit Port.....	5
1.2.12 Common Port and Edge Port.....	6
1.2.13 Aging of the MAC Address Table (FLUSH MAC FDB).....	7
1.2.14 Complete Flag of Ring.....	7
1.3 Types of EAPS Packets.....	7
1.4 Fast Ethernet Ring Protection Mechanism.....	8
1.4.1 Polling mechanism.....	8
1.4.2 Notification of Invalid Link of Transit Node.....	9
1.4.3 Channel Status Checkup Mechanism of the Sub-Ring Protocol Packet on the Major ring.....	10
Chapter 2 Fast Ethernet Ring Protection Configuration.....	17
2.1 Requisites Before Configuration.....	17
2.2 MEAPS Configuration Tasks.....	18
2.3 Fast Ethernet Ring Protection Configuration.....	18
2.3.1 Configuring the Master Node.....	18
2.3.2 Configuring the Transit Node.....	19
2.3.3 Configuring the Edge Node and the Assistant Node.....	20
2.3.4 Enters the switch configuration mode.....	21
2.3.5 Configuring the Ring Port.....	22
2.3.6 Browsing the State of the Ring Protection Protocol.....	22
Chapter 3 Appendix.....	23
3.1 Working Procedure of MEAPS.....	23
3.1.1 Ethernet ring complete state.....	23
3.1.2 Link-Down.....	24
3.1.3 Recovery.....	25
3.2 MEAPS configuration.....	27
3.2.1 Configuration Example.....	27
3.3 Unfinished Configurations (to be continued).....	33

Chapter 1 MEAPS Introduction

1.1 MEAPS Overview

Ethernet automatic protection switching (EAPS) is a protocol specially applied in Ethernet link layer. 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.

EAPS only supports the single-ring structure, while 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:

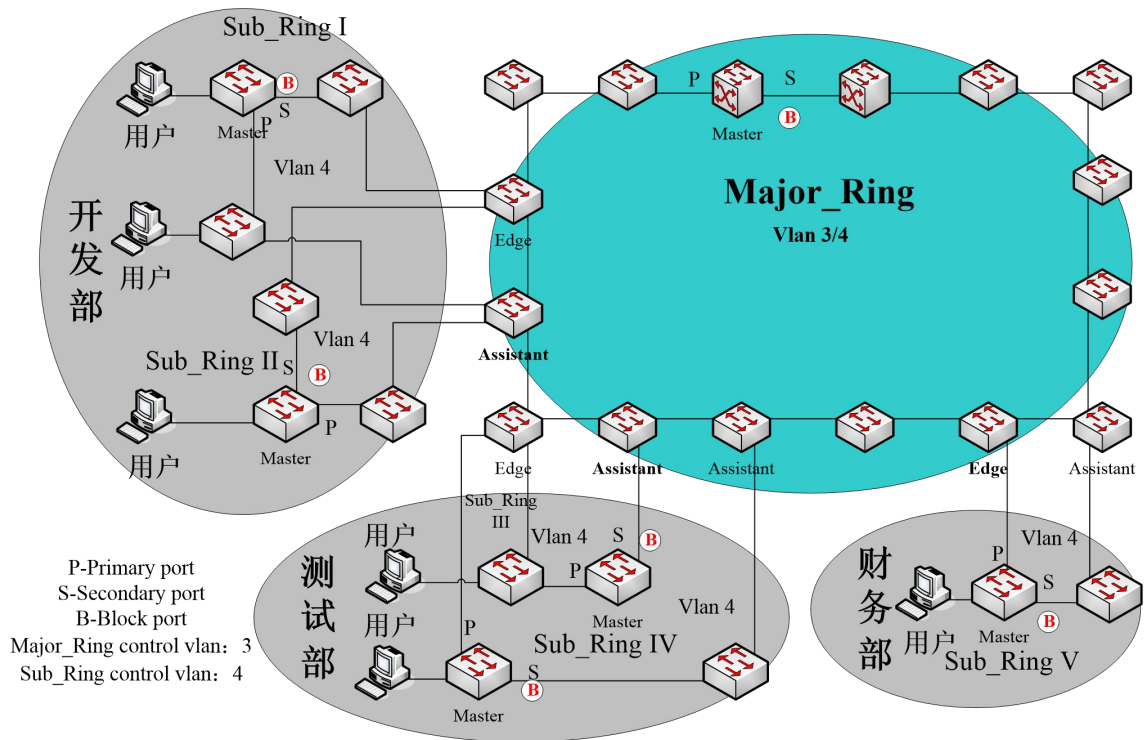


Figure 1 MEAPS Structure

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.

1.2 Basic Concepts of MEAPS

1.2.1 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 the following figure.

One MEAPS domain has the following factors: MEAPS ring, control VLAN, master node, transit node, edge node and assistant edge node.

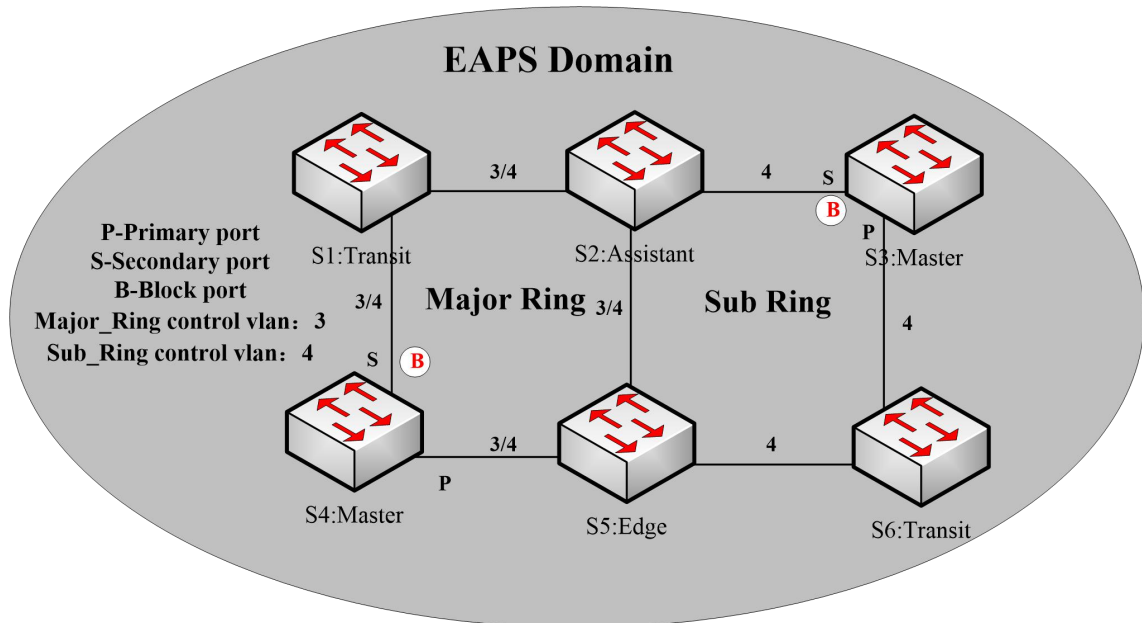


Figure-2 Simple MEAPS model

1.2.2 Ring

One ring corresponds to an 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.

1.2.3 Major 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 major ring should be added into the main control VLAN and the sub control VLAN at the same time. See the following figure.

1.2.4 Sub 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 sub ring should be added into the sub control VLAN. See the following figure.

1.2.5 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.

1.2.6 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.

1.2.7 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.

1.2.8 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.

1.2.9 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.

1.2.10 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.

1.2.11 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.

1.2.12 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 EdgePreforwarding 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.

1.2.13 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.

1.2.14 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.

The state symbol of the ring network helps user to judge the topology state of the current network.

1.3 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	Notes:
--------------------	--------

Loopback detection (HEALTH)	It is transmitted by the master node to detect whether the topology of the ring network is complete.
LINK-DOWN (LINK-DOWN)	Indicates that link interruption happens in the ring. This kinds of packets are transmitted by the transit node.
Ethernet ring interruption aging address table (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.
Ethernet ring recovering 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.
Major 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.

1.4 Fast Ethernet Ring Protection Mechanism

1.4.1 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.

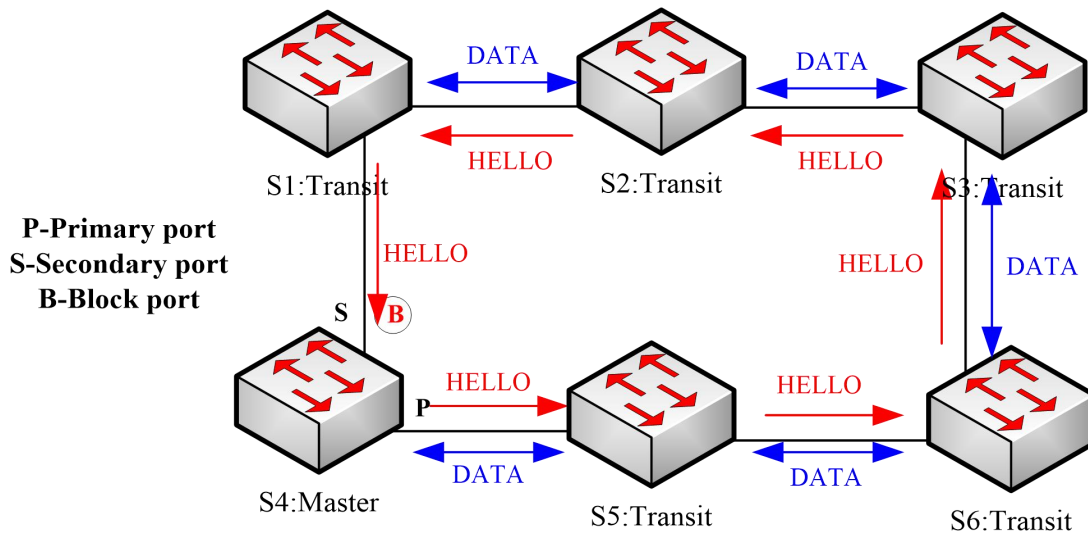


Figure 3 Polling mechanism

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.

1.4.2 Notification of Invalid Link of Transit Node

The link status change notification mechanism provides a faster mechanism of changing Ethernet ring topology 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.

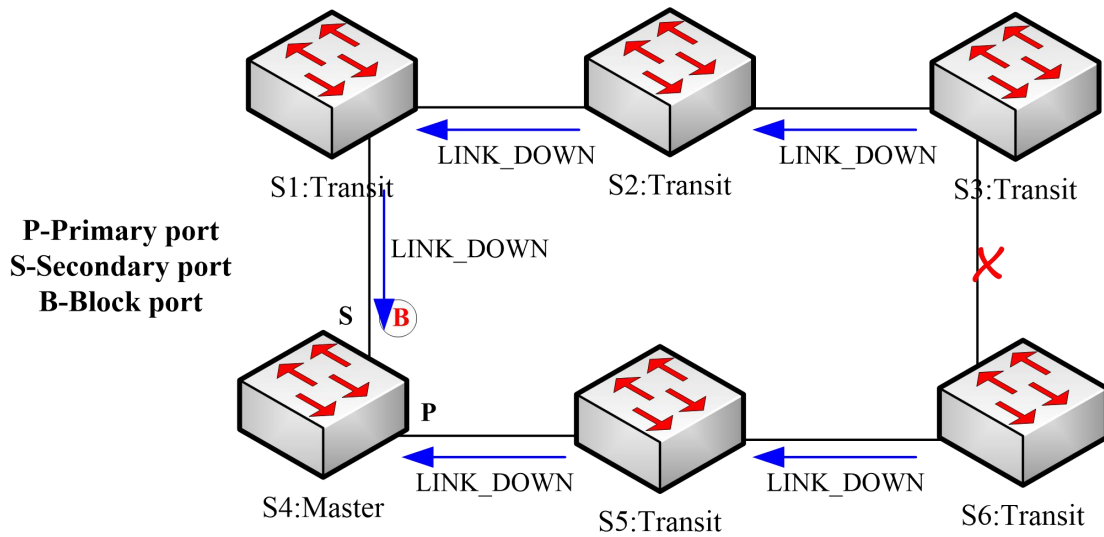


Figure 4 Link status change's notification

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.

Remark

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.

1.4.3 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:

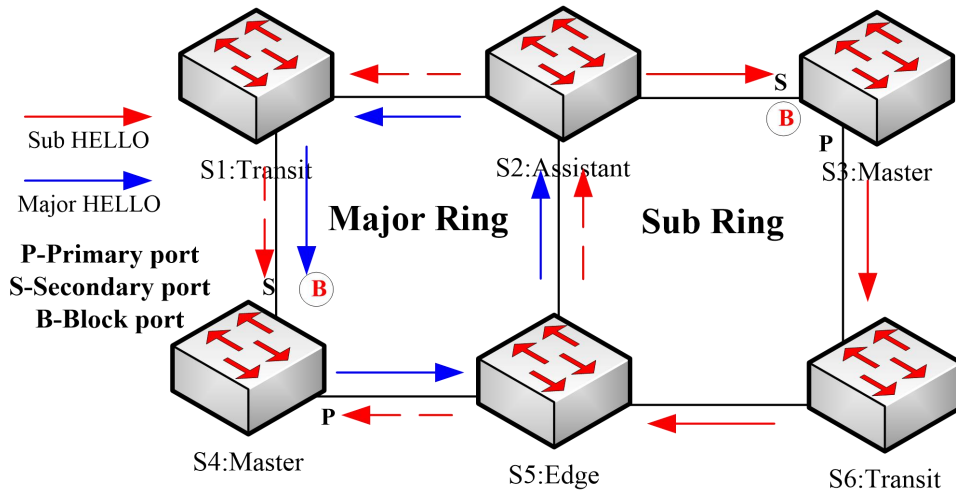


Figure 5 Intersection of the major ring and the sub ring

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.

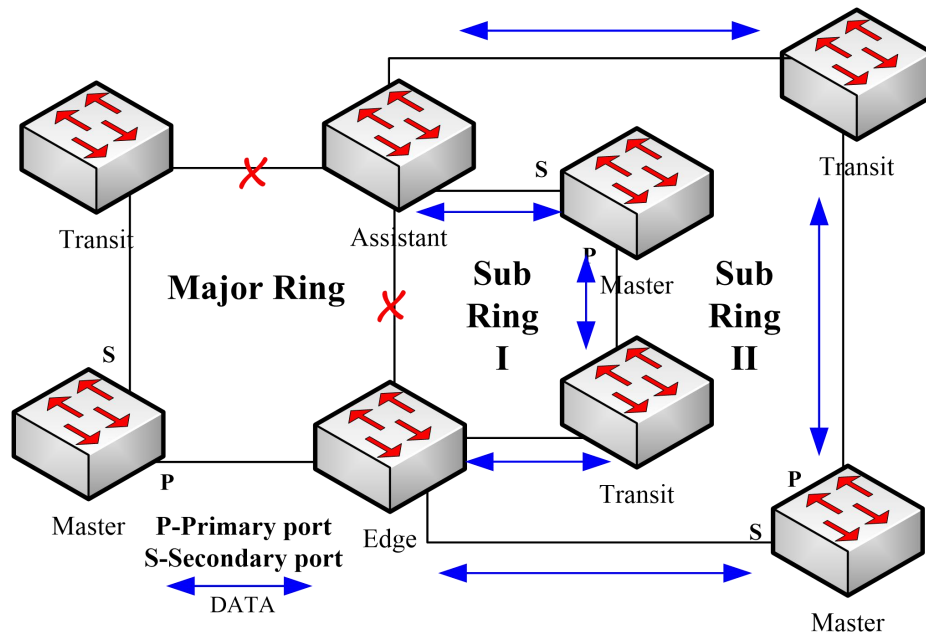


Figure 6 Broadcast storm triggered by the dual homing networking mode

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:

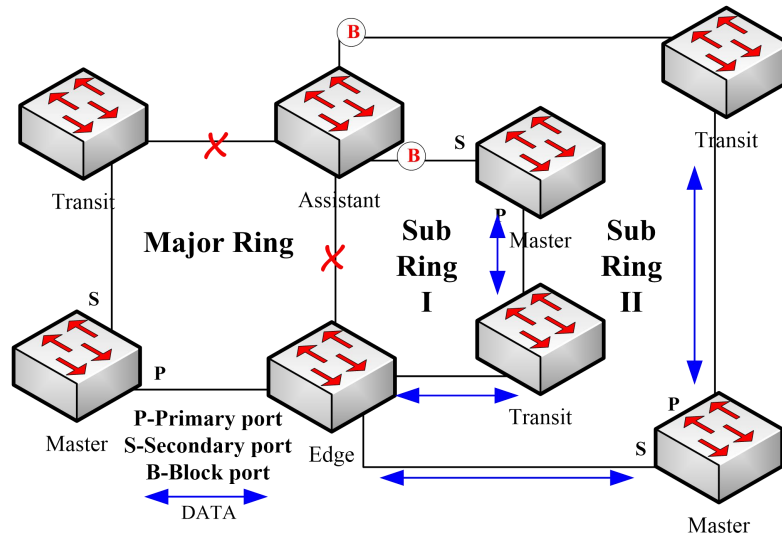


Figure 7 Results of the channel status checkup mechanism

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.

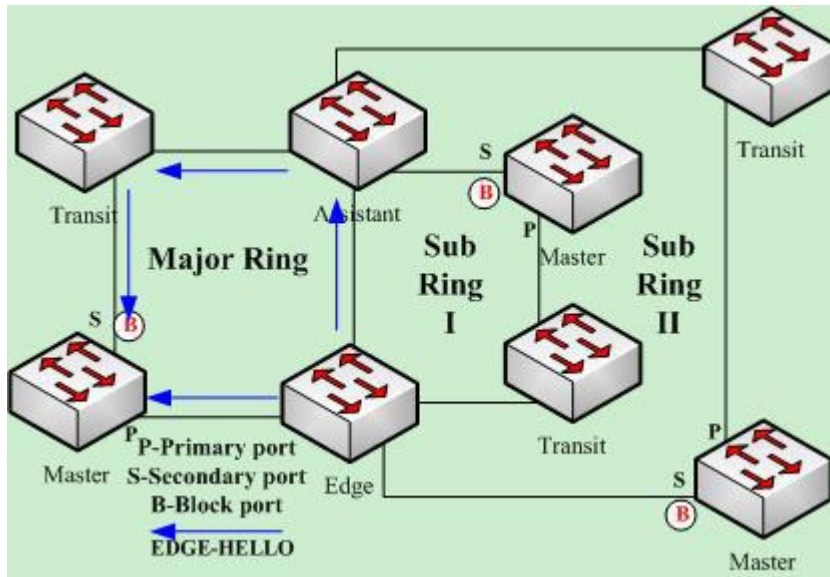


Figure 8 Check the channel status on the major ring between the edge node and the assistant node.

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. See Figure-9. If the assistant edge node cannot receive EDGE-HELLO packets forwarded by the edge node, the channel is interrupted. Therefore, the assistant edge node changes the status of edge port to Edge-Preforwarding and sending LINK-DOWN to notify the master node.

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.

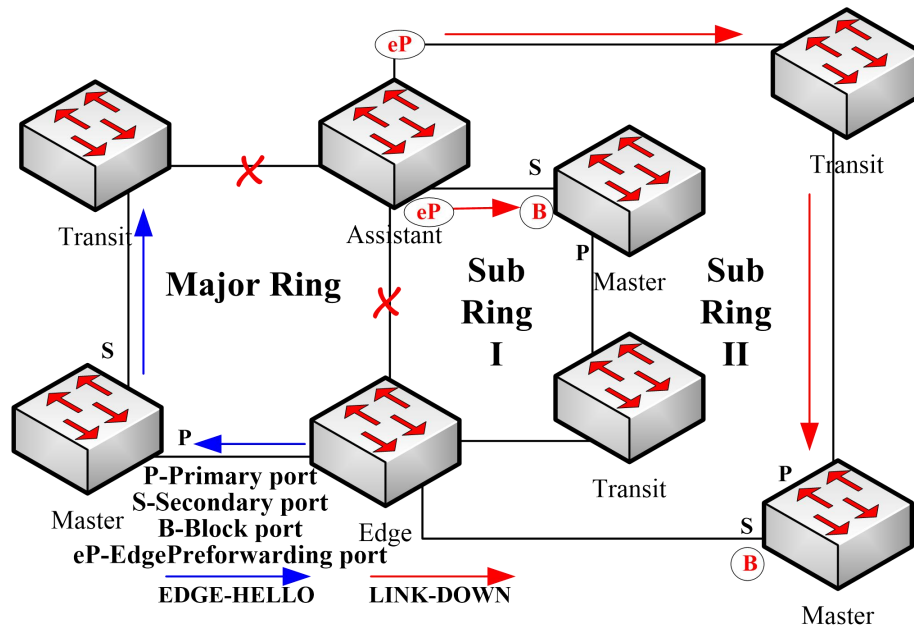


Figure 9 The edge node blocks the edge port at the interruption of the channel.

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.

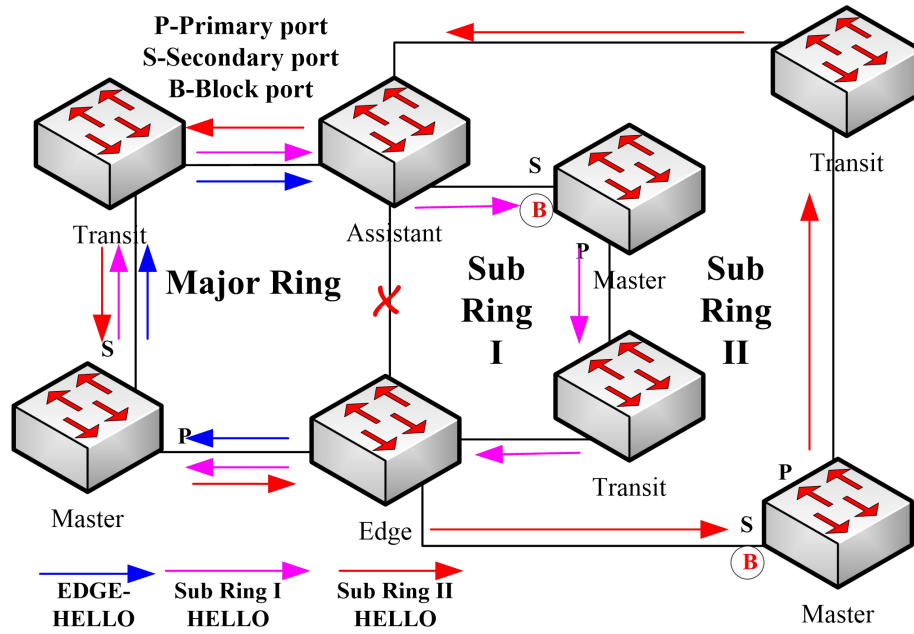


Figure 10 Channel recovery

Chapter 2 Fast Ethernet Ring Protection Configuration

2.1 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 instance, after configuring the master node and all transmission nodes, connect network cables for the secondary port the master node. If the ring network is connected in the case that the configuration is not finished, the broadcast storm may easily occur.
- Enable Ethernet ring protection protocol compatible with STP. The users are allowed to set “no spanning-tree”, SSTP, RSTP, PVST and MSTP.
- 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. But a same physical port cannot be simultaneously set to support MEAPS and EAPS.

2.2 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](#)

2.3 Fast Ethernet Ring Protection Configuration

2.3.1 Configuring the Master Node

Configure a switch to be the master node of a ring network according to the following steps:

Command	Purpose
Switch# config	Enters the switch configuration mode.
Switch_config# mether-ring id1 domain id2	Sets a node and enters the node configuration mode. <i>id1</i> :instance ID of a node; <i>id2</i> :instance ID of a domain(<i>id2</i> =0 can be omitted)
Switch_config_ring1# master-node	It is an obligatory step. Configures the node type to be a master node.

Switch_config_ring1# major-ring [sub-ring]	It is an obligatory step. Sets the node's level to be one of the major or sub ring node.
Switch_config_ring1# control-vlan <i>vlan-id</i>	It is an obligatory step. Sets the control VLAN and establishes VLAN "id" and VLAN "id+1". <i>vlan-id</i> : ID of the control VLAN
Switch_config_ring1# hello-time <i>value</i>	This step is optional. Configures the cycle for the master node to transmit the HEALTH packets. <i>value</i> :It is a time value ranging from 1 to 10 seconds and the default value is 3 seconds.
Switch_config_ring1# fail-time <i>value</i>	This step is optional. Configures the time for the secondary port to wait for the HEALTH packets. <i>value</i> :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.

2.3.2 Configuring the Transit Node

Configure a switch to be the transit node of a ring network according to the following steps:

Command	Purpose
Switch# config	Enters the switch configuration mode.
Switch_config# mether-ring id1 domain id2	Sets a node and enters the node configuration mode. <i>id1</i> :instance ID of a node; <i>id2</i> :instance ID of a domain(<i>id2</i>

	=0 can be omitted
Switch_config_ring1# transit -node	It is an obligatory step. Configures the node type to be a transit node.
Switch_config_ring1# major-ring[sub-ring]	It is an obligatory step. Sets the node's level to be one of the major or sub ring node.
Switch_config_ring1# control-vlan <i>vlan-id</i>	It is an obligatory step. Sets the control VLAN and establishes VLAN "id" and VLAN "id+1". <i>vlan-id</i> : ID of the control VLAN
Switch_config_ring1# pre-forward-time <i>value</i>	This step is optional. Run the following command to configure the time of maintaining the pre-forward state on the transit port. <i>value</i> :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#	

2.3.3 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 <i>id1</i> domain <i>id2</i>	Sets a node and enters the node configuration mode. <i>id1</i> :instance ID of a node; <i>id2</i> :instance ID of a domain(<i>id2</i> =0 can be omitted)
Switch_config_ring1# edge-node[assistant-node]	It is an obligatory step. 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 <i>vlan-id</i>	It is an obligatory step. Sets the control VLAN and establishes VLAN "id" and VLAN "id+1". <i>vlan-id</i> : ID of the control VLAN
Switch_config_ring1# pre-forward-time <i>value</i>	This step is optional. Configures the time of maintaining the pre-forwarding state of the edge port. <i>value</i> :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#	

2.3.4 Enters the switch configuration 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. <i>id1</i> :instance ID of a node; <i>id2</i> :instance ID of a domain(<i>id2</i> =0 can be omitted)
Switch_config_ring1# edge-node[assistant-node]	It is an obligatory step. 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	It is an obligatory step. Sets the control VLAN and establishes VLAN "id" and VLAN "id+1". <i>vlan-id</i> : ID of the control VLAN
Switch_config_ring2# single-subring-mode	It is an obligatory step. Without configuring the command, the Ethernet ring configuration can also be finished. However, it cannot enter the single ring networking mode. 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	This step is optional. Configures the time of maintaining the pre-forwarding state of the edge port. <i>value</i> :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#	

2.3.5 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 <i>intf-name</i>	Enters the interface configuration mode.
Switch_config_intf#mether-ring <i>id1 domain id2 primary-port [secondary-port transit-port common-port edge-port]</i>	Configures the type of the port of Ethernet ring. <i>id1</i> :instance ID of a node; <i>id2</i> :instance ID of a domain(<i>id2</i> =0 can be omitted)
Switch_config_intf#exit	Exits from interface configuration mode.

Note:

The command **no mether-ring** *id1 domain id2 primary-port [secondary-port | transit-port | common-port | edge-port]* can be used to delete the ring port configuration.

2.3.6 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	Browoses the summary information about the ring protection protocol and the ports of ring.
show mether-ring <i>id1 domain id2</i>	Browoses the summary information about the designated ring protection protocol and the ports of ring. <i>id1</i> :instance ID of a node; <i>id2</i> :instance ID of a domain(<i>id2</i> =0 can be omitted)
show mether-ring <i>id1 domain id2 detail</i>	Browoses the detailed information about the designated ring protection protocol and the port of Ethernet ring.
show mether-ring <i>id1 domain id2 interface intf-name</i>	Browoses the states of the designated ring ports or those of the designated common ports.

Chapter 3 Appendix

3.1 Working Procedure of MEAPS

MEAPS adopts three protection mechanisms to support the single-ring or evel-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.

3.1.1 Ethernet ring 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.

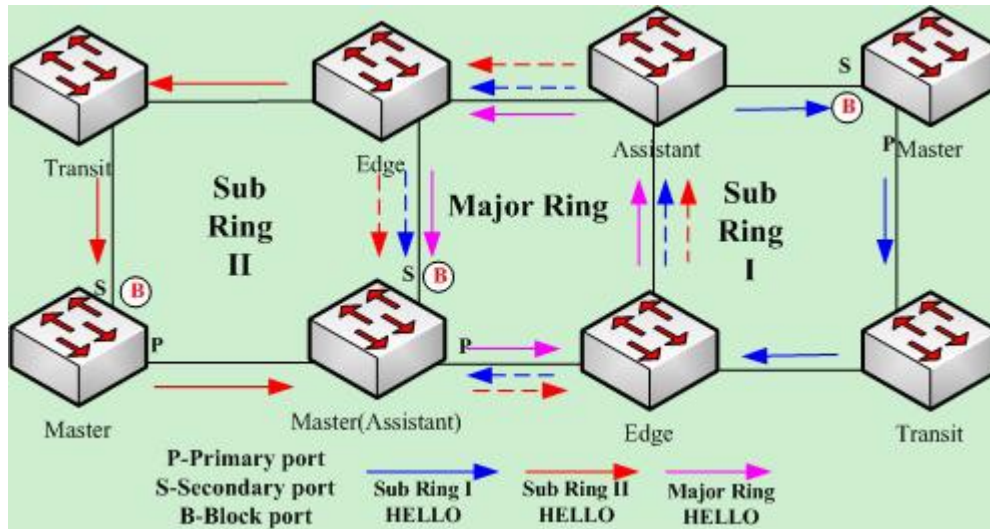


Figure 11 Complete state

3.1.2 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 complete 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.

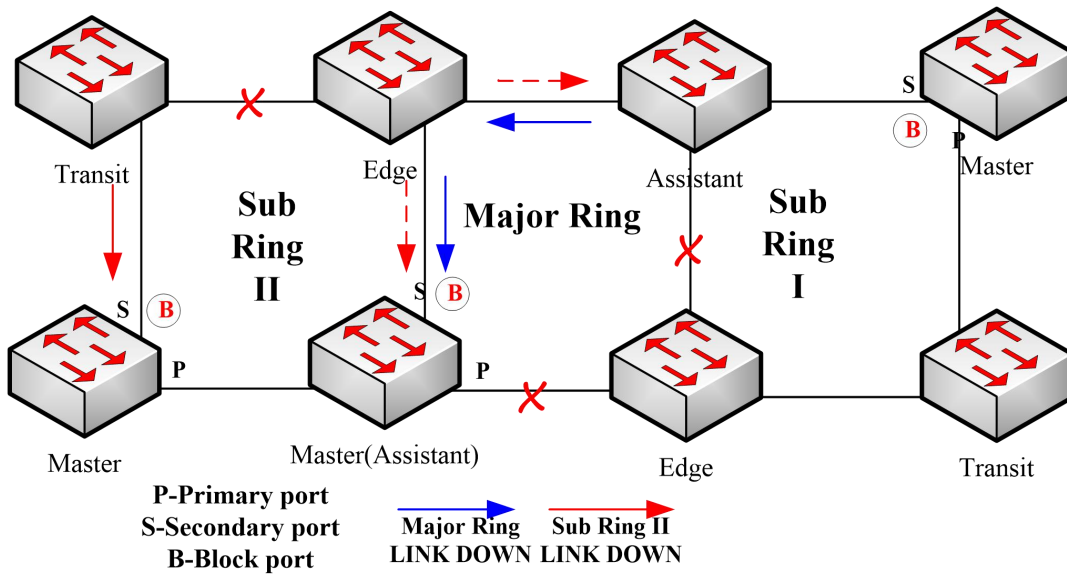


Figure 12 Ring transmitting the trouble and notifying the master node

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.

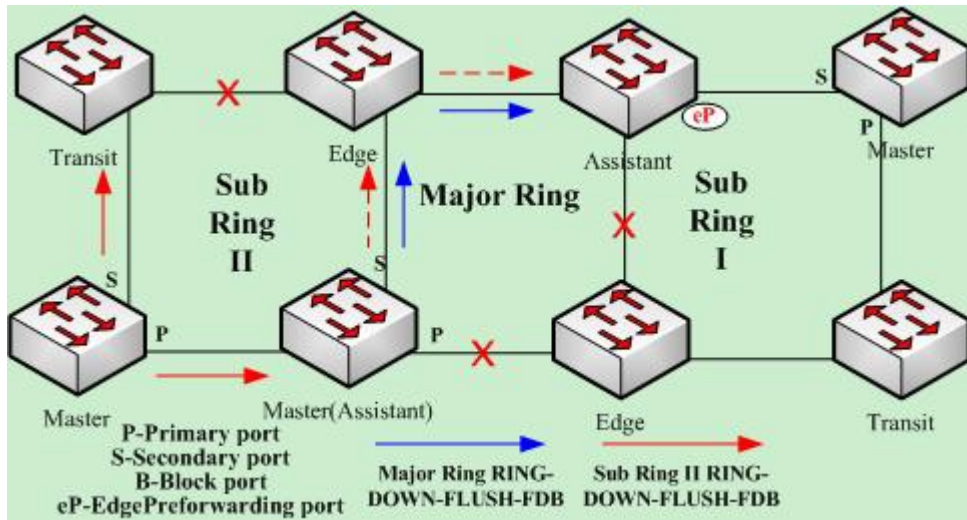


Figure 13 Ring transmitting troubles and refreshing FDB

3.1.3 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.

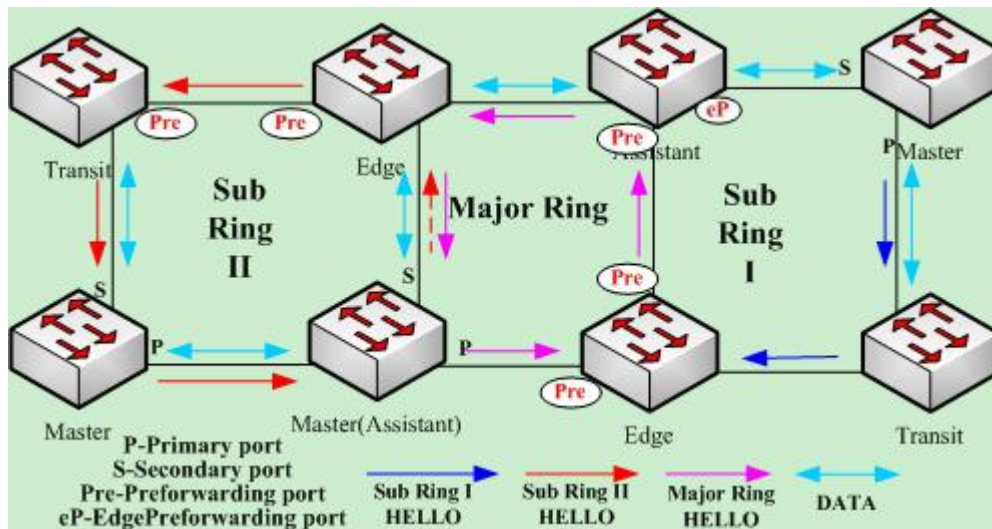


Figure 14 Recovery of the ring's link and the shift of the transit node to preforwarding

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.

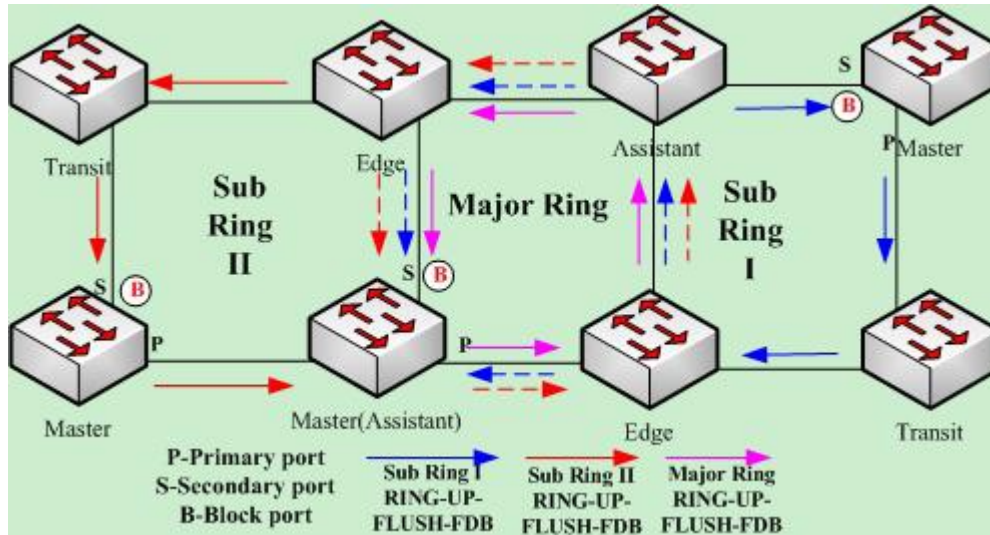


Figure 15 Recovery of the ring

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.

3.2 MEAPS configuration

3.2.1 Configuration Example

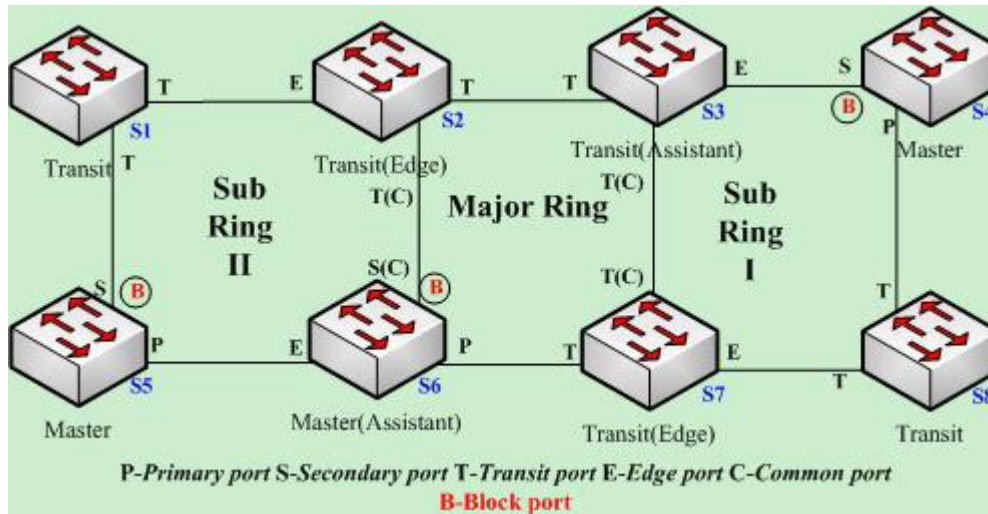


Figure 2.1 Fast Ethernet Ring Protection Configuration Example

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. 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 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 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 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 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 sub-ring edge node, 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 4:

```
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
```

3.3 Unfinished Configurations (to be continued)

- Basic non-configured information: ring network role, ring network class and control VLAN. There is one exception, when role edge-node or assistant-node is

configured for the node, the default class of the ring network is sub-ring. 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.

- Basic information conflict: the node role is edge-node or assistant-node, the default ring network class is sub-ring. When the configuration ring network class is major-ring, indication information will be shown.
- Major ring node missing on the sub-ring: when the node role is edge-node or assistant-node, the existence of its node is on the major ring node. If the sub-ring node of edge-node or assistant-node is created in a forced way without relevant major ring node, there will be indication information (look up the MEAPS status at this time with the command of show and the basic information is complete, but the indication information of state is still init, which shows that the ring network node configuration is not complete.)
- Control vlan configuration conflict: when the control vlan configured for the node conflicts with other nodes with finished configuration, there will be indication information (look up the MEAPS status at this time with the command of show and the basic information is complete, but the indication information of state is still init, which means that the ring network node configuration is not complete.)
- When the sub-ring node is configured based on the configuration of certain major ring node, the id of sub-ring node shall be larger than the id of corresponding major ring node; otherwise, the creation is unsuccessful and there will be indication information.

UDLD Configuration

Table of Contents

Chapter 1 Unidirectional Link Detection (UDLD).....	1
1.1 UDLD Overview.....	1
1.1.1 UDLD Mode.....	1
1.1.2 Running Mechanism.....	2
1.1.3 Port state.....	2
1.1.4 Maintaining the Cache of the Neighbor.....	2
1.1.5 Echo Detection.....	3
1.2 UDLD Configuration Task List.....	3
1.3 UDLD Configuration Tasks.....	3
1.3.1 Globally Enabling or Disabling UDLD.....	3
1.3.2 Enabling or Disabling the UDLD Interface.....	4
1.3.3 Sets the message interval of the aggressive mode.....	4
1.3.4 Restarts the interface shut down by UDLD.....	4
1.3.5 Displaying the UDLD State.....	5
1.4 Configuration Example.....	7
1.4.1 Network Environment Requirements.....	7
1.4.2 Network Topology.....	7
1.4.3 Configuration Procedure.....	7

Chapter 1 Unidirectional Link Detection (UDLD)

1.1 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 users.

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.

1.1.1 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.

1.1.2 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 FEF1 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 FEF1 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 16 seconds.

1.1.3 Port state

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.

1.1.4 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 temporarily 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.

1.1.5 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.

1.2 UDLD Configuration Task List

- Globally Enabling or Disabling UDLD
- Enabling or Disabling the UDLD Interface
- Setting the Message Interval of the Aggressive Mode
- Restarts the interface shut down by UDLD.
- Displaying the UDLD State

1.3 UDLD Configuration Tasks

1.3.1 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.

1.3.2 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.

1.3.3 Sets 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 <i>time</i>	Sets the message interval of the aggressive mode.

1.3.4 Restarts 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.

UDLD Configuration

Command	Purpose
udld reset	Restarts the interface shut down by UDLD.

1.3.5 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 <i>interface</i>	Run the following command to display 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 GigaEthernet0/1
---
Port enable administrative configuration setting: Enabled interface UDLD
configuration state
Port enable operational state: Enabled interface UDLD starting state
Current bidirectional state: Bidirectional or not
Current operational state: Advertisement                UDLD operating state
Message interval: 15                                  information interval
Time out interval: 5                                  timeout interval
    Entry 1                                           cache item
    ---
    Expiration time: 42                                expiration aging time
    Cache Device index: 1                              information index
number
    Device ID: CAT0611Z0L9                             neighbor device ID
    Port ID: GigaEthernet0/1                           Connecting interface
ID
    Neighbor echo 1 device: S35000202                 Neighbor's neighbor's
device ID
    Neighbor echo 1 port: GigaEthernet0/1             Neighbor's neighbor's
interface ID

    Message interval: 15                               neighbor's
```

UDLD Configuration

```

information interval
    Time out interval: 5                               neighbor's
timeout interval
    UDLD Device name: Switch

Interface GigaEthernet0/2
---
Port enable administrative configuration setting: Disabled
Port enable operational state: Disabled
Current bidirectional state: Unknown

Interface GigaEthernet0/3
---
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 g0/1
Interface GigaEthernet0/1
---
Port enable administrative configuration setting: Enabled interface UDLD
configuration state
Port enable operational state: Enabled interface UDLD starting state
Current bidirectional state: Bidirectional or not
Current operational state: Advertismment                UDLD operating state
Message interval: 15                                   information interval
Time out interval: 5                                   timeout interval
    Entry 1                                             cache item
    ---
    Expiration time: 42                                 expiration aging time
    Cache Device index: 1                               information index
number
    Device ID: CAT0611Z0L9                             neighbor device ID
    Port ID: GigaEthernet0/1                           Connecting interface
ID
    Neighbor echo 1 device: S35000202                 Neighbor's neighbor's ID
    Neighbor echo 1 port: GigaEthernet0/1             Neighbor's neighbor's
interface ID

    Message interval: 15                               neighbor's
information interval
    Time out interval: 5                               neighbor's
timeout interval
    UDLD Device name: Switch

```

1.4 Configuration Example

1.4.1 Network Environment Requirements

Configure LLDP protocol in the global configuration or on the port connecting two switches.

1.4.2 Network Topology

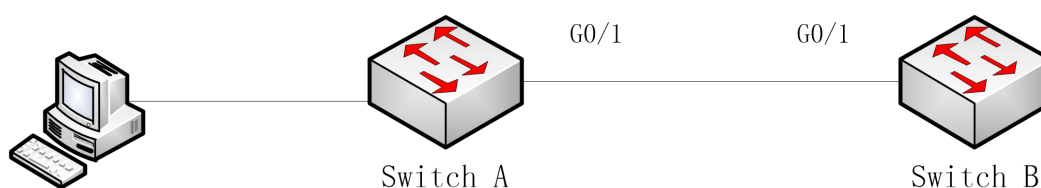


Figure 2 Network Topology

1.4.3 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
```

UDLD Configuration

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: Advertisement

Message interval: 15

UDLD Configuration

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: Advertisement

Message interval: 15

Time out interval: 15

Entry 1

Expiration time: 36

Cache Device index: 1

Device ID: S35043000

UDLD Configuration

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:

- 1.Detection phase: In this phase, the UDLD packets are transmitted every other second.
- 2.Unknown phase: In this phase, the UDLD packets are transmitted every seven seconds.
- 3.Known bidirectional/unidirectional connection phase: Once a link is established and labeled as bidirectional, UDLD will transmit a probe/echo message every 16 seconds.

IGMP-SNOOPING Configuration

Table of Contents

Chapter 1 IGMP-Snooping Configuration.....	1
1.1 IGMP-Snooping Configuration Tasks.....	1
1.1.1 Enabling/Disabling IGMP Snooping of VLAN.....	2
1.1.2 Adding/Deleting the Static Multicast Address of VLAN.....	2
1.1.3 Configuring Immediate-Leave of VLAN.....	2
1.1.4 Configuring the Static Routing Port of VLAN.....	3
1.1.5 Configuring IP ACL of Generating Multicast Forward Table.....	3
1.1.6 Configuring the Function to Filter Multicast Message without Registered Destination Address.....	3
1.1.7 Configuring the Router Age timer of IGMP-snooping.....	4
1.1.8 Configuring the Response Timer of IGMP Snooping.....	4
1.1.9 Configuring Querier of IGMP-snooping.....	5
1.1.10 Configuring Querier Time Timer of IGMP-snooping.....	5
1.1.11 Configuring Forward-L3-to-Mrouter of IGMP-Snooping to Forward the Data Packets to the Routing Port.....	6
1.1.12 Configuring the Sensitive Mode and Value of IGMP-Snooping.....	6
1.1.13 Configuring v3-leave-check of IGMP-Snooping.....	7
1.1.14 Configuring forward-wrongiif-within-vlan of IGMP-Snooping.....	7
1.1.15 Configuring IPACL of IGMP-snooping.....	7
1.1.16 Configuring max multicast IP address number of IGMP-snooping.....	8
1.1.17 IGMP-snooping monitoring and maintenance.....	8
1.1.18 IGMP-Snooping Configuration Example.....	10

Chapter 1 IGMP-Snooping Configuration

1.1 IGMP-Snooping Configuration Tasks

The task of IGMP-snooping is to maintain the relationship between VLAN and group address and to update simultaneously with the multicast changes, enabling the switch to forward data according to the topology structure of the multicast group. The main functions of IGMP-snooping are shown as follows:

- (1) Listening IGMP message;
- (2) Maintaining the relationship table between VLAN and group address;
- (3) 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 the Static Multicast Address of VLAN
- Configuring immediate-leave of VLAN
- Configuring the static routing port of VLAN
- Configuring IPACL of Generating Multicast Forward Table
- Configuring the function to filter multicast message without registereddestination address
- Configuring the Router Age timer of IGMP-snooping
- Configuring the Response Time timer of IGMP-snooping
- Configuring IGMP Querier of IGMP-snooping
- Configuring Querier Time Timer of IGMP-snooping
- Configuring Forward-L3-to-Mrouter of IGMP-Snooping to Forward the Data Packets to the Routing Port
- Configuring the Sensitive Mode and Value of IGMP-Snooping
- Configuring v3-leave-check of IGMP-Snooping
- Configuring forward-wrongiif-within-vlan of IGMP-Snooping.

- Configuring IPACL of IGMP-snooping
- Configuring max multicast IP address number of IGMP-snooping
- IGMP-snooping monitoring and maintenance
- IGMP-snooping Configuration Example

1.1.1 Enabling/Disabling IGMP Snooping of VLAN

Run the following commands in global configuration mode.

Command	Purpose
ip igmp-snooping [vlan <i>vlan_id</i>]	Enabling/Disabling IGMP Snooping of VLAN
no ip igmp-snooping [vlan <i>vlan_id</i>]	Resumes the default settings.

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 disabled.

For instance, to enable IGMP-snooping on VLAN3 and keep it after you restart the system, run command "no ip IGMP-snooping", then configure "ip IGMP-snooping VLAN 3" and save the configuration.

1.1.2 Adding/Deleting the Static Multicast Address of VLAN

Hosts that do not support IGMP can receive corresponding multicast message by configuring the static multicast address.

Run the following commands in global configuration mode.

Command	Purpose
ip igmp-snooping vlan <i>vlan_id</i> static <i>A.B.C.D</i> interface <i>intf</i>	Adds the static multicast address of VLAN.
no ip igmp-snooping vlan <i>vlan_id</i> static <i>A.B.C.D</i> interface <i>intf</i>	Deletes static multicast address of VLAN.

1.1.3 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.

Run the following commands in global configuration mode.

Command	Operation
ip igmp-snooping vlan <i>vlan_id</i> immediate-leave	Configures the immediate-leave function of the VLAN.
no ip igmp-snooping vlan <i>vlan_id</i> immediate-leave	Sets immediate-leave of VLAN to its default value.

The immediate-leave characteristic of VLAN is disabled by default.

1.1.4 Configuring the Static Routing Port 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 the following commands in global configuration mode.

Command	Purpose
ip igmp-snooping vlan <i>vlan_id</i> mrouter interface <i>intf</i>	Add the static routing port of VLAN.
no ip igmp-snooping vlan <i>vlan_id</i> mrouter interface <i>intf</i>	Delete the static routing port of VLAN.

1.1.5 Configuring IP ACL of Generating Multicast Forward Table

Run following commands 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 <i>word</i>	Adds IPACL in generating multicast forwarding table.
no ip igmp-snooping policy	Deletes IPACL in generating multicast forwarding table.

1.1.6 Configuring the Function to Filter Multicast Message without Registered Destination Address

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	Operation
---------	-----------

ip igmp-snooping dlf-drop	Drops multicast message whose destination fails to be found.
no ip igmp-snooping dlf-drop	Resume the default settings (forward)

Note:

- 1) The attribute is configured for all VLANs.
- 2) The default method for the switch to handle this type of message is forward (message of this type will be broadcasted within VLAN).

1.1.7 Configuring the Router Age timer of IGMP-snooping

The router age timer is used to monitor whether the IGMP querier exists or not; the IGMP querier maintenance is used to maintain and manage the multicast address by sending the query packets and IGMP snooping works by independence on the communication between IGMP querier and host.

Run the following commands in global configuration mode.

Command	Operation
ip igmp-snooping timer router-age <i>timer_value</i>	Sets the value of the router age of IGMP Snooping.
no ip igmp-snooping timer router-age	Resumes the default value of the router age of IGMP Snooping.

Note:

The settings of the timer requires to refer to the query period settings of the IGMP querier for it cannot be smaller than the query period; you are recommended to set the router age timer to the triple of the query period.

By default the router age timer is set to be 260 seconds of IGMP snooping.

1.1.8 Configuring the Response Timer of IGMP Snooping

The response time timer means the threshold time for the host to report the multicast after IGMP querier sends the query packets; if this report packet is not received after the timer ages, the switch will delete this multicast address.

Run the following commands in global configuration mode.

Command	Operation
ip igmp-snooping timer response-time <i>timer_value</i>	Sets the value of the response time of IGMP Snooping.
no ip igmp-snooping timer response-time	Resumes the default value of the response time of IGMP Snooping.

Note:

The value of the timer cannot be set too small, or the multicast communication may be unstable.

By default the response time is set to be 15 seconds of IGMP snooping.

1.1.9 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.

Run the following commands in global configuration mode.

Command	Operation
[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.

1.1.10 Configuring Querier Time Timer of IGMP-snooping

Querier Time timer is the time interval of the switch (acts as local IGMP query) forwards query packets. After aging, the timer broadcasts query packets within vlan.

Run the following commands in 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

The IGMP-snooping querier function is disabled by default. By default IGMP-snooping querier is shut down. The default time interval of Query messages is 200 seconds.

Note:

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.

1.1.11 Configuring Forward-L3-to-Mrouter of IGMP-Snooping to Forward the Data Packets to the Routing 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 initiated, all the downstream router ports can be learned. 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 L3 multicast is enabled in multiple switch cascading, the upstream devices can only learn the downstream vlan ports through the multicast routing protocol and there is no IGMP packet exchange between the upstream and downstream devices. Hence the snooping of the upstream devices cannot learn the specific physical ports that the downstream devices connect and the upstream devices will send the multicast packets to all physical ports in the local vlan. After this command is enabled, the upstream devices can forward the multicast packets to the physical ports that the downstream devices connect, preventing the multicast packets to be broadcast in the downstream vlan.

Run the following commands in global configuration mode.

Command	Operation
[no] ip igmp-snooping forward-l3-to-mrouter	Sets the forward-l3-to-mrouter function of IGMP-snooping.

By default, the IGMP-snooping forward-l3-to-mrouter is disabled.

Note:

This command can be used to send the data packets to the multicast routing port, but the switchchip can limit the source-data-port, so the data packets will not be sent to the port of source data, but to the downstream multicast routing port that is registered on PIM-SM.

1.1.12 Configuring the Sensitive Mode and Value of IGMP-Snooping

If IGMP-snooping sensitive is enabled, the router-age of mrouter in active state will be set to sensitive value when the port in trunk mode is shut down, and then the query packets will be sent out rapidly.

Run the following commands in global configuration mode.

Command	Operation
[no] ip igmp-snooping sensitive [value [3-30]]	Sets IGMP-snooping sensitive. The value parameter is the current router-age of mrouter in active state.

By default, IGMP-snooping sensitive is disabled.

Note:

When it is in sensitive mode, the update of router-age through sensitive value is only for the current period; the next router-age will resume to the time router-age.

1.1.13 Configuring v3-leave-check of IGMP-Snooping

If v3-leave-check of IGMP-snooping is enabled, the special query packet will be sent after the v3-leave packet is received; otherwise, no following actions will be taken after the v3-leave packet is received.

Run the following commands in global configuration mode.

Command	Operation
[no] ip igmp-snooping v3-leave-check	Sets v3-leave-check of IGMP-Snooping. After the v3-leave packet is received, the special query packet will be sent.

1.1.14 Configuring forward-wrongiif-within-vlan of IGMP-Snooping.

If forward-wrongiif-within-vlan of IGMP-snooping is enabled, the multicast packets that are received from the incorrect vlan interface will be taken to carry out L2 forward in the source VLAN and then forwarded to the relative group ports in the local vlan; otherwise, the multicast will be dropped.

Run the following commands in global configuration mode.

Command	Operation
[no] ip igmp-snooping forward-wrongiif-within-vlan	Sets forward-wrongiif-within-vlan of IGMP-snooping.

By default, IGMP-snooping forward-wrongiif-within-vlan is enabled.

Note:

The ip igmp-snooping forward-wrongiif-within-vlan command takes its importance only when L3 multicast is enabled.

1.1.15 Configuring IPACL of IGMP-snooping

Enable IPACL function of IGMP-snooping and determine the packets of some multicast IP address are to be deleted or ignored.

Run the following commands in physical interface configuration mode.

Command	Operation
---------	-----------

ip igmp-snooping policy word	Adding multicast message's IPACL which need to be dealt with port.
no ip igmp-snooping policy	Deleting multicast message's IPACL which need to be dealt with port.

1.1.16 Configuring max multicast IP address number of IGMP-snooping

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.

Run the following commands in physical interface 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.

1.1.17 IGMP-snooping monitoring and maintenance

Run the following commands in EXEC mode:

Command	Operation
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 groups	Displays information about the multicast group of IGMP-snooping.
show ip igmp-snooping statistics	Displays statistics information about 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
```

```
Dif-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);

Displays information about the multicast group of IGMP-snooping.

```
switch# show ip igmp-snooping groups
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

The following example shows the timers of IGMP snooping:

```
switch#show ip igmp-snooping timers
vlan 1 mrouter on port 3: 251 means the timeout time of the aging timer of the router.
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.
```

The IGMP snooping statistics information is displayed below:

```
switch#show ip igmp-snooping statistics
vlan 1
-----
v1_packets:0      IGMP v1  packet number
v2_packets:6      IGMP v2  packet number
v3_packets:0      IGMP v3  packet number
general_query_packets:5  Quantity of general query packets
special_query_packets:0  Quantity of special query packets
join_packets:6    Number of report packets
leave_packets:0   Number of Leave packets
send_query_packets:0  Rserveed statistics option
err_packets:0     Quantity of error packets
```

The information about IGMP snooping debug is shown below:

```

switch#debug ip igmp-snooping packet
Jan  1 02:22:28 IGMP-snooping: Receive IGMPv3 report from G0/1, vlan 1:
Jan  1 02:22:28 IGMP-snooping: Flood packet from G0/1 to vlan 1 rc = 0.
Jan  1 02:22:29 IGMP-snooping: Receive IGMPv3 report from G0/1, vlan 1:
Jan  1 2:22:29 AM IGMP-snooping: Flood packet from G0/1 to vlan 1 rc = 0.
Jan  1 2:22:38 AM IGMP-snooping: Receive IGMPv3 report from G0/1, vlan 1:
Jan  1 2:22:38 AM IGMP-snooping: Flood packet from G0/1 to vlan 1 rc = 0.
Jan  1 2:22:39 AM IGMP-snooping: Receive IGMPv3 report from G0/1, vlan 1:
Jan  1 2:22:39 AM IGMP-snooping: Flood packet from G0/1 to vlan 1 rc = 0.
Jan  1 2:23:11 AM IGMP-snooping: Receive IGMPv3 report from G0/1, vlan 1:
Jan  1 2:23:11 AM IGMP-snooping: Flood packet from G0/1 to vlan 1 rc = 0.
Jan  1 2:23:12 AM IGMP-snooping: Receive IGMPv3 report from G0/1, vlan 1:
Jan  1 2:23:12 AM IGMP-snooping: Flood packet from G0/1 to vlan 1 rc = 0.

```

The information about IGMP snooping debug timer is shown below:

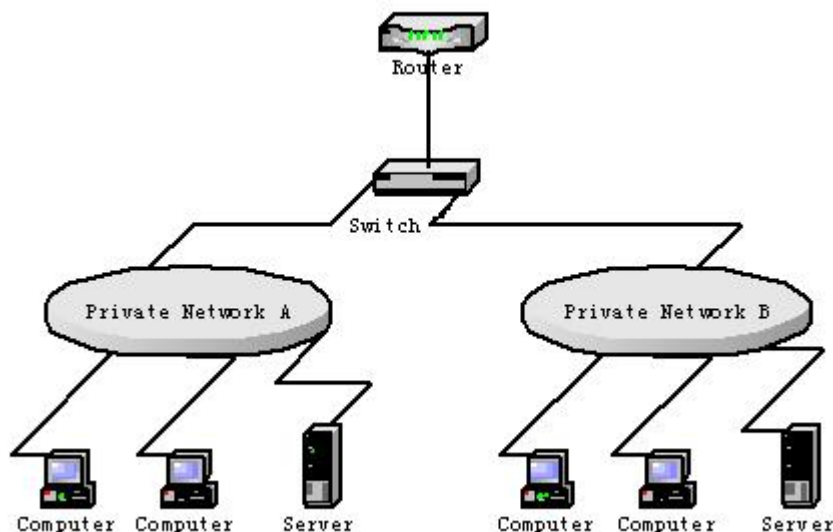
```

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. Inquering the
response timer expiry

```

1.1.18 IGMP-Snooping Configuration Example

The network topology is shown in figure 1.



Configuring Switch

- (1) Enable IGMP-snooping of VLAN 1 connecting Private Network A.

```
Switch_config#ip igmp-snooping vlan 1
```

- (2) Enable IGMP-snooping of VLAN 2 connecting Private Network B.

```
Switch_config#ip igmp-snooping vlan 2
```


OAM Configuration

Table of Contents

Chapter 1 OAM Configuration.....	1
1.1 OAM Overview.....	1
1.1.1 OAM Protocol's Attributes.....	1
1.1.2 OAM Mode.....	2
1.1.3 Components of the OAM Packet.....	3
1.2 OAM Configuration Task List.....	4
1.3 OAM Configuration Tasks.....	5
1.3.1 Enabling OAM on an Interface.....	5
1.3.2 Configuring OAM Link Monitoring.....	5
1.3.3 Configuring the Trouble Notification from Remote OAM Entity.....	7
1.3.4 Displaying the Information about OAM Protocol.....	8
1.4 Configuration Example.....	9
1.4.1 Network Environment Requirements.....	9
1.4.2 Network Topology.....	9
1.4.3 Configuration Procedure.....	9

Chapter 1 OAM Configuration

1.1 OAM Overview

EFM OAM of IEEE 802.3ah provides point-to-point link trouble/performance detection on the single link. However, EFM OAM cannot be applied to EVC and so terminal-to-terminal Ethernet monitoring cannot be realized. OAM PDU cannot be forwarded to other interfaces. Ethernet OAM regulated by IEEE 802.3ah is a relatively slow protocol. The maximum transmission rate is 10 frames per second and the minimum transmission rate is 1 frame per second.

1.1.1 OAM Protocol's Attributes

- Support 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.

1.1.2 OAM Mode

The device can conduct the OAM connection through two modes: active mode and passive mode. The device capacity in different mode is compared in table 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 there is a request that the peer must be in ACTIVE mode.	Yes
Allowing to transmit specified OAM PDU	Yes	Yes

After the Ethernet OAM connection is established, the OAM entities at two terminals maintain connection by transmitting the Information OAM PDU packets. If the Information OAM PDU packet from the peer OAM entity is not received in five seconds, the connection times out and a new OAM connection then requires to be established.

1.1.3 Components of the OAM Packet

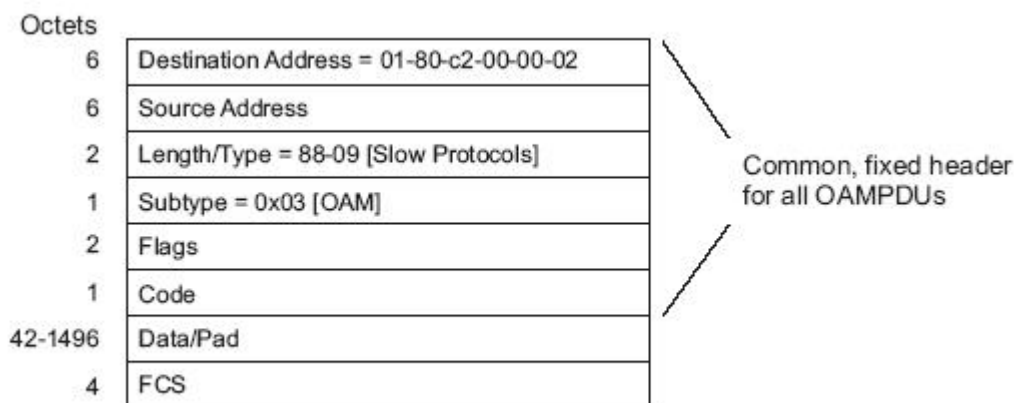


Figure 57-9—OAMPDU frame structure

Figure 1 Components of the OAM packet

The following are the meanings of the fields of the OAM packet:

- Destination address: means the destination MAC address of the Ethernet OAM packet.
- Source address: Source MAC address of the Ethernet OAM packet It is the MAC address of the transmitter terminal's port and also a unicast MAC address.
- Length/Type: Always adopts the Type encoding. The protocol type of the Ethernet OAM packet is 0x8809.
- Subtype: The subtype of the protocol for Ethernet OAM packets is 0x03.
- Flags: a domain where the state of Ethernet OAM entity is shown
- Code: a domain where the type of the OAMPDU packet is shown
- Data/Pad: a domain including the OAMPDU data and pad values
- checksum of the frame

Table 3 Type of the CODE domain

CODE	OAMPDU
00	Information
01	Event Notification
02	Variable Request
03	Variable Response
04	Loopback Control
05-FD	Reserved
FE	Organization Specific
FF	Reserved

The Information OAM PDU packet is used to transmit the information about the state of the OAM entity to the remote OAM entity to maintain the OAM connection.

The Event Notification OAMPDU packet is used to monitor the link and report the troubles occurred on the link between the local and remote OAM entities.

The Loopback control OAMPDU packet is mainly used to control the remote loopback, including the state of the OAM loopback from the remote device. The packet contains the information to enable or disable the loopback function. You can open or shut down the remote loopback according to the contained information.

1.2 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

1.3 OAM Configuration Tasks

1.3.1 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: <ul style="list-style-type: none"> ● 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 2 and 30 seconds and its default value is 5 seconds.

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.

1.3.2 Configuring OAM Link Monitoring

You can configure the low threshold and the high threshold of OAM link monitoring.

The procedure to configure the remote OAM trouble indication on an interface is shown in the following table:

Procedure	Command	Purpose
-----------	---------	---------

OAM Configuration

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}	<p>Sets the high and low threshold of the periodical event of the error signal, which triggers the error link events.</p> <p>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.</p> <p>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.</p> <p>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.</p>
Step5	ethernet oam link-monitor frame {threshold {high { symbols none} low {symbols}} window symbols}	<p>Sets the high and low thresholds of the error frame event, which triggers the link events of error frame.</p> <p>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.</p> <p>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.</p> <p>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.</p>
Step6	ethernet oam link-monitor frame-period {threshold {high { symbols none} low {symbols}} window symbols}	<p>Sets the high and low thresholds of the period event of error frame, which triggers the link events of error frame period.</p> <p>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.</p> <p>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.</p> <p>The window parameter is used to configure the window size of the round-query period. The unit of</p>

		<p>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.</p>
Step7	<p>ethernet oam link-monitor frame-seconds {threshold {high { symbols none} low {symbols}} window symbols}</p>	<p>Sets the high and low thresholds of the second event of error frame, which triggers the link events of error frame's second.</p> <p>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.</p> <p>The threshold high parameter is used to configure the low threshold. Its unit is second. It ranges between 0 and 900 and its default value is 1.</p> <p>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.</p>
Step8	<p>ethernet oam link-monitor receive-crc {threshold {high { symbols none} low {symbols}} window symbols}</p>	<p>Sets the high and low thresholds of the error CRC frame event, which triggers the link events of CRC checksum error.</p> <p>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.</p> <p>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.</p> <p>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.</p>

1.3.3 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: <ul style="list-style-type: none"> ● The critical-event parameter is used to enable an interface to enter the errdisabled state when an undesigned 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.

The 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. router can transmit and receive the Dying Gasp packet. When the local port enters the err disabled 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.

1.3.4 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. <ul style="list-style-type: none"> ● 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. The OAM running information includes the control variables in some

	protocols and the latest 10 times status changing records.
--	------------------------------------------------------------

1.4 Configuration Example

1.4.1 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.

1.4.2 Network Topology

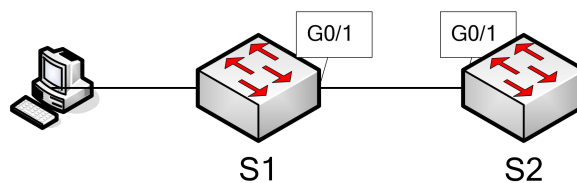


Figure 2 Network Topology

1.4.3 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.

CFM and Y1731 Configuration

Table of Contents

Chapter 1 Overview.....	1
1.1 Stipulation.....	1
1.1.1 Format Stipulation in the Command Line.....	1
Chapter 2 CFM Configuration.....	2
2.1 CFM Configuration Task List.....	2
2.2 CFM Maintenance Task List.....	2
2.3 CFM Configuration.....	2
2.3.1 Adding the Maintenance Domain.....	2
2.3.2 Adding the Maintenance Association.....	2
2.3.3 Adding MIP (Maintenance domain Intermediate Point).....	2
2.3.4 Adding MEP (Maintenance association End Point).....	3
2.3.5 Starting CFM.....	3
2.4 CFM Maintenance.....	3
2.4.1 Using the Loopback Function.....	3
2.4.2 Using the Linktrace Function.....	3
2.5 Configuration Example.....	4

Chapter 1 Overview

1.1 Stipulation

1.1.1 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.
<i>{italic}</i>	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.
< <i>italic</i> >	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.

Chapter 2 CFM Configuration

2.1 CFM Configuration Task List

- Adding the Maintenance Domain
- Adding the Maintenance Association
- Adding MIP (Maintenance domain Intermediate Point)
- Adding MEP (Maintenance association End Point)
- Starting CFM

2.2 CFM Maintenance Task List

- Using the Loopback Function
- Using the Linktrace Function

2.3 CFM Configuration

2.3.1 Adding the Maintenance Domain

Configuration mode: Global

Command	Purpose
ethernet cfm md mdnf {string} mdn <char_string> [level <0-7> creation <MHF_creation_type> sit <sender_id_type> ip <IP_address>]	Adds a maintenance domain whose name is char_string. Note: 【1】 The system enters the maintenance domain configuration mode after the maintenance domain is added.

2.3.2 Adding the Maintenance Association

Configuration mode: maintenance domain

Command	Purpose
ma manf {string} <char_string> ci {100ms 1s 10s 1min 10min} meps <mepids> [vlan <1-4094> creation <MHF_creation_type> sit <sender_id_type> ip <IP_address>]	Adds a maintenance association whose name is char_string.

2.3.3 Adding MIP (Maintenance domain Intermediate Point)

Configuration mode: physical interface

CFM Configuration

Command	Purpose
ethernet cfm mip add level <0-7> [vlan <1-4094>]	Adds a designated VLAN and hierarchical MIP to the designated physical interface.

2.3.4 Adding MEP (Maintenance association End Point)

Configuration mode: physical interface

Command	Purpose
ethernet cfm mep add mdnf {string} <char_string> manf {string} <char_string> mepid <1-8191> rmepid <1-8191> [direction {up down} ip <ip_address> lap {all mac rCCM eCCM xcon none}]	Adds a designated maintenance domain and an MEP to the designated physical interface.

2.3.5 Starting CFM

Configuration mode: Global

Command	Purpose
ethernet cfm {enable}	Starts CFM.

2.4 CFM Maintenance

2.4.1 Using the Loopback Function

Configuration mode: EXEC

Command	Purpose
ethernet cfm loopback mdnf {string} <char_string> manf {string} <char_string> mepid <1-8191> mac <AA:BB:CC:DD:EE:FF> number <1-64>	Uses a designated MEP to conduct loopback towards itself.

2.4.2 Using the Linktrace Function

Configuration mode: EXEC

Command	Purpose
ethernet cfm linktrace mdnf {string} <char_string> manf {string} <char_string> mepid <1-8191> mac	Uses a designated MEP to conduct loopback towards itself.

<pre><AA:BB:CC:DD:EE:FF> [ttl {1-255} fdb-only {yes}] <char_string> manf {string} <char_string> mepid <1-8191> mac <AA:BB:CC:DD:EE:FF> ttl <1-255></pre>	
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

2.5 Configuration Example

Users want to add a maintenance domain whose name is customer and hierarchy is 5, set a customer1 maintenance association for vlan1, configure the transmission interval of CCM of the maintenance association to 1s (MEP1, MEP2, MEP2009) and at last add an MEP whose MEPID is 2009 to physical port1 and designate its remote MEP as 2008.

```
Switch_config#ethernet cfm md mdnf string customer level 5
```

```
Switch_config_cfm#ma manf string customer1 vlan 1 ci 1s meps 1-2,2009
```

```
Switch_config_cfm#interface g0/1
```

```
Switch_config_g0/1#ethernet cfm mep add mdnf string customer manf string customer1 mepid
2009 mep 2008 direction DOWN lap ALL
```

```
Switch_config_g0/1#exit
```

```
Switch_config#ethernet cfm enable
```

DHCP-Snooping Configuration

Table of Contents

Chapter 1 DHCP-Snooping Configuration.....	1
1.1 IGMP-Snooping Configuration Tasks.....	1
1.1.1 Enabling/Disabling DHCP-Snooping.....	1
1.1.2 Enabling DHCP-Snooping in a VLAN.....	1
1.1.3 Enabling DHCP anti-attack in a VLAN.....	2
1.1.4 Setting an Interface to a DHCP-Trusting Interface.....	2
1.1.5 Enabling/Disabling binding table fast update function.....	2
1.1.6 Enabling DAI in a VLAN.....	3
1.1.7 Setting an Interface to an ARP-Trusting Interface.....	3
1.1.8 Enabling Source IP Address Monitoring in a VLAN.....	3
1.1.9 Setting an Interface to the One Which is Trusted by IP Source Address Monitoring.....	3
1.1.10 Setting DHCP-Snooping Option 82.....	4
1.1.11 Setting the Policy of DHCP-Snooping Option82 Packets.....	5
1.1.12 Setting the TFTP Server for Backing up Interface Binding.....	6
1.1.13 Setting a File Name for Interface Binding Backup.....	6
1.1.14 Setting the Interval for Checking Interface Binding Backup.....	6
1.1.15 Setting Interface Binding Manually.....	7
1.1.6 Monitoring and Maintaining DHCP-Snooping.....	7
1.1.17 Example of DHCP-Snooping Configuration.....	8

Chapter 1 DHCP-Snooping Configuration

1.1 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
- Enabling DHCP-Snooping in a VLAN
- Enabling DHCP anti-attack in a VLAN.
- Setting an Interface to a DHCP-Trusting Interface
- Enabling/Disabling binding table fast update function
- Enabling DAI in a VLAN
- Setting an Interface to an ARP-Trusting Interface
- Enabling Source IP Address Monitoring in a VLAN
- Setting an Interface to the One Which is Trusted by IP Source Address Monitoring
- Setting DHCP-Snooping Option 82
- Setting the Policy of DHCP-Snooping Option82 Packets
- Setting the TFTP Server for Backing up Interface Binding
- Setting a File Name for Interface Binding Backup
- Setting the Interval for Checking Interface Binding Backup
- Setting Interface Binding Manually
- Monitoring and Maintaining DHCP-Snooping
- Example of DHCP-Snooping Configuration

1.1.1 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.

1.1.2 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 <i>vlan_id</i>	Enables DHCP-snooping in a VLAN.
no ip dhcp-relay snooping vlan <i>vlan_id</i>	Disables DHCP-snooping in a VLAN.

1.1.3 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 <i>vlan_id</i> max-client <i>number</i>	Enabling DHCP anti-attack in a VLAN.
no ip dhcp-relay snooping vlan <i>vlan_id</i> max-client	Disables DHCP anti-attack in a VLAN.

1.1.4 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.

1.1.5 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.
-----------------------------------------------------	---------------------------------------------------------

1.1.6 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 <i>vlanid</i>	Enables dynamic ARP monitoring on all distrusted ports in a VLAN.
no ip arp inspection vlan <i>vlanid</i>	Disables dynamic ARP monitoring on all distrusted ports in a VLAN.

1.1.7 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.

1.1.8 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 <i>vlanid</i>	Enables source IP address checkup on all distrusted interfaces in a VLAN.
no ip verify source vlan <i>vlanid</i>	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.

1.1.9 Setting anInterface 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.

1.1.10 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]}	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]}	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.

1.1.11 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).

1.1.12 Setting 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 <i>ip-address</i>	Configures the IP address of the TFTP server which is to back up interface binding.
no ip dhcp-relay snooping database-agent <i>ip-address</i>	Cancel the TFTP Server for backing up interface binding.

1.1.13 Setting 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 <i>name</i> [timestamp]	Configures a file name for interface binding backup.
no ip dhcp-relay snooping db-file	Cancel a file name for interface binding backup.

1.1.14 Setting 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, it need be backed up again. The default time interval is 30mins.

Run the following commands in global configuration mode.

Command	Operation
<code>ip dhcp-relay snooping write-immediately</code>	Configures DHCP Snooping immediate backup when the binding information changes.
<code>no ip dhcp-relay snooping {write-time write-immediately}</code>	Resumes the interval of checking interface binding backup to the default settings.
<code>ip dhcp-relay snooping write-time num</code>	Configures the interval for checking interface binding backup. The unit is min.
<code>no ip dhcp-relay snooping write-time</code>	Resumes the interval of checking interface binding backup to the default settings.

1.1.15 Setting 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
<code>ip source binding MAC IP interface name [vlan vlan-id]</code>	Configures Interface Binding Manually
<code>no ip source binding MAC IP vlan vlan-id</code>	Cancels an interface binding item.

1.1.6 Monitoring and Maintaining DHCP-Snooping

Run the following commands in EXEC mode:

Command	Operation
<code>show ip dhcp-relay snooping</code>	Displays the information about DHCP-snooping configuration.
<code>show ip dhcp-relay snooping binding</code>	Displays the effective address binding items on an interface.
<code>show ip dhcp-relay snooping binding all</code>	Displays all binding items which are generated by DHCP snooping.
<code>[no] debug ip dhcp-relay [snooping </code>	Enables or disables the switch of DHCP

binding event all]	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:

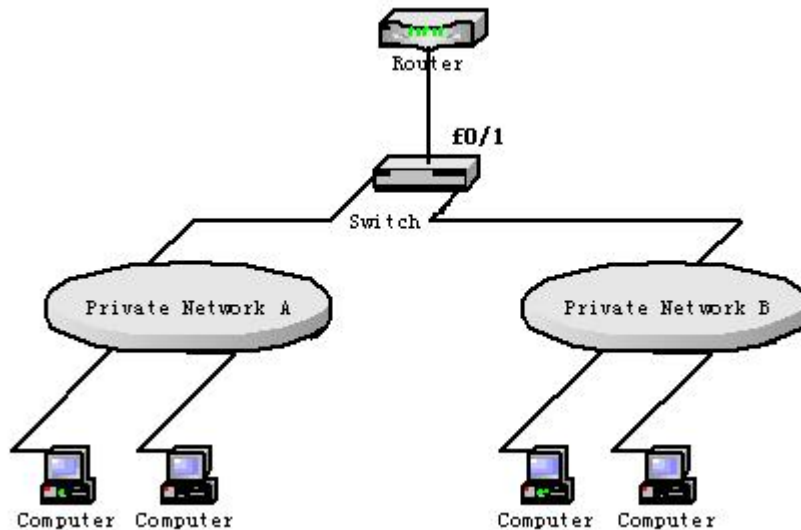
```
switch#show ip dhcp-relay snooping binding all
Hardware Address      IP Address      remainder time Type          VLAN      interface
00-e0-0f-32-1c-59    192.2.2.1      infinite          MANUAL     1
GigaEthernet0/2
00-e0-0f-26-23-89    192.2.2.101    86400             DHCP_SN    3
GigaEthernet0/3
```

The following shows 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
```

1.1.17 Example of DHCP-Snooping Configuration

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

MACFF Configuration

Table of Contents

Chapter 1 MACFF Configuration.....	1
1.1 MACFF Configuration Tasks.....	1
1.1.1 Enabling or Disabling MACFF.....	1
1.1.2 Enabling MACFF in VLAN.....	1
1.1.3 Configuring the Default AR of MACFF in VLAN.....	2
1.1.4 Configuring other ARs of MACFF in VLAN.....	2
1.1.5 Specifying a Physical Port to Shut down MACFF.....	2
1.1.6 Enabling MACFF Debugging.....	2
1.1.7 MACFF Configuration Example.....	3

Chapter 1 MACFF Configuration

1.1 MACFF Configuration Tasks

MACFF is to isolate downlink ports of the same VLAN in a switch from exchanging inter-access packets, enabling these packets to be allocated to the default gateway of client through DHCP server and then to downlink ports. By capturing the ARP packets between downlink ports, MACFF can prevent downlink ports from learn ARPs; MACFF replies the gateway's MAC address, enabling all inter-access packets among all downlink ports to pass through the gateway.

Note: MACFF needs the support of DHCP Snooping, so before enabling MACFF you have to make sure that DHCP Snooping works normally. ICMP redirection on the gateway is disabled by default. The VLAN management address must be configured for MACFF-enabled switch.

- Enabling MACFF in VLAN
- Configuring the Default AR of MACFF in VLAN
- Configuring other ARs of MACFF in VLAN
- Specifying a Physical Port to Shut down MACFF

1.1.1 Enabling or Disabling MACFF

Run the following commands in global configuration mode.

Command	Purpose
macff enable	Enables MACFF.
no macff enable	Resumes the default settings.

This command is used to enable MACFF in global configuration mode. After this command is run, all ARP packets are listened by switch.

Note: You have to make sure that DHCP Snooping is enabled before configuring this command. If the client obtains the address of a switch before this command is run, the switch cannot add the corresponding binding relationship.

1.1.2 Enabling MACFF in VLAN

If MACFF is enabled in a VLAN, the ARP packets received from all DHCP-snooping untrusted physical port of all VLAN will be monitored. If the destination IP address is the IP address of any DHCP client, on which the physical port that receives the ARP packets is located, these ARP packets will be dropped; if these are ARP response packets, these packets will also be dropped. If other DHCP client, default gateway or other service address requests from the port, their corresponding mac address will replay ARP request.

Note: The VLAN on which MACFF is enabled must be configured to have a management address. DHCP snooping shall also be enabled on this VLAN.

Run the following commands in global configuration mode.

Command	Purpose
macff vlan <i>vlan_id</i> enable	Enables MACFF in a VLAN.
no macff vlan <i>vlan_id</i> enable	Disables MACFF in a VLAN.

1.1.3 Configuring the Default AR of MACFF in VLAN

When you set the address on client manually (or DHCP server does not configure the default route option3, it is not recommended to use DHCP server in this way), the switch shall automatically enables default AR as the MACFF-specified default gateway. There is only one default AR.

Run the following commands in global configuration mode.

Command	Purpose
macff vlan <i>vlan_id</i> default-ar <i>A.B.C.D</i>	Sets the default AR of MACFF in VLAN.
no macff vlan <i>vlan_id</i> default-ar <i>A.B.C.D</i>	Deletes the default AR of MACFF in VLAN.

Note: Before configuring this command, you can run ip source binding *xx:xx:xx:xx:xx:xx* *A.B.C.D* interface name to add the client binding table on the switch. If you do not do this, MACFF will regard the manually configured client as illegal client and MACFF will not serve this client.

1.1.4 Configuring other ARs of MACFF in VLAN

After other ARs of MACFF are configured, MACFF allows DHCP client to access these ARs directly without forwarding packets via the default gateway allocated by DHCP server.

This function can be applied on some servers in the network segment of client or on other service addresses.

Run the following commands in global configuration mode.

Command	Purpose
macff vlan <i>vlan_id</i> other_ar <i>A.B.C.D</i>	Configures other ARs of MACFF in VLAN.
no macff vlan <i>vlan_id</i> other_ar <i>A.B.C.D</i>	Deletes other ARs of MACFF in VLAN.

1.1.5 Specifying a Physical Port to Shut down MACFF

If you specify a physical port to close MACFF, packets on this port will not be isolated and ARP packets will not be monitored.

Run the following commands in physical interface configuration mode.

Command	Operation
macff disable	Specifies a physical port to shut down MACFF.
no macff disable	Specifies a physical port to enable MACFF (it is enabled by default).

In default settings, the ports are allowed to enable MACFF.

1.1.6 Enabling MACFF Debugging

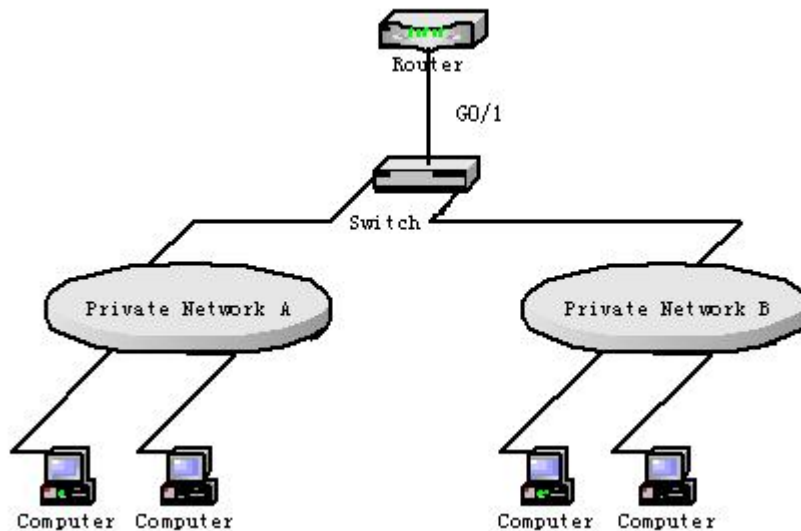
Run the following commands in global configuration mode.

Command	Operation
---------	-----------

debug macff	Enabling MACFF Debugging
no debug macff	Disabling MACFF Debugging

1.1.7 MACFF Configuration Example

The network topology is shown in figure 1.



Configuring Switch

Enable MACFF in VLAN1, which connects private network A. The default gateway allocated by DHCP server is 192.168.2.1.

```
Switch_config#arp 192.168.2.1 00:e0:0f:17:92:ed vlan 1
```

```
Switch_config#ip dhcp-relay snooping
```

```
Switch_config#ip dhcp-relay snooping vlan 1
```

```
Switch_config#macff enable
```

```
Switch_config#macff vlan 1 enable
```

Enable MACFF in VLAN2, which connects private network B. The default gateway allocated by DHCP server is 192.168.2.2 (If necessary, the default gateway can also be 192.168.2.1).

```
Switch_config#arp 192.168.2.2 00:e0:0f:ea:74:ee vlan 2
```

```
Switch_config#ip dhcp-relay snooping vlan 2
```

```
Switch_config#macff vlan 2 enable
```

(3) Sets the ports that connect DHCP server, default gateway and other ARs respectively to be trusted.

```
Switch_config_g0/1#dhcp snooping trust
```

(4) If the downlink host A of VLAN 1 is manually configured IP and default gateway, the IP address is 192.168.2.102 and the MAC address is 6c:62:6d:59:18:b7. The default gateway, 192.168.2.1, enables MACFF to take effect. (If the client is not configured manually, this step will not be performed)

```
Switch_config#arp 192.168.2.1 00:e0:0f:17:92:ed vlan 1
```

```
Switch_config#ip source binding 6c:62:6d:59:18:b7 192.168.2.102
interface GigaEthernet0/1
```

```
Switch_config#macff vlan 1 default-ar 192.168.2.1
```

(5) Specify a physical port in MACFF-enabled VLAN to shut down MACFF.

```
Switch_config_g0/1#macff disable
```

(6) Configures other ARs that are in the same network segment of client. MACFF allows the client to perform direct access without the help of gateway. (The ports where other APs are should be set to trusted ports)

```
Switch_config_g0/1#macff disable
```

Layer-2 Tunnel Configuration

Table of Contents

Chapter 1 Layer-2 (L2) Tunnel Protocol Configuration.....	1
1.1 Overview.....	1
1.2 Layer-2 (L2) Tunnel Protocol Configuration.....	1
1.3 L2 Protocol Tunnel Configuration Example.....	1

Chapter 1 Layer-2 (L2) Tunnel Protocol Configuration

1.1 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.

1.2 Layer-2 (L2) Tunnel Protocol Configuration

Run the following commands to set the L2 tunnel function on a L2 protocol:

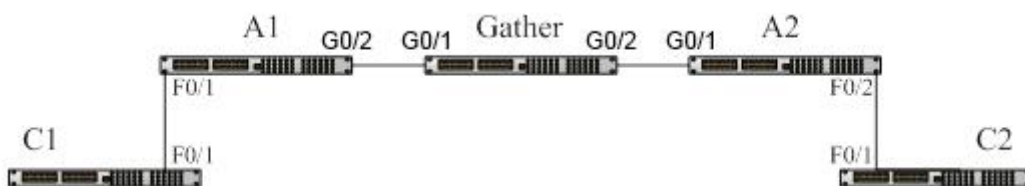
Command	Usage Guidelines
config	Enters the global configuration mode.
interface <intf_name>	Enters the interface configuration mode of an OLT port. Only the OLT ports support the L2 tunnel (including physical ports and aggregation ports)
[no] l2protocol-tunnel [stp]	Sets the L2 protocol, which is used to enable the tunnel function, on this OLT 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.

1.3 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:

- (1) 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.
- (2) 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.

Loopback Detection Configuration

Table of Contents

Chapter 1 Loopback Detection Configuration.....	1
1.1 Introduction to Loopback Detection.....	1
1.1.1 Format of Loopback Detection Packet.....	1
1.2 Loopback Detection Configuration Task List.....	2
1.3 Loopback Detection Configuration.....	2
1.3.1 Configuring Global Loopback Detection.....	2
1.3.2 Configuring Loopback Detection of the Port.....	3
1.3.3 Configuring Loopback Detection for Certain VLANs.....	3
1.3.4 Configuring Loopback Detection Time.....	3
1.3.5 Configuring Loopback-Detection Control.....	3
1.3.6 Configuring Loopback Detection Destination MAC.....	4
1.3.7 Configuring Loopback Detection Existence.....	4
1.3.8 Configuring the Upper Threshold the Loop Detection Frame Received Every Minute.....	5
1.3.9 Configuring to Enable or Disable Frame Number Detection Function.....	5
1.3.10 Showing Loopback Detection Global Configuration Information.....	5
1.3.11 Showing Loopback Detection Interface.....	5
1.4 Configuration Example.....	5

Chapter 1 Loopback Detection Configuration

1.1 Introduction to Loopback Detection

Loopback in the network may cause the equipment repeatedly forward the broadcast, multicast and unknown unicast, resulting in the waste of network resources or the network breakdown. In order to timely inform the user the conditions of the network connection and configuration, a detection mechanism is necessary. So there is the Loopback Detection. It can detect if there is a loopback in the port of the equipment, i.e. forward packets from the port regularly and detect whether the packets are sent back from the forwarding port. If there is a loopback in the port, Loopback Detection will forward the warning information timely to the network management system. Thus, the equipment can avoid long-time off-line. Besides, the equipment supports three modes of port controls: block, no MAC learning, and shutdown (error-disable).

The OLT supports:

- the loopback detection of the port;
- the destination MAC address of the loopback detection packet; the loopback detection packet forwarded by each port can be configured;
- the loopback detection for certain VLANs (at most 10) ;
- the loopback-detection hello-time and loopback-detection recovery-time;
- three modes of port controls: block, no MAC learning, and shutdown (error-disable);
- loopback detection existence configuration.

1.1.1 Format of Loopback Detection Packet

Field	Length/Byte	Value
DMAC	6	0x0180C2B0000A (Default, can be configured)
SMAC	6	MAC address of OLT system
TPID	2	0x8100,VLAN tag type
TCI	2	The concrete value of VLAN tag, priority, VLAN ID
TYPE	2	Type: Protocol type, value 0x9001

Loopback Detection Configuration

CODE	2	The subtype of the protocol, represents loopback detection, value 0x0001
VERSION	2	0x0000, reserve at present
Length	2	0x0008, the length of the loopback detection packet head
RESERVE	2	Reserve the field
SYSMAC	6	MAC address of OLT system
SEQUENCE	4	Serial number of the packet, it will be automatically generated before forwarding the packet
DiID	4	Port number, the 85 product is global port number
End	2	0x0000 end mark

1.2 Loopback Detection Configuration Task List

- Configuring Global Loopback Detection
- Configuring Loopback Detection of the Port
- Configuring Loopback Detection for Certain VLANs
- Configuring Loopback Detection Time
- Configuring Loopback-Detection Control
- Configuring Loopback Detection Destination MAC
- Configuring Loopback Detection Existence
- Configuring the Upper Threshold the Loop Detection Frame Received Every Minute
- Configuring to Enable or Disable Frame Number Detection Function
- Showing Loopback Detection Global Configuration Information
- Showing Loopback Detection Interface

1.3 Loopback Detection Configuration

1.3.1 Configuring Global Loopback Detection

Enable or disable the global loopback detection. The global commands are invalid for all physical ports. The loopback detection will take effect only when enabling the global loopback detection. The port configuration is invalid if the loopback detection disables.

Command	Purpose
[no] loopback-detection	Configure the global loopback detection.

1.3.2 Configuring Loopback Detection of the Port

This command can be used to enable or disable loopback detection on a specified port. However, this settings takes effect only after loopback detection is enabled globally.

Command	Purpose
[no] loopback-detection enable	Configuring Port Loop Check

1.3.3 Configuring Loopback Detection for Certain VLANs

After loopback detection is configured on a specified VLAN, the port transmits multiple detection packets of specified VLAN tag regularly and the number of these detection packets transmitted by this port can be up to 10.

Note that: The port must be in the configured VLAN and the VLAN must be created, or the configuration is invalid. Specifically, if the port configures the loopback detection to the trunk mode in VLAN2-VLAN8 and trunk vlan-allowed is VLAN 5-8, packets with 2-4tag from OLT cannot be forwarded through the port and the configuration is invalid. Meanwhile, configure trunk vlan-untagged to 2-8, so that the forwarded packets with vlan tag. The relevant VLAN must be created, or the tag with VLAN id will be invalid.

Command	Purpose
[no] loopback-detection vlan-control <i>vlanlist</i>	Configure the loopback detection for certain VLANs

1.3.4 Configuring Loopback Detection Time

Command	Purpose
[no] loopback-detection hello-time <i>time</i>	Configure loopback-detection recovery-time

As the network is in change, the loopback detection is a lasting process. The port forwards loopback detection packets regularly. The time interval, i.e. loopback-detection hello-time is 3 seconds in default.

Command	Purpose
[no] loopback-detection recovery-time <i>time</i>	Configure loopback-detection recovery-time

Configure the recovery time after the loopback is disappeared. The loopback is regarded to be disappeared if the port doesn't receive the forwarded loopback detection packet in 10s. It is recommended that the recovery time is at least 3 times of the packet forwarding time and the recovery time is more than 10s than the hello-time.

1.3.5 Configuring Loopback-Detection Control

Command	Purpose
---------	---------

Loopback Detection Configuration

[no] loopback-detection control {block learning shutdown}	Configure loopback detection control
----------------------------------------------------------------------------	--------------------------------------

If there is a loopback in the network, control the port by command `[no] loopback-detection control`. The port has three controlled modes: block, no MAC learning, shutdown (error-disable). The trap warning information will be forwarded no matter what control mode is configured. The trap configuration is by default.

After loopback detection is enabled globally, the port on which loopback detection is enabled transmits the loopback detection packets and receives the already transmitted loopback detection packets. Four control actions are conducted on the port:

Block: When detecting the loopback, the port will be isolated from other ports and the data forwarded into the port cannot be forwarded to other ports. When the port is in the state of protocol down, the MAC address table will age simultaneously.

Nolearn: Prohibit port MAC learning. When detecting the loopback, the port will have no MAC learning but the MAC address table ages.

Shutdown: Disable the port. When detecting the loopback, the port forwards trap warning information, ages the MAC address table and automatically disables the port (error-disable). Thus, the port cannot forward the packet until the error-disable-recover time.

Trap: The port only report warning. When detect the loopback, the port only reports warning and ages MAC address. The default controlled configuration of the port is trap.

When the port is in block, the packet will not be forwarded into it and the port will continue forward the loopback detection packet. When the loopback disappears in detection, the port will automatically recover. By default, if the forwarded loopback detection packet is not received in 10s, the loopback will be regarded as disappeared. In block state

In block, the port protocol is down; in shutdown, the port link is directly down.

1.3.6 Configuring Loopback Detection Destination MAC

Command	Purpose
[no] loopback-detection dest-mac <i>Mac-address</i>	Configure the loopback detection dest-mac address

The default loopback detection destination mac is 01-80-C2-00-00-0a. If the user has configured, the MAC address configured by the user will be taken as the destination mac address.

1.3.7 Configuring Loopback Detection Existence

Command	Purpose
[no] loopback-detection existence	Configure loopback detection existence

This command is mainly used to solve the problem that loopback exists on a port or not when this port is up and its loopback detection function takes effect. When the controlled action of this port is set to shutdown, it is improper to regard that loopback exists on this port for a shutdown port has already not forwarded packets. There is no loopback by default.

1.3.8 Configuring the Upper Threshold the Loop Detection Frame Received Every Minute

Command	Purpose
[no] loopback-detection frames-threshold <i>frames-threshold</i>	Configures the upper threshold the loop detection frame received every minute.

Configures the upper threshold the loop detection frame received every minute. The default value is 10.

1.3.9 Configuring to Enable or Disable Frame Number Detection Function

Command	Purpose
[no] loopback-detection frames-monitor	Configures to enable or disable frame number detection function

Configures to enable or disable frame number detection function

1.3.10 Showing Loopback Detection Global Configuration Information

Command	Purpose
show loopback-detection	Show global loopback detection configuration

It is mainly used for showing global loopback detection information, including global configuration, loopback existence and some configuration information.

1.3.11 Showing Loopback Detection Interface

Command	Purpose
show loopback-detection interface <i>intf</i>	Show loopback detection interface

It is mainly used for showing loopback detection information, including the timer value and the packet information.

1.4 Configuration Example

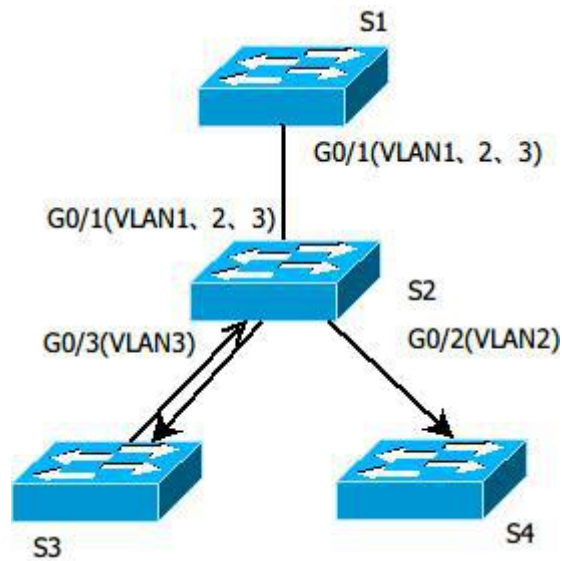


Figure 1.1 Loopback Detection Configurations

As shown in Figure 1.1, port OLT S1 designates loopback detection of certain VLAN (1,2,3):

Switch S1:
 Configure interface GigaEthernet0/1:
 switchport trunk vlan-untagged 1-3
 switchport mode trunk
 loopback-detection enable
 loopback-detection control block
 loopback-detection vlan-control 1-5
 Global Configuration:
 loopback-detection
 vlan 1-3

Switch S2:
 Configure interface GigaEthernet0/1:
 switchport mode trunk
 Configure interface GigaEthernet0/2:
 switchport mode trunk
 Configure interface GigaEthernet0/3:
 switchport mode trunk
 Global Configuration:
 vlan1-3

Switch S3:
 Configure interface GigaEthernet0/1:
 switchport pvid 3

If S3 has loopback and PVID of the port is 3, the packets will forward back to G5/1 of S1. S1 will block G5/1 if there is loopback.

QoS Configuration

Table of Contents

Chapter 1 QoS Configuration.....	1
1.1 QoS Overview.....	1
1.1.1 QoS Concept.....	1
1.1.2 Terminal-To-Terminal QoS Model.....	1
1.1.3 Queue Algorithm of QoS.....	2
1.1.4 Weighted Random Early Detection.....	3
1.2 QoSConfiguration Task List.....	4
1.3 QoS Configuration Tasks.....	5
1.3.1 Setting the GlobalCoSPriority Queue.....	5
1.3.2 Setting the Bandwidth of the CoS Priority Queue.....	5
1.3.3 Setting the Schedule Policy of the CoS Priority Queue.....	6
1.3.4 Setting the Default CoS Value of a Port.....	6
1.3.5 Setting the CoS Priority Queue of a Port.....	7
1.3.6 Setting the CoS Priority Queue of a Port.....	7
1.3.7 Setting the Schedule Policy of the CoS Priority Queue of the Port.....	8
1.3.8 Setting the CoS Priority Queue based on dscp.....	8
1.3.9 Establishing the QoS Policy Mapping.....	9
1.3.10 Setting the Description of the QoS Policy Mapping.....	9
1.3.11 Setting the Matchup Data Flow of the QoS Policy Mapping.....	9
1.3.12 Setting the Actions of the Matchup Data Flow of the QoS Policy Mapping.....	11
1.3.13 Applying the QoS Policy on a Port.....	12
1.3.14 Applying QoS policy globally.....	12
1.3.15 Setting the trust mode.....	13
1.3.16 Displaying the QoS Policy Mapping Table.....	13
1.4 QoS Configuration Example.....	13
1.4.1 Example for Applying the QoS Policy on a Port.....	13

Chapter 1 QoS Configuration

If you care to use your bandwidth sufficiently and your network resources efficiently, you must pay attention to QoS configuration.

1.1 QoS Overview

1.1.1 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.

1.1.2 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.

1. 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

forehand 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).

2. 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).

1.1.3 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).

1. 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.

2. 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.

3. (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.

4. 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.

1.1.4 Weighted Random Early Detection

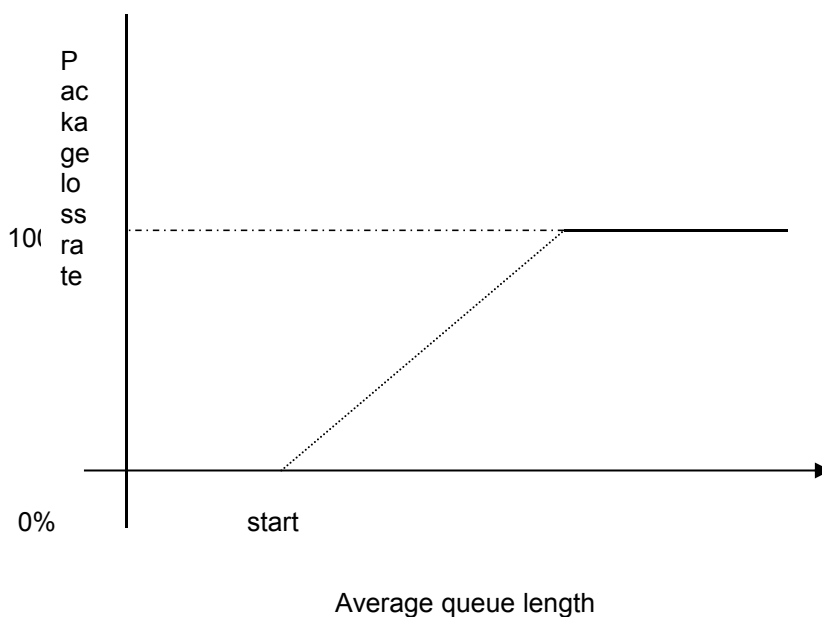
Congestion avoidance and traditional packet loss mechanism

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. Congestion prevention is a mechanism of traffic control, which monitors the network resource and drop the packet autonomously when the network is in overload. 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 SRED algorithm is adopted to prevent TCP global synchronization. SRED 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 SRED 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. SRED 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.

SRED 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, Slope and Drop priority. Parameters of each queue can be configured according to the requirement.



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, the higher the drop rate.

The drop rate increases linearly with the queue length.

1.2 QoSConfiguration 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 GlobalCoSPriority Queue
- [Setting the Bandwidth of theCoSPriority Queue](#)
- [Setting the Schedule Policy of theCoSPriority Queue](#)
- [To set](#) the minimum bandwidth or the maximum bandwidth of the port cos queue, run the previous commands.
- Setting Weighted SRED (Simple Random Early Detection)
- [Setting the DefaultCoSValue of a Port](#)
- [Setting theCoSPriority Queue of 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
- [Displaying the QoS Policy Mapping Table](#)
- Setting the trust mode.

1.3 QoS Configuration Tasks

1.3.1 Setting the GlobalCoSPriority 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 aCoSPriority 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 privileged mode and run the following commands as follows to setCoSPriority queue.

Command	Purpose
config	Enters the global configuration mode.
[no] cos map <i>quid cos1..cosn</i>	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 .

1.3.2 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 as follows to set the bandwidth of theCoSPriority queue.

Command	Purpose
config	Enters the global configuration mode.
[no] scheduler weight bandwidth <i>weight1...weightn</i>	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.

1.3.3 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 EXEC 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.

1.3.4 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 EXEC 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.

QoS Configuration

[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.

1.3.5 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 globalCoSpriority queue.

Enter the privilege mode and run the following commands to set the defaultCoSvalue 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.

1.3.6 Setting the CoS Priority Queue of a Port

When a bandwidth of the priority queue is set on a L2 port, the bandwidth of the priority queue will be used by the L2 port; otherwise, you should conduct the configuration of a globalCoSpriority queue.

Run the following commands as follows to set the bandwidth of theCoSpriority queue.

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.

QoS Configuration

exit	Goes back to the EXEC mode.
write	Saves the settings.

1.3.7 Setting the Schedule Policy of the CoS Priority Queue of the Port

When a bandwidth of the priority queue is set on a L2 port, the schedule policy of the priority queue will be used by the L2 port; otherwise, you should conduct the configuration of a globalCoSschedule policy.

Enter the following EXEC configuration mode and set the schedule policy of CoS priority queue.

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.
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.
write	Saves the settings.

1.3.8 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 EXEC mode and run the following commands to set the defaultCoSvalue of a port.

Command	Purpose
config	Enters the global configuration mode.
[no]dscp map word { cos cos-value }	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.

1.3.9 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 EXEC 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 <i>name</i>	Entersthe configuration modeof the QoS policy map. <i>name</i> stands for the name of the policy.
exit	Exits from the global configuration mode.
exit	Goes back to the EXEC mode.

1.3.10 Setting the Description of the QoS Policy Mapping

Enter the EXEC 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 <i>name</i>	Entersthe configuration modeof the QoS policy map. <i>name</i> stands for the name of the policy.
description <i>description-text</i>	Sets the descriptionof the QoSpolicy. <i>description-text</i> stands for the text to describe the policy.
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.

1.3.11 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.

QoS Configuration

Enter the policy 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 <i>cos</i> icos <i>icos</i> vlan <i>vlanid</i> ivlan <i>ivlanid</i> ethernet-type <i>ethernet-type</i> precedence <i>precedence-value</i> dscp <i>dscp-value</i> tos <i>tos-value</i> diffserv <i>diffserv-value</i> ip <i>ip-access-list</i> ipv6 <i>ipv6-access-list</i> mac <i>mac-access-list</i> }	Matches up with any packet. Configures the matching COS value; the valid range is 0 to 7. Configures the matching interior tag COS value; the valid range is 0 to 7. <i>vlanid</i> stands for the matched VLAN, which ranges from 1 to 4094. <i>ivlanid</i> stands for the matched inner VLAN, which ranges from 1 to 4094. <i>ethernet-type</i> stands for the matched packet type, which is between 0x0600 and 0xFFFF. <i>precedence-value</i> stands for the priority field in tos of IP packet (5-7 of tos), which ranges from 0 to 7. <i>dscp-value</i> stands for the dscp field in tos of IP packet (2-7 of tos), which ranges from 0 to 63. <i>tos-value</i> stands for latency, throughput, reliability and cost fields in tos of IP packet(1-4 of tos), which ranges from 0 to 15. <i>diffserv-value</i> stands for the entire tos field: 8, 0-255. <i>ip-access-list</i> stands for the name of the matched IP access list. The name has 1 to 20 characters. <i>ipv6-access-list</i> stands for the name of the matched IP 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.
no classify { cos icos vlan ivlan ethernet-type precedence dscp tos diffserv ip ipv6 mac }	
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.

1.3.12 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 EXEC 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	Entersthe configuration modeof 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 addvlanid ivlanid} monitor session-value quequ quequ-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}	Max-band stands for the occupied maximum bandwidth: 1-65535. Unit: 16Kbps Configures policing. Configures policing. Sets the matched COS field to cos-value 0-7. drop means to drop the matched packets. 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 icos filed of matched flow, 0~7; ivlan ID Sets replacing or adding interior vlanid; the range is 1 to 4094. session-value Send the packets to monitor interface; the range is 1-4. quequ-value Sets the queue mapping value 1-8. Interface-id Redirects the egress port of the matched flow. Stat-packet Calculates the number of packets. Stat-byte Calculate the number of bytes. vlan ID Sets replacing or adding exterior vlanid; the range is 1-4094. copy-to-cpu Sets forwarding the packet to

QoS Configuration

	CPU.
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.

1.3.13 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 EXEC 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	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.
exit	Goes back to the global configuration mode.
exit	Goes back to the EXEC mode.

1.3.14 Applying QoS policy globally

Enter EXEC mode and run the following commands to apply the QoS policy globally.

Command	Purpose
config	Enters the global configuration mode.
[no] qos policy name ingress	Applying 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.

1.3.15 Setting the 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 queue by default.

Configuring the trust mode in EXEC mode as follows:

Command	Purpose
config	Enters the global configuration mode.
[no] qos trust { cos dscp untrust }	Configuring the trust mode in the global configuration mode. untrust means any mode is not trusted.
exit	Goes back to the EXEC mode.

1.3.16 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 EXEC mode to display the QoS policy mapping table.

Command	Purpose
show policy-map [<i>policy-map-name</i> <i>interface</i> <i>global</i>]	Displays all or some designated QoS policy maps. policy-map-name stands for the name of QoS mapping table. Interface means to apply the QoS policy on a port; Global means to apply QoS policy globally;

1.4 QoS Configuration Example

1.4.1 Example for Applying the QoS Policy on a Port

The following example shows how to configure a policy of dropping packets which meets IP access list on interface 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
```

QoS Configuration

```
policy-map pmap
classify ip ipacl
action drop
interface g0/2
qos policy pmap ingress
```

DoS Attack Prevention Configuration

Table of Contents

Chapter 1 DoS Attack Prevention Configuration.....	1
1.1 DoS Attack Overview.....	1
1.1.1 Concept of DoS Attack.....	1
1.1.2 DoS Attack Type.....	1
1.2 DoS Attack Prevention Configuration Task List.....	2
1.3 DoS Attack Prevention Configuration Tasks.....	2
1.3.1 Configuring Global Dos Attack Prevention.....	2
1.3.2 Configuring DOS Attack Prevention Function.....	2
1.4 DoS Attack Prevention Configuration Example.....	3

Chapter 1 DoS Attack Prevention Configuration

1.1 DoS Attack Overview

1.1.1 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.

1.1.2 DoS Attack Type

Hackers will make different types of DoS attack packets to attack the servers. The following are common DoS attack packets:

1.1.2.1 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.

1.1.2.2 TearDrop

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.

1.1.2.3 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.

1.1.2.4 Land Attack

The attacker makes a special SYN message (the source address and the destination address 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. Land attack can be classified into IP land

DoS Attack Prevention Configuration

and MAC land.

1.2 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:

1.3 DoS Attack Prevention Configuration Tasks

1.3.1 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 as follows:

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 drop packets longer than icmp-value, so that death PING attack can be prevented. The range of icmp-value is 0 to 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/UDP packets whose source port IDs are destination port IDs. Configures mac to prevent those packets whose source MAC addresses equal to destination MAC addresses. Configures tcpflags to prevent those TCP packets containing illegal TCP flags. Configures tcpfrag to prevent those TCP packets whose minimum TCP header is tcpfrag-value. Configures tcpsmurf to prevent those TCP packets whose destination addresses equal to broadcast addresses. Configures icmpsmurf to prevent those ICMP packets whose destination addresses equal to broadcast addresses. Configures ipsmurf to prevent those IP packets whose destination addresses equal to broadcast addresses.
exit	Goes back to the EXEC mode.
write	Saves the settings.

1.3.2 Configuring DOS Attack Prevention Function

You can display the Dos attack prevention configurations through the show command.

DoS Attack Prevention Configuration

Run the following command in EXEC mode to display the configured DoS attackprevention functions.

Command	Purpose
show dos	Displays Dos attack prevention configuration.

1.4 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 sourceIPs are destination IPs in global mode.

```
config
```

```
dos enable ip
```

Attack Prevention Configuration

Table of Contents

Chapter 1 Attack Prevention Introduction.....	1
1.1 Overview of Filter.....	1
1.2 The Mode of Filter.....	1
Chapter 2 Attack Prevention Configuration.....	2
2.1 Attack Prevention Configuration Tasks.....	2
2.2 Attack Prevention Configuration.....	2
2.2.1 Configuring the Attack Filter Parameters.....	2
2.2.2 Configuring the Attack Prevention Type.....	2
2.2.3 Enabling the Attack Prevention Function.....	3
2.2.4 Checking the State of Attack Prevention.....	3
Chapter 3 Attack Prevention Configuration Example.....	5
3.1 Using Filter ARP to Protect the LAN.....	5
3.2 Using Filter IP to Protect Layer-3 Network.....	5

Chapter 1 Attack Prevention Introduction

1.1 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 OLT 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.

1.2 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.

Chapter 2 Attack Prevention Configuration

2.1 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

2.2 Attack Prevention Configuration

2.2.1 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 <i>time</i>	Sets the attack filter period to <i>time</i> . Its unit is second.
Switch_config# filter threshold [arp bpdu dhcp igmp ip icmp] <i>value</i>	Sets the attack filter threshold to <i>value</i> .
Switch_config# filter block-time <i>time</i>	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 <i>time</i>	Sets the filter polling period in Hybrid mode. Its unit is second.
Switch_config# filter polling threshold [arp bpdu dhcp igmp ip icmp icmpv6] <i>value</i>	Sets the filter polling threshold 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	Sets shutdown of the port when detecting the attack source in raw mode.

2.2.2 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 detection.
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 bpdud	Enables BPDUD 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 detection 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:

1. 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.

2.2.3 Enabling the Attack Prevention Function

After all parameters for attack prevention are set, you can start up the attack prevention function. Note that small parts of processor source will be occupied when the attack prevention function is started.

Command	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.

2.2.4 Checking the State of Attack Prevention

After attack prevention is started, you can run the following command to check the state of attack prevention:

Command	Purpose
show filter	After attack prevention is started, you

Attack Prevention Introduction

	can run the following command to check the state of attack prevention:
show filter summary	Checks the parameter configuration and summary information of Filter.

Chapter 3 Attack Prevention Configuration Example

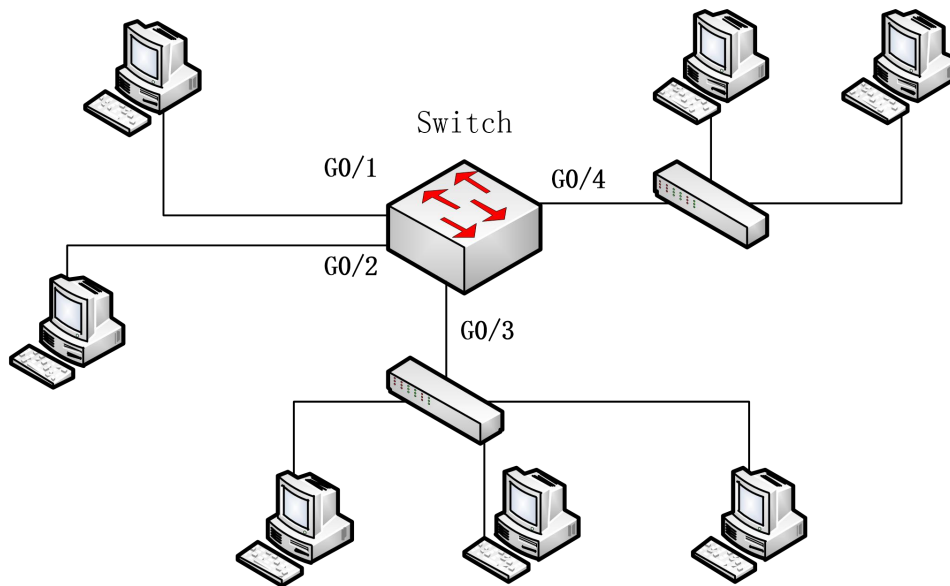
Note:

The examples shown in this chapter is only a reference for Filter configuration.

Please configure according to your actual network condition.

3.1 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:

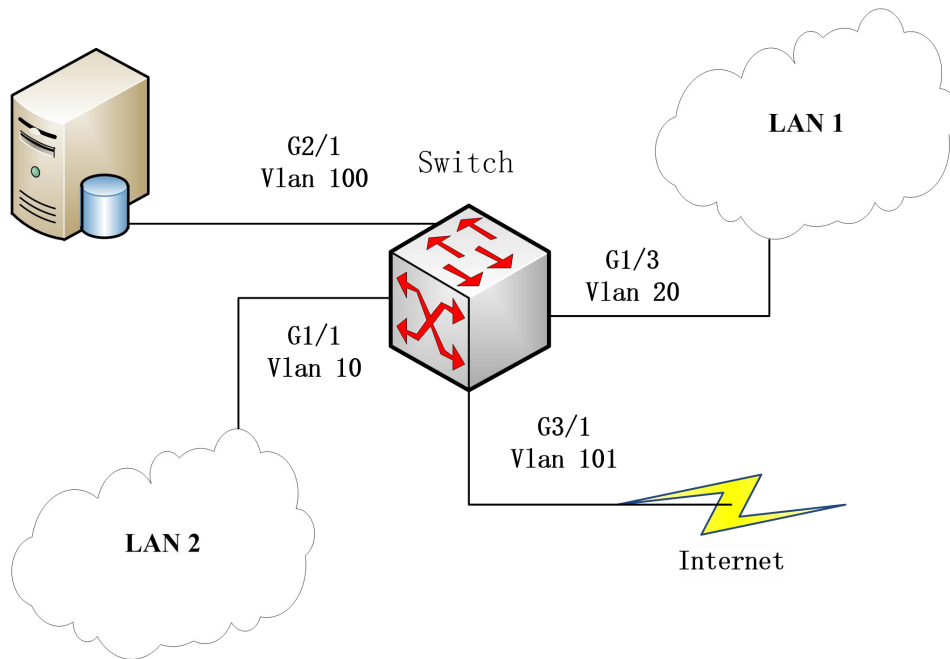
```
Switch_config_intf# exit
```

```
Switch_config# filter mode raw
```

```
Switch_config# filter enable
```

3.2 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
```

Network Protocol Configuration

Table of Contents

Chapter 1 Configuring IP Addressing.....	1
1.1 IP Introduction.....	1
1.1.1 IP.....	1
1.2 Configuring IP Address Task List.....	1
1.3 Configuring IP Address.....	2
1.3.1 Configuring IP Address at the Network Interface.....	2
1.3.2 Configuring Multiple IP Addresses at the Network Interface.....	2
1.3.3 Configuring Address Resolution.....	3
1.3.4 Detecting and Maintaining IP Addressing.....	5
1.4 IP Addressing Example.....	6
Chapter 2 Configuring DHCP.....	7
2.1 Overview.....	7
2.1.1 DHCP Application.....	7
2.1.2 Advantages of DHCP.....	7
2.1.3 DHCP Terms.....	7
2.2 Configuring DHCP Client.....	8
2.2.1 Configuration Task List of DHCP Client.....	8
2.2.2 DHCP Client Configuration Tasks.....	8
2.2.3 DHCP Client Configuration Example.....	9
Chapter 3 IP Service Configuration.....	10
3.1 Configuring IP Service.....	10
3.1.1 Managing IP Connection.....	10
3.1.2 Configuring Performance Parameters.....	12
3.1.3 Detecting and Maintaining IP Network.....	13
3.2 Configuring Access List.....	14
3.2.1 Filtering IP Packet.....	14
3.2.2 Creating Standard and Extensible IP Access List.....	15
3.2.3 Applying the Access List to the Interface.....	16
3.2.4 Extensible Access List Example.....	16
3.3 Configuring IP Access List Based on Physical Port.....	17
3.3.1 Filtering IP Packet.....	17
3.3.2 Creating Standard and Extensible IP Access List.....	17
3.3.3 Applying ACL on Ports.....	18
3.3.4 Extensible Access List Example.....	19

Chapter 1 Configuring IP Addressing

1.1 IP Introduction

1.1.1 IP

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

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

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

1.2 Configuring IP Address Task List

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

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

For creating IP addressing in the network, refer to section “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

1.3 Configuring IP Address

1.3.1 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	Status
A	0.0.0.0	Reserved
	1.0.0.0 to 126.0.0.0	Available
	127.0.0.0	Reserved
B	128.0.0.0 to 191.254.0.0	Available
	191.255.0.0	Reserved
C	192.0.0.0	Reserved
	192.0.1.0 to 223.255.254.0	Available
	223.255.255.0	Reserved
D	224.0.0.0 to 239.255.255.255	Multicast address
E	240.0.0.0 to 255.255.255.254	Reserved
	255.255.255.255	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 <i>ip-address mask</i>	Configure the main IP address of the interface.

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

Note:

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

1.3.2 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 <i>ip-address mask secondary</i>	Configure multiple IP addresses on the network interface.

Note:

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

1.3.3 Configuring Address Resolution

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

1. Creating address resolution

An IP device may have two addresses: local address (local network segment or device uniquely identified by LAN) and network address (representing the network where the device is located). The local address is the address of the link layer because the local address is contained in the message header at the link layer, and is read and used by devices at the link layer. The 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 <i>seconds</i>	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 <i>value</i>	Set the interval for sending free ARP message on the interface. The default value is 120 seconds.

- To set the maximum retransmissions of the Re-Detect packets, run the following command.
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 <i>number</i>	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 address

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 <i>name address</i>	Statically map the host name to the IP address.

1.3.4 Detecting and Maintaining IP Addressing

To detect and maintain the network, run the following command:

1. Clearing cache, list and database

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.

2. Displaying statistics data about system and network

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

All relative operations are listed in the following table. For how to use these commands, refer to Chapter “IP Addressing Commands”. Run the following commands in management mode:

Command	Purpose
show arp	Display content in the ARP table.
show hosts	Display the cache table about hostname-to-IP mapping.
show ip interface [<i>type number</i>]	Displays the state of a port.
ping { <i>host address</i> }	Test the reachability of the network node.

1.4 IP Addressing Example

The following case shows how to configure the IP address on interface VLAN11.

```
interface vlan 11
```

```
ip address 202.96.2.3 255.255.255.0
```

Chapter 2 Configuring DHCP

2.1 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.

2.1.1 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 an OLT that can access DHCP connects multiple hosts, the OLT can obtain an IP address
- From the DHCP server through the DHCP relay and then distribute the address to the hosts.

2.1.2 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

2.1.3 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.

2.2 Configuring DHCP Client

2.2.1 Configuration Task List of DHCP Client

- Obtaining an IP address
- Specifying an address for DHCP server
- Configuring DHCP parameters
- Monitoring DHCP

2.2.2 DHCP Client Configuration Tasks

1. Obtaining an IP address

Run the following command on the VLAN interface to obtain an IP address through the DHCP protocol for an interface.

Command	Function
ip address dhcp	Sets the IP address of an Ethernet interface through DHCP.

2. 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 <i>ip-address</i>	Specifies the IP address of the DHCP server.

The command is optional when you perform operations to "obtain an IP address".

3. 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 <i>seconds</i>	Specifies the acceptable minimum lease time.
ip dhcp client retransmit <i>count</i>	Specifies the retransmission times for DHCP packet.
ip dhcp client select <i>seconds</i>	Specify the interval for SELECT.
ip dhcp client class_identifier <i>WORD</i>	Specify the classification code of the provider.
ip dhcp client client_identifier <i>hrd_ether</i>	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".

4. 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.

2.2.3 DHCP Client Configuration Example

DHCP Client configuration example is shown below:

1. 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”.

3.1 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.

3.1.1 Managing IP Connection

The IP protocol provides a series of services to control and manage IP connections. Most of these services are provided by ICMP. The ICMP message is sent to the host or other routing switches when the routing switch or the access server detects faults in the IP message header. ICMP is mainly defined in RFC 792.

Perform the following different operations according to different IP connection conditions:

1. Sending ICMP unreachable message

If the system receives a message and cannot send it to the destination, such as no routes, the system will send an ICMP-unreachable message to the source host. The function of the system is enabled by default.

If the function is disabled, you can run the following command in interface configuration mode to enable the function.

Command	Purpose
ip unreachable	Enable the function to send an ICMP-unreachable message.

2. Sending ICMP redirection message

Sometimes the host selects an unfavorable route. After a routing switch on the route receives a message from the host, it is to check the routing table and then forward the message through the message-receiving interface to another routing switch that is in the same network segment as the host. In this case, the routing switch notifies the source host of directly sending the message with the destination to another routing switch without winding itself. The redirection message requires the source host to discard the original route and take more

direct route suggested in the message. Many host's operating system adds a host route to its routing table. However, the routing switch is more willing to trust information obtained through the routing protocol. Therefore, the routing switch would not add the host route according to the information.

The function is enabled by default. If the hot standby routing switch protocol is configured on the interface, the function is automatically disabled. However, the function will not be automatically enabled even if the hot standby routing switch protocol is canceled.

To enable the function, run the following command in interface configuration mode:

Command	Purpose
ip redirects	Permit sending the ICMP redirection message.

3. Sending ICMP mask response message

Sometimes the host must know the network mask. To get the information, the host can send the ICMP mask request message. If the routing switch can confirm the mask of the host, it will respond with the ICMP mask response message. By default, the routing switch can send the ICMP mask response message.

To send the ICMP mask request message, run the following command in interface configuration mode:

Command	Purpose
ip mask-reply	Send the ICMP mask reply message.

4. Supporting route MTU detection

The system supports the IP route MTU detection mechanism defined by RFC 1191. The IP route MTU detection mechanism enables the host to dynamically find and adjust to the maximum transmission unit (MTU) of different routes. Sometimes the routing switch detects that the received IP message length is larger than the MTU set on the message forwarding interface. The IP message needs to be segmented, but the "unsegmented" bit of the IP message is reset. The message, therefore, cannot be segmented. The message has to be dropped. In this case, the routing switch sends the ICMP message to notify the source host of the reason of failed forwarding, and the MTU on the forwarding interface. The source host then reduces the length of the message sent to the destination to adjust to the minimum MTU of the route.

If a link in the route is disconnected, the message is to take other routes. Its minimum MTU may be different from the original route. The routing switch then notifies the source host of the MTU of the new route. The IP message should be packaged with the minimum MTU of the route as much as possible. In this way, the segmentation is avoided and fewer message is sent, improving the communication efficiency.

Relevant hosts must support the IP route MTU detection. They then can adjust the length of IP message according to the MTU value notified by the routing switch, preventing segmentation during the forwarding process.

5. Setting IP maximum transmission unit (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
<code>ip mtu bytes</code>	Set IP MTU of the interface.

6. Authorizing IP source route

The routing switch checks the IP header of every message. The routing switch supports the IP header options defined by RFC 791: strict source route, relax source route, record route and time stamp. If the OLT 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 OLT 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
<code>ip source-route</code>	Authorizing IP source route.

3.1.2 Configuring Performance Parameters

Run the following command to adjust IP performance.

1. Setting the Wait Time for TCP Connection

When the routing switch performs TCP connection, it considers that the TCP connection fails if the TCP connection is not created during the wait time. The routing switch then notifies the upper-level program of the failed TCP connection. You can set the wait time for TCP connection. The default value of the system is 75 seconds. The previous configuration has no

impact on TCP connections that the switch forwards. It only affects TCP connections that are created by the switch itself.

Run the following command in global configuration mode to set the wait time for TCP connections:

Command	Purpose
ip tcp synwait-time <i>seconds</i>	Set the wait time for TCP connection.

2. Setting the Size of TCP Windows

The default size of TCP windows is 2000 byte. Run the following command in global configuration mode to change the default window size:

Command	Purpose
ip tcp window-size <i>bytes</i>	Set the size of TCP windows.

3.1.3 Detecting and Maintaining IP Network

To detect and maintain the network, run the following command:

1. 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:

2. 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.

3. Displaying statistics data about system and network

The system can display the content in the cache, list and database. These statistics data can help you know the usage of systematic sources and solve network problems.

Run the following commands in EXEC mode. For details, refer to “IP Service Command”.

Command	Purpose
show ip access-lists <i>name</i>	Display the content of one or all access lists.
show ip sockets	Display all socket information about the routing switch.
show ip traffic	Show IP protocol statistics data

show tcp	Show all TCP connection status information
show tcp brief	Briefly display information about TCP connection states.
show tcp statistics	Display the statistics data about TCP
show tcp tcb	Display information about the designated TCP connection state.

4. Displaying debugging information

When problem occurs on the network, you can run debug to display the debugging information.

Run the following command in 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 Internet IP message.
debug ip packet	To display the information about IP interaction, run debug ip raw.
debug ip tcp	Display the interaction information about TCP.
debug ip udp	Display the interaction information about UDP.

3.2 Configuring Access List

3.2.1 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:

- (1) Create the access list by designating the access list name and conditions.
- (2) Apply the access list to the interface.

3.2.2 Creating Standard and Extensible IP Access List

Use a character string to create an IP access list.

Note:

The standard access list and the extensible access list cannot have the same name.

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

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] [totalen eq gt lt length] [t 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.
Exit	Log out from the access list configuration mode.

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

Note:

When you create the access list, the end of the access list includes the implicit deny sentence by default. If the mask is omitted in the relative IP host address access list, 255.255.255.255 is supposed to be the mask.

After the access list is created, the access list must be applied on the route or interface. For details, refer to section 4.2.3 “Applying the Access List to the Interface”.

3.2.3 Applying the Access List to the Interface

After the access list is created, you can apply it to one or multiple interfaces including the in interfaces and out interfaces.

Run the following command in interface configuration mode.

Command	Purpose
<code>ip access-group name {in out}</code>	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.

3.2.4 Extensible Access List Example

In the following example, the first line allows any new TCP to connect the destination port after port 1023. The second line allows any new TCP to connect the SMTP port of host 130.2.1.2.

```
ip access-list extended aaa
permit tcp any 130.2.0.0 255.255.0.0 gt 1023
permit tcp any 130.2.1.2 255.255.255.255 eq 25
interface vlan 10
ip access-group aaa in
```

Another example to apply the extensible access list is given. Suppose a network connects the Internet, you expect any host in the Ethernet can create TCP connection with the host in the Internet. However, you expect the host in the Internet cannot create TCP connection with the host in the Ethernet unless it connects the SMTP port of the mail host.

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 example, 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
```

3.3 Configuring IP Access List Based on Physical Port

3.3.1 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:

- (1) Create the access list by designating the access list name and conditions.
- (2) Applying ACL on a port

3.3.2 Creating Standard and Extensible IP Access List

Use a character string to create an IP access list.

Note:

The standard access list and the extensible access list cannot have the same name.

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

Command	Purpose

Network Protocol Configuration

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] [totalen 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.
{deny permit} protocol any any [precedence precedence] [tos tos] [log] [time-range time-range] [location location] [donotfragment-set] [donotfragment-notset] [is-fragment] [not-fragment] [totalen 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 ACL is established, it must be applied on the lines or ports. For details, refer to section “Applying the Access List to the Interface”.

3.3.3 Applying ACL on Ports

After an ACL is established, it can be applied on the ingress of one or many interfaces.

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. However, if the access control list forbids the destination address, the system will drop the packet and then returns an ICMP unreachable packet.

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

3.3.4 Extensible Access List Example

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.

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
```

IP ACL Application Configuration

Table of Contents

Chapter 1 IP ACL Application Configuration.....	1
1.1 Applying the IP Access Control List.....	1
1.1.1 Applying the IP Access Control List.....	1

Chapter 1 IP ACL Application Configuration

1.1 Applying the IP Access Control List

1.1.1 Applying the IP Access Control List

After an ACL is established, it can be applied on one or many slots or globally.

Run the following command to apply IPv6 ACL on a port:

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 it 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 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 to an interface or cancels it on the interface in the global configuration mode. NameIP: Name of the ip access list Vlan THE ACCESS LIST IS APPLIED IN INGRESS. WordVLAN RANGE TABLE Add ADD VLAN RANGE TABLE Remove Delete vlan range table
exit	Goes back to the EXEC mode.
write	Saves the settings.

Note: In the global configuration mode, the IP access list can be applied to VLAN and in the

IP ACL Application Configuration

interface configuration mode, the IP access list cannot be applied to VLAN.

IPv6 Protocol Configuration

Table of Contents

Chapter 1 IPv6 Protocol Configuration.....	1
1.1 IPv6 Protocol Configuration.....	1
1.2 Enabling IPv6.....	1
1.2.1 Setting the IPv6 Address.....	1
Chapter 2 Setting the IPv6 Services.....	3
2.1 Setting the IPv6 Services.....	3
2.1.1 Managing the IPv6 Link.....	3

Chapter 1 IPv6 Protocol Configuration

1.1 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. Otherwise, there will be no IPv6 address and the protocol will not be enabled.

To enable the IPv6 protocol, users should finish the following task:

- Setting at least one IPv6 address in VLAN interface configuration mode

1.2 Enabling IPv6

1.2.1 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.

Type	Referred Format	Usage Guidelines
Unicast address	2001:0:0:0:0DB8:800:200C:417A/64	2001:0:0:0:0DB8:800:200C:417A is address. Meanwhile the prefix length of the address must be specified (such as 64 in the reference format)
Multicast address	FF01:0:0:0:0:0:101	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. Packets forwarding to any broadcast address will "route" to the VLAN port with one configured broadcast address nearest to the sender.

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.

To set a global IPv6 address in VLAN interface configuration mode, run the following commands.

Command	Purpose
ipv6 address autoconfig	Sets a global address automatically.
ipv6 address [ipv6-address/prefix-length general-prefix prefix-name sub-bits/prefix-length] [eui-64]	Sets a global address.
ipv6 address X:X:X:X::X/<0-128> anycast	Sets an address of unicast/broadcast/multicast.

Note:

- When IPv6 is enabled through the configuration of a global address, all interconnected IPv6 device can be handled by IPv6.
- If a link-local address has not been set before the configuration of the global address, the system will set a link-local address automatically.

Chapter 2 Setting the IPv6 Services

2.1 Setting the IPv6 Services

After IPv6 is enabled, all services provided by IPv6 can be set. The configurable IPv6 service is shown below:

- (1) Managing the IPv6 Link

2.1.1 Managing the IPv6 Link

IPv6 provides a series of services to control and manage the IPv6 link. This series of services includes:

- (1) Setting the MTU of IPv6
- (2) Setting IPv6 redirection
- (3) Setting IPv6 destination unreachability
- (4) Setting IPv6 ACL

1. Setting the MTU of IPv6

All interfaces have a default IPv6 MTU. If the IP message length exceeds MTU, the routing switch segments the message.

To set IPv6 MTU on a specific interface, run the following command in interface configuration mode:

Command	Purpose
<code>ipv6 mtu bytes</code>	Sets IPv6 MTU on an interface.

2. Setting IPv6 redirection

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 switch that is in the same network segment as the host. In this case, the switch notifies the source host of directly sending the message with the destination to another 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 switch would not add the host route according to the 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 enable IPv6 redirection, run the following command:

Command	Purpose
<code>ipv6 redirects</code>	Allows IPv6 to transmit the redirection packets.

3. Setting IPv6 Destination Unreachability

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 unreachable	Allowing 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 <i>WORD</i> { in out }	Filters the IPv6 packets in the reception or transmission direction (in: receive; out: transmit) on a VLAN interface.

MLD-Snooping Configuration

Table of Contents

Chapter 1 MLD-Snooping Configuration.....	1
1.1 IPv6 Multicast Overview.....	1
1.2 MLD-Snooping Multicast Configuration Tasks.....	1
1.2.1 Enabling/Disabling MLD-Snooping Multicast.....	1
1.2.2 Enabling/Disabling the Solicitation of Hardware Forward of Multicast Group....	2
1.2.3 Adding/Deleting the Static Multicast Address of VLAN.....	2
1.2.4 Setting Router Age Timer of MLD-Snooping.....	2
1.2.5 Setting Response Time Timer of MLD-Snooping.....	3
1.2.6 Configuring Querier of MLD-Snooping.....	3
1.2.7 Setting the Port of the Static Multicast Router.....	4
1.2.8 Enabling/Disabling Immediate Leave.....	4
1.2.9 Monitoring and Maintaining MLD-Snooping Multicast.....	4

Chapter 1 MLD-Snooping Configuration

1.1 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 realizes the above functions by listening the query message and report message of MLD-Snooping, MLD-Snooping can function properly only when it works on the multicast router, that is, the switch must periodically receive the MLD-Snooping query information from the router. The router age timer of MLD-Snooping must be set to a time value that is bigger than the group query period of the multicast router connecting MLD-Snooping. You can check the multicast router information in each VLAN by running `show ipv6 mld-snooping`.

1.2 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

1.2.1 Enabling/Disabling MLD-Snooping Multicast

Run the following commands in global configuration mode.

Command	Purpose
<code>ipv6 mld-snooping</code>	Enables MLD snooping multicast.

no ipv6 mld-snooping	Disables MLD snooping.
-----------------------------	------------------------

Note:

After MLD-Snooping is enabled, when DLF occurs on multicast packets (that is, the destination address is not registered in the swap chip through the MLD-Snooping), all multicast packets whose destination addresses are not registered on any port will be dropped.

1.2.2 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.

1.2.3 Adding/Deleting the Static Multicast Address of VLAN

The static multicast address can make some MLD-Snooping hosts receive the corresponding multicast packets.

Run the following commands in global configuration mode.

Command	Purpose
ipv6 mld-snooping vlan <i>vlan_id</i> static X:X:X::X interface <i>intf_name</i>	Adds the static multicast address of VLAN.
no ipv6 mld-snooping vlan <i>vlan_id</i> static X:X:X::X interface <i>intf_name</i>	Deletes static multicast address of VLAN.

1.2.4 Setting Router Age Timer of MLD-Snooping

The router age timer is used to monitor whether the MLD-Snooping querier exists or not; the MLD-Snooping querier maintenance is used to maintain and manage the multicast address by sending the query packets and MLD-Snooping works by independence on the communication between MLD-Snooping querier and host.

Run the following commands in global configuration mode.

Command	Operation
ipv6 mld-snooping timer router-age <i>timer_value</i>	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 the timer requires to refer to the query period settings of the MLD-Snooping querier for it cannot be smaller than the query period; you are recommended to set the router age timer to the triple of the query period.

By default the router age timer is set to be 260 seconds of MLD-Snooping.

1.2.5 Setting Response Time Timer of MLD-Snooping

The Response Time timer means the threshold time for the host to report the multicast after MLD-Snooping querier sends the query packets; if this report packet is not received after the timer ages, the switch will delete this multicast address.

Run the following commands in global configuration mode.

Command	Operation
ipv6 mld-snooping timer response-time <i>timer_value</i>	Sets the value of the response time of MLD-Snooping.
no ipv6 mld-snooping timer response-time	Resumes the default value of the response time of MLD-Snooping.

Note:

The value of the timer cannot be set too small, or the multicast communication may be unstable.

By default the response time is set to be 10 seconds of MLD-Snooping.

1.2.6 Configuring Querier of MLD-Snooping

If the multicast router does not exist in VLAN where MLD-snooping is activated, the querier function of MLD-snooping can be used to imitate the multicast router to regularly send MLD-snooping query message. (The function is global, that is, it can be enabled or disabled in VLAN where MLD-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 MLD-snooping, enabling MLD-snooping to work properly.

Run the following commands in global configuration mode.

Command	Operation
[no] ipv6 mld-snooping querier [address [ip_addr]]	Configures the querier of MLD-snooping. The optional parameter address is the source IP address of query message.

The IGMP-snooping querier function is disabled by default. By default, the source IP address of the fake Query packet is FE80::3FF:FEFE:FD00:1.

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.

1.2.7 Setting the Port of the Static Multicast Router

After a port is set to be a static multicast port, all the MLD-Snooping report packets and done packets will be transmitted to this port.

Run the following commands in global configuration mode.

Command	Operation
ipv6 mld-snooping vlan <i>WORD</i> mrouter interface <i>inft_name</i>	Sets the static multicast router's port of MLD snooping in Vlan word.
no ipv6 mld-snooping vlan <i>WORD</i> mrouter interface <i>inft_name</i>	Deletes the static multicast router's port of MLD snooping in Vlan word.

1.2.8 Enabling/Disabling Immediate Leave

Run the following commands in global configuration mode.

Command	Purpose
ipv6 mld-snooping vlan <i>WORD</i> immediate-leave	Enables the immediate-leave functionality.
no ipv6 mld-snooping vlan <i>WORD</i> immediate-leave	Resumes the default settings.

1.2.9 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:

```

Switch#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);

```

Displays the multicast group of MLD-Snooping.

```

Switch#show ipv6 mld--snooping groups

Vlan Group          Type Port(s)
-----
1 FF02::1:FF32:1B9B MLD  G0/3
1 FF02::1:FF00:2    MLD  G0/3
1 FF02::1:FF00:12   MLD  G0/3
1 FF02::1:FF13:647D MLD  G0/3
2 FF02::1:FF00:2    MLD  G0/2
2 FF02::1:FF61:9901 MLD  G0/2

```

Displays MLD-Snooping Snooping Timer

```

Switch#show ipv6 mld-snooping timers

vlan 1 Querier on port 0 : 251
#
Querier on port 0: 251 means the timeout time of the ageing timer of the router.
vlan 2 multicast address 3333.0000.0005 response time : this shows the time period from
receiving a multicast query packet to the present; if there is no host to respond when the timer
times out, the port will be canceled.

```

The MLD-snooping statistics information is displayed below:

```

Switch#show ipv6 mld-snooping statistics

vlan 1
-----
v1_packets:0          quantity of v1 packets
v2_packets:6          quantity of v2 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
send_query_packets:0  Quantity of sending packets
err_packets:0        Quantity of error packets

```

Displays multicast mac information of the operating MLD-Snooping

Switch#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

Neighbor Discovery Configuration

Table of Contents

Chapter 1 Neighbor Discovery Configuration.....	1
1.1 Neighbor Discovery Overview.....	1
1.1.1 Address Resolution.....	2

Chapter 1 Neighbor Discovery Configuration

1.1 Neighbor Discovery 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.

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. If the neighbor is both router and host, it needs address resolution.
- (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.

1.1.1 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.

NTP Configuration

Table of Contents

- Chapter 1 Overview..... 1
 - 1.1 Stipulation..... 1
 - 1.1.1 Format Stipulation in the Command Line..... 1
- Chapter 2 NTP Configuration..... 2
 - 2.1 Overview..... 2
 - 2.2 NTP Configuration..... 2
 - 2.2.1 Configure the Equipment As an NTP Server..... 2
 - 2.2.2 Configure NTP Authentication Function..... 2
 - 2.2.3 Configure NTP Association..... 3

Chapter 1 Overview

1.1 Stipulation

1.1.1 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.
<i>{italic}</i>	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.
< <i>italic</i> >	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.

Chapter 2 NTP Configuration

2.1 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.

2.2 NTP Configuration

2.2.1 Configure 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.)

2.2.2 Configure NTP Authentication Function

Configuration mode: Global

Command	Purpose
ntp authentication enable	Enable the authentication function (disabled by default).
ntp authentication key <i>keyid</i> md5 <i>password</i>	Configure NTP md5 authentication <i>keyid</i> and corresponding keys.
ntp authentication trusted-key <i>keyid</i>	Configure the <i>keyid</i> corresponding key as the trusted key.

2.2.3 Configure NTP Association

Configuration mode: Global

Command	Purpose
ntp server <i>ip-address</i> [version number key keyid]*	Configure the IP address of NTP server; the version number, key number, and the encryption key can be designated.
ntp peer <i>ip-address</i> [version number key keyid]*	The following command can be used to configure NTP peer IP address of the device, designated version number and 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.