



# Configuration Preparation



# Table of Contents

Chapter 1 Configuration Preparation .....	1
1.1 Port Number of the Switch .....	1
1.2 Preparation Before Switch Startup .....	1
1.3 Acquiring Help .....	2
1.4 Command Modes .....	2
1.5 Canceling a Command .....	3
1.6 Saving Configuration .....	3

# Chapter 1 Configuration Preparation

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

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

## 1.1 Port Number of the Switch

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

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

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

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

**Note:**

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

## 1.2 Preparation Before Switch Startup

Do the following preparatory works before the switch is configured:

- (1) Set the switch's hardware according to the requirements of the manual.
- (2) Configure a PC terminal simulation program.
- (3) Determine the IP address layout for the IP network protocols.

## 1.3 Acquiring Help

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

- Enter a question mark. The currently available command list is displayed.  
Switch> ?
- Enter several familiar characters and press the space key. The available command list starting with the entered familiar characters is displayed.  
Switch> s?
- Enter a command, press the space key and enter the question mark. The command parameter list is displayed.  
Switch> show ?
- Press the “up” key and the commands entered before can be displayed. Continue to press the “up” key and more commands are to be displayed. After that, press the “down” key and the next command to be entered is displayed under the current command.

## 1.4 Command Modes

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

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

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

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

```
Switch> enter
Password: <enter password>
Switch# config
Switch_config# interface f0/1
Switch_config_f0/1# quit
Switch_config# quit
Switch#
```

## 1.5 Canceling a Command

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

```
no ip routing
```

## 1.6 Saving Configuration

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

# Basic Configuration

# Table of Contents

Chapter 1 System Management Configuration.....	1
1.1 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 .....	4
1.2 Basic System Management Configuration .....	5
1.2.1 Configuring Ethernet IP address .....	5
1.2.2 Configuring default route .....	5
1.2.3 Using ping to test network connection state.....	5
Chapter 2 Terminal Configuration.....	7
2.1 VTY Configuration Introduction .....	7
2.2 Configuration Task.....	7
2.2.1 Relationship between line and interface .....	7
2.3 Monitor and Maintenance .....	7
2.4 VTY Configuration Example .....	7
CHAPTER 3 SSH Configuration Commands .....	8
3.1 Introduction.....	8
3.1.1 SSH server.....	8
3.1.2 SSH client .....	8
3.1.3 Function .....	8
3.2 Configuration Tasks .....	8
3.2.1 Configuring the authentication method list .....	8
3.2.2 Configuring the access control list.....	8
3.2.3 Configuring the authentication timeout value .....	9
3.2.4 Configuring the times of authentication retrying .....	9
3.2.5 Configuring the login silence period .....	9
3.2.6 Enabling sftp .....	9
3.2.7 Enabling sshd.....	9
3.2.8 Enabling SSH server.....	10
3.3 SSH server Configuration Example.....	10
3.3.1 Access control list.....	10
3.3.2 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	Description
<b>format</b>	Formats the file system and delete all data.
<b>dir</b> [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
<b>delete</b> filename	Deletes a file. The system will prompt if the file does not exist.
md dirname	Creates a directory.
rd dirname	Deletes a directory. The system will prompt if the directory is not existed.
more filename	Displays the content of a file. If the file content cannot be displayed by one page, it will be displayed by pages.
cd	Changes the path of the current file system.
pwd	Displays the current path.

#### 1.1.3 Starting up from a file manually

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

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

##### Parameter description

Parameter	Description
<i>local_filename</i>	A file name stored in the flash memory Users must enter the file name.

##### Example

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



### 1.1.4 Updating software

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

There are two ways of software update in monitor mode.

#### a. Through TFTP

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

The previous 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.

#### Parameter description

Parameter	Description
ip_addr	IP address of the tftp server If there is no specified IP address, the system will prompt you to enter the IP address after the <b>copy</b> 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#
```

#### b. Through serial port communication protocol—zmodem

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

```
monitor#download c0 <local_filename>
```

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

#### Parameter description

Parameter	Description
-----------	-------------

<i>local_filename</i>	Filename stored in the flash Users must enter the filename.
-----------------------	--

### Example

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

```
monitor#download c0 switch.bin
```

Prompt: speed[9600]?115200

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



Figure 1-1 Send files

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

After the file is transferred, the following information appears:

```
ZMODEM:successfully receive 36 blocks ,18370 bytes
```

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

**Note:**

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

#### 1.1.5 Updating configuration

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

a. Through TFTP

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

b. Through serial port communication protocol—zmodem.

```
monitor#download c0 startup-config
```

### 1.1.6 Using ftp to perform the update of software and configuration

```
config #copy ftp flash [ip_addr|option]
```

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

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

#### Parameter description

Parameter	Description
login-nam	Username of the ftp server If there is no specified username, the system will prompt you to enter the username after the <b>copy</b> command is run.
login-password	Password of the ftp server If there is no specified password, the system will prompt you to enter the password after the <b>copy</b> command is run.
nchecksize	The size of the file is not checked on the server.
vrf	Provides vrf binding function for the device that supports MPLS.
blksize	Size of the data transmission block Default value: 512
ip_addr	IP address of the ftp server If there is no specified IP address, the system will prompt you to enter the IP address after executing the <b>copy</b> command.
active	Means to connect the ftp server in active mode.
passive	Means to connect the ftp server in passive mode.
type	Set the data transmission mode (ascii or binary)

#### Example

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

```
config#copy ftp flash
```

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

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

```
Prompt: Source file name[]?main.bin
```

```
Prompt: Remote-server ip address[]?192.168.20.1
```

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

```
or
```

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

```
#####
#####
FTP:successfully receive 3377 blocks ,1728902 bytes
config#
```

**Note:**

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

## 1.2 Basic System Management Configuration

### 1.2.1 Configuring Ethernet IP address

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

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

Parameter description

Parameter	Description
<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 Configuring default route

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

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

Parameter description

Parameter	Description
<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.

#### Parameter description

Parameter	Description
<i>ip_address</i>	Destination IP address

#### Example

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

## Chapter 2 Terminal Configuration

### 2.1 VTY Configuration Introduction

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

### 2.2 Configuration Task

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

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

#### 2.2.1 Relationship between line and interface

##### a. Relationship between synchronous interface and VTY line

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

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

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

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

### 2.3 Monitor and Maintenance

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

### 2.4 VTY Configuration Example

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

```
config#line vty 0 32
config_line#length 0
```

## CHAPTER 3 SSH Configuration Commands

### 3.1 Introduction

#### 3.1.1 SSH server

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

#### 3.1.2 SSH client

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

#### 3.1.3 Function

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

### 3.2 Configuration Tasks

#### 3.2.1 Configuring the authentication method list

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

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

Command	Purpose
ip sshd auth_method STRING	Configures the authentication method list.

#### 3.2.2 Configuring the access control list

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

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

Command	Purpose
ip sshd access-class STRING	Configures the access control list.

### 3.2.3 Configuring the authentication timeout value

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

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

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

### 3.2.4 Configuring the times of authentication retrying

If the times for failed authentications exceed the maximum times, SSH server will not allow you to retry authentication unless a new connection is established. The maximum times for retrying authentication is 3 by default.

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

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

### 3.2.5 Configuring the login silence period

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

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

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

### 3.2.6 Enabling sftp

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

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

Command	Purpose
ip sshd sftp	Enables sftp.

### 3.2.7 Enabling sshd

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



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

Command	Purpose
ip sshd save	Enables sshd

### 3.2.8 Enabling SSH server

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

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

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

## 3.3 SSH server Configuration Example

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

### 3.3.1 Access control list

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

### 3.3.2 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

Network Management Configuration

---

Chapter 1 Network Management Configuration..... 1

1.1 Configuring SNMP..... 1

1.1.1 Introduction..... 1

1.1.2 SNMP Configuration Tasks..... 3

1.1.3 Configuration Example ..... 10

1.2 RMON Configuration..... 11

1.2.1 RMON Configuration Task..... 11

# Chapter 1 Network Management Configuration

## 1.1 Configuring SNMP

### 1.1.1 Introduction

The SNMP system includes the following parts:

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

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

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

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

#### 1. SNMP notification

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

SNMP notification can be treated as trap or inform request to send. Since the receiving side doesn't send any reply when receiving a trap, this leads to the receiving side cannot be sure that the trap has been received. Therefore the trap is not reliable. In

comparison, SNMP management side that receives "inform request" uses PDU that SNMP echoes as the reply for this information. If no "inform request" is received on the management side, no echo will be sent. If the receiving side doesn't send any reply, then you can resend the "inform request". Then notifications can reach their destination.

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

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

## 2. SNMP version

System of our company supports the following SNMP versions:

SNMPv1---simple network management protocol, a complete Internet standard, which is defined in RFC1157.

SNMPv2C--- Group-based Management framework of SNMPv2, Internet test protocol, which is defined in RFC1901.

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

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

SNMPv1 uses group-based security format. Use IP address access control list and password to define the management side group that can access to agent MIB. SNMPv3 provides secure access to devices by a combination of authenticating and encrypting packets over the network.

The security features provided in SNMPv3 are:

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

- 2 -

an unauthorized source.

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

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

### 3. Supported MIB

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

Our system provides its own MIB extension for each system.

#### 1.1.2 SNMP Configuration Tasks

- Configuring SNMP view
- Creating or modifying the access control for SNMP community
- Configuring the contact method of system administrator and the system's location
- Defining the maximum length of SNMP agent data packet
- Monitoring SNMP state
- Configuring SNMP trap
- Configuring 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.

Command	Purpose
<b>snmp-server view</b> <i>name oid</i> [ <b>excluded</b>   <b>included</b> ]	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
<b>snmp-server community</b> [0 7] <i>string</i> [ <b>view</b> <i>view-name</i> ] [ <b>ro</b>   <b>rw</b> ] [ <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. You can use the following commands in global configuration mode.

Command	Purpose
<b>snmp-server contact</b> <i>text</i>	Sets the character string for the linkman of the node.
<b>snmp-server location</b> <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. Use the following command in global configuration mode:

Command	Purpose
<b>snmp-server packetsize</b> <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
<b>show snmp</b>	Monitor the SNMP state.



## 6. Configuring SNMP trap

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

Configuring the system to send trap

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

Command	Purpose
<b>snmp-server host</b> <i>host</i> [ <i>hostv6 host</i> community-string [ <i>trap-type</i> ]	Specifies the receiver of the trap message.
<b>snmp-server host</b> [ <i>hostv6 host</i> [ <i>vrf word</i> ] [ <i>udp-port port-num</i> ] [ <i>permit deny event-id</i> ] {{ <i>version [v1   v2c   v3]</i>   {{ <i>informs   traps</i>   <i>auth [noauth]</i> }} <i>community-string/user</i> [ <i>authentication   configure snmp</i> ]	Specifies the receiver, version number and username of the trap message.  Note: For the trap of SNMPv3, you must configure SNMP engine ID for the host before the host is configured to receive the trap message.

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

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

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

- Modifying the running parameter of the trap

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

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

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

## 7. Configuring the SNMP binding source address

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

## Network Management Configuration

Command	Purpose
<b>snmp source-addr</b> <i>ipaddress</i>	Set the source address for the SNMP message.

### 8. Configuring snmp-server udp-port

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

Command	Purpose
<b>snmp-server udp-port</b> <i>portnum</i>	Set SNMP server udp-port number

### 9. Configuring SNMPv3 group

Run the following command to configure a group.

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

### 10. Configuring SNMPv3 user

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

### 11. Configuring snmp-server encryption

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

Command	Purpose
<b>snmp-server encryption</b>	Use ciphertext to show SHA password and MD5 password.

## 12. Configuring snmp-server trap-source

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

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

## 13. Configuring snmp-server trap-timeout

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

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

## 14. Configuring snmp-server trap-add-hostname

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

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

## 15. Configuring snmp-server trap-logs

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

Command	Purpose
<b>snmp-server trap-logs</b>	Enable snmp-server trap-logs to record the forwarding record of trap as logs.

## 16. Configuring snmp -dos-max retry times

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

Command	Purpose
<b>snmp-server set-snmp-dos-max retry times</b>	Set password retry times for logging in snmp in five minutes.

It should be used cooperatively with snmp-server host.

### 17. Configuring keep-alive times

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

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

### 18. Configuring snmp-server nencode

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

Command	Purpose
<b>snmp-server nencode text</b>	Corresponds to snmp private MIB variables.

### 19. Configuring snmp-server event-id

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

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

### 20. Configuring snmp-server getbulk-timeout

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

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

## 21. Configuring snmp-server getbulk-delay

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

Command	Purpose
<b>snmp-server getbulk-delay ticks</b>	To avoid snmp occupies excessive CPU,set snmp- server getbulk-delay ticks. Unit: centisecond.

## 22. Showing snmp running information

Use the command show snmp to monitor the input and output of SNMP, including illegal community strings, faults and the number of request variable.

Command	Purpose
<b>show snmp host</b>	Show SNMP trap host information.
<b>show snmp view</b>	Show snmp view information.
<b>show snmp mibs</b>	Show snmp mibs registration information.
<b>show snmp group</b>	Show snmp group information
<b>show snmp user</b>	Show snmp user information.

## 23. Showing snmp debug information

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

Command	Purpose
<b>debug snmp error</b>	Enable the debug switch of SNMP error.
<b>debug snmp event</b>	Enable the debug switch of snmp event.
<b>debug snmp packet</b>	Enable the debug switch of snmp packet

## 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.

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

## 1.2 RMON Configuration

### 1.2.1 RMON Configuration Task

RMON configuration tasks include:

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

## 1. Configuring rMon alarm for switch

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

Command	Purpose
<b>config</b>	Enter the global configuration mode.
<b>rmon alarm index variable</b> <i>interval</i> <b>{absolute   delta} rising-threshold</b> <i>value [eventnumber] falling-threshold</i> <i>value [eventnumber] [owner</i> <i>string] [repeat]</i>	<p>Add a rMon alarm item.</p> <p><b>index</b> is the index of the alarm item. Its effective range is from 1 to 65535.</p> <p><b>variable</b> is the object in the monitored MIB. It must be an effective MIB object in the system. Only objects in the Integer, Counter, Gauge or Time Ticks type can be detected.</p> <p><b>interval</b> is the time section for sampling. Its unit is second. Its effective value is from 1 to 2147483647.</p> <p><b>absolute</b> is used to directly monitor the value of MIB object.</p> <p><b>Delta</b> is used to monitor the value change of the MIB objects between two sampling.</p> <p><b>value</b> is the threshold value when an alarm is generated.</p> <p><b>Event number</b> is the index of an event that is generated when a threshold is reached. Event number is optional.</p> <p><b>Owner string</b> is to describe the information about the alarm.</p> <p><b>Repeat</b> is to repeat trigger event.</p>
<b>exit</b>	Enter the management mode again.
<b>write</b>	Save the configuration.

After a rMon alarm item is configured, the device will obtain the value of variable-specified oid after an interval. The obtained value will be compared with the previous value according to the 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 rMon event for switch

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

Step	Command	Purpose
1.	<b>config</b>	Enter the global configuration mode.
2.	<b>rmon event index</b> [ <b>description</b> <i>string</i> ] [ <b>log</b> ] [ <b>owner</b> <i>string</i> ] [ <b>trap</b> <i>community</i> ] [ <b>ifctrl</b> <i>interface</i> ]	Add a rMon event item.  <b>index</b> means the index of the event item. Its effective range is from 1 to 65535.  <b>description</b> means the information about the event.  <b>log</b> means to add a piece of information to the log table when a event is triggered.  <b>trap</b> means a trap message is generated when the event is triggered.  <b>community</b> means the name of a community.  <b>ifctrl interface</b> is the interface controlling event shutdown.  <b>owner string</b> is to describe the information about the alarm.
3.	<b>exit</b>	Enter the management mode again.
4.	<b>write</b>	Save the configuration.

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

## 3. Configuring rMon statistics for switch

The rMon statistics group is used to monitor the statistics information on every port of the device.

The steps to configure the rMon statistics are as follows:

Step	Command	Purpose
1.	<b>config</b>	Enter the global configuration mode.



## Network Management Configuration

2.	<b>interface iftype ifid</b>	Enter the port mode. iftype means the type of the port. ifid means the ID of the interface.
3.	<b>rmon collection stats index</b> [owner string]	Enable the statistics function on the port. <b>index</b> means the index of the statistics. <b>owner string</b> is to describe the information about the statistics.
4.	<b>exit</b>	Enter the global office mode.
5.	<b>exit</b>	Enter the management mode again.
6.	<b>write</b>	Save the configuration.

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

#### 4. Configuring rMon history for switch

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

Step	Command	Purpose
1.	config	Enter the global configuration command.
2.	interface iftype ifid	Enter the port mode. iftype means the type of the port. ifid means the ID of the interface.

## Network Management Configuration

3.	<code>rmon collection history index [bucket-number] [interval second] [owner owner-name]</code>	<p>Enable the history function on the port.</p> <p><b>index</b> means the index of the history item.</p> <p>Among all data collected by history item, the latest bucket-number items need to be saved. You can browse the history item of the Ethernet to obtain these statistics values.</p> <p>The default value is 50 items.</p> <p><b>second</b> means the interval to obtain the statistics data every other time. The default value is 1800 seconds.</p> <p><b>owner string</b> is used to describe some information about the history item.</p>
4.	<code>exit</code>	Enter the global office mode again.
5.	<code>exit</code>	Enter the management mode again.
6.	<code>write</code>	Save the configuration.

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

Note:

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

## 5. Displaying rMon configuration of switch

Run show to display the rMon configuration of the switch.

Command	Purpose
<code>show rmon [alarm] [event] [statistics] [history]</code>	<p>Displays the rmon configuration information.</p> <p><b>alarm</b> means to display the configuration of the alarm item.</p> <p><b>event</b> 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>

- 15 -

Network Management Configuration

---

	<p><b>statistics</b> means to display the configuration of the statistics item and statistics values that the device collects from the port.</p> <p><b>history</b> 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 Method Lists .....	2
1.1.5 AAA Configuration Process .....	3
1.1.6 Overview of the AAA Configuration Process .....	4
1.2 AAA 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 AAA 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 Example .....	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 .....	13
1.5.1 Local Account Policy Configuration Task List .....	13
1.5.2 Local Account Policy Configuration Task .....	13
1.5.3 Local Account Policy Example .....	15
Chapter 2 Configuring RADIUS .....	17
2.1 Introduction .....	17
2.1.1 RADIUS Introduction .....	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 .....	20
2.4.3 Specifying RADIUS Authentication .....	20
2.4.4 Specifying RADIUS Authorization .....	20
2.4.5 Specifying RADIUS Accounting .....	21
2.5 RADIUS Configuration Examples .....	21
2.5.1 RADIUS Authentication and Authorization Example .....	21
2.5.2 RADIUS Application Example .....	22
Chapter 3 TACACS+ Configuration .....	23
3.1 TACACS+ Overview .....	23
3.1.1 The Operation of TACACS+ Protocol .....	23

Table of Contents

---

3.2 TACACS+ Configuration Process..... 24

3.3 TACACS+ Configuration Task List..... 24

3.4 TACACS+ Configuration Task ..... 25

    3.4.1 Assigning TACACS+ server..... 25

    3.4.2 Setting up TACACS+ Encrypted Secret Key ..... 25

    3.4.3 Assigning to use TACACS+ to do authentication ..... 26

    3.4.4 Assigning to use TACACS+ for authorization ..... 26

    3.4.5 Assigning to use TACACS+ for accounting ..... 26

3.5 TACACS+ Configuration Example..... 26

    3.5.1 TACACS+ authentication example ..... 26

    3.5.2 TACACS+ Authorization Example ..... 27

    3.5.3 TACACS+ Accounting Example ..... 27

# Chapter 1 AAA Configuration

## 1.1 AAA Overview

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

### 1.1.1 AAA Security Service

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

- **Authentication**—Provides the method of identifying users, including login and password dialog, challenge and response, messaging support, and, depending on the security protocol you select, encryption.

Authentication is the way a user is identified prior to being allowed access to the network and network services. You configure AAA authentication by defining a named list of authentication methods, and then applying that list to various interfaces. The method list defines the types of authentication to be performed and the sequence in which they will be performed; it must be applied to a specific interface before any of the defined authentication methods will be performed. The only exception is the default method list (which is named "default"). The default method list is automatically applied to all interfaces if no other method list is defined. A defined method list overrides the default method list.

All authentication methods, except for local, line password, and enable authentication, must be defined through AAA. For information about configuring all authentication methods, including those implemented outside of the AAA security services, refer to the chapter "Configuring Authentication."

- **Authorization**—Provides the method for remote access control, including one-time authorization or authorization for each service, per-user account list and profile, user group support, and support of IP, IPX, ARA, and Telnet.

AAA authorization works by assembling a set of attributes that describe what the user is authorized to perform. These attributes are compared to the information contained in a database for a given user and the result is returned to AAA to determine the user's actual capabilities and restrictions. The database can be located locally on the access server or router or it can be hosted remotely on a RADIUS or TACACS+ security server. Remote security servers, such as RADIUS and TACACS+, authorize users for specific rights by associating attribute-value (AV) pairs, which define those rights with the appropriate user. All authorization methods must be defined through AAA.

As with authentication, you configure AAA authorization by defining a named list of authorization methods, and then applying that list to various interfaces. For information about configuring authorization using AAA, refer to the chapter "Configuring Authorization."

- Accounting—Provides the method for collecting and sending security server information used for billing, auditing, and reporting, such as user identities, start and stop times, executed commands (such as PPP), number of packets, and number of bytes.

Accounting enables you to track the services users are accessing as well as the amount of network resources they are consuming. When AAA accounting is activated, the network access server reports user activity to the RADIUS or TACACS+ security server (depending on which security method you have implemented) in the form of accounting records. Each accounting record is comprised of accounting AV pairs and is stored on the access control server. This data can then be analyzed for network management, client billing, and/or auditing. All accounting methods must be defined through AAA. As with authentication and authorization, you configure AAA accounting by defining a named list of accounting methods, and then applying that list to various interfaces. For information about configuring accounting using AAA, refer to the chapter "Configuring Accounting."

### 1.1.2 Benefits of Using AAA

AAA provides the following benefits:

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

### 1.1.3 AAA Principles

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

### 1.1.4 Method Lists

A method list is a sequential list that defines the authentication methods used to authenticate a user. Method lists enable you to designate one or more security protocols to be used for authentication, thus ensuring a backup system for authentication in case the initial method fails. Cisco IOS software uses the first method listed to authenticate users; if that method does not respond, Cisco IOS software



selects the next authentication method in the method list. This process continues until there is successful communication with a listed authentication method or the authentication method list is exhausted, in which case authentication fails.

The software attempts authentication with the next listed authentication method only when there is no response from the previous method. If authentication fails at any point in this cycle—meaning that the security server or local username database responds by denying the user access—the authentication process stops and no other authentication methods are attempted. The following figure shows a typical AAA network configuration that includes four security servers: R1 and R2 are RADIUS servers, and T1 and T2 are TACACS+ servers.

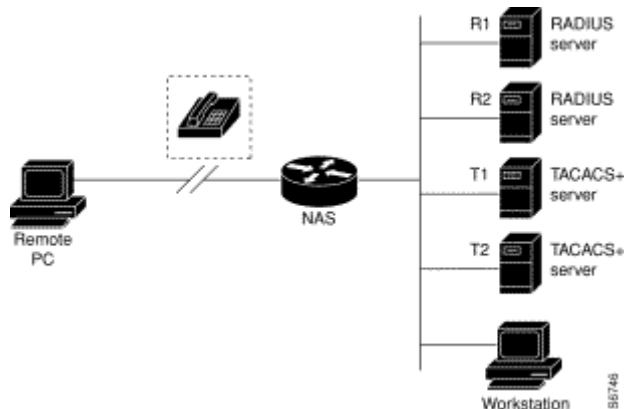


Figure 1-1 Typical AAA Network Configuration

Suppose the system administrator has defined a method list where R1 will be contacted first for authentication information, then R2, T1, T2, and finally the local username database on the access server itself. When a remote user attempts to dial in to the network, the network access server first queries R1 for authentication information. If R1 authenticates the user, it issues a PASS response to the network access server and the user is allowed to access the network. If R1 returns a FAIL response, the user is denied access and the session is terminated. If R1 does not respond, then the network access server processes that as an ERROR and queries R2 for authentication information. This pattern continues through the remaining designated methods until the user is either authenticated or rejected, or until the session is terminated. If all of the authentication methods return errors, the network access server will process the session as a failure, and the session will be terminated.

A FAIL response is significantly different from an ERROR. A FAIL means that the user has not met the criteria contained in the applicable authentication database to be successfully authenticated. Authentication ends with a FAIL response. An ERROR means that the security server has not responded to an authentication query. Because of this, no authentication has been attempted. Only when an ERROR is detected will AAA select the next authentication method defined in the authentication method list.

### 1.1.5 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.

## 1.1.6 Overview of the AAA Configuration Process

Configuring AAA is relatively simple after you understand the basic process involved. To configure security on a Cisco router or access server using AAA, follow this process:

- If you decide to use a separate security server, configure security protocol parameters, such as RADIUS, TACACS+, or Kerberos.
- Define the method lists for authentication by using an AAA authentication command.
- Apply the method lists to a particular interface or line, if required.
- (Optional) Configure authorization using the `aaa authorization` command.
- (Optional) Configure accounting using the `aaa accounting` command.

## 1.2 AAA Authentication Configuration

### 1.2.1 AAA Authentication Configuration Task List

- Configuring Login Authentication Using AAA
- Configuring PPP Authentication Using AAA
- Enabling Password Protection at the Privileged Level
- Configuring Message Banners for AAA Authentication
- AAA authentication `username-prompt`
- AAA authentication `password-prompt`
- Establishing Username Authentication
- Enabling Password

### 1.2.2 AAA Authentication Configuration Task

To configure AAA authentication, perform the following configuration processes:

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

### 1.2.2.1 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.

To configure login authentication by using AAA, use the following commands beginning in global configuration mode:

Command	Purpose
<code>aaa authentication login {default   list-name} method1 [method2...]</code>	Enables AAA globally.
<code>line [ console   vty ] line-number [ending-line-number]</code>	Enters line configuration mode for the lines to which you want to apply the authentication list.
<code>login authentication {default   list-name}</code>	Applies the authentication list to a line or set of lines.

The list-name is a character string used to name the list you are creating. The method argument refers to the actual method the authentication algorithm tries. The additional methods of authentication are used only if the previous method returns an error, not if it fails. To specify that the authentication should succeed even if all methods return an error, specify `none` as the final method in the command line.

For example, to specify that authentication should succeed even if (in this example) the TACACS+ server returns an error, enter the following command:

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

**Note:**

Because the `none` keyword enables any user logging in to successfully authenticate, it should be used only as a backup method of authentication.

The following table lists the supported login authentication methods.:

Keyword	description
<code>enable</code>	Uses the enable password for authentication.
<code>group name</code>	Uses named server group for authentication.
<code>group radius</code>	Uses the list of all RADIUS servers for authentication.
<code>line</code>	Uses the line password for authentication.
<code>local</code>	Uses the local username database for authentication.
<code>local-case</code>	Uses case-sensitive local username authentication.
<code>none</code>	Uses no authentication.

(1) Login Authentication Using Enable Password

Use the `aaa authentication login` command with the `enable` method keyword to specify the enable password as the login authentication method. For example, to

specify the enable password as the method of user authentication at login when no other method list has been defined, enter the following command:

```
aaa authentication login default enable
```

(2) Login Authentication Using Line Password

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

```
aaa authentication login default line
```

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

(3) Login Authentication Using Local Password

Use the aaa authentication login command with the local method keyword to specify that the Cisco router or access server will use the local username database for authentication. For example, to specify the local username database as the method of user authentication at login when no other method list has been defined, enter the following command:

```
aaa authentication login default local
```

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

(4) Login Authentication Using Group RADIUS

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

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

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

### 1.2.2.2 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
<b>aaa authentication enable default</b> <i>method1 [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	Description
enable	Uses the enable password for authentication.
group <i>group-name</i>	Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the aaa group server radius or aaa group server tacacs+ command.
group radius	Uses the list of all RADIUS hosts for authentication.
line	Uses the line password for authentication.
none	Uses no authentication.

### 1.2.2.3 Configuring Message Banners for AAA Authentication

AAA supports the use of configurable, personalized login and failed-login banners. You can configure message banners that will be displayed when a user logs in to the system to be authenticated using AAA and when, for whatever reason, authentication fails.

- Configuring a Login Banner

To configure a banner that will be displayed whenever a user logs in (replacing the default message for login), use the following commands in global configuration mode:

Command	Purpose
<b>aaa authentication banner <i>delimiter</i></b> <i>text-string delimiter</i>	Creates a personalized login banner.

- Configuring a Failed-Login Banner

To configure a message that will be displayed whenever a user fails login (replacing the default message for failed login), use the following commands in global configuration mode:

Command	Purpose
<b>aaa authentication fail-message <i>delimiter</i></b> <i>text-string delimiter</i>	Creates a message to be displayed when a user fails login.

#### Instruction

To create a login banner, you need to configure a delimiting character, which notifies the system that the following text string is to be displayed as the banner, and then the text string itself. The delimiting character is repeated at the end of the text string to signify the end of the banner. The delimiting character can be any single character in the extended ASCII character set, but once defined as the delimiter, that character cannot be used in the text string making up the banner.

### 1.2.2.4 AAA authentication username-prompt

To change the text displayed when users are prompted to enter a username, use the aaa authentication username-prompt command in global configuration mode. To return to the default username prompt text, use the no form of this command. username:

The aaa authentication username-prompt command does not change any dialog that is supplied by a remote TACACS+ server. Use the following command to configure in global configuration mode:

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

<b>aaa authentication username-prompt</b> <i>text-string</i>	String of text that will be displayed when the user is prompted to enter an username.
---	---

### 1.2.2.5 AAA authentication password-prompt

To change the text displayed when users are prompted for a password, use the `aaa authentication password-prompt` command in global configuration mode. To return to the default password prompt text, use the `no` form of this command.

password:

The `aaa authentication password-prompt` command does not change any dialog that is supplied by a remote TACACS+ server. Use the following command to configure in global configuration mode:

Command	Purpose
<b>aaa authentication password-prompt</b> <i>text-string</i>	String of text that will be displayed when the user is prompted to enter a password.

### 1.2.2.6 Enabling password

To set a local password to control access to various privilege levels, use the `enable password` command in global configuration mode. To remove the password requirement, use the `no` form of this command.

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

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

## 1.2.3 AAA Authentication Configuration Example

### 1.2.3.1 RADIUS Authentication Example

This section provides one sample configuration using RADIUS.

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

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

The lines in this sample RADIUS authentication and authorization configuration are defined as follows.:

- The `aaa authentication login radius-login radius local` command configures the router to use RADIUS for authentication at the login prompt. If RADIUS returns an error, the user is authenticated using the local database.
- The `aaa authentication ppp radius-ppp radius` command configures the software to use PPP authentication using CHAP or PAP if the user has not already logged in. If the EXEC facility has authenticated the user, PPP authentication is not performed.

- The `aaa authorization network radius-network radius command command` queries RADIUS for network authorization, address assignment, and other access lists.
- The `login authentication radius-login` command enables the `radius-login` method list for line 3.

## 1.3 AAA Authorization Configuration

### 1.3.1 AAA Authorization Configuration Task List

- Configuring EXEC Authorization using AAA

### 1.3.2 AAA Authorization Configuration Task

To configure AAA authorization, perform the following configuration processes:

(1) If you decide to use a separate security server, configure security protocol parameters, such as RADIUS, TACACS+, or Kerberos.

(2) Define the method lists for authorization by using an AAA authorization command.

(3) Apply the method lists to a particular interface or line, if required.

#### 1.3.2.1 Configuring EXEC Authorization Using AAA

Use the `aaa authorization` command to enable authorization

Use `aaa authorization exec` command to run authorization to determine if the user is allowed to run an EXEC shell. This facility might return user profile information such as autocommand information.

Use line configuration command `login authorization` to apply these lists. Use the following command in global configuration mode:

Command	Purpose
<code>aaa authorization exec {default   list-name} method1 [method2...]</code>	Establishes global authorization list.
<code>line [console   vty ] line-number [ending-line-number]</code>	Enters the line configuration mode for the lines to which you want to apply the authorization method list.
<code>login authorization {default   list-name}</code>	Applies the authorization list to a line or set of lines(in line configuration mode).

The keyword `list-name` is the character string used to name the list of authorization methods.

The keyword method specifies the actual method during authorization process. Method lists enable you to designate one or more security protocols to be used for authorization, thus ensuring a backup system in case the initial method fails. The system uses the first method listed to authorize users for specific network services; if that method fails to respond, the system selects the next method listed in the method list. This process continues until there is successful communication with a listed authorization method, or all methods defined are exhausted. If all specified methods fail to respond, and you still want the system to enter the EXEC shell, you should specify none as the last authorization method in command line.

Use default parameter to establish a default list, and the default list will apply to all interfaces automatically. For example, use the following command to specify radius as the default authorization method for exec:

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

**Note:**

If no method list is defined, the local authorization service will be unavailable and the authorization is allowed to pass..

The following table lists the currently supported EXEC authorization mode:

Keyword	Description
group <i>WORD</i>	Uses a named server group for authorization.
group radius	Uses radius authorization.
local	Uses the local database for authorization.
if-authenticated	Allows the user to access the requested function if the user is authenticated.
none	No authorization is performed.

### 1.3.3 AAA Authorization Example

#### 1.3.3.1 EXEC local authorization example

```
aaa authentication login default local
aaa authorization exec default local
!
username exec1 password 0 abc privilege 15
username exec2 password 0 abc privilege 10
username exec3 nopassword
username exec4 password 0 abc user-maxlinks 10
username exec5 password 0 abc autocommand telnet 172.16.20.1
!
```

The lines in this sample RADIUS authorization configuration are defined as follows:

- The aaa authentication login default local command defines the default method list of login authentication. This method list applies to all login authentication servers automatically.



- The aaa authorization exec default local command defines default method list of exec authorization. The method list automatically applies to all users that need to enter exec shell.
- Username is exec1, login password is abc, EXEC privileged level is 15(the highest level), that is, when user exec1 whose privileged level is 15 logs in exec shell, all commands can be checked and performed.
- Username is exec2, login password is abc, EXEC privileged level is 10, that is, when user exec2 whose privileged level is 10 logs in EXEC shell, commands with privileged level less than 10 can be checked and performed.
- Username is exec3, no password is needed for login.
- Username is **exec4**, login password is **abc**, the maximum links of the user is 10.
- Username is **exec5**, login password is **abc**, user performs telnet 172.16.20.1 immediately when logging in exec shell.

## 1.4 AAA Accounting Configuration

### 1.4.1 AAA Accounting Configuration Task List

- Configuring Connection Accounting using AAA
- Configuring Network Accounting using AAA

### 1.4.2 AAA Accounting Configuration Task

To configure AAA accounting, perform the following configuration processes:

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

#### 1.4.2.1 Configuring Accounting Connection Using AAA

Use the **aaa accounting** command to enable AAA accounting.

To create a method list to provide accounting information about all outbound connections made from the network access server, use the aaa accounting connection command.

Command	Purpose
<b>aaa accounting connection</b> {default   <i>list-name</i> } {start-stop   stop-only   none} <b>group</b> <i>groupname</i>	Establishes global accounting list.

The keyword list-name is used to name any character string of the establishing list. The keyword method specifies the actual method adopted during accounting process.

The following table lists currently supported connection accounting methods:

Keyword	Description
group <i>WORD</i>	Enables named server group for accounting.
group radius	Enables radius accounting.
none	Disables accounting services for the specified line or interface.
stop-only	Sends a "stop" record accounting notice at the end of the requested user process.
start-stop	RADIUS or TACACS+ sends a "start" accounting notice at the beginning of the requested process and a "stop" accounting notice at the end of the process.

#### 1.4.2.2 Configuring Network Accounting Using AAA

Use the `aaa accounting` command to enable AAA accounting.

To create a method list to provide accounting information for SLIP, PPP, NCPs, and ARAP sessions, use the `aaa accounting network` command in global configuration mode.

Command	Purpose
<code>aaa accounting network {default   list-name} {start-stop   stop-only   none} group groupname</code>	Enables global accounting list.

The keyword list-name is used to name any character string of the establishing list. The keyword method specifies the actual method adopted during accounting process.

The following table lists currently supported network accounting methods:

Keyword	Description
group <i>WORD</i>	Enables named server group for accounting.
group radius	Enables radius accounting.
none	Disables accounting services for the specified line or interface.
stop-only	Sends a "stop" record accounting notice at the end of the requested user process.
start-stop	RADIUS or TACACS+ sends a "start" accounting notice at the beginning of the requested process and a "stop" accounting notice at the end of the process.

#### 1.4.2.3 AAA Accounting Update

To enable periodic interim accounting records to be sent to the accounting server, use the `aaa accounting update` command in global configuration mode. To disable interim accounting updates, use the `no` form of this command.

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

<b>aaa accounting update</b> [newinfo] [periodic number]	Enables AAA accounting update.
---	--------------------------------

If the newinfo keyword is used, interim accounting records will be sent to the accounting server every time there is new accounting information to report. An example of this would be when IP Control Protocol (IPCP) completes IP address negotiation with the remote peer. The interim accounting record will include the negotiated IP address used by the remote peer.

When used with the periodic keyword, interim accounting records are sent periodically as defined by the argument number. The interim accounting record contains all of the accounting information recorded for that user up to the time the accounting record is sent.

When using both the newinfo and periodic keywords, interim accounting records are sent to the accounting server every time there is new accounting information to report, and accounting records are sent to the accounting server periodically as defined by the argument number. For example, if you configure the `aaa accounting update newinfo periodic number` command, all users currently logged in will continue to generate periodic interim accounting records while new users will generate accounting records based on the newinfo algorithm.

#### 1.4.2.4 AAA accounting suppress null-username

To prevent the AAA system from sending accounting records for users whose username string is NULL, use the `aaa accounting suppress null-username` command in global configuration mode. To allow sending records for users with a NULL username, use the `no` form of this command.

- **aaa accounting suppress null-username**

## 1.5 Local Account Policy Configuration

### 1.5.1 Local Account Policy Configuration Task List

- Configuring local authentication policy
- Configuring local authorization policy
- Configuring local password policy
- Configuring local policy group

### 1.5.2 Local Account Policy Configuration Task

#### 1.5.2.1 Configuring local authentication policy

To configure local authentication policy, use the `localauthen WORD` command in global configuration mode.

- (1) The login max-tries within a certain time

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

The local authentication policy can be used in a local policy group or in a local account. The latter is the preferred one.

#### 1.5.2.2 Configuring local authorization policy configuration

To configure the local authorization policy, use the **localauthor WORD** command in global configuration mode.

- (1) Authorize the privileged one for the login users

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

The local authorization policy can be used in a local policy group or in a local account. The latter is the preferred one.

#### 1.5.2.3 Configuring local password policy configuration

To configure the local password policy, use the **localpass WORD** command in global configuration mode.

- (1) Distinguish the password and the user name.

**non-user**

- (2) Check the history password. (The renewed password and the history password must be different. There are 20 history records.)

**non-history**

- (3) Set the password constitution. (Make the password as complicated as possible.)

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

- (4) The minimum length of the password (Make the password as complicated as possible.)

**min-length <1-127>**

- (5) The password validity (The password validity starts from the time the account is configured or the password is modified.)

**validity 1d2h3m4s**

The local password policy can be used in a local policy group or in a local account. The latter is the preferred one.

#### 1.5.2.4 Configuring local policy group

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

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

**local authen-group** *WORD*

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

**local author-group** *WORD*

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

**local pass-group** *WORD*

- (4) Local account configuration: set the max connection links or freeze for the policy group

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

- (5) Local account configuration: set the account in 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 lines in this sample local account policy configuration are defined as follows: :

- The aaa authentication login default local command defines the default method list of login authentication. This method list applies to all login authentication servers automatically.
- The aaa authorization exec default local command defines default method list of exec authorization. The method list automatically applies to all users that need to enter exec shell.
- 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.

### 2.1 Introduction

#### 2.1.1 RADIUS Introduction

RADIUS is a distributed client/server system that secures networks against unauthorized access. In the implementation, RADIUS clients run on switches and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.

RADIUS has been implemented in a variety of network environments that require high levels of security while maintaining network access for remote users.

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

- Networks with multiple-vendor access servers, each supporting RADIUS. For example, access servers from several vendors use a single RADIUS server-based security database. In an IP-based network with multiple vendors' access servers, dial-in users are authenticated through a RADIUS server that has been customized to work with the Kerberos security system.
- Networks in which a user must only access a single service. Using RADIUS, you can control user access to a single host, to a single utility such as Telnet, or to a single protocol such as Point-to-Point Protocol (PPP). For example, when a user logs in, RADIUS identifies this user as having authorization to run PPP using IP address 10.2.3.4 and the defined access list is started.
- Networks that require resource accounting. You can use RADIUS accounting independent of RADIUS authentication or authorization. The RADIUS accounting functions allow data to be sent at the start and end of services, indicating the amount of resources (such as time, packets, bytes, and so on) used during the session. An Internet service provider (ISP) might use a freeware-based version of RADIUS access control and accounting software to meet special security and billing needs.

RADIUS is not suitable in the following network security situations::

- Multiprotocol access environments. RADIUS does not support the following protocols::  
AppleTalk Remote Access (ARA)

NetBIOS Frame Control Protocol (NBFCP)

- NetWare Asynchronous Services Interface (NASI)
- X.25 PAD connections
- Switch-to-switch situations. RADIUS does not provide two-way authentication.
- Networks using a variety of services. RADIUS generally binds a user to one service model.

### 2.1.2 RADIUS Operation

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

- (1) The user is prompted for and enters a username and password.
- (2) The username and encrypted password are sent over the network to the RADIUS server.
- (3) The user receives one of the following responses from the RADIUS server:
  - a. ACCEPT—The user is authenticated.
  - b. REJECT—The user is not authenticated and is prompted to reenter the username and password, or access is denied.
  - c. CHALLENGE—A challenge is issued by the RADIUS server. The challenge collects additional data from the user.
  - d. CHANGE PASSWORD—A request is issued by the RADIUS server, asking the user to select a new password.

The ACCEPT or REJECT response is bundled with additional data that is used for EXEC or network authorization. You must first complete RADIUS authentication before using RADIUS authorization. The additional data included with the ACCEPT or REJECT packets consists of the following:

Services that the user can access, including Telnet, rlogin, or local-area transport (LAT) connections, and PPP, Serial Line Internet Protocol (SLIP), or EXEC services.

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

## 2.2 RADIUS Configuration 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::

- You may use the aaa authorization global command to authorize specific user functions. For more information about using the aaa authorization command, refer to the chapter "Configuring Authorization."
- You may use the aaa accounting command to enable accounting for RADIUS connections. For more information about using the aaa accounting command, refer to the chapter "Configuring Accounting."

## 2.3 RADIUS Configuration Task List

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

## 2.4 RADIUS Configuration Task

### 2.4.1 Configuring Switch to RADIUS Server Communication

The RADIUS host is normally a multiuser system running RADIUS server software from Livingston, Merit, Microsoft, or another software provider.

A RADIUS server and a Cisco router use a shared secret text string to encrypt passwords and exchange responses.

To configure RADIUS to use the AAA security commands, you must specify the host running the RADIUS server daemon and a secret text (key) string that it shares with the router.

To configure per-server RADIUS server communication, use the following command in global configuration mode:

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

	the router and a RADIUS server.
--	---------------------------------

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

Command	Purpose
<b>radius-server retransmit</b> <i>retries</i>	Specifies how many times the switch transmits each RADIUS request to the server before giving up (the default is 2).
<b>radius-server timeout</b> <i>seconds</i>	Specifies for how many seconds a switch waits for a reply to a RADIUS request before retransmitting the request.
<b>radius-server deadline</b> <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
<b>radius-server vsa send</b> [authentication]	Enables the network access server to recognize and use VSAs as defined by RADIUS IETF attribute 26.

## 2.4.3 Specifying RADIUS Authentication

After you have identified the RADIUS server and defined the RADIUS authentication key, you must define method lists for RADIUS authentication. Because RADIUS authentication is facilitated through AAA, you must enter the `aaa authentication` command, specifying RADIUS as the authentication method. For more information, refer to the chapter "Configuring Authentication."

## 2.4.4 Specifying RADIUS Authorization

AAA authorization lets you set parameters that restrict a user's access to the network. Authorization using RADIUS provides one method for remote access control, including one-time authorization or authorization for each service, per-user account list and profile, user group support, and support of IP, IPX, ARA, and Telnet. Because RADIUS authorization is facilitated through AAA, you must issue the `aaa authorization`

command, specifying RADIUS as the authorization method. For more information, refer to the chapter "Configuring Authorization."

### 2.4.5 Specifying RADIUS Accounting

The AAA accounting feature enables you to track the services users are accessing as well as the amount of network resources they are consuming. Because RADIUS accounting is facilitated through AAA, you must issue the `aaa accounting` command, specifying RADIUS as the accounting method. For more information, refer to the chapter "Configuring Accounting."

## 2.5 RADIUS Configuration Examples

### 2.5.1 RADIUS Authentication and Authorization Example

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

```
aaa authentication login use-radius group radius local
```

The lines in this sample RADIUS authentication and authorization configuration are defined as follows:

```
aaa authentication login use-radius radius local
```

configures the router to use RADIUS for authentication at the login prompt. If RADIUS returns an error, the user is authenticated using the local database. In this example, `use-radius` is the name of the method list, which specifies RADIUS and then local authentication.

#### RADIUS Authentication, Authorization, and Accounting Example

The following example shows a general configuration using RADIUS with the AAA command set:

```
radius-server host 1.2.3.4
radius-server key myRaDiUSpassWoRd
username root password AlongPassword
aaa authentication login admins radius local
line vty 1 16
login authentication admins
```

The lines in this example RADIUS authentication, authorization, and accounting configuration are defined as follows:

`radius-server host` command defines the IP address of the RADIUS server host. ;

`radius-server key` command defines the shared secret text string between the network access server and the RADIUS server host.

`aaa authentication login admins group radius local` command defines the authentication method list "dialins," which specifies that RADIUS authentication and then (if the RADIUS server does not respond) local authentication will be used on serial lines using PPP.

login authentication admins command applies the "admins" method list for login authentication.

## 2.5.2 RADIUS Application Example

The following example shows how to define the general configuration through the AAA command set:

```
radius-server host 1.2.3.4
radius-server key myRaDiUSpassWoRd
username root password AlongPassword
aaa authentication login admins radius local
line vty 1 16
login authentication admins
```

In the example above, each command line has its own meaning. See the following content:

The command **radius-server host** defines the IP address of the RADIUS server.

The command **radius-server key** defines the shared pin between the network access server and the RADIUS server.

The command **aaa authentication login admins radius local** defines the authentication method list **admins**, which first specifies RADIUS as the authentication method and then uses the local authentication if the RADIUS server does not respond.

The command **login authentication admins** specifies the method list **admins** as the login authentication method.

## 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

##### 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.

**Notice:**

*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:

<b>ACCEPT</b>	User passes authentication, and service begins. If network access server is configured as requiring service authorization, authorization begins at this moment.
<b>REJECT</b>	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.
<b>ERROR</b>	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.
<b>CONTINUE</b>	It prompts user to enter additional authentication information.

## 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+ to do authentication. More information about command *aaa authentication*, please refer to "Authentication Configuration".

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

## 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
<b>tacacs-server host</b> <i>ip-address</i>  [ <b>single-connection</b>   <b>multi-connection</b> ] [ <b>port</b> <i>integer</i> ] [ <b>timeout</b> <i>integer</i> ] [ <b>key</b> <i>string</i> ]	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 router's waiting response from server.
- Use parameter *key* to assign the encrypted and decrypted secret keys for messages.

#### Notice:

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 key* 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

<b>tacacs-server key</b> <i>keystring</i>	To set up the encrypted secret key matched with the encrypted secret key used by TACACS+ server.
---	--

**Notice:**

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

### 3.4.3 Assigning to use TACACS+ to do 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.

## 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* used during login authentication. If authentication is needed, key word *tacacs+* means the authentication is by TACACS+. If TACACS+ does not respond during authentication period, key word *local* indicates to use the local database on network access server to do 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 Example

```
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 is needed, keyword *tacacs+* means the authentication is processed by TACAS+. If TACACS+ does not respond during authentication, keyword *local* indicates to use the local database on the network access server to do 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 HTTP Switch Configuration.....	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 on 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 It is used to set the HTTPS port.....	2
Chapter 2 Configuration Preparation.....	4
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.....	5
2.2 Accessing a Switch through Secure Links.....	5
2.3 Introduction of Web Interface .....	5
2.3.1 Top Control Bar .....	6
2.3.2 Navigation Bar.....	7
2.3.3 Configuration Area .....	7
2.3.4 Bottom Control Bar.....	8
2.3.5 Configuration Area .....	8
Chapter 3 Basic Configuration.....	9
3.1 IP Address Configuration.....	9
3.2 Hostname Configuration.....	10
3.3 Time Management.....	10
Chapter 4 Configuration of the Physical Interface .....	12
4.1 Configuring Port Description .....	12
4.2 Configuring the Attributes of the Port .....	13
4.3 Rate control .....	13
4.4 Port mirroring.....	13
4.5 Loopback Detection.....	14
4.6 Port security .....	14
4.6.1 IP Binding Configuration.....	14
4.6.2 MAC Binding Configuration.....	15
4.6.3 Setting the Static MAC Filtration Mode .....	15
4.6.4 Static MAC Filtration Entries .....	15
4.6.5 Setting the Dynamic MAC Filtration Mode .....	16
4.7 Storm control .....	16
4.7.1 Broadcast Storm Control.....	16
4.7.2 Multicast Storm Control.....	17
4.7.3 Unknown Unicast Storm Control .....	18

4.8 Port Protect Group Configuration .....	18
4.8.1 Port Protect Group List.....	18
4.8.2 Port Protect Group Interface Configuration.....	19
4.9 POE Management.....	19
4.9.1 POE Global Configuration.....	19
4.9.2 POE Global Real-time Information.....	20
4.9.3 POE Port List .....	20
4.9.4 POE Ports' Policy Power-up.....	21
4.9.5 POE Ports' Power Real-time Information.....	22
4.9.6 POE Ports' Other Real-time Information .....	22
Chapter 5 Layer-2 Configuration .....	23
5.1 VLAN Settings .....	24
5.1.1 VLAN List .....	24
5.1.2 VLAN Settings.....	24
5.2 GVRP Configuration.....	25
5.2.1 GVRP Global Attribute Configuration .....	25
5.2.2 Global Interface Attribute Configuration .....	25
5.3 STP Configuration .....	25
5.3.1 STP Status Information .....	25
5.3.2 Configuring the Attributes of the STP Port .....	26
5.4 IGMP-Snooping Configuration .....	27
5.4.1 IGMP-Snooping Configuration .....	27
5.4.2 IGMP-Snooping VLAN List.....	27
5.4.3 Static Multicast Address .....	28
5.4.4 Multicast List .....	29
5.5 Setting Static ARP .....	29
5.6 Static MAC Address Configuration .....	30
5.7 LLDP Configuration .....	31
5.7.1 Configuring the Global Attributes of LLDP .....	31
5.7.2 LLDP Port Attribute Configuration .....	32
5.8 DDM Configuration.....	32
5.9 Port Aggregation Configuration .....	32
5.9.1 Port Aggregation Configuration .....	32
5.10 Ring Protection Configuration .....	33
5.10.1 EAPS Ring List.....	33
5.10.2 EAPS Ring Configuration.....	34
5.10.3 Configuring Load Balance of Port Aggregation Group.....	34
5.11 MEAPS Configuration.....	35
5.11.1 MEAPS Ring Configuration .....	35
5.11.2 MEAPS Ring Configuration .....	35
5.12 GMRP Configuration .....	36
5.12.1 GMRP Global Configuration.....	36
5.12.2 GMRP Interface Configuration .....	37
5.12.3 GMRP Multicast Member List.....	38
5.12 PTP Configuration .....	38
5.12.1 PTP Global Configuration.....	38

5.12.2 PTP Interface Configuration .....	39
5.12.3 PTP VLAN Configuration.....	39
5.12.4 PTP Unicast Configuration .....	39
5.13 Backup Link Protocol Configuration .....	40
5.13.1 Backup Link Protocol Global Configuration.....	40
5.13.2 Backup Link Protocol Interface Configuration .....	41
5.14 DHCP Snooping Configuration.....	41
5.14.1 DHCP Snooping Global Attribute Configuration .....	41
5.14.2 DHCP Snooping VLAN Attribute Configuration .....	42
5.14.3 DHCP Snooping Interface Attribute Configuration .....	43
5.14.4 DHCP Snooping Manual Binding Configuration.....	43
5.15 MTU Configuration .....	44
5.16 PDP Configuration.....	44
5.16.1 Configuring the Global Attributes of PDP .....	44
5.16.2 PDP Interface Attribute Configuration .....	45
Chapter 6 Layer-3 Configuration .....	46
6.1 Configuring the VLAN Interface.....	46
Chapter 7 Advanced Configuration .....	48
7.1 QoS Configuration.....	48
7.1.1 Configuring QoS Port.....	48
7.1.2 Global QoS Configuration .....	49
7.2 IP Access Control List.....	50
7.2.1 Setting the Name of the IP Access Control List.....	50
7.2.2 Setting the Rules of the IP Access Control List.....	50
7.2.3 Applying the IP Access Control List.....	52
7.3 MAC Access Control List.....	52
7.3.1 Setting the Name of the MAC Access Control List.....	52
7.3.2 Setting the Rules of the MAC Access Control List .....	52
7.3.3 Applying the MAC Access Control List .....	53
Chapter 8 Network Management Configuration .....	54
8.1 SNMP Configuration.....	54
8.1.1 SNMP Community Management.....	54
8.1.2 SNMP Host Management.....	55
8.2 RMON .....	55
8.2.1 RMON Statistic Information Configuration .....	55
8.2.2 RMON History Information Configuration.....	56
8.2.3 RMON Alarm Information Configuration.....	57
8.2.4 RMON Event Configuration.....	57
Chapter 9 Diagnosis Tools .....	59
9.1 Ping .....	59
9.1.1 Ping .....	59
Chapter 10 System Management.....	61
10.1 User Management.....	61
10.1.1 User List.....	61
10.1.2 Establishing a New User .....	62

- 10.1.3 User Group Management..... 62
- 10.1.4 Password Group Management ..... 63
- 10.1.5 Authentication Group Configuration ..... 64
- 10.1.6 Author-Group Management..... 64
- 10.2 Log Management ..... 65
- 10.3 Managing the Configuration Files..... 65
  - 10.3.1 Exporting the Configuration Information..... 66
  - 10.3.2 Importing the Configuration Information ..... 66
- 10.4 Software Management ..... 66
  - 10.4.1 Backing up the IOS Software ..... 67
  - 10.4.2 Upgrading the IOS Software ..... 67
- 10.5 Rebooting the Device ..... 68

# Chapter 1 HTTP Switch Configuration

## 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
ip http language {chinese   english}	Sets the prompt language of Web configuration to <b>Chinese</b> or <b>English</b> .

### 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 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 { portNumber }	Sets 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	Enables the HTTP service.
ip http {timeout}	Configures the timeout time of HTTP abnormal packets.

### 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	Sets the HTTP access mode.

### 1.1.5 Setting the Maximum Number of VLAN Entries on 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	Sets the HTTPS access mode.

### 1.2.2 It is used to set 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.

Parameter	Remarks
ip http secure-port	Sets the HTTPS port.

<i>{portNumber}</i>	
---------------------	--

## Chapter 2 Configuration Preparation

### 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 **192.168.0.1** 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 in figure 1. Both the original username and the password are "admin", which is capital sensitive.

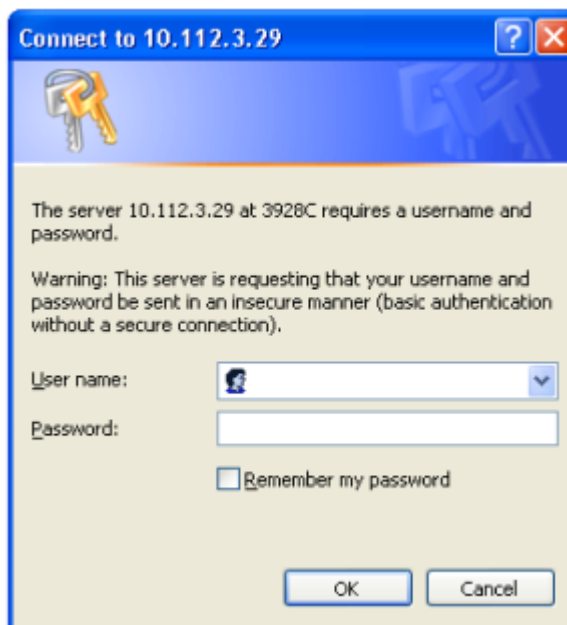


Figure 1: ID checkup of WEB login

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 **ip http server** command in global configuration mode and start the Web service.
5. Run **username** to set the username 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 **write** to store 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 **ip http server** command in global configuration mode and start the Web service.
5. Run **username** to set the username 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 **no ip http http-access enable** to forbid to access the switch through insecure links.
8. Enter **write** to store 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) and then press the **Enter** key. Then the switch can be accessed through the secure links.

## 2.3 Introduction of Web Interface

The Web homepage appears after login, as shown in figure 2:

The screenshot shows the web configuration interface for a SWITCH. At the top right, there are links for 'Save All | Logout | Port Pane'. On the left, a navigation menu includes 'Device Status', 'Device Info', 'Interface State', 'Interface Flow', 'Mac Address Table', 'Log Query', 'Basic Config', 'Port Config', 'L2 Config', 'Advanced Config', 'Network Mgr.', 'Diagnostic Tool', and 'System Mgr.'. The main content area is titled 'Device Info' and contains a 'System Information' table with the following data:

Device Type	SWITCH
BIOS Version	0.3.5
Firmware Version	2.1.1B
Serial No.	200-20013040101
MAC Address	FCFA.F749.0F00
IP Address	192.168.1.79
Current Time	1970-1-1 0:1:20
Uptime	0 Day -0 Hour -1 Minute -20 Second
CPU Usage	1%
Memory Usage	4294967230%

A 'Refresh' button is located below the table.

Figure 2: Web homepage

The whole 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](#) | [Logout](#) | [Port Panel](#) | [About](#)

Figure 3: Top control bar

Save All	Write the current settings to the configuration file of the device. It is equivalent to the execution of the <b>write</b> 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.

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

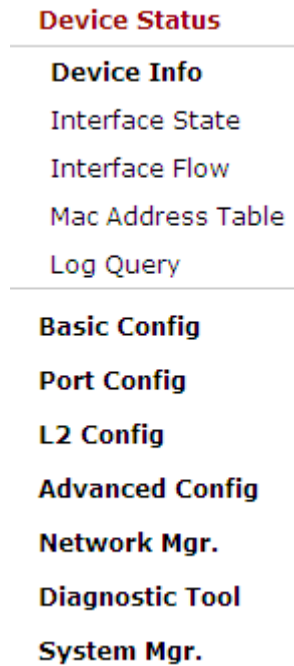


Figure 4 Navigation bar

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 sub-item. 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

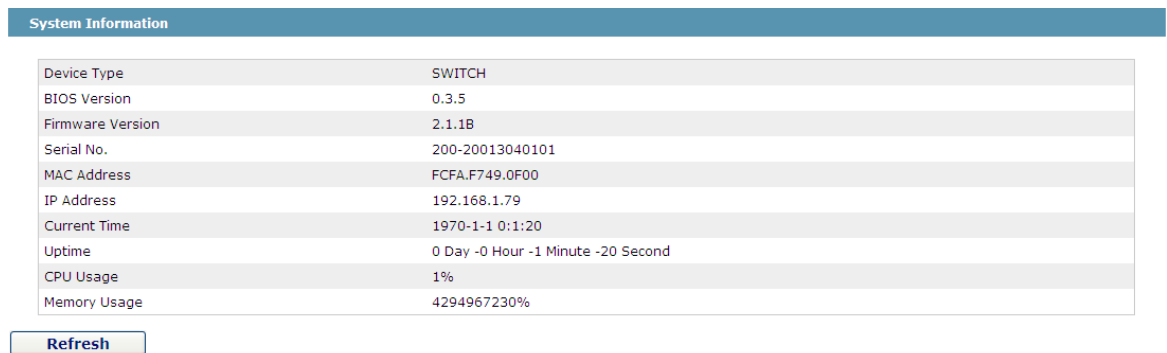


Figure 5 Configuration Area

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 Bottom Control Bar

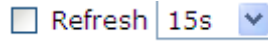


Figure 6: Bottom control bar

If you click the **About** button on the top control bar, the bottom control bar appears. The main function of the bottom control bar is to realize the automatic refreshing of the configuration display area. For example, if you click “Interface Flow” in the navigation bar and then click “Refresh”, the flow of the interface can be continuously monitored.

After you click “Refresh”, the countdown of the next-time refresh will appear on the left side. You can modify the countdown settings by clicking the dropdown list.

---

**Note:**

The smaller the countdown value is set, that is, the higher the frequency is, the higher the CPU usage is.

---

### 2.3.5 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 reset.
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

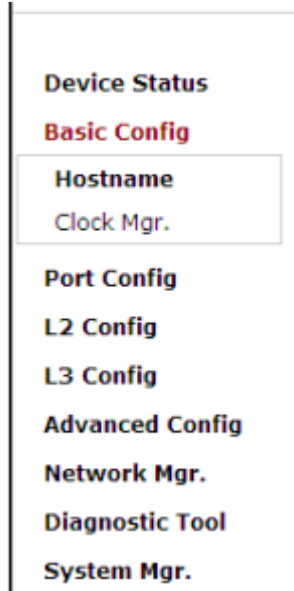


Figure 1 A list of basic configuration

### 3.1 IP Address Configuration

If you click **Basic Config** -> **IP Address Config** in the navigation bar, the **IP Address Configuration** page appears, as shown in figure 2.

**IP Address Configuration**

Configure IP address of interface VLAN.

MAC Address	5c:cc:ff:21:04:69
IP address*	<input type="text" value="90.0.0.2"/>
MASK address**	<input type="text" value="255.255.0.0"/>
Default Gateway	<input type="text" value="90.0.0.255"/>

**Help**

#Configure the IP address of interface VLAN for accessing the switch.

Figure 2 IP address configuration



This page is used to set the IP address of Interface Vlan 1, the management interface of the device. In initial conditions, the MAC address of the device, the IP address, mask and gateway of the interface will appear on this page. After the content is modified on this page, click "Apply" to finish the modification of the address; click "Reset" to restore the content of the page to the initial unchanged content.

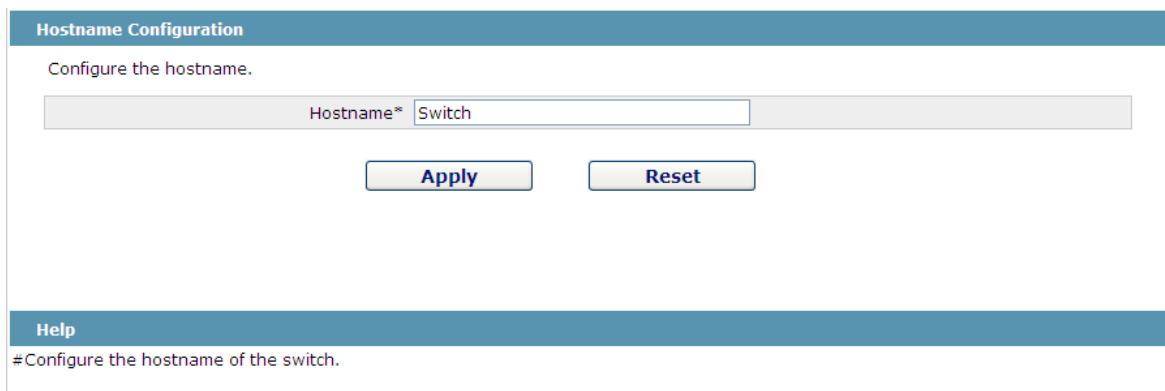
The items with the asterisk symbol "\*" are ones where you must enter values. "Default gateway" is an optional item, which can be null.

**Note:**

On the Web page, you can only set the IP address of Interface Vlan1; if the L3 switch is used and more Vlan interfaces need be created, please make configuration after a successful login through the console port or Telnet.

## 3.2 Hostname Configuration

If you click **Basic Config -> Hostname Config** in the navigation bar, the **Hostname Configuration** page appears, as shown in figure 3.



Hostname Configuration

Configure the hostname.

Hostname\* Switch

Apply Reset

Help

#Configure the hostname of the switch.

Figure 3 Hostname configuration

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".

## 3.3 Time Management

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

**Time Setting**

System Time

Select Time-Zone	(GMT)Greenwich Mean Time,Dublin,London,Lisbon	
<input checked="" type="radio"/> Set Time Manually	Set Time <input type="text" value="1970"/> Year <input type="text" value="01"/> Month <input type="text" value="01"/> Day <input type="text" value="00"/> Hour <input type="text" value="10"/> Minute(s) <input type="text" value="10"/> Second	
<input type="radio"/> Network Time Synchronization		
SNTP Server One	<input type="text"/>	
SNTP Server Two	<input type="text"/>	
SNTP Server Three	<input type="text"/>	
Synchronization Interval	<input type="text" value="1"/>	Minute(s)

Figure 4 Clock management

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



Figure 1: Physical port configuration list

### 4.1 Configuring Port Description

If you click **Physical port config -> Port description Config** in the navigation bar, the **Port description Configuration** page appears, as shown in figure 2.

Port	Port Description
G0/1	<input type="text"/>
G0/2	<input type="text"/>
G0/3	<input type="text"/>
G0/4	<input type="text"/>

Figure 2: Port description configuration

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 **Physical port config -> Port attribute Config** in the navigation bar, the **Port Attribute Configuration** page appears, as shown in figure 3.

Port	Status	Speed	Duplex	Flow Control	Medium
G0/1	Up	Auto	Auto	Off	Auto
G0/2	Up	Auto	Auto	Off	Auto
G0/3	Up	Auto	Auto	Off	Auto
G0/4	Up	Auto	Auto	Off	Auto
G0/5	Up	Auto	Auto	Off	Auto
G0/6	Up	Auto	Auto	Off	Auto
G0/7	Up	Auto	Auto	Off	Auto
G0/8	Up	Auto	Auto	Off	Auto
G0/9	Up	Auto	Auto	Off	Auto
G0/10	Up	Auto	Auto	Off	Auto

Figure 3 Configuring the port attributes

On this page you can modify the on/off status, rate, duplex mode, flow control status and medium type of a port.

Note:

1. The Web page does not support the speed and duplex mode of the fast-Ethernet port.
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 control

If you click **Physical port Config -> Port rate-limit Config** 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	Disable	64kbps	(1-15625)	Disable	64kbps	(1-15625)
G0/2	Disable	64kbps	(1-15625)	Disable	64kbps	(1-15625)
G0/3	Disable	64kbps	(1-15625)	Disable	64kbps	(1-15625)
G0/4	Disable	64kbps	(1-15625)	Disable	64kbps	(1-15625)
G0/5	Disable	64kbps	(1-15625)	Disable	64kbps	(1-15625)
G0/6	Disable	64kbps	(1-15625)	Disable	64kbps	(1-15625)
G0/7	Disable	64kbps	(1-15625)	Disable	64kbps	(1-15625)
G0/8	Disable	64kbps	(1-15625)	Disable	64kbps	(1-15625)
G0/9	Disable	64kbps	(1-15625)	Disable	64kbps	(1-15625)
G0/10	Disable	64kbps	(1-15625)	Disable	64kbps	(1-15625)

Figure 4: Port's rate limit

On this page you can set the reception speed and transmission speed of a port. By default, all ports have no speed limited.

## 4.4 Port mirroring

If you click **Physical port Config -> Port Mirror** in the navigation bar, the **Port Mirror Config** page appears, as shown in figure 4-5.

Mirrored Port	Mirror Mode
<input type="checkbox"/> G0/1	RX
<input checked="" type="checkbox"/> G0/2	TX

Figure 4-5 Port mirror configuration

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 Loopback Detection

If you click **Physical port Config -> Port loopback detection** in the navigation bar, the **Setting the port loopback detection** page appears, as shown in figure 4-6.

Port	Status	Keepalive Period
G0/1	Enable	3333 (0-32767)Seconds

Figure 4-6: Port loopback detection

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 **Physical port Config -> Port Security -> IP bind** in the navigation bar, the **Configure the IP-Binding Info** page appears, as shown in figure 4-7.

Interface Name	Detail
G0/1	<a href="#">Detail</a>

Figure 4-7 IP binding configuration

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	<a href="#">Edit</a>
<input type="checkbox"/>	2	192.168.0.3	<a href="#">Edit</a>

Figure 4-8 Setting the binding of the source IP address

## 4.6.2 MAC Binding Configuration

If you click **Physical port Config -> Port Security -> MAC bind** in the navigation bar, the **Configure the MAC-Binding Info** page appears, as shown in figure 4-10.

Interface Name	Detail
G0/1	<a href="#">Detail</a>

Figure 4-9 MAC binding configuration

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	<a href="#">Edit</a>
<input type="checkbox"/>	2	1234.1234.1235	<a href="#">Edit</a>

Figure 4-10 Setting the binding of the source MAC address

## 4.6.3 Setting the Static MAC Filtration Mode

If you click **Physical 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 4-11.

Interface Name	Port Mode	Static MAC Filtration Mode
G0/1	Access	<a href="#">Disable</a>

Figure 4-11: Setting the static MAC filtration mode

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 **Physical 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	<a href="#">Detail</a>

Figure 4-12: Static MAC filtration entry list

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	<a href="#">Edit</a>

Figure 4-13: Setting static MAC filtration entries

#### 4.6.5 Setting the Dynamic MAC Filtration Mode

If you click **Physical 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 4-14.

Interface Name	Dynamic MAC Filtration Mode	Max MAC Address
G0/1	Disable	1 (1-4095)

Figure 4-14: Setting the dynamic MAC filtration mode

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 **Physical 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	Disable	(1-1638400) 100PPS
G0/2	Disable	(1-1638400) 100PPS
G0/3	Disable	(1-1638400) 100PPS
G0/4	Disable	(1-1638400) 100PPS
G0/5	Disable	(1-1638400) 100PPS
G0/6	Disable	(1-1638400) 100PPS
G0/7	Disable	(1-1638400) 100PPS

Figure 5 Broadcast storm control

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

G0/38	Disable ▾		(1-1638400) 100PPS
G0/39	Disable ▾		(1-1638400) 100PPS
G0/40	Disable ▾		(1-1638400) 100PPS
G0/41	Disable ▾		(1-1638400) 100PPS
G0/42	Disable ▾		(1-1638400) 100PPS
G0/43	Disable ▾		(1-1638400) 100PPS
G0/44	Disable ▾		(1-1638400) 100PPS
G0/45	Disable ▾		(1-1638400) 100PPS
G0/46	Disable ▾		(1-1638400) 100PPS
G0/47	Disable ▾		(1-1638400) 100PPS
G0/48	Disable ▾		(1-1638400) 100PPS
T1/1	Disable ▾		(1-1638400) 100PPS
T1/2	Disable ▾		(1-1638400) 100PPS
T1/3	Disable ▾		(1-1638400) 100PPS
T1/4	Disable ▾		(1-1638400) 100PPS
T1/5	Disable ▾		(1-1638400) 100PPS
T1/6	Disable ▾		(1-1638400) 100PPS
T1/7	Disable ▾		(1-1638400) 100PPS
T1/8	Disable ▾		(1-1638400) 100PPS



Figure 6 Setting the broadcast storm control

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

G0/39	Disable <input type="button" value="v"/>		(1-1638400) 100PPS
G0/40	Disable <input type="button" value="v"/>		(1-1638400) 100PPS
G0/41	Disable <input type="button" value="v"/>		(1-1638400) 100PPS
G0/42	Disable <input type="button" value="v"/>		(1-1638400) 100PPS
G0/43	Disable <input type="button" value="v"/>		(1-1638400) 100PPS
G0/44	Disable <input type="button" value="v"/>		(1-1638400) 100PPS
G0/45	Disable <input type="button" value="v"/>		(1-1638400) 100PPS
G0/46	Disable <input type="button" value="v"/>		(1-1638400) 100PPS
G0/47	Disable <input type="button" value="v"/>		(1-1638400) 100PPS
G0/48	Disable <input type="button" value="v"/>		(1-1638400) 100PPS
T1/1	Disable <input type="button" value="v"/>		(1-1638400) 100PPS
T1/2	Disable <input type="button" value="v"/>		(1-1638400) 100PPS
T1/3	Disable <input type="button" value="v"/>		(1-1638400) 100PPS
T1/4	Disable <input type="button" value="v"/>		(1-1638400) 100PPS
T1/5	Disable <input type="button" value="v"/>		(1-1638400) 100PPS
T1/6	Disable <input type="button" value="v"/>		(1-1638400) 100PPS
T1/7	Disable <input type="button" value="v"/>		(1-1638400) 100PPS
T1/8	Disable <input type="button" value="v"/>		(1-1638400) 100PPS



Figure 7 Unknown unicast storm control

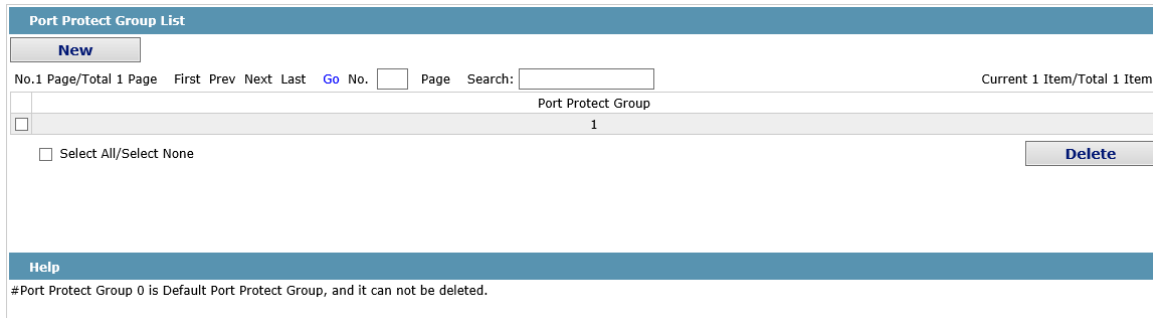
In the **Threshold** column you can enter the threshold of the broadcast packets. The legal threshold range for each port is given behind the threshold.

## 4.8 Port Protect Group Configuration

Click "Port Config" -> "Port Protect Group Config" in the navigation bar, and enter the configuration page of Port Protect Group List and Port Protect Group Interface Config.

### 4.8.1 Port Protect Group List

Click "Port Config" -> "Port Protect Group Config" -> "Port Protect Group List" in the navigation bar, and enter the configuration page of "Port Protect Group List".



**Port Protect Group List**

**New**

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

No.	Port Protect Group
1	1

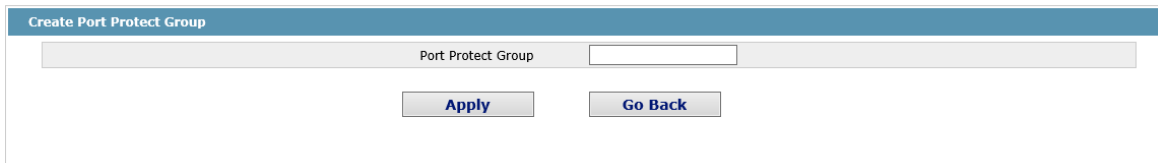
Select All/Select None **Delete**

**Help**

#Port Protect Group 0 is Default Port Protect Group, and it can not be deleted.

Click “New” to create a new port protect group, as shown in the above figure.

Tick one port protect group and delete it. The port protect group is 0 by default, which cannot be deleted.



**Create Port Protect Group**

Port Protect Group

**Apply** **Go Back**

### 4.8.2 Port Protect Group Interface Configuration

Click "Port Config" -> “Port Protect Group Config” -> “Port Protect Group Interface Config” in the navigation bar, and enter the configuration page of “Port Protect Group Interface Config”.

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, other ports can only be configured with the default protect group.

## 4.9 POE Management

### 4.9.1 POE Global Configuration

Click “physical port configuration” and “POE management” in turn to enter POE global configuration page.

**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	Start	
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

Configuring POE related configuration like power supply management mode and etc at this page.

Notice:

Occupied low priority's threshold means when user's power supply meets threshold the low priority port would be at disable status. Prohibited low priority power-up threshold means when user's power supply reaches its threshold the low priority port would be disconnected.

#### 4.9.2 POE Global Real-time Information

Click "physical port configuration", "POE management" and "POE global real-time information" in turn on the navigation bar to enter POE global real-time information page.

**POE Global Realtime Info**

POE Chip	PD69000	
POE Port Number	8	
PSE Total Power	300000	
PSE Uage Threshold	100%	
PSE Alarm Power	100	
PSE Consumed Power	0	
PSE Temperature	0	

Check POE chipset, POE port quantity and other information as above on this page.

#### 4.9.3 POE Port List

Click "physical port configuration", "POE management" and "POE port list" on navigation bar in turn to enter POE port list page.

**POE Interface List**

**Filters**

Port Type: All Slot Num: All Name(s):  Help

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	
g0/8	30000 mw	Low Priority	Disable	

**Help**

#The port that cannot be configured with POE will not be displayed  
 #When the Power Management Mode is auto, both the Port Max Power and the Port Priority cannot be configured. If it need to be configured, you can switch to the POE Mgr and change the Power Management Mode to Preemptive

Each of POE port's maximum power, priority and mandatory power-up could be configured at this page; illustrative information could also be added on the port at this page.

**Notice:**

This page only shows ports which support POE. When power management mode is automatic, port's maximum power and priority cannot be configured. If willing to configure maximum power and priority, please switch to POE management page and set power management mode as seizing.

#### 4.9.4 POE Ports' Policy Power-up

Click "physical port configuration", "POE management" and "POE ports' policy power-up" in turn on navigation bar to enter POE ports' policy power-up management page.

**POE Port Policy Power**

**Filters**

Port Type: All Slot Num: All Name(s):  Help

Port	POE Function	Time Range
g0/1	Enable	
g0/2	Enable	
g0/3	Enable	
g0/4	Enable	
g0/5	Enable	
g0/6	Enable	
g0/7	Enable	
g0/8	Enable	

**Help**

#The port that cannot be configured with POE will not be displayed  
 #Time Range can be configured by Advanced Config->Time Range Config

Two controlling methods of ports' power-up can be configured at this page. One is to open and shut down ports directly; the other is to power up based on time phase.

#### 4.9.5 POE Ports' Power Real-time Information

Click "physical port configuration", "POE management" and "POE ports power real-time information" in turn on navigation bar to enter POE ports' power real-time information.

**POE Interface Power List**

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

Port	Current Power	Setting Max Power	Average Power	Peak Power	Bottom Power
g0/1	0mw	0mw	-	-	-
g0/2	0mw	0mw	-	-	-
g0/3	0mw	0mw	-	-	-
g0/4	0mw	0mw	-	-	-
g0/5	0mw	0mw	-	-	-
g0/6	0mw	0mw	-	-	-
g0/7	0mw	0mw	-	-	-
g0/8	0mw	0mw	-	-	-

PSE Total Power    0

**Help**

#The port that cannot be configured with POE will not be displayed

#When the Power Counter is 0, the Average Power, the Peak Power and the Bottom Power will not be shown

At this page, you could check POE ports' current power, set real time information like the maximum power, average power, peak power, valley power and etc.

#### 4.9.6 POE Ports' Other Real-time Information

Click "physical port configuration", "POE management" and "POE port other real-time information" in turn on navigation bar to enter POE ports' other real-time information page.

**POE Port Other Info**

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

Port	POE Port Detection Status	POE Port Power Supply	POE IEEE Class	POE Port Current
g0/1	Fault	Signal	0	0mA
g0/2	Fault	Signal	0	0mA
g0/3	Fault	Signal	0	0mA
g0/4	Fault	Signal	0	0mA
g0/5	Fault	Signal	0	0mA
g0/6	Fault	Signal	0	0mA
g0/7	Fault	Signal	0	0mA
g0/8	Fault	Signal	0	0mA

**Help**

#The port that cannot be configured with POE will not be displayed

POE port detection status, POE port power-up status, POE IEEE Class and POE port electric current information could be checked at this page.

## Chapter 5 Layer-2 Configuration

<b>Device Status</b>
<b>Basic Config</b>
<b>Port Config</b>
<b>L2 Config</b>
VLAN Config
VLAN Interface
GVRP Config
LLDP Config
STP Config
IGMP Snooping
Static ARP
Static MAC Config
DDM Config
Port Channel
Ring Protection
Multiple Ring Protection
BackupLink Config
DHCP Snooping Config
MTU Config
PDP Config
<b>L3 Config</b>
<b>Advanced Config</b>
<b>Network Mgr.</b>
<b>Diagnostic Tool</b>
<b>System Mgr.</b>

Figure 1: Layer-2 configuration list

## 5.1 VLAN Settings

### 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	<a href="#">Edit</a>

Figure 2 VLAN configuration

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 Settings

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	<input type="text" value="2"/>		
		VLAN Name	<input type="text" value="VLAN0002"/>		
Port	Default VLAN	Mode	Untag or not	Allow or not	
G0/1	<input type="text" value="1"/> <1-4094>	Access	No	Yes	
G0/2	<input type="text" value="1"/> <1-4094>	Access	No	Yes	
G0/3	<input type="text" value="1"/> <1-4094>	Access	No	Yes	
G0/4	<input type="text" value="1"/> <1-4094>	Access	No	Yes	
G0/5	<input type="text" value="1"/> <1-4094>	Access	No	Yes	
G0/6	<input type="text" value="1"/> <1-4094>	Access	No	Yes	
G0/7	<input type="text" value="1"/> <1-4094>	Access	No	Yes	
G0/8	<input type="text" value="1"/> <1-4094>	Access	No	Yes	
G0/9	<input type="text" value="1"/> <1-4094>	Access	No	Yes	
G0/10	<input type="text" value="1"/> <1-4094>	Access	No	Yes	
G0/11	<input type="text" value="1"/> <1-4094>	Access	No	Yes	
G0/12	<input type="text" value="1"/> <1-4094>	Access	No	Yes	

Figure 3 Revising VLAN configuration

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

If you click **Layer-2 Config -> GVRP Config -> GVRP Global Config** in the navigation bar, the **GVRP Global Config** page appears, as shown the following Figure.

Figure 9 GVRP Global Configuration

You can enable or disable the global GVRP protocol and sets whether the dynamic vlan is only effective on the registration interface.

### 5.2.2 Global Interface Attribute Configuration

If you click **Layer-2 Config -> GVRP Config -> GVRP Interface Config** in the navigation bar, the **GVRP Interface Config** page appears, as shown the following Figure.

Port	GVRP Status
G0/1	Enable

Figure 10 Global Interface Attribute Configuration

To enable or disable GVRP protocol on the GVRP interface configuration.

## 5.3 STP Configuration

### 5.3.1 STP Status Information

If you click **Layer-2 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	FCFA.F72E.09A1
Hello Time	2 (1-10)s
Max Age	20 (6-40)s
Forward Delay	15 (4-30)s
BPDU Terminal	Disable

**STP Port's State**

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

Interface	Role	State	Cost	Priority.Port ID	Type
G0/1	Root	FWD	20000	128.1	P2p

Figure 10 Configuring the global attributes of STP

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

On the local STP configuration page, you can modify the running STP mode by clicking the Protocol type dropdown box. The STP 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 Property
G0/1	Enable	128	0	Auto
G0/2	Enable	128	0	Auto
G0/3	Enable	128	0	Auto
G0/4	Enable	128	0	Auto
G0/5	Enable	128	0	Auto
G0/6	Enable	128	0	Auto
G0/7	Enable	128	0	Auto
G0/8	Enable	128	0	Auto

Figure 11 Configuring the attributes of RSTP

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

If you click **Layer-2 Config -> IGMP snooping**, the IGMP-Snooping configuration page appears.

Figure 12 IGMP-snooping configuration

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

If you click **Layer-2 Config -> IGMP snooping vlan list**, the **IGMP-Snooping VLAN list** page appears.

	VLAN ID	Status of the IGMP Snooping Vlan	Immediate-leave	Multicast Router's Port	Operate
<input type="checkbox"/>	1	Running	Disable	SWITCH(querier);	<a href="#">Edit</a>

Figure 13: IGMP-snooping VLAN list

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.

The screenshot shows a configuration page for a VLAN. At the top, there is a field for 'VLAN ID' with the value '2'. Below this, there are two dropdown menus: 'Status of the IGMP Snooping Vlan' set to 'Enable' and 'Immediate-leave' set to 'Disable'. The main area is divided into two columns: 'Configured Mrouter Port List' on the left, containing 'G0/1' and 'G0/12', and 'Available Port List' on the right, containing a scrollable list of ports from G0/10 to G0/20. Between these columns are two buttons: '>>' and '<<'. At the bottom, there are three buttons: 'Apply', 'Reset', and 'Go Back'.

Figure 14: Static routing port of IGMP VLAN

When an IGMP-Snooping VLAN is created, its VLAN ID can be modified; but when the IGMP-Snooping VLAN is modified, its VLAN ID cannot be modified.

You can click “>>” and “<<” to delete and add a routing port.

### 5.4.3 Static Multicast Address

If you click **Static multicast address**, the **Setting the static multicast address** page appears.

The screenshot shows two parts of the configuration interface. The top part is titled 'Static Multicast Address Config' and contains three input fields: 'VLAN ID', 'Multicast IP Address', and 'Assignment Port' (a dropdown menu). Below these fields is an 'Apply' button. The bottom part is titled 'Static Multicast List Info' and features a table with columns for 'VLAN ID', 'Group', and 'Port'. Above the table are navigation controls including 'No. 0 Page/Total 0 Page', 'First', 'Prev', 'Next', 'Last', 'Go No.', 'Page', and a search box. Below the table is a checkbox for 'Select All/Select None' and two buttons: 'Delete' and 'Refresh'. A 'Help' link is located at the bottom left of the page.

Figure 15 Multicast List

On this page, the currently existing static multicast groups and port groups in each static multicast group are shown.

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.

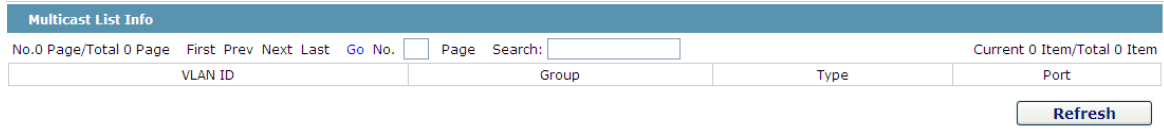


Figure 16 Multicast List

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

If you click **Layer-2 Config -> Static ARP Config**, the static ARP configuration page appears.

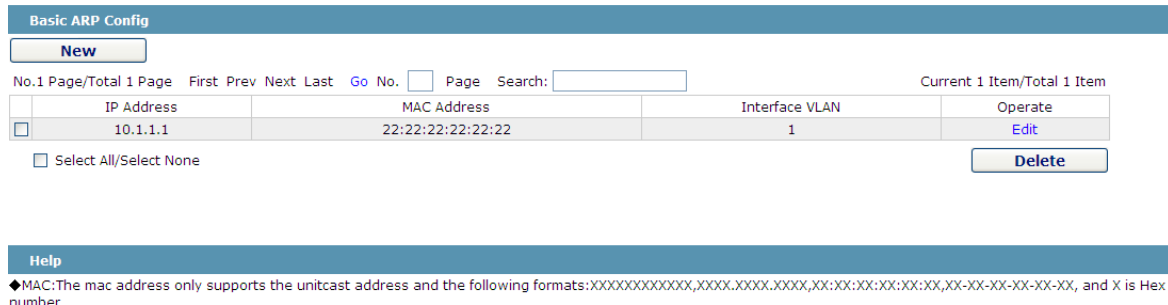


Figure 17 Displaying static ARP

You can click **New** to add an ARP entry. If the **Alias** column is selected, it means to answer the ARP request of the designated IP address.

If you click Edit, you can modify the current ARP entry.

If you click Cancel, you can cancel the chosen ARP entry.

**ARP Config**

Configure the corresponding MAC address of an IP address

IP Address*	<input type="text"/>
MAC Address*	<input type="text"/>
Interface VLAN*	<input type="text"/>

**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

Figure 18 Setting static ARP

## 5.6 Static MAC Address Configuration

If you click **Layer-2 Config -> Static MAC Config -> Static MAC List**, the **Static MAC Address List Info** page appears.

**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

Index	Static MAC Address	VLAN ID	Port	Operate
1	1022.3344.5566	1	GO/8	<a href="#">Edit</a>

Select All/Select None

Figure 22 Setting Static MAC Address List Info

Click **New** to designate static MAC address and VLAN. The unicast MAC address can only configure one interface. Multiple MAC addresses can configure multiple interfaces.

Click **Edit** to modify the static MAC address.

Click **Delete** to delete the selected MAC address table.

Static MAC Address Config

<b>Static MAC Address</b>	<input type="text"/>
<b>VLAN ID</b>	<input type="text"/>
<div style="border: 1px solid #ccc; padding: 5px;">Configured Port List</div> <div style="border: 1px solid #ccc; height: 100px; width: 100%;"></div>	<div style="border: 1px solid #ccc; padding: 5px;">Available Port List</div> <div style="border: 1px solid #ccc; padding: 5px;">                 G0/1                  G0/2                  G0/3                  G0/4                  G0/5                  G0/6                  G0/7                  G0/8                  G0/9                  G0/10             </div>
<input style="margin-right: 20px;" type="button" value=" &gt;&gt; "/> <input style="margin-left: 20px;" type="button" value=" &lt;&lt; "/>	
<input type="button" value="Apply"/>	<input type="button" value="Reset"/>
<input type="button" value="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

Figure 19 Static MAC Address Config

## 5.7 LLDP Configuration

### 5.7.1 Configuring the Global Attributes of LLDP

If you click **Layer-2 Config -> LLDP Config -> LLDP Global Config** in the navigation bar, the **Basic Config of LLDP Protocol** page appears, as shown in the following Figure.

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

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.

Figure11 Configuring the Global Attributes of LLDP

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. Its default value is 120s.

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

### 5.7.2 LLDP Port Attribute Configuration

If you click **Layer-2 Config -> LLDP Config -> LLDP Interface Config** in the navigation bar, the **LLDP Port Config** page appears.

Port	Receive LLDP Packet	Send LLDP Packet
G0/1	Enable ▾	Enable ▾

Figure 12 Configuring the LLDP port

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

## 5.8 DDM Configuration

If you click **L2 Config -> DDM Config** in the navigation bar, the **DDM configuration** page appears, as shown in figure 5-21.

Figure 5-21: DDM configuration

## 5.9 Port Aggregation Configuration

### 5.9.1 Port Aggregation Configuration

If you click **Layer-2 Config -> Port Channel-> Port Channel**, the **Port Aggregation Config** page appears.

Port Aggregation Config							
<a href="#">New</a>							
No.1 Page/Total 1 Page		First	Prev	Next	Last	Go No. <input type="text"/>	Page Search: <input type="text"/>
						Current 1 Item/Total 1 Item	
	Aggregation Group	Mode	Configure port members	Valid port members	Speed	State	Operate
<input type="checkbox"/>	P1	Static	G0/6,G0/9			down	<a href="#">Edit</a>
<input type="checkbox"/> Select All/Select None							<a href="#">Delete</a>
Help							

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

Figure 25 Port Aggregation Information

Click **New** to create an aggregation group. It can configure 32 aggregation groups in maximum and each group is with 8 physical ports into aggregation. Click **Delete** to delete the selected aggregation group. Click “**Reset**” to modify the setting.

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

Figure 26 Port Aggregation Configuration

If you create an aggregation group, it is optional; if you modify the aggregation group, it is not optional.

When the aggregation port has a member port, the user can select the aggregation mode: static, LACP Active and LACP Passive.

You can click “>>” and “<<” to delete and add an aggregation member port.

## 5.10 Ring Protection Configuration

### 5.10.1 EAPS Ring List

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

Ring ID	Node Type	Ring Description	Control VLAN	Status	Hello	Fail	Preforward	Primary Port/Forwarding/Link Status	Secondary Port/Forwarding/Link Status
<input type="checkbox"/> Select All/Select None <span style="float: right;"> <input type="button" value="Delete"/> <input type="button" value="Refresh"/> </span>									

Figure 19 EAPS Ring List

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.

Figure 20 EAPS ring configuration

#### Note:

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.

### 5.10.3 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.

If you click **Layer-2 Config -> Port Channel-> Port Channel Group Loading Balance**, the **Configuring Load Balance of Port Aggregation Group** page appears.

Configuring Load Balance of Port Aggregation Group

Port Channel	Loading Balance Mode
P1	SRC MAC <span style="font-size: small;">▼</span>

Apply
Reset

Figure 27 Configuring the aggregation mode for different aggregation groups

## 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"/>	1	2	Major Ring	Master Node	2	1	23	3	G0/5	Primary-Port	G0/11	Secondary-Port	<a href="#">Edit</a>

Select All/Select None
 Delete

Figure 30 Multiple Ring Protection Configuration

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.

### 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.

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

Figure 31 New MEAPS Global Configuration

**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 GMRP Configuration

### 5.12.1 GMRP Global Configuration

Click “ layer 2 configuration” and “GMRP configuration” in turn on navigation bar to enter GMRP global configuration page.

**GMRP Global Status**

GMRP Global Status Enable

**GMRP VLAN List**

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

Serial number	GMRP VLAN ID
<input type="checkbox"/> Select All/Select None	

**Help**

#GMRP function is effective simultaneously to 16 VLANs at most

GMRP global status could be enabled and disabled at this page; as well as VLAN which is used for GMRP configuration.

**Notice:**  
GMRP function could only be valid maximum for 16 VLANs at the same time.

### 5.12.2 GMRP Interface Configuration

Click “layer 2 configuration”, “GMRP configuration” and “GMRP interface configuration” in turn on navigation bar to enter GMRP interface configuration page.

**Configuring Interface GMRP**

Port Name	GMRP Status	Operate
g0/1	Enable <input type="button" value="v"/>	<a href="#">Detail</a>
g0/2	Enable <input type="button" value="v"/>	<a href="#">Detail</a>
g0/3	Enable <input type="button" value="v"/>	<a href="#">Detail</a>
g0/4	Enable <input type="button" value="v"/>	<a href="#">Detail</a>
g0/5	Enable <input type="button" value="v"/>	<a href="#">Detail</a>
g0/6	Enable <input type="button" value="v"/>	<a href="#">Detail</a>
g0/7	Enable <input type="button" value="v"/>	<a href="#">Detail</a>
g0/8	Enable <input type="button" value="v"/>	<a href="#">Detail</a>
g0/9	Enable <input type="button" value="v"/>	<a href="#">Detail</a>
g0/10	Enable <input type="button" value="v"/>	<a href="#">Detail</a>
g0/11	Enable <input type="button" value="v"/>	<a href="#">Detail</a>
g0/12	Enable <input type="button" value="v"/>	<a href="#">Detail</a>
g0/13	Enable <input type="button" value="v"/>	<a href="#">Detail</a>
g0/14	Enable <input type="button" value="v"/>	<a href="#">Detail</a>
g0/15	Enable <input type="button" value="v"/>	<a href="#">Detail</a>
g0/16	Enable <input type="button" value="v"/>	<a href="#">Detail</a>

**Help**

#Before enabling GMRP on port, please enable the global GMRP

**Notice:**  
Please open global GMRP first, if GMRP needs to be enabled on ports.

### 5.12.3 GMRP Multicast Member List

Click “layer 2 configuration”, “GMRP configuration” and “GMRP multicast member list” in turn on navigation bar to enter GMRP interface configuration page.

GMRP Multicast List Info			
No.0 Page/Total 0 Page	First Prev Next Last	Go No. <input type="text"/>	Page Search: <input type="text"/>
			Current 0 Item/Total 0 Item
Index	VLAN ID	Multicast MAC Address	Port
			<input type="button" value="Refresh"/>

This page shows current GMRP multicast member information, including VLAN, multicast MAC address and member port.

## 5.12 PTP Configuration

### 5.12.1 PTP Global Configuration

Click “L2 Config” -> “PTP Config” -> “PTP Global” in the navigation bar, and enter PPT basic configuration page.

PTP Basic Config	
Device Type	Boundary <input type="button" value="v"/>
PTP Settings	Enable PTP <input type="button" value="v"/>
Load Protocol	Unicast <input type="button" value="v"/>
Domain Filtration Settings	Close <input type="button" value="v"/>
The timeout of delay_req record	5 <input type="text"/>
Setting the default PTP data set	
Default Priority1	128 <input type="text"/>
Default Priority2	128 <input type="text"/>
Default Domain	0 <input type="text"/>
PTP Time Properties Settings	
Offset Between UTC And TAI	0 <input type="text"/>
Leap59	0 <input type="button" value="v"/>
Leap61	0 <input type="button" value="v"/>
Timetraceable	0 <input type="button" value="v"/>
Freqtraceable	0 <input type="button" value="v"/>
Timescale	1 <input type="button" value="v"/>
Timesource	160 <input type="text"/>
Regulator Settings	
Proportion Constant	2 <input type="text"/>
Integration Constant	10 <input type="text"/>
Differentiation Constant	0 <input type="text"/>
Sync Process Mechanism	
Domain 0	Straight Forwar <input type="button" value="v"/>
Domain 1	Straight Forwar <input type="button" value="v"/>
Domain 2	Straight Forwar <input type="button" value="v"/>
Domain 3	Straight Forwar <input type="button" value="v"/>
Clock Frequency Synchronization	
Synchronization Settings	Enable <input type="button" value="v"/>
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

On this page you can configure parameters such as enable/disable or timeout of the PTP.

### 5.12.2 PTP Interface Configuration

Click “L2 Config” -> “PTP Config” -> “PTP Interface” in the navigation bar, and enter PPT interface configuration page.

Port	Create the PTP port	IEEE1588 Transport Protocol	Delay Measurement Mechanism	Designated Disable	Transmission Interval of Announce Packets	Announce Receipt Timeout	Transmission Interval of Sync Packets	Transmission Interval of PdelayReq Packets
g0/1	True	unicast	e2e	Disable	1	10	-1	-1

On this page you can create PTP interface, IEEE1588 Transport Protocol and Delay Measurement Mechanism.

**Note:**  
The page can only be configured after enabling the PTP Transport Protocol.

### 5.12.3 PTP VLAN Configuration

Click “L2 Config” -> “PTP Config” -> “PTP VLAN Config” in the navigation bar, and enter PPT VLAN configuration page.

PTP VLAN Config

VLAN ID	PTP Disable
1	Disable
2	Disable
3	Disable
4	Disable

On this page you can enable/disable PTP of the vlan.

### 5.12.4 PTP Unicast Configuration

Click “L2 Config” -> “PTP Config” -> “PTP Unicast Config” in the navigation bar, and enter the PTP Unicast Config page.

Port PTP Unicast Attribute List

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

Port	Unicast State	IP Address	Operate
<input type="checkbox"/> g0/1	enable		<a href="#">Edit</a>

Select All/Select None

Click “Edit” to edit the attribute of the PTP Unicast Configuration:

**PTP Unicast Attribute Config**

Port Name	g0/1
Announce	<input type="text" value="100"/>
Sync	<input type="text" value="100"/>
Delay-Resp	<input type="text" value="100"/>
PDelay-Resp	<input type="text" value="100"/>
IP Address	<input type="text"/>

**Help**

- ◆The Packets of announce, sync, delayresp, pdelayresp has default interval for sending 100s.
- ◆The port only supports a unicast address, set multiples unicast address on the same port, only one address is available.

## 5.13 Backup Link Protocol Configuration

### 5.13.1 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		<a href="#">Edit</a>

Select All/Select None

Figure 32 Backup Link Protocol Global Configuration

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	<input type="text" value="No Preemption"/>
Preemption Delay	<input type="text"/>

Figure 33 Backup Link Protocol Global Configuration

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.

### 5.13.2 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 25 Item/Total 25 Item	
Interface Name	Group ID	Interface Attribute	MMU Attribute	Shareload VLAN	Operate					
G0/1	2	Active Port			<a href="#">Edit</a>					
G0/2					<a href="#">Edit</a>					
G0/3					<a href="#">Edit</a>					
G0/4					<a href="#">Edit</a>					

Figure 34 Backup Link Protocol Interface Configuration

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" value="2"/>
Interface Attribute	Active Port <input type="button" value="v"/>
MMU Attribute	<input type="text" value=""/> <input type="button" value="v"/>
Shareload VLAN	<input type="text" value=""/>
<input type="button" value="Apply"/> <input type="button" value="Reset"/> <input type="button" value="Go Back"/>	

**Help**  
 ♦Share Load VLAN can be Only Configured On The Backup Port

Figure 35 Backup Link Protocol Interface Configuration

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.

## 5.14 DHCP Snooping Configuration

### 5.14.1 DHCP Snooping Global Attribute Configuration

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

DHCP Snooping Global Config	
DHCP Snooping Global Config	Enable <input type="button" value="v"/>
TFTP Server IP To Save the Port Binding Relationship	<input type="text"/>
TFTP File Name To Save the Port Binding Relationship	<input type="text"/>
Update Interval To Save the Port Binding Relationship	<input type="text" value="30"/>
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	



Figure 36 DHCP Snooping Global Configuration

Enable global DHCP Snooping protocol, the switch is to monitor all DHCP packets and form the corresponding binding relationship. If the client obtains the address of a switch before the global DHCP Snooping protocol is enabled, the switch cannot add the corresponding binding relationship.

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.

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.

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.

#### 5.14.2 DHCP Snooping VLAN Attribute Configuration

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

DHCP Snooping VLAN Config	
Enable DHCP Snooping VLAN	<input type="checkbox"/>
Enable Dynamic ARP Inspection VLAN	<input type="checkbox"/>
Enable Verify Source VLAN	<input type="checkbox"/>

Figure 37 DHCP Snooping VLAN Configuration

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.

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.

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.

### 5.14.3 DHCP Snooping Interface Attribute Configuration

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

Port	DHCP Trust Port	ARP Inspection Trust Port	IP Source Trust Port
G0/1	<input type="text" value="Distrust"/>	<input type="text" value="Distrust"/>	<input type="text" value="Distrust"/>

Figure 38 DHCP Snooping Interface Attribute Configuration

If an interface is set to be a DHCP-trusting interface, the DHCP packets received from this interface will not be checked.

ARP monitoring is not enabled on those trusted interfaces. The interfaces are distrusted ones by default.

Sets an interface to the one with a trusted source IP address.

### 5.14.4 DHCP Snooping Manual Binding Configuration

If you click **Layer-2 Config -> DHCP Snooping Config -> DHCP Interface Binding List Manual Config** on the navigation bar, the **DHCP Manual Port List** page appears.

DHCP Manual Binding Port List

No.1 Page/Total 1 Page	First Prev Next Last	Go No. <input type="text"/>	Page Search: <input type="text"/>	Current 1 Item/Total 1 Item
------------------------	----------------------	-----------------------------	-----------------------------------	-----------------------------

No.	MAC Address	IP Address	Interface Name	VLAN
<input type="checkbox"/>	10-22-33-44-55-66	192.168.0.1	GigaEthernet0/1	1

Select All/Select None

Help

◆Manual binding list is prior to the dynamic binding list, and the mac address is the only index of the binding item.

Figure 39 DHCP Manual Binding Port List

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.

Click **New** to create DHCP Snooping manual Binding Port Item.

**DHCP Manual Binding Port List Config**

MAC Address*	<input type="text"/>
IP Address*	<input type="text"/>
Port	G0/1 <input type="button" value="v"/>
VLAN ID*	<input type="text"/>

**Help**  
 ♦MAC:The mac address supports the following formats:XXXXXXXXXXXX,XXXX.XXXX.XXXX,XX:XX:XX:XX:XX:XX,XX-XX-XX-XX-XX-XX, and X is Hex number

Figure 39 DHCP Manual Binding Port List Configuration

## 5.15 MTU Configuration

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

**MTU Config**

MTU  (1500-13312)

**Help**  
 ♦Configure the size of the system mtu, whose default value is 1500

Figure 40 MTU Configuration

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

## 5.16 PDP Configuration

### 5.16.1 Configuring the Global Attributes of PDP

If you click **Layer-2 Config -> PDP Config -> PDP Global Config** in the navigation bar, the **Basic Config of PDP Protocol** page appears.

**Basic Config of PDP Protocol**

Protocol State	Open the PDP protocol <input type="button" value="v"/>
HoldTime Settings	<input type="text" value="180"/> (10-255)s
Setting the packet transmission cycle	<input type="text" value="60"/> (5-254)s
Protocol Version	Version2 <input type="button" value="v"/>

**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.

Figure 41 Basic Config of PDP Protocol

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

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

### 5.16.2 PDP Interface Attribute Configuration

If you click **Layer-2 Config -> PDP Config-> PDP Interface Config** in the navigation bar, the **Protocol Port Config** page appears.

Port	Status
G0/1	Enable PDP <input type="button" value="v"/>

Figure 42 PDP Interface Attribute Configuration

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

## Chapter 6 Layer-3 Configuration

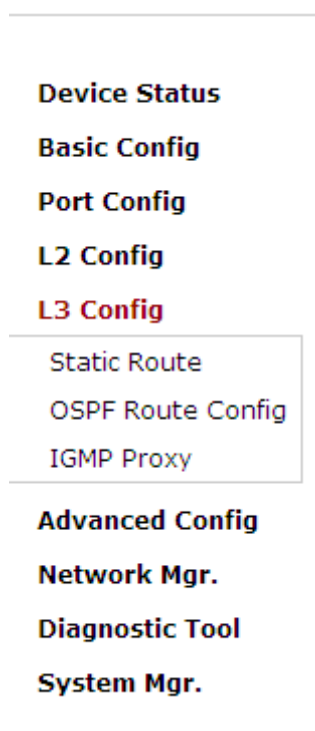


Figure 1: Layer-3 configuration list

Note:  
Only layer-3 switches have the layer-3 configuration.

### 6.1 Configuring the VLAN Interface

If you click **Layer-3 Config -> VLAN interface Config**, the **Configuring the VLAN interface** page appears.

	Name of the VLAN Interface	IP Attribute	IP Address	□□□□
<input type="checkbox"/>	1	Manual Config	192.168.1.79/24;	□□

Select All/Select None

Figure 2: Configuring the VLAN interface

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*	<input type="text"/>
IP Attribute*	Manual Config <input type="button" value="v"/>

Primary IP Address

IP Address*	<input type="text"/>
MASK address*	<input type="text"/>

Secondary IP Address 1

IP Address*	<input type="text"/>
MASK address*	<input type="text"/>

Secondary IP Address 2

IP Address*	<input type="text"/>
MASK address*	<input type="text"/>

**Help**

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

Figure 3: VLAN interface configuration

---

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

---

## Chapter 7 Advanced Configuration



Figure 1 A list of advanced configuration

### 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	0
G0/2	0
G0/3	0
G0/4	0
G0/5	0
G0/6	0
G0/7	0
G0/8	0
G0/9	0
G0/10	0
G0/11	0

Figure 2 Configuring the QoS Port

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 Config -> Global QoS Config**, the **Port's QoS parameter configuration** page appears.

**QoS Config**

**Schedule Policy**

Schedule Policy: sp

Queue 1	Queue 2	Queue 3	Queue 4
1 (1-15)	1 (1-15)	1 (0-15)	1 (0-15)
Queue 5	Queue 6	Queue 7	Queue 8
1 (0-15)	1 (0-15)	1 (0-15)	1 (0-15)

**COS-to-queue map**

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

**Help**

- ◆ If you want to configure the cos value of the interface, please goto QoS Interface Configuration.
- ◆ if the bandwidth of queue has been set to 0, the queue after this also must be set to 0

Figure 3 Configuring global QoS attributes

In WRR schedule mode, you can set the weights of the QoS queues. There are 4 queues, among which



queue 1 has the lowest priority and queue 4 has 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.

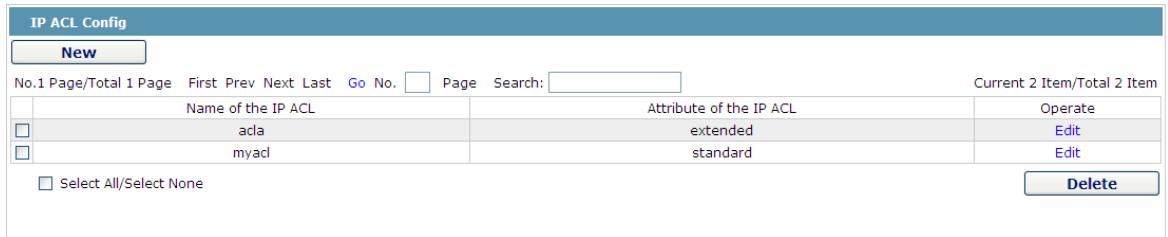


Figure 9: IP access control list configuration

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

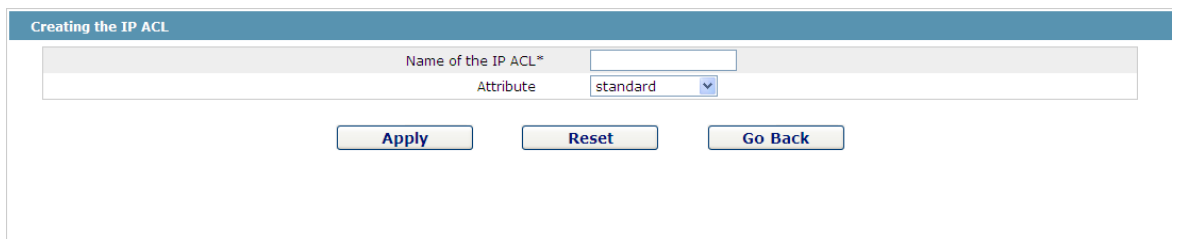


Figure 10: Creating a name of the IP access control list

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

### 7.2.2 Setting the Rules of the IP Access Control List

#### ➤ Standard IP access control list

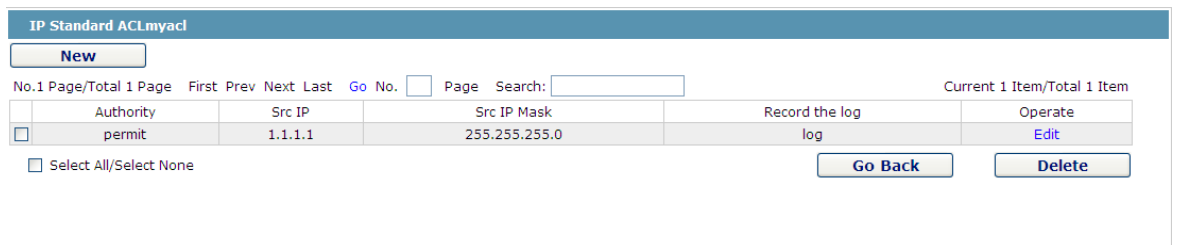


Figure 11: Standard IP access control list

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 ListmyadItem

Authority	permit	
Src IP Type	Specify IP	
Src IP*	1.1.1.1	
Src IP Mask	255.255.255.0	
Src IP Range*		-
Log	<input checked="" type="checkbox"/>	

Apply
Reset
Go Back

Figure 12: Setting the Rules of the standard IP access control list

➤ Extended IP access control list

Extended IP ACLacla

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	Tos	Precedence	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	1.1.1.1/255.255.255.0		any		10								log	Edit

Select All/Select None    
Go Back
Delete

Figure 13: Extended IP access control list

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.

Authority	permit	
Mask Type	Mask	
Protocol Number*	0	
Src IP Type	Specify IP	
Src IP*	1.1.1.1	
Src IP Mask*	255.255.255.0	
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	10	
Tos		
Precedence		
Do not fragment		
Fragmented Packet		
Offset		
Length of the IP Packet		
Time-to-live Value		
Log	<input checked="" type="checkbox"/>	
Location	1	

Apply
Reset
Go Back

Figure 14: Setting the Rules of the extended IP access control list

### 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	<input type="text" value="myacl"/>	<input type="text"/>
G0/2	<input type="text"/>	<input type="text" value="acla"/>
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"/>
G0/8	<input type="text"/>	<input type="text"/>

Figure 15: Applying the IP access control list

## 7.3 MAC Access Control List

### 7.3.1 Setting the Name of the MAC 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

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

Name of the MAC Access Control List	Operate
<input type="checkbox"/> Select All/Select None	<input type="button" value="Delete"/>

Figure 4: MAC access control list configuration

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

Creating MAC ACL

Name of the MAC ACL\*

Figure 5: Setting the name of MAC access control list

### 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.

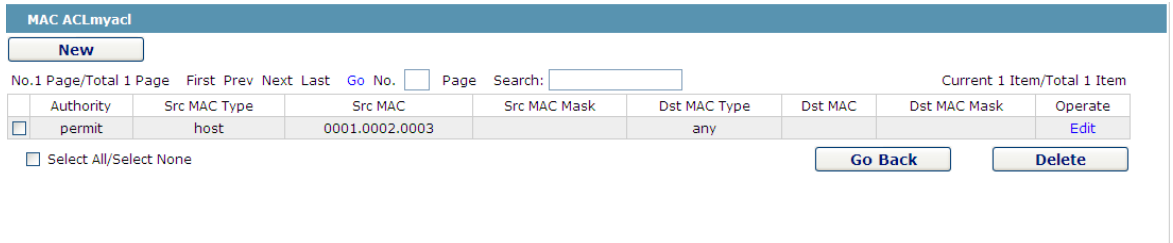


Figure 6: Specific MAC access control list configuration

Click **New** to add a rule of the MAC access control list. Click **Cancel** to delete a rule of the MAC access control list.

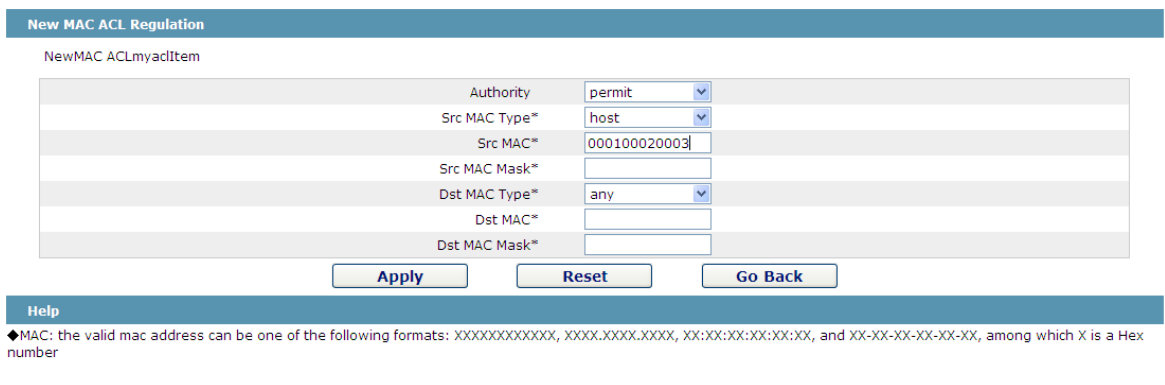


Figure 7: Setting the Rules of the MAC Access Control List

### 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"/>

Figure 8: Applying the MAC access control list

## Chapter 8 Network Management Configuration

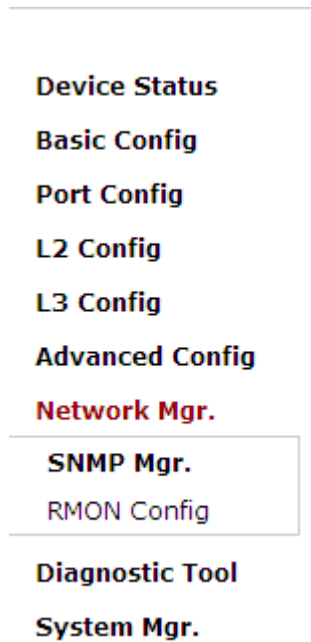


Figure 1: Network management configuration list

### 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

SNMP Community Mgr | SNMP Host Mgr

**SNMP Community Management**

[New](#)

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

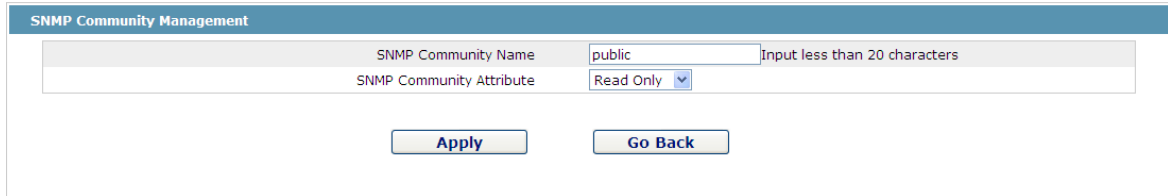
	SNMP Community Name	SNMP Community Encryption	SNMP Community Attribute	Operate
<input type="checkbox"/>	public	False	RO	<a href="#">Edit</a>

Select All/Select None [Delete](#)

Figure 2 SNMP community management

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.

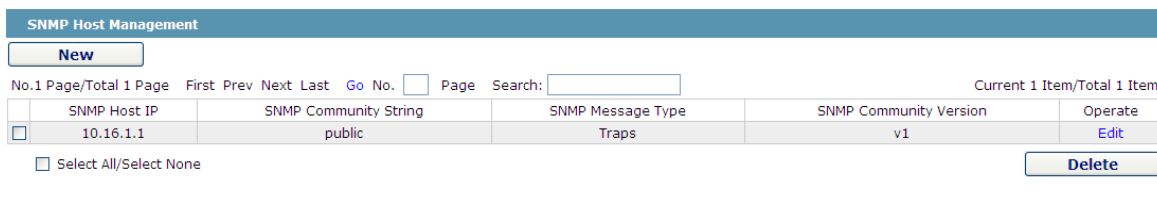


The screenshot shows the 'SNMP Community Management' configuration page. It features a header bar with the title. Below it, there are two input fields: 'SNMP Community Name' with the value 'public' and a note 'Input less than 20 characters', and 'SNMP Community Attribute' with a dropdown menu set to 'Read Only'. At the bottom, there are two buttons: 'Apply' and 'Go Back'.

Figure 4.2 SNMP community management settings

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



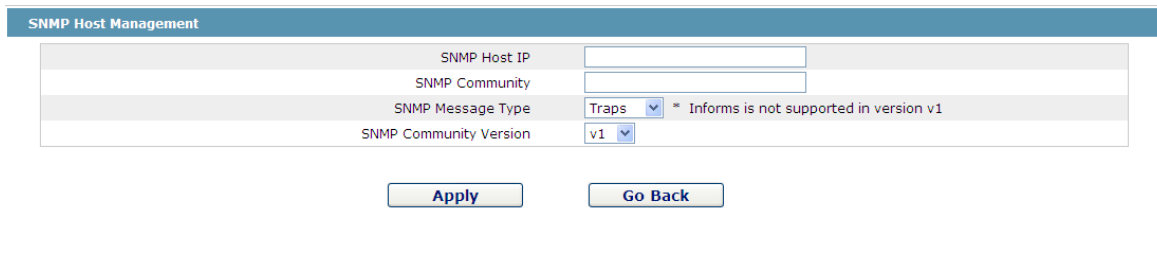
The screenshot shows the 'SNMP Host Management' page. It includes a 'New' button, a table with one row of data, and a 'Delete' button. The table has columns for 'SNMP Host IP', 'SNMP Community String', 'SNMP Message Type', 'SNMP Community Version', and 'Operate'. Below the table is a 'Select All/Select None' checkbox.

No.	Page/Total	1 Page	First	Prev	Next	Last	Go	No.	Page	Search:	Current	1 Item/Total	1 Item
<input type="checkbox"/>	10.16.1.1	public	Traps	v1	Edit								

Figure 4 SNMP host management

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 'SNMP Host Management' configuration page. It features a header bar with the title. Below it, there are four input fields: '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'). At the bottom, there are two buttons: 'Apply' and 'Go Back'.

Figure 5 SNMP host management settings

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	G0/1	
Index	1	(1-65535)
Owner	demon	
<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		

Figure 6 Configuring the RMON statistic information

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	G0/1	
Index		(1-65535)
Sampling Number	50	(1-65535)
Sampling Interval	1800	(1-3600)
Owner	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		

Figure 7 Configuring the RMON history information

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	1	(1-65535)
MIB Node	IfnOctets	
OID	1.3.6.1.2.1.2.2.1.10	
Interface	G0/1	
Alarm type	absolute	
Sampling Interval	5	(1-2147483647)
Rising Threshold	5	(-2147483648 - 2147483647)
Rising Event Index	2	(1-65535)
Falling Threshold	6	(-2147483648 - 2147483647)
Falling Event Index	3	(1-65535)
Owner	default	Enter less than 31 characters*

**Help**

- ◆The owner can be empty
- \*◆The string you totally entered is limited in 255 characters

Figure 8 Configuring the RMON alarm information

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

Figure 9 RMON event configuration

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



Figure 1: Diagnosis tool list

## 9.1 Ping

### 9.1.1 Ping

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

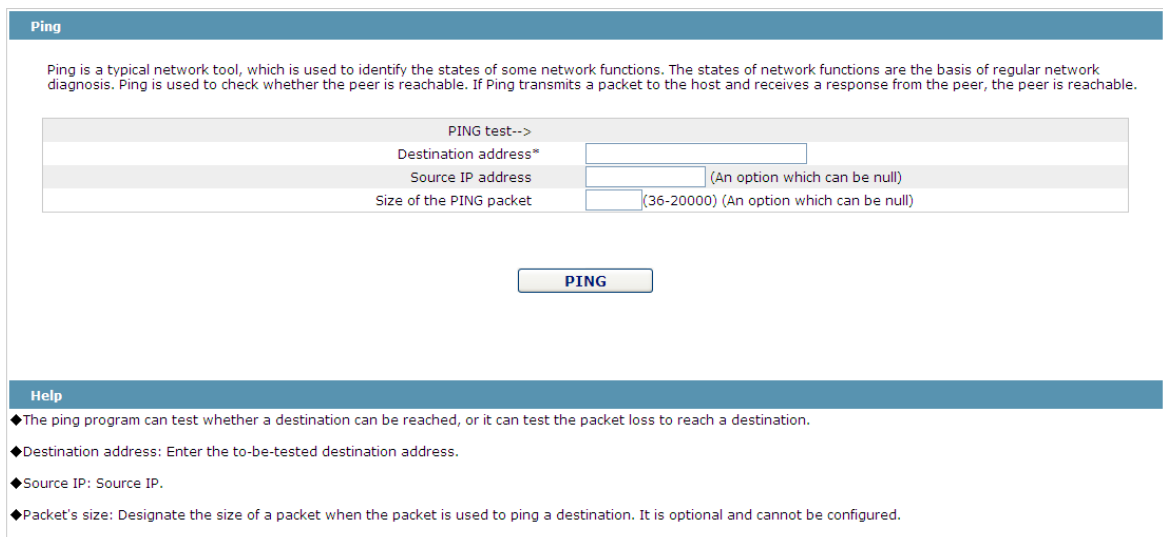


Figure 2 Ping

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

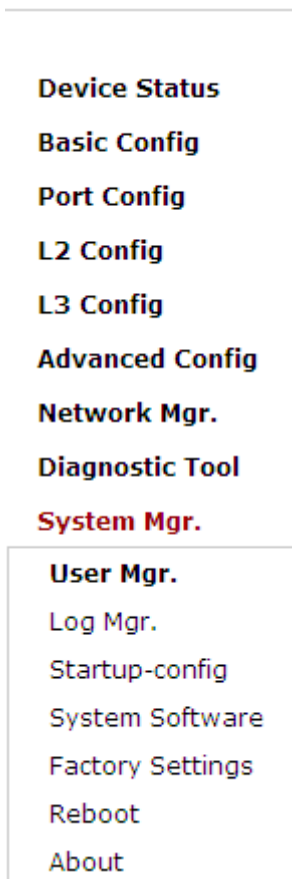


Figure 1 Navigation list of system management

### 10.1 User Management

#### 10.1.1 User List

If you click **System Manage -> User Manage**, 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	<a href="#">Edit</a>

Select All/Select None

Delete

**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.

Figure 2 User list

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"/>

Apply

Reset

Go Back

Figure 3 Creating new users

In the “User name” text box, enter a name, which contains letters, numbers and symbols except “?”, “\”, “&”, “#” and the "Space" symbol. \ " & #和空格以外的字符。

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

In the “User permission” dropdown box set the user's permission. The “System administrator” user can browse the status of the device and conduct relevant settings, while the limited user can only browse the status of the device.

### 10.1.3 User Group Management

If you click **New** on the **User Mgr.** page, the **User Group Management** page appears.

**User Group Mgr.**

**New**

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

No.	Serial Number	Group Name	Pass-Group Rule	Authen-Group Rule	Author-Group Rule	Operate	Detail
<input type="checkbox"/>	1	group				<a href="#">Edit</a>	<a href="#">Detail</a>

Select All/Select None **Delete**

Figure 4 User group list

Click **New** to create a new user group.

Click **Delete** to delete the user group.

**User Group Config**

User Group Name*	<input type="text"/>
Pass-Group Name	<input type="text"/>
Authen-Group Name	<input type="text"/>
Author-Group Name	<input type="text"/>

Apply
Reset
Go Back

- Help**
- ◆The user group mustn't exist.
  - ◆Rule must exist.

Figure 5 User group configuration

The User Group Name must be different with the existing group names. The user group cannot be created until the Pass-Group name, Authen-Group Name and Author-Group Name are specified. Configuring the Pass-Group name, Authen-Group Name and Author-Group Name in another 3 pages.

### 10.1.4 Password Group Management

Click **Pass-Group Mgr.** and the **Pass-Group Mgr.** page appears.

**Pass-Group Mgr.**

**New**

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

No.	Serial Number	Pass-Group Name	Same as the username	Min Length	Validity	Number	Lower-letter	Upper-letter	Special-character	Operate
<input type="checkbox"/>	1	password1	Can be same			Must	Must	Must	Must	<a href="#">Edit</a>

Select All/Select None **Delete**

Figure 6 Password Group Management

Click **New** to create a new password rule.

Click **Delete** to delete the password rule.

**Pass-Group Config**

Pass-Group Name*	<input type="text"/>
Same as Username	Can <input type="button" value="v"/>
Contain Number	Must <input type="button" value="v"/>
Contain Lower-letter	Must <input type="button" value="v"/>
Contain Upper-letter	Must <input type="button" value="v"/>
Contain Special-character	Must <input type="button" value="v"/>
Min Length	<input type="text"/> (1-127)
Validity	0 <input type="text"/> d 0 <input type="text"/> h 0 <input type="text"/> m 0 <input type="text"/> s

In the **Pass-Group Configuration**, the password can be set whether to be **Same as Username**, **Contain Number**, **Contain Lower-letter**, **Contain Upper-letter**, **Contain Special-character**, **Min Length** and **validity**.

The rule can be applied to the user management. The password is valid only when it conforms to the rule.

### 10.1.5 Authentication Group Configuration

Click **Authen-Group Mgr.** on the navigation bar, and **Authen-Group Mgr.** appears.

**Authen-Group Config**

Authen-Group Name*	<input type="text"/>
Max try times	<input type="text"/> (1-9)
Duration for all tries	0 <input type="text"/> d 0 <input type="text"/> h 0 <input type="text"/> m 0 <input type="text"/> s

- Help**
- ◆ Configure the Authen-Group
  - ◆ 'Max Try Times' and 'Duration for all tries' must be entered at the same time

Figure 7 Pass Group Configuration

Click **New** to create a new authorization rule.

Click **Delete** to delete the authorization rule.

The **Max try times** and **Duration of all tries** can be configured or not. But they must be adjusted simultaneously.

### 10.1.6 Author-Group Management

If you click **Author-Group Mgr.** and the **Author-Group Mgr.** page appears.

**Author-Group Mgr.**

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

	Serial Number	Author-Group Name	Precedence	Operate
<input type="checkbox"/>	1	1	System administrator	<a href="#">Edit</a>

Select All/Select None

Figure 8 Author Group Management

Click **New** to create a new authorization rule.

Click **Delete** to delete the new authorization rule.

Figure 9 Author Group Configuration

The authorization rule determines the user's access: Administrator or Limited user. The **Administrator** has full access to the configuration and the **Limited user** only has access to check the configuration.

## 10.2 Log Management

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

Figure 4 Log management

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 Manage -> Configuration file**, the **Configuration file** page appears.



### 10.3.1 Exporting the Configuration Information

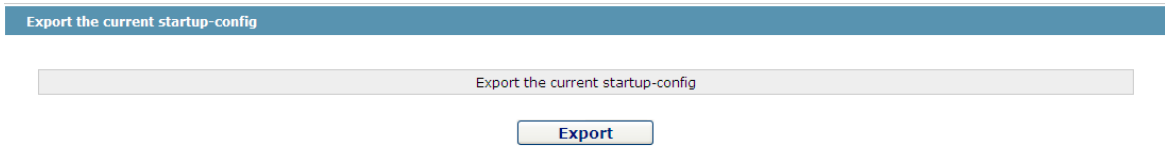


Figure 5 Exporting the configuration file

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

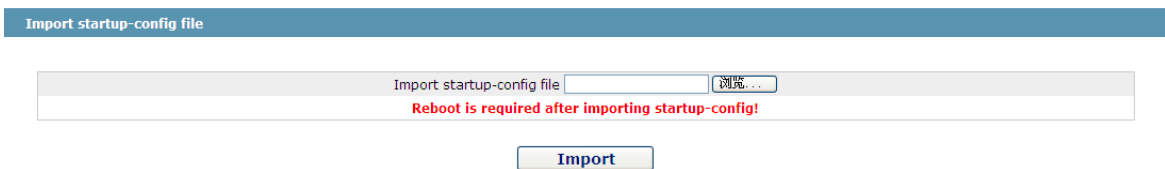


Figure 6 Importing the configuration files

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

If you click **System Manage -> Software Upgrade**, the software management page appears.

### 10.4.1 Backing up the IOS Software

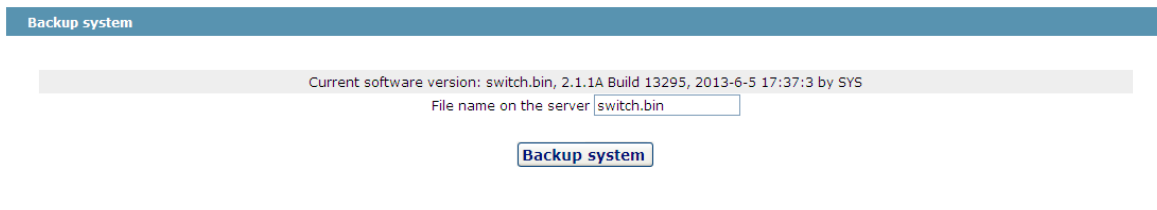


Figure 7 Backing up IOS

On this page the currently running software version is displayed. If you want to backup IOS, please click “Backuping IOS”; then on the browser the file download dialog box appears; click “Save” to store the IOS file to the disk of the PC, mobile storage device or other network location.

**Note:**

The default name of IOS document is “Switch.bin”. It is suggested to modify it as a name which is detectable and searchable when its backup is created.

### 10.4.2 Upgrading the IOS Software

**Note:**

1. Please make sure that your upgraded IOS matches the device type, because the matchable IOS will not lead to the normal startup of the device.
2. The upgrade of IOS probably takes one to two minutes; when the “updating” button is clicked, the IOS files will be uploaded to the device.
3. If errors occur during upgrade, please do not restart the device or cut off the power of the device, or the device cannot be started. Please try the upgrade again.
4. After the upgrade please save the configuration and then restart the device to run the new IOS.

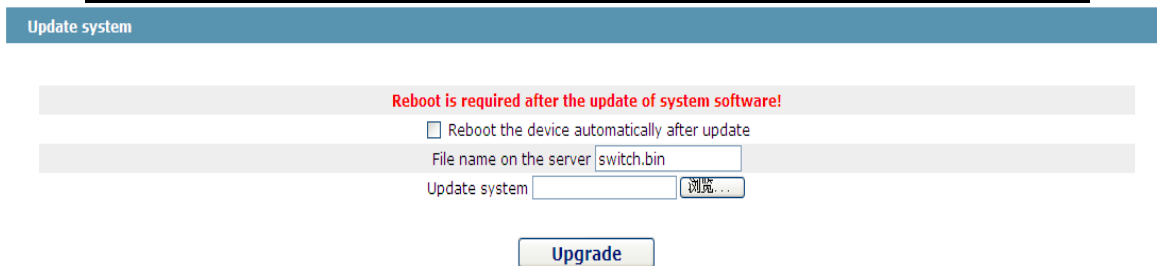


Figure 8 Upgrading the IOS software

The upgraded IOS is always used to solve the already known problems or to perfect a specific function. If you device run normally, do not upgrade your IOS software frequently.

If IOS need be upgraded, please first enter the complete path of the new IOS files in the textbox on the right of “Upgrading IOS”, or click the “Browsing” button and select the new IOS files on your computer, and then click “Updating”.

## 10.5 Rebooting the Device

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

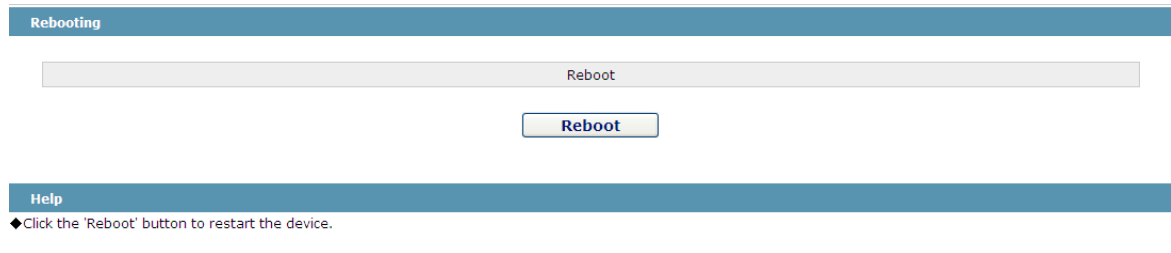


Figure 10 Rebooting the device

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 Introduction .....	1
1.1 Supported Interface Types .....	1
1.2 Interface Configuration Introduction .....	2
Chapter 2 Interface Configuration.....	4
2.1 Configuring Interface Common Attribute .....	4
2.1.1 Adding Description .....	4
2.1.2 Configuring Bandwidth .....	4
2.1.3 Configuring Time Delay .....	4
2.2 Monitoring and Maintaining Interface .....	5
2.2.1 Checking Interface State .....	5
2.2.2 Initializing and Deleting Interface .....	5
2.2.3 Shutting down and Enabling Interface .....	5
2.3 Setting the Ethernet Interface .....	6
2.3.1 Choosing an Ethernet Interface .....	6
2.3.2 Configuring the Rate .....	6
2.3.3 Configuring the Duplex Mode of an Interface .....	6
2.3.4 Configuring Flow Control on an Interface.....	7
2.4 Configuring Logistical Interface .....	7
2.4.1 Configuring Aggregation Interface.....	7
2.4.2 Configuring VLAN Interface .....	7
Chapter 3 Interface Configuration Example.....	8
3.1 Configuring Public Attribute of Interface .....	8
3.1.1 Interface Description Example .....	8
3.1.2 Interface Shutdown Example .....	8

## Chapter 1 Introduction

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

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

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

### 1.1 Supported Interface Types

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

Interface Type	Task	Reference
Ethernet interface	Configures Ethernet interface. Configures fast Ethernet interface. Configures gigabit Ethernet interface.	<i>Configuring Ethernet Interface</i>
Logical Interface	Loopback interface Null interface VLAN interface	<i>Configuring Logistical Interface</i> The loopback interface and null interface are only configured on layer-3 switch. User can configure the VLAN interface on layer-2 switch.
	Aggregation interface	<i>Configuring Logistical Interface</i>

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

The supported Ethernet interfaces of our switch include:

- Ethernet interface
- Fast Ethernet interface
- Gigabit Ethernet interface

The supported logical interface of our switch include:

- loopback interface
- null interface
- aggregation interface

- VLAN interface

## 1.2 Interface Configuration Introduction

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

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

```
Switch#show interface
GigaEthernet1/1 is down, line protocol is down
Hardware is Fast Ethernet, Address is 0009.7cf7.7dc1
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Auto-duplex, Auto-speed
input flow-control is off, output flow-control is off
ARP type: ARPA, ARP Timeout 04:00:00
Last input never, output 17:52:52, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue :0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
1 packets input, 64 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog, 0 multicast, 0 pause input
0 input packets with dribble condition detected
1 packets output, 64 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier, 0 PAUSE output
0 output buffer failures, 0 output buffers swapped out
To configure gigabit Ethernet interface g1/1, enter the following content:
interface GigaEthernet0/1
The switch prompts "config_g1/1".
```

**Note:**

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

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



## Chapter 2 Interface Configuration

### 2.1 Configuring Interface Common Attribute

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

#### 2.1.1 Adding Description

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

Command	Description
<b>description</b> <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	Description
<b>bandwidth</b> <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	Description
<b>delay</b> <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 Interface

The following tasks can monitor and maintain interface:

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

### 2.2.1 Checking Interface State

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

Use the following commands:

Command	Description
<b>show interface</b> [type [slot port]]	Displays interface state.
<b>show running-config</b>	Displays current configuration.

### 2.2.2 Initializing and Deleting Interface

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

Command	Description
<b>no interface type</b> [slot port]	Initializes physical interface or deletes virtual interface.

### 2.2.3 Shutting down and Enabling Interface

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

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

Command	Description
<b>shutdown</b>	Shuts down an interface.
<b>no shutdown</b>	Enables an interface.

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

## 2.3 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
<b>interface gig Ethernet</b> [slot/port]	Enters the gigabit-Ethernet interface configuration mode.

The **show interface gig Ethernet** [slot/port] command can be used to show the state of the PON interface, while the **show interface gig Ethernet** command can be used to show the state of the gigabit-Ethernet interface.

### 2.3.2 Configuring the Rate

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

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

**Note:**

The speed of the optical interface is fixed. For example, the speeds of GBIC and GE-FX are 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.

### 2.3.3 Configuring the Duplex Mode of an Interface

By default, the Ethernet interface can be auto. The duplex mode for the gigbit interface is always auto.

Command	Purpose
<b>duplex</b> {full auto}	Sets the duplex mode of an Ethernet interface.

<b>No duplex</b>	Resumes the default settings. The duplex mode is auto-negotiation.
------------------	--

### 2.3.4 Configuring Flow Control on an Interface

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

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

## 2.4 Configuring Logistical Interface

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

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

### 2.4.1 Configuring Aggregation Interface

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

Run the following command to define the aggregation interface:

Command	Description
<b>Interface port-aggregator</b> <i>number</i>	Configures the aggregation interface

### 2.4.2 Configuring VLAN Interface

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

Run the following command to define VLAN interface:

Command	Description
<b>Interface vlan</b> <i>number</i>	Configures VLAN interface.

## Chapter 3 Interface Configuration Example

### 3.1 Configuring Public Attribute of Interface

#### 3.1.1 Interface Description Example

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

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

#### 3.1.2 Interface Shutdown Example

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

```
interface GigaEthernet0/1
shutdown
```

The following example shows how to enable the interface:

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

# 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.

Step	Command	Description
1	<b>interface range</b> <i>type slot</i> / <i>&lt;port1 - port2   port3&gt;</i> [ , <port1 - port2 port3>]	Enters the range mode. All ports included in this mode accord to the following conditions: <ol style="list-style-type: none"> <li>(1) The slot number is set to <b>slot</b>.</li> <li>(2) The port numbers before/after the hyphen must range between port1 and port2, or equal to port3.</li> <li>(3) Port 2 must be less than port 1</li> <li>(4) There must be space before/after the hyphen or the comma.</li> </ol>

### 1.1.3 Configuration Example

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

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



# Port Physical Characteristics Configuration

# Table of Contents

Chapter 1 Port Physical Characteristics Configuration ..... 1

    1.1 Configuring the Ethernet Interface ..... 1

        1.1.1 Configuring Rate ..... 1

        1.1.2 Configuring the Duplex Mode of an Interface ..... 1

        1.1.3 Configuring Flow Control on the Interface ..... 1

# Chapter 1 Port Physical Characteristics Configuration

## 1.1 Configuring the Ethernet Interface

The section describes how to configure the Ethernet interface. The switch supports the 10Mbps Ethernet and the 100Mbps fastEthernet. The detailed configuration is shown as follows. The step described in section 1.1.1 is mandatory. Steps described in other sections are optional.

### 1.1.1 Configuring Rate

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

Run the following command to configure the Ethernet rate:

命令	作用
Speed {10 100 auto}	Set the rate of fast Ethernet to 10M, 100M or auto-negotiation.
No speed	Resume the default settings—auto-negotiation.

**Note:**

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

### 1.1.2 Configuring the Duplex Mode of an Interface

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

Command	Purpose
<b>duplex {full   auto}</b>	Sets the duplex mode of the Ethernet.
<b>No duplex</b>	Resumes the default setting. The duplex mode is auto-negotiation.

### 1.1.3 Configuring Flow Control on the Interface

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

Command	Purpose
<b>flow-control {on   off}</b>	Enable or disable the flow control on the interface.

## Port Physical Characteristics Configuration

---

<b>no flow-control</b>	Resume the default settings. The default settings have no flow control.
------------------------	--

**Note:**

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

## Port Additional Characteristics Configuration

# Table of Contents

- Chapter 1 Interface Configuration ..... 1
  - 1.1 Configuring the Ethernet Interface ..... 1
    - 1.1.1 Configuring Flow Control for the Port ..... 1
    - 1.1.2 Configuring the Rate Unit for the Port ..... 1
    - 1.1.3 Configuring the Storm Control on the Port ..... 2
- Chapter 2 Secure Port Configuration ..... 3
  - 2.1 Overview ..... 3
  - 2.2 Configuration Task of the Secure Port ..... 3
  - 2.3 Configuring the Secure Port ..... 3
    - 2.3.1 Configuring the Secure Port Mode ..... 3
    - 2.3.2 Configuring the Static MAC Address of the Secure Port ..... 4

## Chapter 1 Interface Configuration

### 1.1 Configuring the Ethernet Interface

The switch supports the 10Mbps/100Mbps Ethernet interfaces. See the following content for detailed configuration. Among the configuration, the first step is mandatory while others are optional.

#### 1.1.1 Configuring Flow Control for the Port

You can control the flow rate on the incoming and outgoing ports through configuration.

Run the following commands in privileged mode to limit the flow rate of the port.

Each band is defaulted as 128 kbps.

Command	Purpose
<b>configure</b>	Enters the global configuration mode.
<b>interface f1/0</b>	Enters the to-be-configured port.
<b>[no] switchport rate-limit band</b> { ingress egress}	Configures the flow rate limits for the port.  The parameter <b>band</b> represents the to-be-limited flow rate.  The parameter <b>ingress</b> means the function works at the incoming port.  The parameter <b>egress</b> means the function works at the outgoing port.
<b>exit</b>	Exits the global configuration mode.
<b>exit</b>	Returns the EXEC mode.

#### 1.1.2 Configuring the Rate Unit for the Port

Run the following commands to modify the rate unit of the flow on a port. The rate unit can be one of these values: 16K, 64K, 128K, 1M, 10M and 40M.

Command	Purpose
<b>Configure</b>	Enters the global configuration mode.
<b>[no] rate-unit count</b>	Configures the rate unit for a port.
<b>exit</b>	Returns the EXEC mode.

### 1.1.3 Configuring the Storm Control on the Port

The ports of the switch may receive the attack by the continuous abnormal unicast (MAC address lookup failing), multicast or broadcast message. In this case, the attacked ports or the whole switch may break down. The storm control mechanism of the port is therefore generated.

Command	Purpose
<b>storm-control {broadcast   multicast   unicast} threshold count</b>	Performs the storm control to the broadcast/multicast/unicast message.
<b>no storm-control {broadcast   multicast   unicast} threshold</b>	Cancels the storm control.



## Chapter 2 Secure Port Configuration

### 2.1 Overview

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

The secure port has the following functions:

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

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

### 2.2 Configuration Task of the Secure Port

- Configuring Secure Port Mode
- Configuring the Static MAC Address of the Secure Port

### 2.3 Configuring the Secure Port

#### 2.3.1 Configuring the Secure Port Mode

There are two static secure port modes: accept and reject. If it is the **accept** mode, only the flow whose source address is same to the local MAC address can be received by the port for communication. If it is the **reject** mode, only the flow whose source address is different to the local MAC address can be received by the port.

Run the following commands in EXEC mode to enable or disable the secure port function:

Command	Purpose
<b>configure</b>	Enters the global configuration mode.
<b>interface</b> g0/1	Enters the to-be-configured port.

## Port Additional Characteristics Configuration

<b>[no] switchport port-security mode static {accept   reject}</b>	Configures the secure port mode.
<b>exit</b>	Goes back to the global configuration mode.
<b>exit</b>	Goes back to the EXEC mode.
<b>write</b>	Saves the configuration.

### 2.3.2 Configuring the Static MAC Address of the Secure Port

After you configure the static MAC address of the secure port, In **accept** mode, the flow whose source address is same to the local MAC address can be received by the port for communication. In **reject** mode, the flow whose source address is different to the local MAC address can be received by the port.

Run the following commands in EXEC mode to configure the static MAC address of the secure port:

Command	Purpose
<b>configure</b>	Enters the global configuration mode.
<b>interface g0/1</b>	Enters the to-be-configured port.
<b>[no] switchport port-security static mac-address mac-addr</b>	Adds or deletes the static MAC address of the secure port. <ul style="list-style-type: none"> <li>• <b>mac-addr</b> is the configured MAC address.</li> </ul>
<b>exit</b>	Goes back to the global configuration mode.
<b>exit</b>	Goes back to the EXEC mode.
<b>write</b>	Saves the configuration.

# Port Mirroring Configuration

## Table of Contents

Chapter 1 Configuring Port Mirroring .....	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

## Chapter 1 Configuring Port Mirroring

### 1.1 Configuring Port Mirroring Task List

- Configuring port mirroring
- Displaying port mirroring information

### 1.2 Configuring Port Mirroring Task

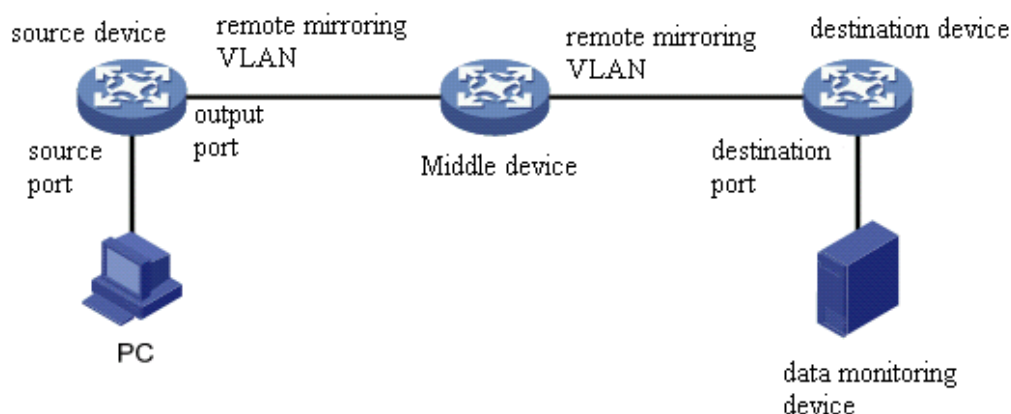
#### 1.2.1 Configuring Port Mirroring

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

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

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

Remote mirroring's schemetic plot is like following:



Configuring remote mirroring function on source device, and mirroring source port's message to the output port while adding configuring RSPAN TAG on the message. Vlan id in this tag is the remote mirroring VLAN. Middle device transfer mirroring message to the destination port by broadcasting. The destination device

transfer message from destination port to data monitoring device by configuration. If the destination device supports port mirroring function, the message could be transferred from destination port to data monitoring device by configuring local mirroring. If the destination device supports the configuration of mac address learning based on vlan, the message could be transferred to data monitoring device by shutting down remote mirroring vlan address learning. If the destination device's qos policy mapping supports the matching of vlan, the message could be transferred to monitoring device by qos policy mapping.

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

Command	Description
config	Enters the global configuration mode.
<b>mirror session</b> <i>session_number</i> { <b>destination</b> { <b>interface</b> <i>interface-id</i> }   <b>source</b> { <b>interface</b> <i>interface-id</i> [,   -] [both   rx   tx ] }	Configures port mirroring. <b>session-number</b> is the number of the port mirroring. <b>destination</b> is the destination port of the mirroring. <b>source</b> is the source port of mirroring. <b>rx</b> means the input data of mirroring. <b>Tx</b> means the output data of mirroring. <b>Both</b> means the input and output data of mirroring.
exit	Enters the management mode again.
write	Saves the configuration.

### 1.2.2 Displaying Port Mirroring Information

Run show to display the configuration information of port mirroring.

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

# POE Configuration

# Contents

Chapter 1 Power Over Ethernet .....	1
1.1 POE Overview .....	1
1.1.1 Introduction to POE Power Supply .....	1
1.1.2 Power-Up Procedure of PoE .....	3
1.2 POE Configuration Task List .....	4
1.3 POE Configuration Tasks .....	4
1.3.1 Displaying the information about POE-related systems .....	4
1.3.2 Configuring the power supply management mode for a switch. ....	4
1.3.3 Configuring the lasting time of the LED in PoE mode. ....	5
1.3.4 Stopping Sending the Trap Notification to Users When Power Supply Changes or Power Alarm Occurs	6
1.3.5 Configuring the percentage between alarm power and the total power. ....	6
1.3.6 Configuring Power Supply Protection .....	6
1.3.7 Configuring the Power Statistics .....	7
1.3.8 Configuring the Standard of PSE Power Supply .....	7
1.3.9 Enabling the Power Supply of a Port .....	7
1.3.10 Configuring the Maximum Power of a Port .....	8
1.3.11 Configuring the Power Supply Priority for a Port .....	9
1.3.12 Configuring the Port Description (usually for PD) .....	9
1.3.13 Configuring the Forced Power Supply .....	9
1.3.14 Configuring the Power Value of the External Power Supply .....	10



# Chapter 1 Power Over Ethernet

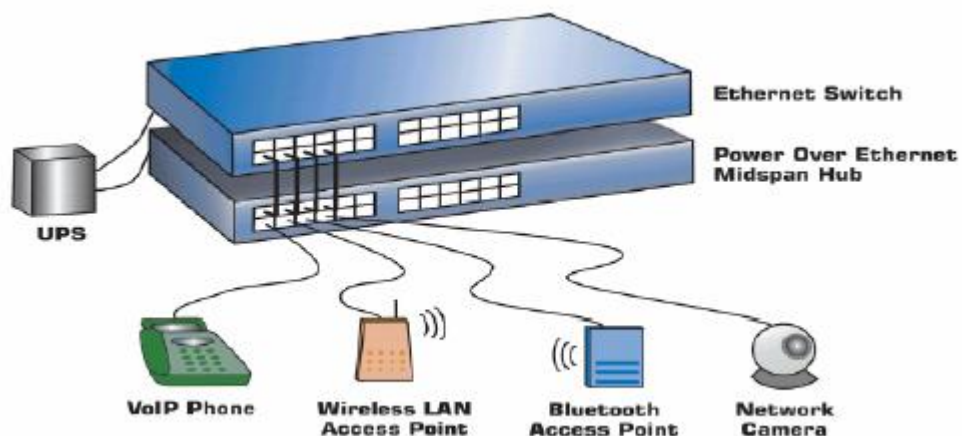
## 1.1 POE Overview

PoE, called Power Over Ethernet, refers that power is supplied through the 10BASE-T, 100BASE-TX and 1000BASE-T Ethernet, and its reliable power supply reaches up to 100 meters at maximum. In this way, the centralized power supply problem of the IP phone, wireless AP, portable device charger, POS machine, camera and data collection and other terminals can be effectively solved. For these terminals, there is no need to consider the problem of indoor power system wiring; the device is supplied with power while access to the network. In terms of universality, the current PoE power supply has also a unified standard; as long as 802.3af Standard which has been released is followed, the problem of adaptability between the devices from different manufacturers can be solved.

### 1.1.1 Introduction to POE Power Supply

According to the definition of the 802.3af Standard, PoE power supply system involves two kinds of device: PSE and PD. PSE (power-sourcing equipment), is primarily used to supply power to other devices, which can be divided into two kinds: Midspan (PoE functions are out of the switch) and Endpoint (PoE functions are integrated into the switch).

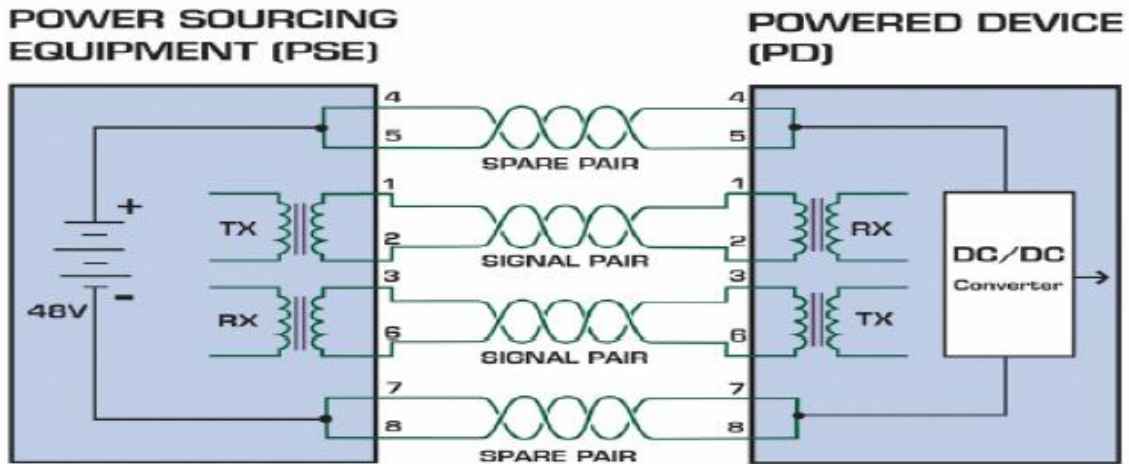
For the PoE-powered devices, their power supply systems are all integrated inside the device, which are the PSE device belonging to Endpoint. Meanwhile, the PD is defined as follows: PD (Powered Device) is the device which is used to receive power in the PoE power supply system, mainly referring to some wireless AP devices or some IP PHONE devices as well as some low power SOHO switches. Its typical networking diagram is as follows:



Meanwhile, 802.3af Standard also defines the PI (Power Interface: The interface between PSE/PD and network cable). At present, two power supply modes: Alternative A (Signal line No. 1, 2, 3, 6) and Alternative B (Free line 4, 5, 7, 8), have been defined, which are described as follows:

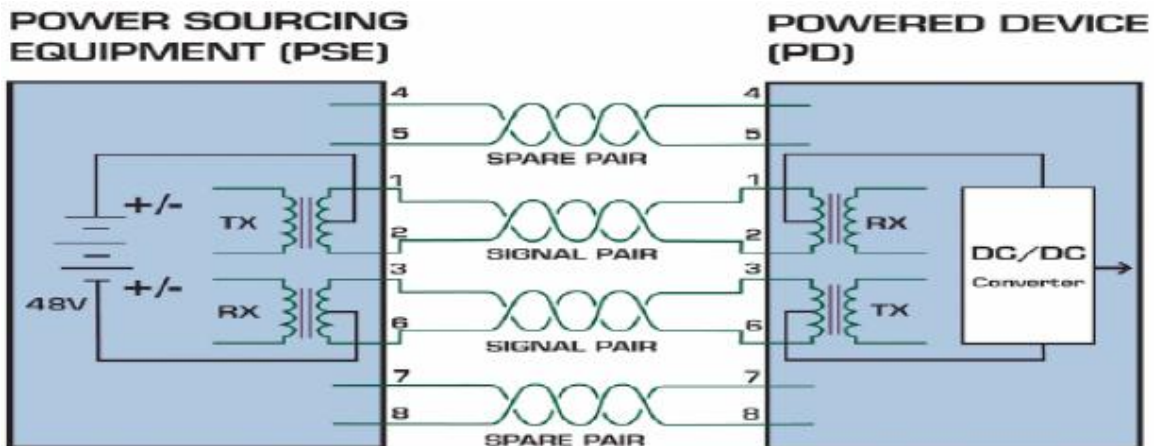
1) Supply the power through the idle pairs — Mode B (Alternative B)

As is shown below, Link 4 and Link 5 form a positive electrode; Link 7 and Link 8 form a negative electrode. PD is powered by PSE.



2) Supply the power through the data pair — Mode A (Alternative A)

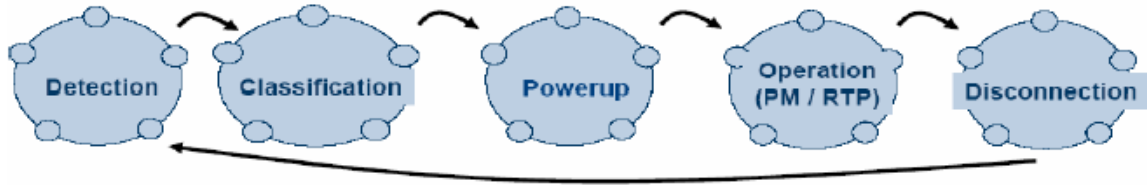
As is shown below, PSE can supply the power to the PD through the data pair. As the DC and the data frequency don't interfere with each other, both the current and data are transmitted through the same pair of lines at the same time. In fact, for the cable, it can be seen as a kind of "reuse". Link 1 and Link 2 can form a positive (or negative) electrode; Link 3 and Link 6 form a negative (or positive) electrode.



In general, the standard PD must support two kinds of ways of receiving power, but the PSE device only needs to support one of them; all products in our Company only support the power supply through the signal lines as PSE switch.

### 1.1.2 Power-Up Procedure of PoE

For PD, the flow of acquiring the power supply is as follows when accessing PSE system:



In the above process, the following steps are mainly described:

1) Detection: PSE detects whether the PD exists.

This step is mainly described as follows: PSE judges the existence of PD through detecting the RC value between the power supply output wire pairs. In the detection phase, the output voltage is 2.8V~10V, and the voltage polarity is consistent with -48V output. Only when PD is detected, PSE will continue to do the next step.

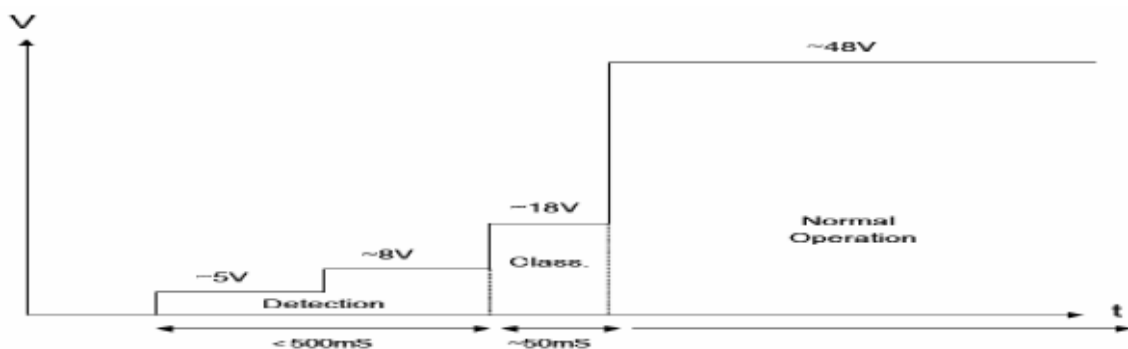
Features of PD existence: a. The DC Resistance is between 19Kohm and 26.5Kohm; b. The capacitance does not exceed 150nF;

2) Classification (optional): PSE determine PD power consumption.

PSE determines the PD power level through detecting the power output current. In the classification phase, the port output voltage is between 15.5V and 20.5V. The voltage polarity is consistent with -48V output.

3) Powerup: PSE supplies the power to the PD. When detecting that the device under the port is the legal PD device and PSE completes the classification of this PD (optional), PSE begins to supply power to this device, whose output voltage is -48V.

4) RTP & Power management: Real-time monitoring; power management. 5) Disconnection: PSE detects whether the PD disconnects — PSE uses a specific method to detect the disconnection of PD. If the PD is disconnected, PSE will close the port to output voltage. The port status returns to “Detection”. For PSE power supply system, its ideal output waveform is shown in the figure below:



## 1.2 POE Configuration Task List

- Displaying configuration
- Configuring the power supply management mode for switch
- Configuring LED mode as the duration of POE
- Not send “trap” to inform the users when the power supply at the port takes changes or sounds the power alarm;
- Configuring the percentage of the alarm power to total power
- Configuring power supply protection
- Configuring power statistics
- Configuring PSE power supply standard
- Configuring port's power supply enabling
- Configuring the maximum power of port
- Configuring the power supply priority of the port
- Configuring the port description, usually describing the PD
- Configuring the forced power supply function of the port

## 1.3 POE Configuration Tasks

### 1.3.1 Displaying the information about POE-related systems.

The global and port information of the POE module can be observed through the display command.

Use the following display commands in the management mode:

<b>Show poe system</b>	Display the POE-related system information
<b>Show poe all</b>	Display POE port information description table
<b>Show poe power</b>	Display all the port power supply information
<b>Show poe interface</b> <i>type slot/port</i>	Display the detailed POE information of the specified port

### 1.3.2 Configuring the power supply management mode for a switch.

By default, the management mode is the automatic mode (auto); in this mode, the maximum power limit of port cannot be set; by default, the maximum port power is that

supported by the chip; the port's power supply priority cannot be set, which is low by default.

In the preemptive mode and non-preemptive mode, the maximum power limit of the port and the power supply priority of the port can be configured.

The preemptive mode and non-preemptive mode are different. In the preemptive mode, in the state of full load, when the high-priority power supply port is connected to the PD, it supplies power normally to the newly connected PD, and the port with the lowest power supply priority is disconnected. In the non-preemptive mode, in the state of full load, when the high-priority power supply port is connected to the PH, the prompt message is given to prompt that the PD is accessed at the high-priority port.

In the global configuration mode, the power supply management mode of the switch can be configured using the following commands:

Step	Command	Purpose
<b>Step 1</b>	<b>config</b>	Enter the global configuration mode
<b>Step 2</b>	<b>poe power-management</b> {auto   preemptive   non-preemptive}	Configure the power supply management mode for switch

In the global configuration mode, use the following commands to further configure system parameters in the non-automatic mode:

When the total power is more than lowDisable, the port fails to supply power; when the total power is less than lowDisable, the port can continue to supply power.

$\text{lowDisable} = \text{Total power} - \text{value}$

When the total power exceeds lowNoConnect, the port whose priority is less than or equal to the lowest priority of current power supply will close the function of power supply enabling.

$\text{lowNoConnect} = \text{lowDisable} - \text{value}$

Step	Command	Purpose
<b>Step1</b>	<b>config</b>	Enter the global configuration mode
<b>Step2</b>	<b>poe power-management</b> {lowDisable   lowNoConnect } <i>value</i>	Configure the system parameters of switch in the non-automatic mode

### 1.3.3 Configuring the lasting time of the LED in PoE mode.

In the global configuration mode, use the following commands to configure the duration when the LED mode is POE:

Step	Command	Purpose
<b>Step1</b>	<b>config</b>	Enter the global configuration mode
<b>Step2</b>	<b>poe led-time</b> <i>time</i>	Configure the duration when the LED mode is POE

Restore default configuration:

Step	Command	Purpose
<b>Step1</b>	<b>config</b>	Enter the global configuration mode
<b>Step2</b>	<b>no poe led-time</b>	Restore the default duration; the default duration is 30 seconds

### 1.3.4 Stopping Sending the Trap Notification to Users When Power Supply Changes or Power Alarm Occurs

In the global configuration mode, use the following commands to configure:

Step	Command	Purpose
<b>Step1</b>	<b>config</b>	Enter the global configuration mode
<b>Step2</b>	<b>poe mib notification-stop</b>	Not send "trap" to inform the users when the power supply at the port takes changes

Restore the default setting:

Step	Command	Purpose
<b>Step1</b>	<b>config</b>	Enter the global configuration mode
<b>Step2</b>	<b>no poe mib notification-stop</b>	By default, send "trap" to inform the users when the power supply at the port takes changes

### 1.3.5 Configuring the percentage between alarm power and the total power.

In the global configuration mode, use the following commands to configure:

Step	Command	Purpose
<b>Step1</b>	<b>config</b>	Enter the global configuration mode
<b>Step2</b>	<b>poe threshold <i>value</i></b>	Configure the percentage of the alarm power to total power

Restore the default setting:

Step	Command	Purpose
<b>Step1</b>	<b>config</b>	Enter the global configuration mode
<b>Step2</b>	<b>no poe threshold</b>	By default, the percentage of the alarm power to total power is 100%.

### 1.3.6 Configuring Power Supply Protection

The power supply protection function of the port can prevent PSE docking against causing the problem.

By default, enable port protection; in the global configuration mode, use the following commands to configure:

Step	Command	Purpose
------	---------	---------

<b>Step1</b>	<b>config</b>	Enter the global configuration mode
<b>Step2</b>	<b>poe pse-unprotect</b>	Disable the port power supply protection

Disable port protection:

Step	Command	Purpose
<b>Step1</b>	<b>config</b>	Enter the global configuration mode
<b>Step2</b>	<b>no poe pse-unprotect</b>	Enable the port power supply protection

### 1.3.7 Configuring the Power Statistics

By default, disable power statistics; in the global configuration mode, use the following commands to configure:

Step	Command	Purpose
<b>Step1</b>	<b>config</b>	Enter the global configuration mode
<b>Step2</b>	<b>poe counter value</b>	Set the power statistic sampling interval

Restore the default setting; disable power statistics:

Step	Command	Purpose
<b>Step1</b>	<b>config</b>	Enter the global configuration mode
<b>Step2</b>	<b>no poe counter</b>	Disable power statistics

### 1.3.8 Configuring the Standard of PSE Power Supply

Select the AF standard — the port's maximum power supply is 15.4W;

Select the AT standard — the port's maximum power supply is 30W;

If selecting MAX, use the latest standard supported by this switch. For the device supporting both AF and AT, select AT; for the device supporting AF instead of AT, select AF.

Step	Command	Purpose
<b>Step1</b>	<b>config</b>	Enter the global configuration mode
<b>Step2</b>	<b>poe standard {AT   AF   MAX}</b>	Configure PSR power supply standard for switch

### 1.3.9 Enabling the Power Supply of a Port

Provide two ways to control the port's power supply enabling: 1. directly enabling and disabling the port; 2. supplying power based on the time range.

#### Method 1:

By default, the port's power supply is enabled; in the port configuration mode, use the following commands to prohibit the port enabling:

Step	Command	Purpose
<b>Step1</b>	<b>config</b>	Enter the global configuration mode
<b>Step2</b>	<b>interface</b> intf-type intf-id	Enter the port configuration mode
<b>Step3</b>	<b>poe disable</b>	Prohibit the port's power supply enabling

Restore the default setting; enable the port's power supply enabling:

Step	Command	Purpose
<b>Step1</b>	<b>config</b>	Enter the global configuration mode
<b>Step2</b>	<b>interface</b> intf-type intf-id	Enter the port configuration mode
<b>Step3</b>	<b>no poe disable</b>	Enable the port's power supply

#### Method 2:

By default, there is no control over the port's power supply enabling based on time range; in the port configuration mode, use the following commands to configure the port's power supply enabling based on time range:

Step	Command	Purpose
<b>Step1</b>	<b>config</b>	Enter the global configuration mode
<b>Step2</b>	<b>interface</b> intf-type intf-id	Enter the port configuration mode
<b>Step3</b>	<b>poe disable time-range</b> <i>name</i>	Configure the control over the port's power supply enabling with the <i>name</i> "disable the port's power supply based on time range"

Restore the default setting; remove the control over the port's power supply enabling based on time range:

Step	Command	Purpose
<b>Step1</b>	<b>config</b>	Enter the global configuration mode
<b>Step2</b>	<b>interface</b> intf-type intf-id	Enter the port configuration mode
<b>Step3</b>	<b>no poe disable time-range</b>	Cancel the control over the port's power supply enabling based on time range"

### 1.3.10 Configuring the Maximum Power of a Port

By default, the port's maximum power is 30000mW; in the port configuration mode, use the following commands to configure:

Step	Command	Purpose
<b>Step1</b>	<b>config</b>	Enter the global configuration mode
<b>Step2</b>	<b>interface</b> intf-type intf-id	Enter the port configuration mode
<b>Step3</b>	<b>poe max-power</b> <i>value</i>	Configure the port's maximum power; the unit is mW

Restore the default setting:



Step	Command	Purpose
<b>Step1</b>	<b>config</b>	Enter the global configuration mode
<b>Step2</b>	<b>interface</b> intf-type intf-id	Enter the port configuration mode
<b>Step3</b>	<b>no poe max-power</b>	By default, the port's maximum power is 30000mW.

### 1.3.11 Configuring the Power Supply Priority for a Port

By default, the port's power supply priority is low; in the port configuration mode, use the following commands to configure:

Step	Command	Purpose
<b>Step1</b>	<b>config</b>	Enter the global configuration mode
<b>Step2</b>	<b>interface</b> intf-type intf-id	Enter the port configuration mode
<b>Step3</b>	<b>poe priority</b> {critical   high   low }	Configure the port's power supply priority: critical > high > low

### 1.3.12 Configuring the Port Description (usually for PD)

By default, the port description is empty; in the port configuration mode, use the following commands to configure:

Step	Command	Purpose
<b>Step1</b>	<b>config</b>	Enter the global configuration mode
<b>Step2</b>	<b>interface</b> intf-type intf-id	Enter the port configuration mode
<b>Step3</b>	<b>poe PD-discription</b> <i>string</i>	Configure the port description

Restore the default setting:

Step	Command	Purpose
<b>Step1</b>	<b>config</b>	Enter the global configuration mode
<b>Step2</b>	<b>interface</b> intf-type intf-id	Enter the port configuration mode
<b>Step3</b>	<b>no poe PD-discription</b>	Remove the description string

### 1.3.13 Configuring the Forced Power Supply

By default, disable the force power supply; in the port configuration mode, use the following commands to configure:

Step	Command	Purpose
<b>Step1</b>	<b>config</b>	Enter the global configuration mode
<b>Step2</b>	<b>interface</b> intf-type intf-id	Enter the port configuration mode
<b>Step3</b>	<b>poe force-power</b>	Enable the port's force power supply

Restore the default setting, and disable the port's force power supply:

Step	Command	Purpose
<b>Step1</b>	<b>config</b>	Enter the global configuration mode
<b>Step2</b>	<b>interface</b> intf-type intf-id	Enter the port configuration mode
<b>Step3</b>	<b>no poe force-power</b>	Disable the port's force power supply

### 1.3.14 Configuring the Power Value of the External Power Supply

When using external power supply, the power value of the external power supply is required to configure to enable the POE to provide the total power of the internal power value plus external power value. This configuration value is the actual power value of external power supply.

By default, not configure the power value of external power supply; in the global configuration mode, use the following commands to configure:

Step	Command	Purpose
<b>Step1</b>	<b>config</b>	Enter the global configuration mode
<b>Step2</b>	<b>poe extern-power</b> <i>value</i>	Configure the power value of external power supply (Unit: W) to enable the total power to be equal to the sum of internal power plus external power.

Restore the default setting in the case of not using the external power supply:

Step	Command	Purpose
<b>Step1</b>	<b>config</b>	Enter the global configuration mode
<b>Step2</b>	<b>no poe extern-power</b>	Make the total power be the default internal power value

# MAC Address Table Attribute Configuration

## Table of Contents

Chapter 1 Configuring MAC Address Attribute .....	1
1.1 MAC Address Configuration Task List .....	1
1.2 MAC address Configuration Task .....	1
1.2.1 Configuring Static Mac Address .....	1
1.2.2 Configuring MAC Address Aging Time .....	1
1.2.3 Displaying MAC Address Table .....	2
1.2.4 Clearing Dynamic MAC Address .....	2

## Chapter 1 Configuring MAC Address Attribute

### 1.1 MAC Address Configuration Task List

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

### 1.2 MAC address Configuration Task

#### 1.2.1 Configuring Static Mac Address

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

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

#### 1.2.2 Configuring MAC Address Aging Time

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

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

Command	Purpose
<b>configure</b>	Enters the global configuration mode

## MAC Address Table Attribute Configuration

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

### 1.2.3 Displaying MAC Address Table

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

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

### 1.2.4 Clearing Dynamic MAC Address

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

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

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

## 802.1x Configuration

# Table of Contents

Chapter 1 Configuring 802.1x..... 1

    1.1 802.1x Configuration Task List ..... 1

    1.2 802.1x Configuration Task ..... 1

        1.2.1 Configuring 802.1x Port Authentication ..... 1

        1.2.2 Configuring 802.1x Multiple Port Authentication ..... 2

        1.2.3 Configuring 802.1x Re-authentication ..... 3

        1.2.4 Configuring Maximum Times for 802.1x ID Authentication ..... 3

        1.2.5 Configuring 802.1x Transmission Frequency ..... 3

        1.2.6 Configuring 802.1x User Binding ..... 4

        1.2.7 Configuring Authentication Method for 802.1x Port ..... 4

        1.2.8 Selecting Authentication Type for 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 ..... 6

        1.2.12 Forbidding Supplicant With Multiple Network Cards ..... 6

        1.2.13 Resuming Default 802.1x Configuration ..... 6

        1.2.14 Monitoring the user state of 802.1x hybrid authentication ..... 6

        1.2.15 Monitoring 802.1x Authentication Configuration and State ..... 7

    1.3 802.1x Configuration Example ..... 7



# Chapter 1 Configuring 802.1x

## 1.1 802.1x Configuration Task List

- Configuring 802.1x port authentication
- Configuring 802.1x multiple port authentication
- Configuring maximum times for 802.1x ID authentication
- Configuring 802.1x re-authentication
- Configuring 802.1x transmission frequency
- Configuring 802.1x user binding
- Configuring authentication method for 802.1x port
- Selecting authentication type for 802.1x port
- Configuring 802.1x accounting
- Configuring guest-vlan
- Forbidding Supplicant with multiple network cards
- Resuming default 802.1x configuration
- Monitoring 802.1x authentication configuration and state

## 1.2 802.1x Configuration Task

### 1.2.1 Configuring 802.1x Port Authentication

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

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

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

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

Run...	To...
<b>dot1x enable</b>	Enable the 802.1x function.

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

Run...	To...
<b>dot1x port-control auto</b>	Configure the 802.1x protocol control method on the port.
<b>aaa authentication dot1x {default  list name} method</b>	Configure the AAA authentication of 802.1x.

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

Run...	To...
<b>dot1x port-control auto</b>	Enables the 802.1x authentication method on the port.
<b>dot1x port-control misc-mab</b>	Enables 802.1x hybrid authentication.
<b>dot1x port-control force-authorized</b>	Approve the mandatory port authentication.
<b>dot1x port-control force-unauthorized</b>	Disapprove the mandatory port authentication.

## 1.2.2 Configuring 802.1x Multiple Port Authentication

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

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

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

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

Run...	To...
<b>dot1x authentication multiple-hosts</b>	Set the 802.1x multiple port authentication. The port is set to <b>up</b> only if one user passes the authentication.

<b>dot1x authentication multiple-auth</b>	Set the 802.1x multiple port authentication. Each user is non-related in authentication.
---	---

### 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.

Run...	To
<b>dot1x re-authentication</b>	Enables the re-authentication function.
<b>dot1x timeout re-authperiod</b> <i>time</i>	Configures the period of the re-authentication function.

### 1.2.4 Configuring Maximum Times for 802.1x ID Authentication

When 802.1x authentication starts or 802.1x authentication is being performed again, 802.1x sends ID authentication request to guest hosts. If the request message is dropped or delayed because network problems, the requirement message will be sent again. If the message is resent certain times, 802.1x stops to send the message and the ID authentication fails.

You can reset the maximum times of ID authentication request according to different network conditions, ensuring the clients are authenticated successfully by the authentication server.

Run the following command in interface configuration command to set the maximum times for ID authentication request:

Run...	To
<b>dot1x reauth-max</b> <i>time</i>	Set the maximum times for ID authentication request.

### 1.2.5 Configuring 802.1x Transmission Frequency

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

Run the following command to configure the transmission frequency:

Run...	To...
<b>dot1x timeout tx-period</b> <i>time</i>	Set the message transmission frequency of 802.1x.

## 1.2.6 Configuring 802.1x User Binding

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

Run...	To...
<b>dot1x user-permit xxxz</b>	Configure a user that is bound to a port.

## 1.2.7 Configuring Authentication Method for 802.1x Port

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

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

Run...	To...
<b>dot1x authentication method yyy</b>	Configure the method of the 802.1x authentication.

## 1.2.8 Selecting Authentication Type for 802.1x Port

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

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

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

Run...	To...
<b>dot1x authen-type {chap eap}</b>	Select chap or eap.

Also run the following command in interface configuration mode:

Run...	To...
<b>dot1x authentication type {chap eap}</b>	Select chap or eap or the configured authentication type 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 MAB is enabled and the peer device, however, neither sends the `eapol_start` packet nor responds to the `request_identity` packet and exceeds the timeout threshold, the switch regards the peer device not to support the 802.1x authentication client and then turns to the MAB authentication.

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

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

Run...	To...
<b>dot1x mab</b>	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:

Run...	To...
<b>dot1x mabformat</b> {1 2 3 4 5 6}	Chooses one MAC address' format from six formats from format 1 to format 6. The default format is 1.

### 1.2.10 Configuring 802.1x Accounting

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

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

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

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

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

Run...	To...
<b>dot1x accounting enable</b>	Enable the dot1x accounting.
<b>dot1x accounting method</b> { <i>method name</i> }	Configure the accounting method. Its default value is <b>default</b> .

### 1.2.11 Configuring 802.1x guest-vlan

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

**Note:**

There is no access right if the authentication fails.

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

Run...	To...
<b>Dot1x guest-vlan</b>	Enable the guest-vlan at all ports.

When the original value of **guest-vlan id** at each port is 0, guest-vlan cannot function even if guest-vlan is enabled in global mode. Only when **guest-vlan id** is configured in port configuration mode, guest-vlan can function.

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

Run...	To...
<b>Dot1x guest-vlan {id(1-4094)}</b>	Enable the vlan id of guest-vlan at all ports.

### 1.2.12 Forbidding Supplicant With Multiple Network Cards

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

Run...	To...
<b>dot1x forbid multi-network-adapter</b>	Forbid the Supplicant with multiple network adapters.

### 1.2.13 Resuming Default 802.1x Configuration

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

Run...	To...
<b>dot1x default</b>	Resume all global configuration to default configuration.

### 1.2.14 Monitoring the user state of 802.1x hybrid authentication

Run the following command to monitor the user state of 802.1x hybrid authentication and confirm the mac addresses of which users are forwarded in the EXEC mode:

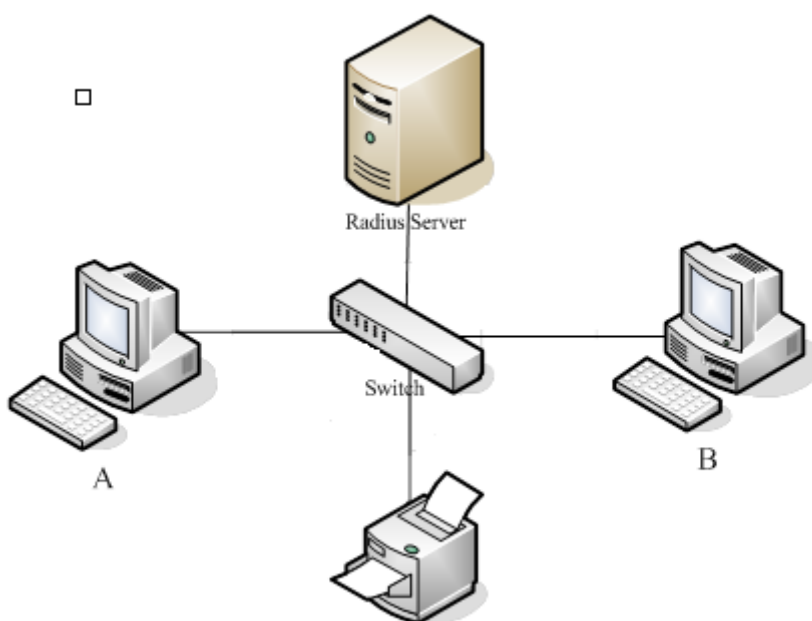
Run...	To...
<b>show dot1x misc-mab-db { interface }</b>	The user state of 802.1x hybrid authentication.

### 1.2.15 Monitoring 802.1x Authentication Configuration and State

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

Run...	To...
<b>show dot1x</b> { interface statistics }	Monitor the configuration and state of 802.1x authentication.

## 1.3 802.1x Configuration Example



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

### Global configuration

```
username switch password 0 TST
username TST password 0 TST
aaa authentication dot1x TST-G0/2 group radius
aaa authentication dot1x TST-G0/4 local
aaa authentication dot1x TST-G0/6 group radius
aaa accounting network dot1x_acc start-stop group radius
dot1x enable
dot1x re-authentication
dot1x timeout re-authperiod 10
```

```
dot1x mabformat 2
dot1x guest-vlan
interface VLAN1
ip address 192.168.20.24 255.255.255.0
!
vlan 1-2
radius-server host 192.168.20.2 auth-port 1812 acct-port 1813
radius-server key TST
```

### Configuring port G0/2

```
interface GigaEthernet0/2
dot1x port-control auto
dot1x authentication method TST-G0/2
dot1x user-permit radius-TST
dot1x accounting enable
dot1x accounting method dot1x_acc
```

### Configuring port G0/4

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

### Configuring port G0/6

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



# 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 VLAN Configuration Task List ..... 3
  - 1.4 VLAN Configuration Task ..... 3
    - 1.4.1 Adding/Deleting VLAN..... 3
    - 1.4.2 Configuring Switch Port..... 3
    - 1.4.3 Creating/Deleting VLAN Interface ..... 4
    - 1.4.4 Monitoring Configuration and State of VLAN ..... 4
    - 1.4.5 Enabling/disabling global Dot1Q Tunnel ..... 5
    - 1.4.6 Dot1Q Tunnel Configuration Examples ..... 5

# Chapter 1 VLAN Configuration

## 1.1 VLAN Introduction

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

There are the following types of Virtual LANs:

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

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

- Vlan-allowed range is supported on the interface.

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

## 1.2 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, which mainly consist of OLTs, 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. Thus, if a received packet has a VLAN tag, the packet become a packet with double tags; if a received packet is untagged, this packet will be added a default VLAN tag of this port.

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

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

Table 1 The packet with a single VLAN tag

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

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

Table 2 Packet with double VLAN tags

#### 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 and 300. The CVLAN ID of IPTV service ranges between 301 and 400. According to the CVLAN ID range, when the PE device receives the user data, add SPVLAN Tag whose SPVLAN ID is 1000 to the bandwidth service and whose SPVLAN ID is 3000 to the IPTV service. The difference between Flat VLAN translation mode and QinQ VLAN translation mode is SPVLAN Tag in the Flat VLAN translation mode is not add to the outside layer of CVLAN Tag, but replace CVLAN Tag directly.

## 1.3 VLAN Configuration Task List

- Adding/Deleting VLAN
- Configuring switch port
- Creating/Deleting VLAN interface
- Monitoring configuration and state of VLAN
- Enabling/disabling global Dot1Q Tunnel
- Dot1Q Tunnel Configuration Examples

## 1.4 VLAN Configuration Task

### 1.4.1 Adding/Deleting VLAN

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

Run the following command to configure VLAN

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

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

### 1.4.2 Configuring Switch Port

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

- The access mode indicates that this port is only subordinate to one vlan and only sends and receives untagged ethernet frame.
- The relay mode indicates that the port connects other switches and the tagged Ethernet frame can be transmitted and received.

- The VLAN translating tunnel mode is a sub mode based on the relay mode. The port looks up the VLAN translation table according to the VLAN tag of received packets to obtain corresponding SPVLAN, and then the switching chip replaces the original tag with SPVLAN or adds the SPVLAN tag to the outside layer of the original tag. When the packets is forwarded out of the port, the SPVLAN will be replaced by the original tag or the SPVLAN tag will be removed mandatorily. Hence, the switch omits different VLAN partitions that access the network, and then passes them without change to the other subnet that connects the other port of the same client, realizing transparent transmission.
- The VLAN tunnel uplink mode is a sub mode based on the relay mode. The SPVLAN should be set when packets are forwarded out of the port. The SPVLAN should be set when packets are forwarded out of the port. If the packets are in the untagged range, all these packets are forwarded out without any change. When the packets are received by the port, their TPIDs will be checked. If difference occurs or they are untagged packets, the SPVLAN tag which contains their own TPID will be added to them as their outer-layer tag.

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

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

Run the following command to configure the switch port:

Run...	To...
<b>switchport pvid</b> <i>vlan-id</i>	Configure pvid of switch port.
<b>switchport mode</b> {access   trunk   dot1q-tunnel-uplink   dot1q-translating-tunnel}	Configure port mode of the switch.
<b>switchport trunk vlan-allowed</b> ...	Configure vlan-allowed range of switch port.
<b>switchport trunk vlan-untagged</b> ...	Configure vlan-untagged range of switch port.

### 1.4.3 Creating/Deleting VLAN Interface

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

Run...	To...
<b>[no] interface vlan</b> <i>vlan-id</i>	Create/Delete a VLAN interface.

### 1.4.4 Monitoring Configuration and State of VLAN

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

Run...	To...
--------	-------

<b>show vlan [ id x   interface intf   dot1q-tunnel [interface intf ]</b>	Display configuration and state of VLAN.
<b>show interface vlan x</b>	Display the states of vlan ports.

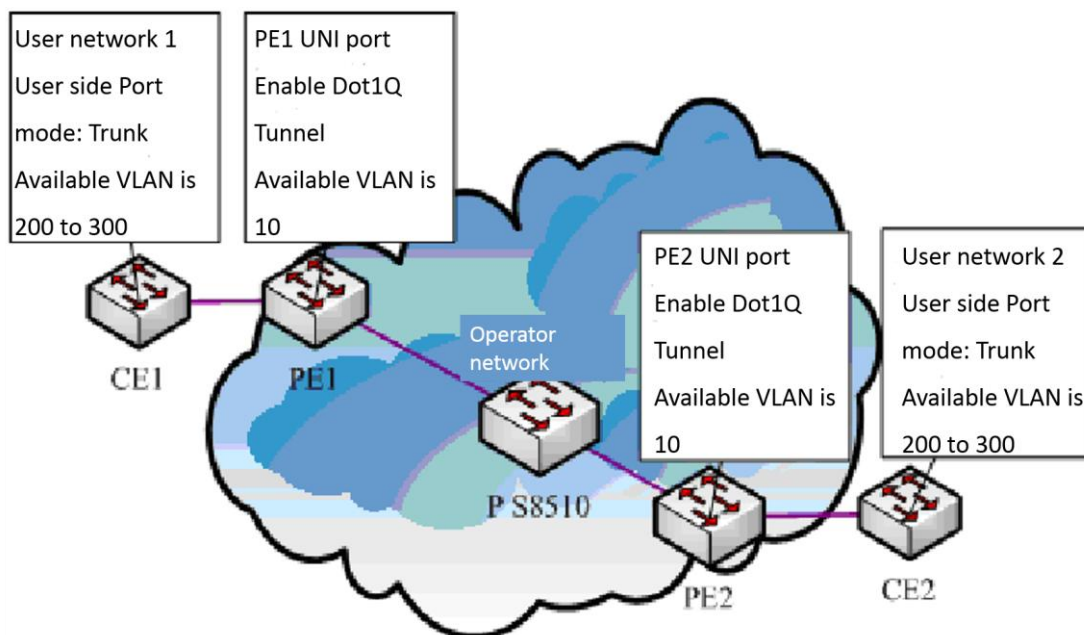
#### 1.4.5 Enabling/disabling global Dot1Q Tunnel

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

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

Run...	To...
<b>dot1q-tunnel</b>	Configures the global dot1q-tunnel on a switch.

#### 1.4.6 Dot1Q Tunnel Configuration Examples



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

The ports of PE are set to be the access port of VLAN 10 and on them Dot1Q Tunnel is enabled. However, the ports of CE still need Trunk VLAN 200-300, enabling the link between CE and PE to be an asymmetrical link. In this case, the public network only needs to distribute users a VLAN ID, 10. No matter how many VLAN IDs of private network are planned in the user's network, the newly distributed VLAN ID of the public network will be mandatorily inserted into the tagged packets when these packets enter the backbone network of ISP. These packets then pass through the backbone network through the VLAN ID of the public network, reach the other side of the backbone

network, that is, the PE devices, get rid of the VLAN tag of the public network, resume the user's packets and at last are transmitted to the CE devices of the users. Therefore, the packets that are forwarded in the backbone network have two layers of 802.1Q tag headers, one being the tag of the public network and the other being the tag of the private network. The detailed flow of packet forwarding is shown as follows:

- 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, our products of different models are configured as follows when they run as PE (PE1 has the same configuration as 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
```



# GVRP Configuration

## Table of Contents

Chapter 1 Configuring GVRP .....	1
1.1 Introduction.....	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 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 Configuring GVRP

## 1.1 Introduction

GVRP (GARP VLAN Registration Protocol GARP VLAN) is a GARP (GARP VLAN Registration Protocol GARP VLAN) application that provides IEEE 802.1Q-compliant VLAN pruning and dynamic VLAN creation on 802.1Q trunk ports.

With GVRP, the switch can exchange the VLAN configuration information with the other GVRP switches, prune the unnecessary broadcast and unknown unicast traffic, and dynamically create and manage the VLANs on the switches that are connected through the 802.1Q trunk ports.

## 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

Perform the following configuration in global configuration mode.

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

It is disabled by default.

### 1.3.2 Dynamic VLAN to Validate only on a Registered Port

Run the following commands in global configuration mode:

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

After this function is enabled, dynamic VLAN takes effect only on the ports on which this dynamic VLAN is registered. After this command is enabled and if a port has not registered a dynamic VLAN, this port will not belong to the dynamic

VLAN even though this port is a trunk port and it allows the dynamic VLAN to pass through.

The function is disabled by default.

### 1.3.3 Enabling/Disabling GVRP on the Interface

Perform the following configuration in interface configuration mode:

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

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

It is enabled by default.

### 1.3.4 Monitoring and Maintenance of GVRP

Perform the following operations in EXEC mode:

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

Display GVRP statistics:

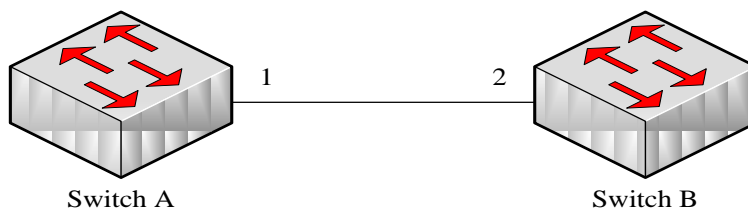
```
switch#show gvrp statistics interface Tthernet0/1
GVRP statistics on port Ethernet0/1
GVRP Status: Enabled
GVRP Failed Registrations: 0
GVRP Last Pdu Origin: 0000.0000.0000
GVRP Registration Type: Normal
```

Display GVRP global state information:

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

## 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.

# GMRP Configuration

## Table of Contents

Chapter 1 Configuring GMRP .....	1
1.1 Introduction .....	1
1.2 Configuration Task List .....	1
1.3 GMRP Configuration Task .....	1
1.3.1 Enabling/Disabling GMRP in Global Configuration Mode .....	1
1.3.2 Enabling/Disabling GMRP on the Port .....	1
1.3.3 Monitoring and Maintaining GMRP .....	2
1.4 Configuration Example .....	2

# Chapter 1 Configuring GMRP

## 1.1 Introduction

GARP Multicast Registration Protocol (GMRP) is based on the Generic Attribute Registration Protocol (GARP). It adopts GARP's mechanism to maintain the multicast MAC table of the switch, which saves network resources because the mechanism prevents multicast message from broadcasting. All GMRP-supported switches can receive multicast MAC address registry information from other switches and dynamically update the local multicast MAC address registry information, including multicast MAC address registry information currently saved in the ports. At the same time, GMRP-supported switches can send their local multicast MAC address registry information to other switches.

## 1.2 Configuration Task List

GMRPConfiguration task list includes the following tasks:

- Enabling/Disabling GMRP in global configuration mode
- Enabling/Disabling GMRP on the port
- Monitoring and maintaining GMRP

## 1.3 GMRP Configuration Task

### 1.3.1 Enabling/Disabling GMRP in Global Configuration Mode

Perform the following configuration in global configuration mode.

Command	Description
<b>gmrp</b> [vlan vlan-id]	Enables GMRP in global configuration mode.
<b>no gmrp</b> [vlan vlan-id]	Resumes GMRP to the default state.

GMRP is disabled by default. Enable GMRP without setting VLAN parameters, VLAN 1-16 takes effect. Disable GMRP without setting VLAN parameters, VLAN of all configured GMRP takes effect.

Note: GMRP can enable 16 VLANs simultaneously.

### 1.3.2 Enabling/Disabling GMRP on the Port

Perform the following configuration in port configuration mode.

Command	Description
<b>gmrp</b>	Enables/Disables GMRP on the port.
<b>no gmrp</b>	Resume GMRP on the port to the default state.



Before enabling GMRP on the port, enable GMRP in global configuration mode. Otherwise, GMRP on the port cannot work. What's more, GMRP has to be configured at the trunk port.

GMRP on the port is enabled by default.

### 1.3.3 Monitoring and Maintaining GMRP

Perform the following configuration in management mode:

Command	Description
<b>show gmrp statistics</b> [ <i>interface port_list</i> ]	Displays GMRP statistics information.
<b>show gmrp status</b>	Displays GMRP information in global mode.
[ no ] <b>debug gmrp</b> { <b>packet</b>   <b>event</b> }	Enables/Disables the debug on-off of GMRP packets and events.

#### 1. Displaying GMRP statistics information

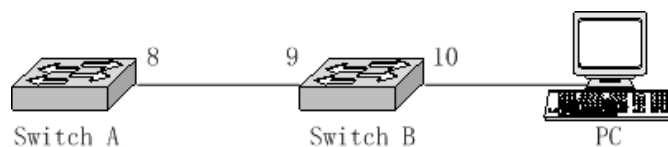
```
switch#show gmrp statistics interface FastEthernet0/6
GMRP statistics on port FastEthernet0/6
GMRP Status: Enabled
GMRP Frames Received: 54
GMRP Frames Transmitted: 27
GMRP Frames Discarded: 0
GMRP Last Pdu Origin: 1234.5678.9abc
```

#### 2. Displaying GMRP information in global mode

```
switch#show gmrp status
GMRP is disabled
```

## 1.4 Configuration Example

The following figure shows the network connection.



To make VLAN configuration information on Switch A the same as that of Switch B, enable GMRP on Switch A and Switch B. The configuration is shown as follows:

- (1) Run the following command to enable GMRP of Switch A in global configuration mode:

```
Switch_config#gmrp
```

- (2) Run the following command to enable GMRP on port 8 at Switch A:

```
Switch_config_f0/8#gmrp
```

- (3) Run the following command to enable GMRP of Switch B in global configuration mode:  
Switch\_config#gmrp
- (4) Run the following command to enable GMRP on port 9 at Switch B:  
Switch\_config\_f0/9#gmrp
- (5) Run the following command to enable GMRP on port 10 at Switch B:  
Switch\_config\_f0/9#gmrp
- (6) Send the message **gmrp join** from the computer connecting port 10 of Switch B to Switch B. The multicast MAC address registered in the message is 01.00.00.00.00.99.
- (7) Check the multicast MAC address table at Switch A to find the record about the MAC address 01.00.00.00.00.99.

**Note:**

- 1) Both the VLAN cluster that port 8 of Switch A belongs to and the VLAN cluster that port 9 of Switch B belongs to contain vlan of the **join** message. Different VLANs cannot communicate with each other directly.
- 2) Check the multicast MAC address table at Switch A before the leaveall timer times out. For easy observation, run **garp timer leaveall** to simultaneously increase the timeout value of leaveall timers of two switches (10 seconds by default).

# 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 Task .....	3
1.3.1 Selecting STP Mode.....	3
1.3.2 Disabling/Enabling STP .....	3
1.3.3 Forbidding/Enable Port's STP .....	3
1.3.4 Configuring the Switch Priority .....	4
1.3.5 Configuring the Hello Time.....	4
1.3.6 Configuring the Max-Age Time.....	4
1.3.7 Configuring the Forward Delay Time.....	4
1.3.8 Configuring the Port Priority .....	5
1.3.9 Configuring the Path Cost .....	5
1.3.10 Configuring Auto-Designated Port.....	5
1.3.11 Monitoring STP State .....	5
1.3.12 Configuring SNMP Trap .....	6
Chapter 2 Configuring RSTP .....	7
2.1 RSTP Configuration Task List.....	7
2.2 RSTP Configuration Task .....	7
2.2.1 Enabling/Disabling Switch RSTP .....	7
2.2.2 Configuring the Switch Priority .....	7
2.2.3 Configuring the Forward Delay Time.....	8
2.2.4 Configuring the Hello Time .....	8
2.2.5 Configuring the Max-Age .....	9
2.2.6 Configuring the Path Cost .....	9
2.2.7 Configuring the Port Priority .....	10
2.2.8 Configuring edge port.....	10
2.2.9 Configuring port's connection type .....	10
2.2.10 Restarting the check of protocol conversion .....	11
Chapter 3 Configuring MTSP.....	12
3.1 MSTP Overview.....	12
3.1.1 Introduction .....	12
3.1.2 MST Domain .....	12
3.1.3 IST, CST, CIST and MSTI.....	12
3.1.4 Port Role .....	14
3.1.5 MSTP BPDU .....	17
3.1.6 Stable State.....	18
3.1.7 Hop Count.....	19
3.1.8 STP Compatibility.....	19
3.2 MSTP Configuration Task List .....	19
3.3 MSTP Configuration Task.....	20

Table of Contents

---

3.3.1 Default MSTP Configuration..... 20

3.3.2 Enabling and Disabling MSTP..... 21

3.3.3 Configuring MST Area ..... 21

3.3.4 Configuring Network Root ..... 22

3.3.5 Configuring Secondary Root ..... 23

3.3.6 Configuring Bridge Priority ..... 24

3.3.7 Configuring STP Time Parameters ..... 24

3.3.8 Configuring Network Diameter ..... 25

3.3.9 Configuring Maximum Hop Count ..... 25

3.3.10 Configuring Port Priority ..... 26

3.3.11 Configuring Path Cost of the Port..... 26

3.3.12 Configuring Edge Port ..... 27

3.3.13 Configuring Port Connection Type ..... 27

3.3.14 Activating MST-Compatible Mode ..... 27

3.3.15 Restarting Protocol Conversion Check ..... 28

3.3.16 Configuring Port's Role Restriction ..... 29

3.3.17 Configuring Port's TCN Restriction ..... 29

3.3.18 Checking MSTP Information ..... 29

# Chapter 1 Configuring STP

## 1.1 STP Introduction

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

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

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

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

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

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

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

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

- (1) Identifier of each bridge
- (2) Path cost of each port
- (3) Port identifier for each port of the bridge

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

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

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

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

**Note:**

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

## 1.2 SSTP Configuration Task List

- Selecting STP Mode
- Disabling/Enabling STP
- Forbidding/Enable Port's STP
- Configuring the Switch Priority
- Configuring the Hello Time
- Configuring the Max-Age Time
- Configuring the Forward Delay Time
- Configuring the Port Priority
- Configuring the Path Cost
- Configuring Auto-Designated Port
- Monitoring STP State

- Configuring SNMP Trap

## 1.3 SSTP Configuration Task

### 1.3.1 Selecting STP Mode

Run the following command to configure the STP mode:

Run...	To...
<b>spanning-tree mode</b> {sstp   rstp}	Select the STP configuration.

### 1.3.2 Disabling/Enabling STP

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

Follow these steps to disable spanning-tree:

command	purpose
<b>no spanning-tree</b>	Disables STP.

To enable spanning-tree, use the following command:

command	purpose
<b>spanning-tree</b>	Enables default mode STP (SSTP).
<b>spanning-tree mode</b> {sstp   rstp   mstp}	Enables a certain mode STP.

### 1.3.3 Forbidding/Enable Port's STP

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

command	purpose
<b>no spanning-tree</b>	Forbidding port to operate STP.

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

Notice:

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



**Notice:**

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

### 1.3.4 Configuring the Switch Priority

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

Follow these steps to configure the switch priority:

command	purpose
<b>spanning-tree sstp priority</b> <i>value</i>	Modifies sstp priority value.
<b>no spanning-tree sstp priority</b>	Returns sstp priority to default value (32768).

### 1.3.5 Configuring the Hello Time

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

Use the following command to configure Hello Time of SSTP:

command	purpose
<b>spanning-tree sstp hello-time</b> <i>value</i>	Configures sstp Hello Time.
<b>no spanning-tree sstp hello-time</b>	Returns sstp Hello Time to default value (4s).

### 1.3.6 Configuring the Max-Age Time

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

Follow these steps to configure the maximum-aging time:

command	purpose
<b>spanning-tree sstp max-age</b> <i>value</i>	Configures the sstp max-age time.
<b>no spanning-tree sstp max-age</b>	Returns the max-age time to default value (20s).

### 1.3.7 Configuring the Forward Delay Time

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

Use the following command to configure sstp forward delay:

command	purpose
<b>spanning-tree sstp forward-time</b> <i>value</i>	Configures sstp Forward time.
<b>no spanning-tree sstp forward-time</b>	Returns forward time to default value (15s).

### 1.3.8 Configuring the Port Priority

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

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

command	purpose
<b>spanning-tree port-priority</b> <i>value</i>	Configures the port priority for an interface.
<b>spanning-tree sstp port-priority</b> <i>value</i>	Modifies sstp port priority.
<b>no spanning-tree sstp port-priority</b>	Returns port priority to default value (128).

### 1.3.9 Configuring the Path Cost

Follow these steps to configure the cost of an interface:

command	purpose
<b>spanning-tree cost</b> <i>value</i>	Configures the cost for an interface.
<b>spanning-tree sstp cost</b> <i>value</i>	Modifies sstp path cost.
<b>no spanning-tree sstp cost</b>	Returns path cost to default value.

### 1.3.10 Configuring Auto-Designated Port

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

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

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

Command	Purpose
<b>spanning-tree designated-auto</b>	Enables the auto-designated port function.
<b>no spanning-tree designated-auto</b>	Disables the auto-designated port function.

### 1.3.11 Monitoring STP State

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

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

### 1.3.12 Configuring SNMP Trap

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

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

---

#### Notice:

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

---

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

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

## Chapter 2 Configuring RSTP

### 2.1 RSTP Configuration Task List

- RSTP Configuration Task List
- RSTP Configuration Task
- Enabling/Disabling Switch RSTP
- Configuring the Switch Priority
- Configuring the Forward Delay Time
- Configuring the Hello Time
- Configuring the Max-Age
- Configuring the Path Cost
- Configuring the Port Priority
- Configuring edge port
- Configuring port's connection type
- Restarting the check of protocol conversion

### 2.2 RSTP Configuration Task

#### 2.2.1 Enabling/Disabling Switch RSTP

Follow these configurations in the global configuration mode:

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

#### 2.2.2 Configuring the Switch Priority

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

Follow these steps to configure the switch priority:

Follow these configurations in the global configuration mode:

command	purpose
<b>spanning-tree rstp priority</b> <i>value</i>	Modifies rstp priority value.
<b>no spanning-tree rstp priority</b>	Returns rstp priority to default value.

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

The bridge priority is configured to 32768 by default.

### 2.2.3 Configuring the Forward Delay Time

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

Follow these configurations in the global configuration mode:

Command	purpose
<b>spanning-tree rstp forward-time</b> <i>value</i>	Configures Forward Delay
<b>no spanning-tree rstp forward-time</b>	Returns Forward Delay Time to default value (15s).

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

The Forward Delay Time of the bridge is 15 seconds.

### 2.2.4 Configuring the Hello Time

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

Follow these configurations in the global configuration mode:

command	purpose
<b>spanning-tree rstp hello-time</b> <i>value</i>	Configures Hello Time
<b>no spanning-tree rstp hello-time</b>	Returns Hello Time to default value.

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

Note: We recommend user to use the default value.

The default Hello Time is 2 seconds.

## 2.2.5 Configuring the Max-Age

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

Follow these configurations in the global configuration mode:

command	purpose
<b>spanning-tree rstp max-age</b> <i>value</i>	Configures the max-age value.
<b>no spanning-tree rstp max-age</b>	Returns the max-age time to default value (20s).

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

The Max Age of bridge is 20 seconds by default.

## 2.2.6 Configuring the Path Cost

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

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

command	purpose
<b>spanning-tree rstp cost</b> <i>value</i>	Configures the cost for an interface.
<b>no spanning-tree rstp cost</b>	Returns path cost to default value.

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

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

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

## 2.2.7 Configuring the Port Priority

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

Follow these configurations in the interface configuration mode:

command	purpose
<b>spanning-tree rstp port-priority</b> <i>value</i>	Configures the port priority for an interface.
<b>no spanning-tree rstp port-priority</b>	Returns the port priority to the default value.

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

The default Ethernet interface priority is 128.

## 2.2.8 Configuring edge port

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

Command	Purpose
<b>spanning-tree rstp edge</b>	Configuring port as edge port.

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

## 2.2.9 Configuring port's connection type

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

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

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

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

Command	Purpose
<b>spanning-tree rstp point-to-point</b> [ <b>force-true</b>   <b>force-false</b>   <b>auto</b> ]	Configuring point-to-point port. force-true: forcing to point-to-point type.

	<p>force-false: forcing to none point-to-point type.</p> <p>Auto: protocol automatically detects port's type.</p>
--	---

### 2.2.10 Restarting the check of protocol conversion

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

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

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

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

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

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



## Chapter 3 Configuring MTSP

### 3.1 MSTP Overview

#### 3.1.1 Introduction

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

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

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

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

#### 3.1.2 MST Domain

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

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

#### 3.1.3 IST, CST, CIST and MSTI

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

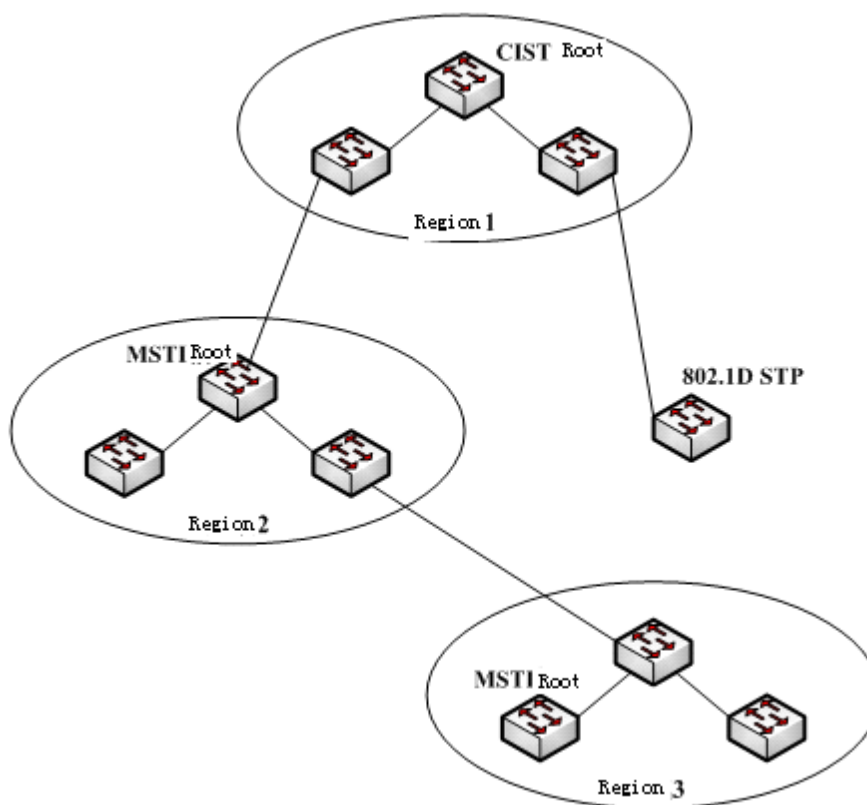


Figure 2.1 MSTP topology

### 1. CIST

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

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

### 2. CST

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

### 3. IST

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

## 4. MSTI

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

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

### 3.1.4 Port Role

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

#### 1. Root port

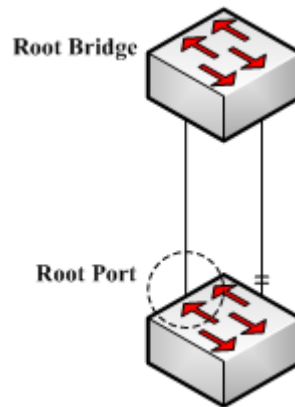


Figure 2.2 Root port

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

#### 2. Alternate port

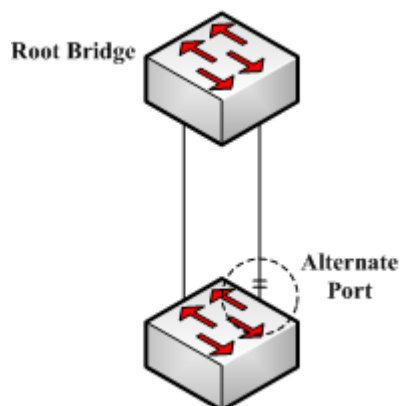


Figure 2.3 Alternate port

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

3. Designated port

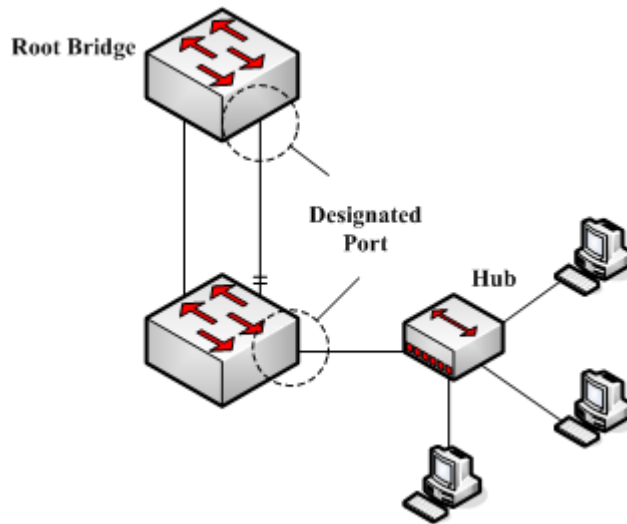


Figure 2.4 Designated port

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

4. Backup port

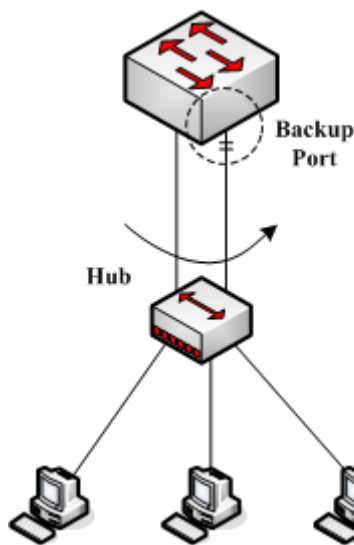


Figure 2.5 Backup port

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

## 5. Master port

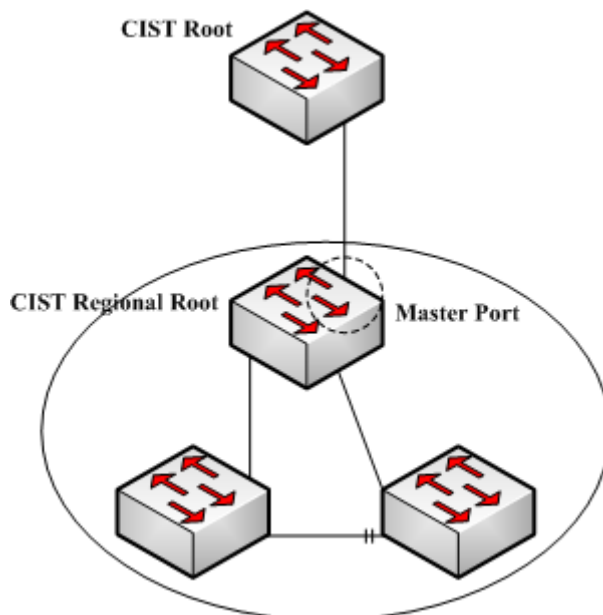


Figure 2.6 Master port

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

## 6. Boundary port

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

## 7. Edge port

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

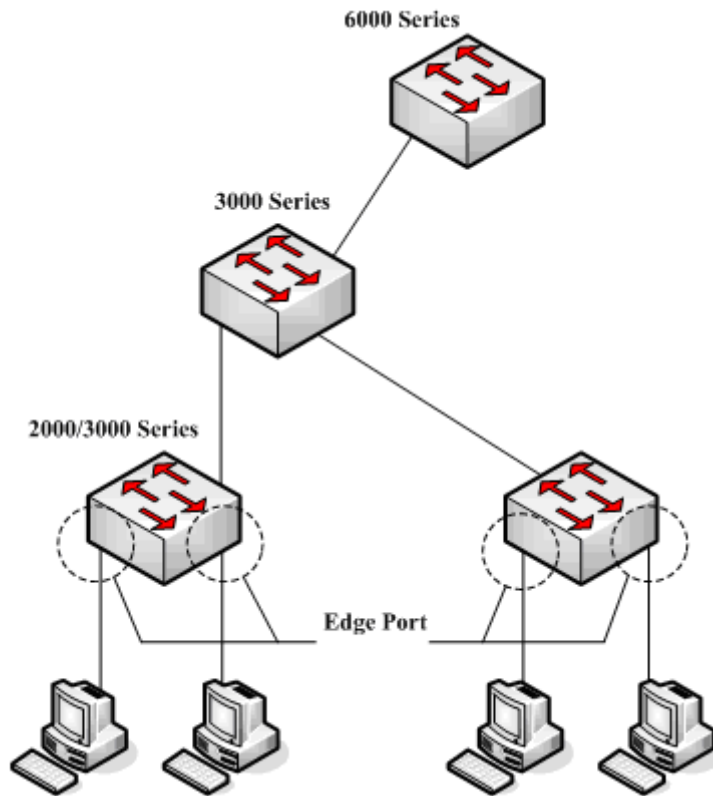


Figure 2.7 Edge port

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

### 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
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 provided its LAN with the minimum-cost path to the CIST root.
- (8) The Alternate port and the Backup port provides connection when the switch, port or the LAN does not work or is removed.
- (9) The MSTI root port provides the minimum cost path to the MSTI regional root.
- (10) The designated port of MSTI provides the minimum cost path to the MSTI regional root.
- (11) A master port provides the connection between the region and the CIST root. In the region, the CIST root port of the CIST regional root functions as the master port of all MSTI in the region.

### 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 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.

## 3.2 MSTP Configuration Task List

- Default MSTP configuration
- Enabling and disabling MSTP



- Configuring MSTP Area
- Configuring Network Root
- Configuring Secondary Root
- Configuring Bridge Priority
- Configuring STP Time Parameters
- Configuring Network Diameter
- Configuring Maximum Hop Count
- Configuring Port Priority
- Configuring Path Cost for the Port
- Configuring Edge Port
- Configuring Port Connection Type
- Activating MST-Compatible Mode
- Restarting Protocol Conversion Check
- Configuring Port's Role Restriction
- Configuring Port's TCN Restriction
- Checking MSTP Information

### 3.3 MSTP Configuration Task

#### 3.3.1 Default MSTP Configuration

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

Maximum-aging Time	20 seconds
Maximum hop count	20

### 3.3.2 Enabling and Disabling MSTP

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

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

Command	Purpose
<b>spanning-tree</b>	Enables STP in default mode.
<b>spanning-tree mode mstp</b>	Enables MSTP.

Run the following command to disable STP:

Command	Purpose
<b>no spanning-tree</b>	Disable the STP.

### 3.3.3 Configuring MST Area

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

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

Run the following command to set the MST area information:

Command	Purpose
<b>spanning-tree mstp name</b> <i>string</i>	Configures the MST configuration name.  <b>string</b> means the character string of the configuration name. It contains up to 32 characters, capital sensitive. The default value is the character string of the MAC address.
<b>no spanning-tree mstp name</b>	Sets the MST configuration name to the default value.
<b>spanning-tree mstp revision</b> <i>value</i>	Sets the MST edit number.  <b>value</b> represents the edit number, ranging from 0 to 65535. The default value is 0.
<b>no spanning-tree mstp revision</b>	Sets the MST edit number to the default value.
<b>spanning-tree mstp instance</b> <i>instance-id</i> <b>vlan</b> <i>vlan-list</i>	Maps VLAN to MSTI.  <b>instance-id</b> represents the instance number of the spanning tree, meaning an MSTI. It ranges from 1 to 15.  <b>vlan-list</b> means the VLAN list that is mapped to the

	<p>spanning tree. It ranges from 1 to 4094.</p> <p><b>instance-id</b> is an independent value representing a spanning tree instance.</p> <p><b>vlan-list</b> can represent a group of VLANs, such as "1,2,3", "1-5" and "1,2,5-10".</p>
<b>no spanning-tree mstp instance</b> <i>instance-id</i>	<p>Cancels the VLAN mapping of MSTI and disables the spanning tree instance.</p> <p><i>instance-id</i> represents the instance number of the spanning tree, meaning an MSTI. It ranges from 1 to 15.</p>

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

Command	Purpose
<b>show spanning-tree mstp region</b>	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 switch through configuration. You can run the command **Spanning-tree mstp Spanning-tree mstp instance-id rootroot** to modify the priority value of the switch in a spanning tree instance from the default value to a sufficiently small value, ensuring the switch turns to be the root in the spanning tree instance.

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

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

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

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

Command	Purpose
<b>spanning-tree mstp instance-id root primary</b> [ <b>diameter net-diameter</b> [ <b>hello-time seconds</b> ] ]	<p>Sets the switch to the root in the designated spanning tree instance.</p> <p><b>instance-id</b> represents the number of the spanning tree instance, ranging from 0 to 15.</p> <p><b>net-diameter</b> represents the network diameter, which is an</p>

	optional parameter. It is effective when <b>instance-id</b> is 0. It ranges from 2 to 7.  <b>seconds</b> represents the unit of the hello time, ranging from 1 to 10.
<b>no spanning-tree mstp instance-id root</b>	Cancels the root configuration of the switch in the spanning tree.  <b>instance-id</b> means the number of the spanning tree instance, ranging from 0 to 15.

Run the following command to check the MSTP message:

Command	Purpose
<b>show spanning-tree mstp</b> [ <b>instance instance-id</b> ]	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 the primary root configuration, after the command to configure the primary root is run, MSTP sets the spanning tree priority of the switch to **28672**. In the case that the priority value of other switches is the default value **32768**, the current switch can be the secondary root.

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

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

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

Run the following command to check the MSTP message:

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

<b>show spanning-tree mstp</b> [ <i>instance instance-id</i> ]	Check the message about the MST instance.
---	---

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

### 3.3.7 Configuring STP Time Parameters

The following are STP time parameters:

- **Hello Time:**  
The interval to send the configuration message to the designated port when the switch functions as the network root.
- **Forward Delay:**  
Time that the port needs when it changes from the **Blocking** state to the **learning** state and to the **forwarding** state in STP mode.
- **Max Age:**  
The maximum live period of the configuration information about the spanning tree.

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

- $2 \times (\text{fwd\_delay} - 1.0) \geq \text{max\_age}$
- $\text{max\_age} \geq (\text{hello\_time} + 1) \times 2$

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

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

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

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

### 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**:

Command	Purpose
<b>spanning-tree mstp diameter</b> <i>net-diameter</i>	Configure <b>net-diameter</b> . The parameter <b>net-diameter</b> ranges from 2 to 7. The default value is 7.
<b>no spanning-tree mstp diameter</b>	Resumes <b>net-diameter</b> to the default value.

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

### 3.3.9 Configuring Maximum Hop Count

Run the following command to configure the maximum hop count.

Command	Purpose
<b>spanning-tree mstp max-hops</b> <i>hop-count</i>	Set the maximum hops. <b>hop-count</b> ranges from 1 to 40. Its default value is 20.

<b>no spanning-tree mstp</b> <i>hop-count</i>	Resume the maximum hop count to the default value.
---	--

### 3.3.10 Configuring Port Priority

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

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

Command	Purpose
<b>spanning-tree mstp</b> <i>instance-id</i> <b>port-priority</b> <i>priority</i>	Sets the priority of the STP port.  <b>instance-id</b> stands for the number of the spanning tree instance, ranging from 0 to 15.  <b>priority</b> 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
<b>spanning-tree port-priority</b> <i>value</i>	Sets the port priority in all spanning tree instances.  <b>value</b> 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
<b>no spanning-tree mstp</b> <i>instance-id</i> <b>port-priority</b>	Resumes the port priority to the default value.
<b>no spanning-tree port-priority</b>	Resumes the port priority to the default value in all spanning tree instances.

### 3.3.11 Configuring Path Cost of the Port

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

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

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

<b>no spanning-tree cost</b>	Resumes the path cost of the port to the default value in all spanning tree instances.
------------------------------	--

### 3.3.12 Configuring Edge Port

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

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

### 3.3.13 Configuring Port Connection Type

If the connection between MSTP-supported switches is the point-to-point direct connection, the switches can rapidly establish connection through handshake mechanism. When you configure the port connection type, set the port connection to the point-to-point type.

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

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

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

Command	Purpose
<b>spanning-tree mstp point-to-point force-true</b>	Sets the port connection type to <b>point-to-point</b> .
<b>spanning-tree mstp point-to-point force-false</b>	Sets the port connection type to <b>shared</b> .
<b>spanning-tree mstp point-to-point auto</b>	Automatically checks the port connection type.
<b>no spanning-tree mstp point-to-point</b>	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 802.1s. In order to be compatible with other MSTPs, especially MSTP that the Cisco switches support, the MSTP protocol can work in MST-compatible mode. Switches running in MSTP-compatible mode can identify the message structure of other MSTPs, check the contained MST regional identifier and establish the MST region.

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



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

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

**Note:**

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

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

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

### 3.3.15 Restarting Protocol Conversion Check

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

**Note:**

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

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

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

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

### 3.3.16 Configuring Port's Role Restriction

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

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

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

### 3.3.17 Configuring Port's TCN Restriction

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

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

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

### 3.3.18 Checking MSTP Information

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

Command	Purpose
<b>show spanning-tree</b>	Checks MSTP information. (Information about SSTP, PVST, RSTP and MSTP can be checked)
<b>show spanning-tree detail</b>	Checks the details of MSTP information. (Information about SSTP, PVST, RSTP and MSTP can be checked)
<b>show spanning-tree interface <i>interface-id</i></b>	Checks the STP interface information. (Information about SSTP, PVST, RSTP and MSTP can be checked)
<b>show spanning-tree mstp</b>	Checks all MST instances.
<b>show spanning-tree mstp region</b>	Checks the MST area configuration.
<b>show spanning-tree mstp instance <i>instance-id</i></b>	Checks information about a MST instance.
<b>show spanning-tree mstp detail</b>	Checks detailed MST information.
<b>show spanning-tree mstp interface <i>interface-id</i></b>	Checks MST port configuration.
<b>show spanning-tree mstp protocol-migration</b>	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 .....	3
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 .....	8
1.2.4 Configuring BPDU Filter.....	9
1.2.5 Configuring Uplink Fast.....	9
1.2.6 Configuring Backbone Fast.....	10
1.2.7 Configuring Root Guard .....	10
1.2.8 Configuring Loop Guard .....	11
1.2.9 Configuring Loop Fast.....	11
1.2.10 Configuring Address Table Aging Protection .....	12
1.2.11 Configuring FDB-Flush.....	13

# Chapter 1 Configuring STP Optional Characteristic

## 1.1 STP Optional Characteristic Introduction

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

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

### 1.1.1 Port Fast

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

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

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

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

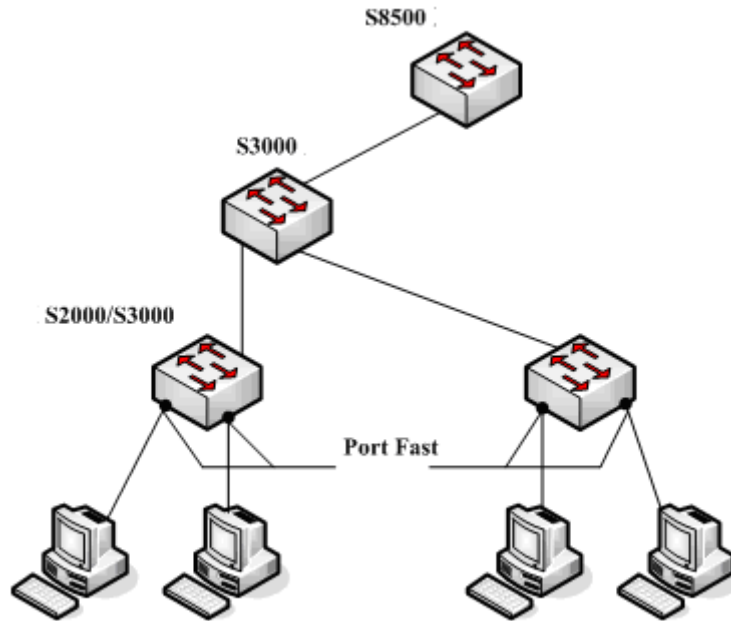


Figure 1.1 Port Fast

**Instruction:**

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

### 1.1.2 BPDU Guard

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

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

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

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

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

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

### 1.1.3 BPDU Filter

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

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

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

### 1.1.4 Uplink Fast

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

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

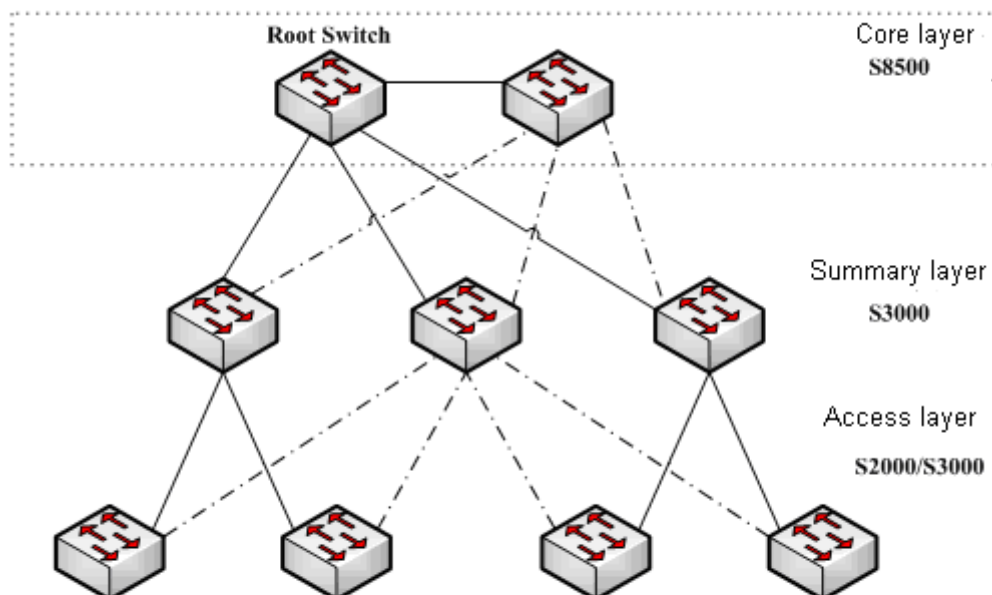


Figure 1.2 Switching network topology

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

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

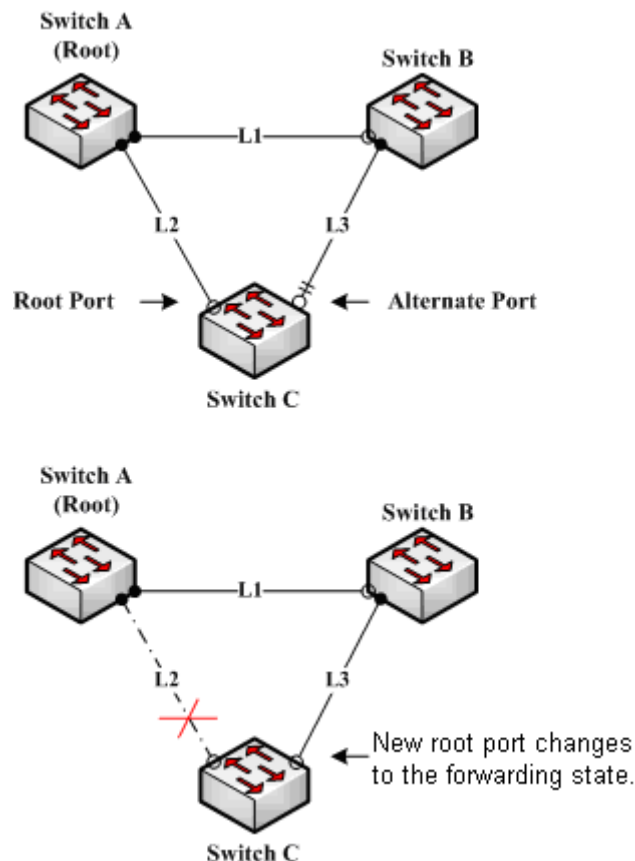


Figure 1.3 Uplink Fast

**Note:**

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

### 1.1.5 Backbone Fast

The **Backbone Fast** feature is a supplement of the **Uplink Fast** technology. The **Uplink Fast** technology makes the redundancy line rapidly work in case the direct connection to the designated switch is disconnected, while the **Backbone Fast** technology detects the indirect-link network blackout in the upper-layer network and boosts the change of the port state.



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

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

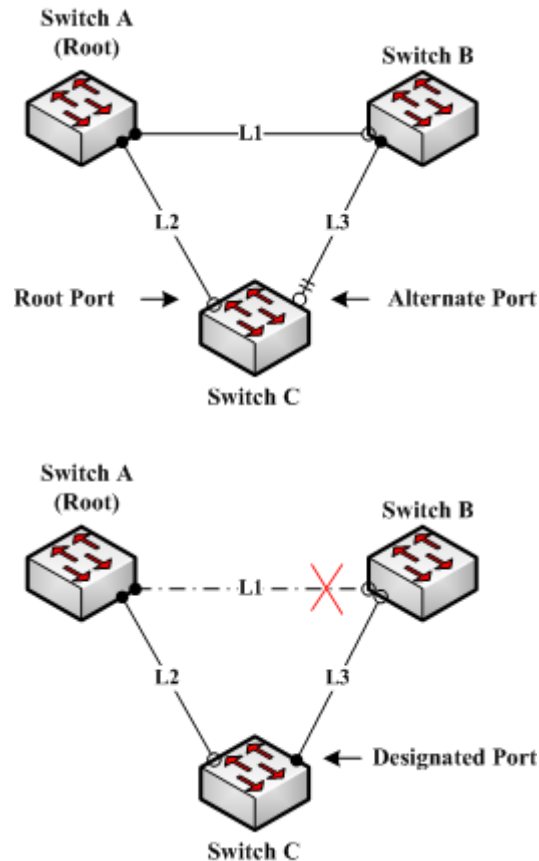


Figure 1.4 Backbone Fast

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

After the Backbone Fast function is enabled, if BPDU with low priority is received at different ports, the switch will perform different actions. If the Alternate port receives the message, the port is updated to the designated port. If the root port receives the low-priority message and there is no other standby port, the switch turns to be the root switch.

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

**Note:**

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

### 1.1.6 Root Guard

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

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

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

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

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

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

**Note:**

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

### 1.1.7 Loop Guard

You can use loop guard to prevent alternate or root ports from becoming designated ports because of a failure that leads to a unidirectional link. This feature is most effective when it is enabled on the entire switched network. Loop guard prevents alternate and root ports from becoming designated ports, and spanning tree does not send BPDUs on root or alternate ports.

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

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

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

**Note:**

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

## 1.2 Configuring STP Optional Characteristic

### 1.2.1 STP Optional Characteristic Configuration Task

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

### 1.2.2 Configuring Port Fast

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

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

command	purpose
<b>spanning-tree port fast default</b>	Globally enables port fast feature. It is valid to all interfaces.
<b>no spanning-tree portfast default</b>	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
<b>spanning-tree portfast</b>	Enables port fast feature on the interface.
<b>no spanning-tree portfast</b>	Disables port fast feature on the interface. It has no effect on the global configuration.

### 1.2.3 Configuring BPDU Guard

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

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

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

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

Follow these steps to globally enable the BPDU guard feature:

command	purpose
<b>spanning-tree portfast bpduguard</b>	Globally enables bpduguard feature. It is valid to all interfaces.
<b>no spanning-tree portfast bpduguard</b>	Globally disables bpduguard feature.

**Instruction:**

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

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

Command	Purpose
<b>spanning-tree bpduguard enable</b>	Enables bpduguard feature on the interface.

<b>spanning-tree bpduguard disable</b>	Disables bpdu guard feature on the interface. It has no effect on the global configuration.
<b>no spanning-tree bpduguard</b>	Disables bpdu guard feature on the interface. It has no effect on the global configuration.

#### 1.2.4 Configuring BPDU Filter

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

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

Command	Purpose
<b>spanning-tree portfast bpdupfilter</b>	Globally enables bpdu filter feature. It is valid to all interfaces.
<b>no spanning-tree portfast bpdupfilter</b>	Globally disables bpdu filter feature.

##### Instruction:

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

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

Command	Purpose
<b>spanning-tree bpdupfilter enable</b>	Enables bpdu filter feature on the interface.
<b>spanning-tree bpdupfilter disable</b>	Disables bpdu filter feature. It has no effect on the global configuration.
<b>no spanning-tree bpdupfilter</b>	Disables bpdu filter feature. It has no influence on the global configuration.

#### 1.2.5 Configuring Uplink Fast

If a switch loses connectivity, it begins using the alternate paths as soon as the spanning tree selects a new root port. By enabling UplinkFast with the spanning-tree uplinkfast global configuration command, you can accelerate the choice of a new root port when a link or switch fails or when the spanning tree reconfigures itself. The root port transitions to the forwarding state immediately without going through the listening and learning states, as it would with the normal spanning-tree procedures.

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

Follow these steps to globally enable UplinkFast.:

Command	Purpose
<b>spanning-tree uplinkfast</b>	Enables uplink fast feature.
<b>no spanning-tree uplinkfast</b>	Disables uplink fast feature.

## 1.2.6 Configuring Backbone Fast

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

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

Follow these steps to globally enable BackboneFast.:

Command	Purpose
<b>spanning-tree backbonefast</b>	Enables backbone fast feature.
<b>no spanning-tree backbonefast</b>	Disables backbone fast feature.

## 1.2.7 Configuring Root Guard

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

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

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

Command	Purpose
<b>spanning-tree guard root</b>	Enables root guard feature on the interface.
<b>no spanning-tree guard</b>	Disables root guard and loop guard features on the interface.
<b>spanning-tree guard none</b>	Disables root guard and loop guard features on the interface.

## 1.2.8 Configuring Loop Guard

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

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

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

Command	Purpose
<b>spanning-tree loopguard default</b>	Globally enables loop guard feature. It is valid to all interfaces.
<b>no spanning-tree loopguard default</b>	Globally disables loop guard.

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

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

## 1.2.9 Configuring Loop Fast

Notice:

Please use this chapter's configuration command under OUR technical engineer's instruction.

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

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

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

	configuration mode
--	--------------------

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

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

### 1.2.10 Configuring Address Table Aging Protection

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

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

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

#### Notice:

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

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

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

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



### 1.2.11 Configuring FDB-Flush

---

Notice:

Please use this chapter's configuration command under OUR technical engineer's instruction.

---

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

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

Command	Purpose
<b>spanning-tree fast-aging flush-fdb</b>	Enabling FDB-Flush
<b>no spanning-tree fast-aging flush-fdb</b>	Disabling FDB-Flush

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

## Layer-2 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 to Aggregation..... 1
    - 1.3.2 Aggregation of Physical Port ..... 2
    - 1.3.3 Selecting Load Balance Method After Port Aggregation ..... 2
    - 1.3.4 Monitoring the Concrete Conditions of Port Aggregation ..... 3

# Chapter 1 Configuring Port Aggregation

## 1.1 Overview

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

Supported Features:

- Static aggregation control is supported  
Bind a physical port to a logical port, regardless whether they can actually bind to a logical port.  
Aggregation control of LACP dynamic negotiation is supported  
Only a physical port that passes the LACP protocol negotiation can bind to a logical port. Other ports won't bind to the logical port.
- Aggregation control of LACP dynamic negotiation is supported  
When a physical port is configured to bind to a logical port, the physical port with LACP negotiation can be bound to a logical port. Other ports cannot be bound to the logical port.
- Flow balance of port aggregation is supported.  
After port aggregation, the data flow of the aggregation port will be distributed to each aggregated physical port.

## 1.2 Port Aggregation Configuration Task

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

## 1.3 Port Aggregation Configuration Task

### 1.3.1 Configuring Logical Channel Used to Aggregation

You should establish a logical port before binding all the physical ports together. The logical port is used to control the channel formed by these binding physical ports.

Use the following command to configure the logical channel:

Command	Description
<code>interface port-aggregator id</code>	Configures aggregated logical channel.

### 1.3.2 Aggregation of Physical Port

To aggregate multiple physical ports into a logical channel, you can use static aggregation or LACP protocol for negotiation.

In the case when the static aggregation is used, it is required that the link of the physical port should be up, and the VLAN attribute of aggregation port and physical port should be identical, and then this port will be aggregated to the logical channel, regardless of whether the current port accords with the conditions of port aggregation and whether the port that connects with the physical port accords with the aggregation conditions.

Prerequisites for ports to be aggregated:

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

LACP packets are exchanged between ports in these modes:

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

If both ports use Passive method, then the aggregation fails. This is because both sides will wait for the other side to launch aggregation negotiation process.

VLAN attributes: PVID, Trunk attribute, vlan-allowed range and vlan-untagged range.

Use the following command to perform aggregation on the physical ports:

Command	Description
<code>aggregator-group <i>agg-id</i> mode { lacp   static }</code>	Configures aggregation option of the physical port.

### 1.3.3 Selecting Load Balance Method After Port Aggregation

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

- src-mac

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

- **dst-mac**

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

- **both-mac**

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

- **src-ip**

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

- **dst-ip**

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

- **both-ip**

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

- **src-port**

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

Use the following command to configure load balance method:

Command	Description
<b>aggregator-group load-balance</b>	Configures load balance method.

### 1.3.4 Monitoring the Concrete Conditions of Port Aggregation

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

Command	Description
<b>show aggregator-group [id] {detail brief summary}</b>	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

Function	Default Settings
Global configuration mode	This function is not enabled by default.
Interface configuration mode	Starts up.
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

To set the PDP packet transmission frequency and the PDP information storage time, you can run the following commands in global configuration mode.

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

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 LLDP Overview .....	1
1.1 LLDP Overview.....	1
1.1.1 Initializing the Protocol .....	1
1.1.2 Initializing LLDP Transmit Mode.....	2
1.1.3 Initializing LLDP Receive 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/enabling LLDP.....	4
1.3.2 Configuring Holdtime.....	4
1.3.3 Configuring Timer.....	4
1.3.4 Configuring Reinit.....	5
1.3.5 Configuring the To-Be-Sent TLV.....	5
1.3.6 Specifying the Port's Configuration and Selecting the To-Be-Sent Expanded TLV .....	6
1.3.7 Configuring the Transmission or Reception Mode .....	8
1.3.8 Specifying the Management IP Address of a Port.....	8
1.3.9 Sending Trap Notification to mib Database .....	9
1.3.10 Configuring the Location Information .....	9
1.3.11 Specifying a Port to Set the Location Information .....	11
1.3.12 Configuring Show-Relative Commands .....	12
1.3.13 Configuring the Deletion Commands .....	12
1.4 Configuration Examples .....	12
1.4.1 Network Environment Requirements .....	12
1.4.2 Network Topology.....	13
1.4.3 Configuration Steps.....	13

# Chapter 1 LLDP Overview

## 1.1 LLDP Overview

The link layer discovery protocol (LLDP) at 802.1AB helps to detect network troubles easily and maintain the network topology. 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.

LLDP is a useful management tool, providing management personnel exact network mapping, traffic data and trouble detection information.

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

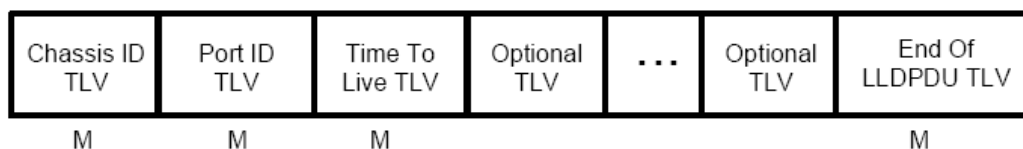
Set LLDP to **transmit-only** in the interface mode. In transmit-only mode, the interface transmits LLDP packets when the state or value of one or more information elements (management object) of the local system change or the transmission timer is timeout. The interface will not transmit LLDP packets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

### 1.1.3 Initializing LLDP Receive Mode

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

### 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

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

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

## 1.2 LLDP Configuration Task List

- Disabling/enabling LLDP
- Configuring Holdtime
  - 错误! 书签自引用无效。imer
- imer
- Configuring Reinit
- Configuring the To-Be-Sent TLV
- Specifying the Port's Configuration and Selecting the To-Be-Sent Expanded TLV
- Configuring the Transmission or Reception Mode
- Specifying the Management IP Address of a Port
- Sending Trap Notification to mib Database



- Configuring the Location Information
- Specifying a Port to Set the Location Information
- Configuring Show-Relative Commands
- Configuring the Deletion Commands

## 1.3 LLDP Configuration Tasks

### 1.3.1 Disabling/enabling LLDP

LLDP is disabled by default. You need start up LLDP before it runs.

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

Command	Purpose
<b>lldp run</b>	Runs LLDP.

Run the following command to disable LLDP:

Command	Purpose
<b>no lldp run</b>	Disables LLDP.

### 1.3.2 Configuring Holdtime

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:

Command	Purpose
<b>lldp holdtime <i>time</i></b>	Configures the timeout time of LLDP.
<b>no lldp holdtime</b>	Resumes the timeout time to the default value, 120 seconds.

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

### 1.3.3 错误！书签自引用无效。imer

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:

Command	Purpose
<b>lldp timer</b> <i>time</i>	Configures the interval of message transmission of LLDP. The value ranges from 5 to 65534. The default time is 30 seconds.
<b>no lldp timer</b>	Resumes the default interval, that is, 30 seconds.

### 1.3.4 Configuring Reinit

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:

Command	Purpose
<b>lldp reinit</b> <i>time</i>	Configures the interval of LLDP to continuously transmit message.
<b>no lldp reinit</b>	Resumes the default interval of continuously transmitting message. The value ranges from 2 to 5. The default interval value is two seconds.

### 1.3.5 Configuring the To-Be-Sent TLV

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

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

Step	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	lldp tlv-select management-address	Optional. Transmits the management address tlv. The management address is usually layer-3 IP address which should be easy to use.
Step3	lldp tlv-select port-description	Optional. Transmits the port description tlv. The port description uses number or letters for description.
Step4	lldp tlv-select system-capabilities	Optional. Transmits the system performance tlv. The system performance refers to the system of transmitting packets such as the switch or router.
Step5	lldp tlv-select system-description	Optional. Transmits system description tlv. The system description is consist of texts including numbers and letters. The system description should include the full name of the system, the hardware version, the software system and the network software.
Step6	lldp tlv-select system-name	Optional. Transmits system name tlv. The name of the system should be the name of the system manager, i.e. the name of the switch.

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

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

### 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:

Step	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	interface intf-type intf-id	Enters the interface configuration mode.
Step3	lldp dot1-tlv-select port-vlan-id	Optional. Sends the 802.1-defined TLV and notifies the PVID of a port.
Step4	lldp dot1-tlv-select protocol-vlan-id	Optional. Sends the 802.1-defined TLV and notifies the PPVID of a port.
Step5	lldp dot1-tlv-select vlan-name	Optional. Sends the 802.1-defined TLV and notifies the VLAN name of a port.
Step6	lldp dot3-tlv-select macphy-config	Optional. Sends the 802.3-defined TLV: a) The bit rate and the communication mode (duplex) on the physical layer; b) Current duplex and the set bit rate; c) Showing whether the setting is the results of auto-negotiation in the initial connection phase or is a compulsory manual behavior;

## LLDP Configuration

Step7	lldp dot3-tlv-select power	Optional. Sends the 802.3-defined TLV and shows the interface allows the power supply connecting to the non-power system through the link.
Step8	lldp dot3-tlv-select link-aggregation	Optional. Sends the 802.3-defined TLV and specifies a port to identify the aggregation if the link can be aggregated.
Step9	lldp dot3-tlv-select max-frame-size	Optional. Sends the 802.3-defined TLV and specifies the size of the maximum frame on a port.
Step10	lldp med-tlv-select network-policy	Optional. Sends the MED-defined TLV and the interface can effectively discover and diagnose VLAN configured error-matching flow and the attribute of layer-2 and layer-3.
Step11	lldp med-tlv-select location	Optional. Sends the MED-defined TLV and specifies the address: a) coordinate-based LCI, which is defined in IETF 3825[6]; b) city's address LCI, which is defined in IETF (refer to Annex B); c) ELIN code of the urgency call service;
Step12	lldp med-tlv-select power-management	Optional. Sends the MED-defined TLV and shows the information of power supply.
Step13	lldp med-tlv-select inventory	Optional. Sends the MED-defined TLV and shows the attribute of detailed inventory.

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

Step	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	interface intf-type intf-id	Enters the interface configuration mode.
Step3	no lldp dot1-tlv-select port-vlan-id	Optional. Sends the 802.1-defined TLV and notifies the PVID of a port.
Step4	no lldp dot1-tlv-select protocol-vlan-id	Optional. Sends the 802.1-defined TLV and notifies the PPVID of a port.
Step5	no lldp dot1-tlv-select vlan-name	Optional. Sends the 802.1-defined TLV and notifies the vlan name of a port.
Step6	no lldp dot3-tlv-select macphy-config	Optional. Sends the 802.3-defined TLV: a) The bit rate and the communication mode (duplex) on the physical layer; b) Current duplex and the set bit rate; c) Showing whether the setting is the results of auto-negotiation in the initial connection phase or is a compulsory manual behavior;
Step7	no lldp dot3-tlv-select power	Optional. Sends the 802.3-defined TLV and shows the interface allows the power supply connecting to the non-power system through the link.

Step8	no lldp dot3-tlv-select link-aggregation	Optional. Sends the 802.3-defined TLV and specifies a port to identify the aggregation if the link can be aggregated.
Step9	no lldp dot3-tlv-select max-frame-size	Optional. Sends the 802.3-defined TLV and specifies the size of the maximum frame on a port.
Step10	no lldp med-tlv-select network-policy	Optional. Sends the MED-defined TLV and the interface can effectively discover and diagnose VLAN configured error-matching flow and the attribute of layer-2 and layer-3.
Step11	no lldp med-tlv-select location	Optional. Sends the MED-defined TLV and specifies the address: a) coordinate-based LCI, which is defined in IETF 3825[6]; b) city's address LCI, which is defined in IETF (refer to Annex B); c) ELIN code of the urgency call service;
Step12	no lldp med-tlv-select power-management	Optional. Sends the MED-defined TLV and shows the information of power supply.
Step13	no lldp med-tlv-select inventory	Optional. Sends the MED-defined TLV and shows the attribute of detailed inventory.

### 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.

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

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

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

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

### 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:

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

Note: Both the no lldp 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

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

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

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

### 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:

Step	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	location elin identifier id WORD	Sets the location elin information, in which id is the elin identifier number and WORD stands for the elin information, which ranges from 10 to 25 bytes.
Step3	location civic identifier id	Enters the location configuration mode.
Step4	language WORD	Sets the language

## LLDP Configuration

Step5	state WORD	Sets the state's (provincial) name, such as shanghai.
Step6	county WORD	Sets the name of a county.
Step7	city WORD	Sets the name of a city.
Step8	division WORD	Sets the name of a division.
Step9	neighborhood WORD	Sets the name of neighborhood.
Step10	street WORD	Sets the name of a street.
Step11	leading-street-dir WORD	Sets the direction of a main street, such as N (north).
Step12	trailing-street-suffix WORD	Sets the suffix of a small street, such as SW.
Step13	street-suffix WORD	Sets the suffix of a street, such as platz.
Step14	number WORD	Sets the street number, such as number 123.
Step15	street-number-suffix WORD	Sets the suffix of the street number, such as number 1/2 of A road.
Step16	landmark WORD	Sets the landmark, such as Colombia University.
Step17	additional-location WORD	Sets the additional location.
Step18	name WORD	Sets the information about a resident, such as Joe's haircut shop.
Step19	postal-code WORD	Sets the postal code.
Step20	building WORD	Sets the information about a building.
Step21	unit WORD	Sets the information about a unit.
Step22	floor WORD	Sets the information about a floor.
Step23	room WORD	Sets the information about a room.
Step24	type-of-place WORD	Sets the type of a place, such as office.
Step25	postal-community WORD	Sets the name of a postal office.
Step26	post-office-box WORD	Sets the name of a postal box, such as 12345.
Step27	additional-code WORD	Sets the additional code.
Step28	country WORD	Sets the name of a country.
Step29	script WORD	Sets the script.

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

Step	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	no location elin identifier id	Deletes the location elin information of elin identifier.
Step3	no location civic identifier id	Deletes the location elin 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.

## LLDP Configuration

Step7	no county	Deletes the name of a county.
Step8	no city	Deletes the name of a city.
Step9	no division	Deletes the name of a division.
Step10	no neighborhood	Deletes the name of neighborhood.
Step11	no street	Deletes the name of a street.
Step12	no leading-street-dir	Deletes the direction of a main street, such as N (north).
Step13	no trailing-street-suffix	Deletes the suffix of a small street, such as SW.
Step14	no street-suffix	Deletes the suffix of a street, such as platz.
Step15	no number	Deletes the street number, such as number 123.
Step16	no street-number-suffix	Deletes the suffix of the street number, such as number 1/2 of A road.
Step17	no landmark	Deletes the landmark, such as Colombia University.
Step18	no additional-location	Deletes the additional location.
Step19	no name	Deletes the information about a resident, such as Joe's haircut shop.
Step20	no postal-code	Deletes the name of a postal office.
Step21	no building	Deletes the information about a building.
Step22	no unit	Deletes the information about a unit.
Step23	no floor	Deletes the information about a floor.
Step24	no room	Deletes the information about a room.
Step25	no type-of-place	Deletes the type of a place, such as office.
Step26	no postal-community	Deletes the name of a postal office.
Step27	no post-office-box	Deletes the name of a postal box, such as 12345.
Step28	no additional-code	Deletes the additional code.
Step29	no country	Deletes the name of a country.
Step30	no script	Deletes the script.

### 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:

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



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

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

### 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
<b>Show lldp errors</b>	Displays the error information about the LLDP module.
<b>Show lldp interface</b> <i>interface-name</i>	Displays the information about port state, that is, the transmission mode and the reception mode.
<b>Show lldp neighbors</b>	Displays the abstract information about the neighbor.
<b>Show lldp neighbors detail</b>	Displays the detailed information about the neighbor.
<b>Show lldp traffic</b>	Displays all received and transmitted statistics information.
<b>Show location elin</b>	Displays the information of location elin.
<b>Show location civic</b>	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 in EXEC mode.

Run the following commands in EXEC mode:

Command	Purpose
<b>clear lldp counters</b>	Deletes all statistics data.
<b>clear lldp table</b>	Deletes all received neighbor information.

## 1.4 Configuration Examples

### 1.4.1 Network Environment Requirements

Configure LLDP protocol on the port connecting two switches.

## 1.4.2 Network Topology

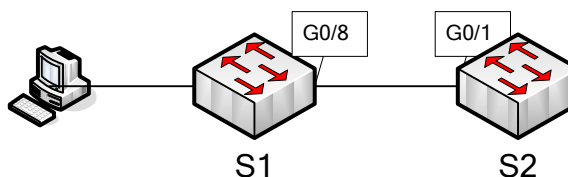


Figure 2 Network Topology

## 1.4.3 Configuration Steps

### 1. Basic Configuration

Configuring switch S1:

```
Switch_config#lldp run
```

```
Switch_config#
```

Configuring switch S2:

```
Switch_config#lldp run
```

```
Switch_config#
```

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

S1:

```
Switch_config#show lldp neighbors
```

Capability Codes:

(R)Router,(B)Bridge,(C)DOCSIS Cable Device,(T)Telephone

(W)WLAN Access Point, (P)Repeater,(S)Station,(O)Other

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

Total entries displayed: 1

```
Switch_config#show lldp neighbors detail
```

chassis id: 00e0.0fac.32ff

port id: Gig0/1

port description: GigaEthernet0/1

system name: Switch

system description: COM(tm) SWITCH Software, Version 4.1.0B

Serial: S24090103

Copyright by COM.

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.

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: COM(tm) SWITCH Software, Version 4.1.0B

Serial: S24090103

Copyright by COM.

Compiled: 2011-9-21 9:24:8 by WRL

Time remaining: 95

system capabilities: R B

enabled capabilities: B

Management Address:

IP: 90.0.0.21

Port VLAN ID -- not advertised

PPVID: 1

VLAN 1 name: Default

Auto Negotiation: supported,enabled

Physical media capabilities:

1000baseX(FD)

1000baseX(HD)

100baseTX(FD)

100baseTX(HD)

Operational MAU type: 2 pair category 5 UTP, full duplex mode(16)

Power Via MDI:

MDI power support --

PSE MDI power support: support

Port class: PSE

PSE MDI power state: enabled

PSE pairs selection control ability: can not be controlled

PSE power pair: signal

Power Classification: Class 0

Link Aggregation:

Aggregation capability: capable of being aggregated

Aggregation status: not currently in aggregation

-----

Total entries displayed: 1

### 3. Location Configuration

Configuring switch S1:

```
Switch_config#lldp run
```

```
Switch_config#
```

Configuring switch S2:

```
Switch_config#lldp run
```

```
Switch_config#location elin identifier 1 1234567890 //Configure elin
information
```

```
Switch_config#location civic identifier 1 //Enter location 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 civic 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 civic // Display civic
configuration information
```

```
civic address information:
```

```
identifier: 1
```

```
City: Shanghai
```

```
Language: English
```

Script: EN

Street: Curie

-----

total: 1

Switch\_config\_g0/8#

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

S1:

Switch\_config#show lldp neighbors

Capability Codes:

(R)Router,(B)Bridge,(C)DOCSIS Cable Device,(T)Telephone

(W)WLAN Access Point, (P)Repeater,(S)Station,(O)Other

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

Total entries displayed: 1

Switch\_config#show lldp neighbors detail

chassis id: 00e0.0fac.32ff

port id: Gig0/1

port description: GigaEthernet0/1

system name: Switch

system description: COM(tm) SWITCH Software, Version 4.1.0B

Serial: S24090103

Copyright by COM.

Compiled: 2011-9-21 9:24:8 by WRL

Time remaining: 109



system capabilities: R B

enabled capabilities: B

Management Address:

IP: 90.0.0.21

Port VLAN ID: 1

Auto Negotiation: supported,enabled

Physical media capabilities:

1000baseX(FD)

1000baseX(HD)

100baseTX(FD)

100baseTX(HD)

Operational MAU type: 2 pair category 5 UTP, full duplex mode(16)

Power Via MDI:

MDI power support --

PSE MDI power support: support

Port class: PSE

PSE MDI power state: enabled

PSE pairs selection control ability: can not be controlled

PSE power pair: signal

Power Classification: Class 0

MED Information:

MED Codes:

(CA)Capabilities, (NP)Network Policy, (LI)Location Identification

(PS)Power via MDI ~CPSE, (PD)Power via MDI ~CPD, (IN)Inventory

Hardware Revision: 0.4.0

Software Revision: 4.1.0B

Serial Number: S24090103

Manufacturer Name: COM

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

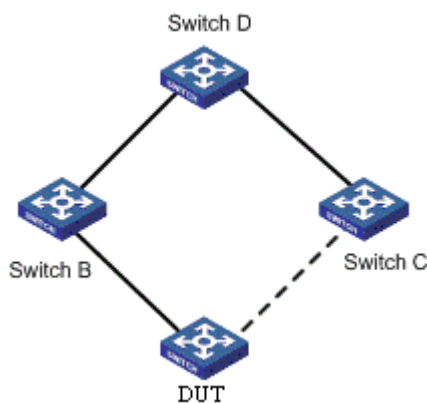
## Table of Contents

Chapter 1 Introduction of Backup Link.....	1
1.1 Overview .....	1
1.2 BackupLink Port Backup .....	1
1.2.1 Configuring 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 .....	2
1.2.6 Delay Preemption.....	3
1.3 VLAN Load Balancing .....	3
1.3.1 Configuration of Load balancing .....	3
1.3.2 Port status Control in Traffic Sharing.....	3
1.4 MAC Address Aging Operation.....	4
1.4.1 Normal Work Mechanism of the Link .....	5
1.4.2 Downlink Fault Handling Mechanism .....	5
1.4.3 Uplink Fault Handling Mechanism.....	6
1.4.4 Link Recovery Processing Mechanism .....	8
Chapter 2 BackupLink Configuration.....	9
2.1 Guidance Notes for BackupLink Configuration .....	9
2.2 BackupLink Configuration Tasks .....	9
2.3 BackupLink Configuration .....	9
2.3.1 Configuring BackupLink Group .....	9
2.3.2 Configuring the Preemption Feature for BackupLink Group .....	10
2.3.3 Configuring Load Balancing for VLAN .....	10
2.3.4 Configuring the MMU Feature for BackupLink Group .....	11
2.3.5 Configuring MonitorLink Group .....	11

# 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 Configuring Backup Port

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

---

Note:

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

## 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 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 VLAN Load Balancing

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

### 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. But for the overlapping VLAN segments, the system will assign them to different MSTs (STG); therefore, when the port of some group is operated, its states in all MSTs (STG) will take change. So, typically, when the load balancing VLAN group is configured, it is better to select the VLAN group without overlapping.

---

### 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:



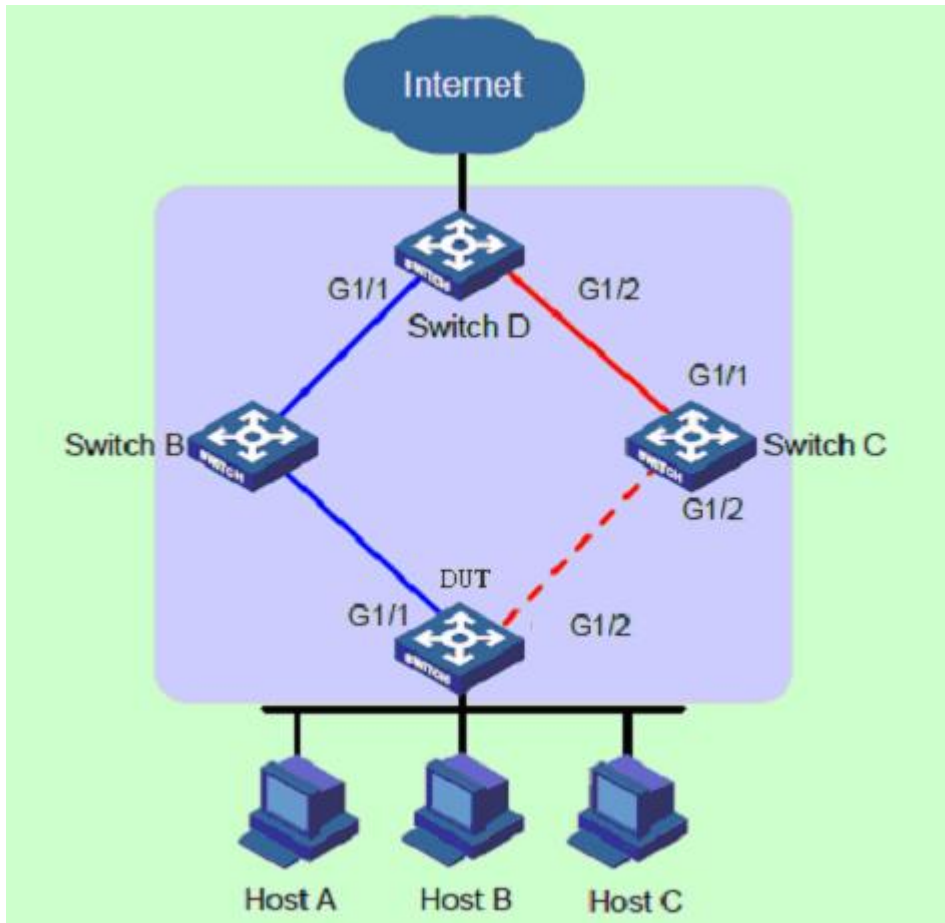


Diagram of BackupLink Address Aging Mechanism

#### 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 “GigaEthernet1/ 1” is switched to the standby state, the secondary port “GigaEthernet1/ 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 GigaEthernet1/ 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 "GigaEthernet1/ 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 "GigaEthernet1/ 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 "GigaEthernet1/ 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; GigaEthernet1/ 1 is the primary port; GigaEthernet1/ 2 is the secondary port. When the primary link where the port "GigaEthernet1/ 1" is faulty, the traffic is switched to the the secondary link where the port "GigaEthernet1/ 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 "GigaEthernet1/ 1" of Switch B is 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.

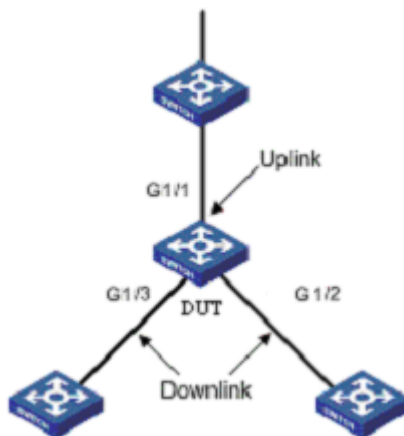


Diagram of MonitorLink Group Concepts Introduction

As is shown above, three ports of DUT (GigaEthernet1/ 1, GigaEthernet1/ 2 and GigaEthernet1 / 3) form a MonitorLink group.

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

“Downlink Port” is a monitor in MonitorLink group, which is another port role of the MonitorLink group specified through the command line. The downlink port of MonitorLink group can be an Ethernet port (electrical or optical), or aggregate interface. As is shown in the above figure, two ports of the DUT, GigaEthernet1/2 and GigaEthernet 3/ 1, 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. GigaEthernet1/ 1 as the primary port is in the forwarding state; GigaEthernet1/ 2 is the secondary port.

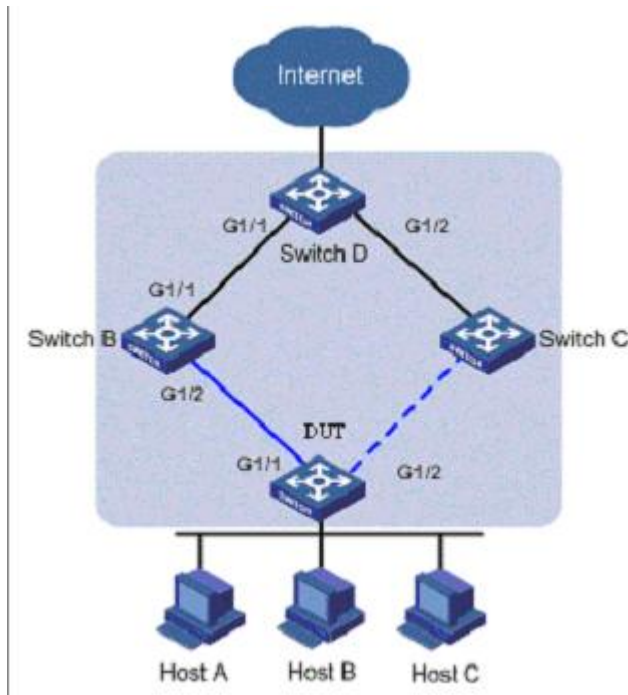


Diagram of MonitorLink operating mechanism

In order to prevent the phenomenon that DUT traffic cannot uplink because of the failure of the link where the port of Switch B, “GigaEthernet 1/ 1”, is, MonitorLink group is configured on Switch B, and the port “GigaEthernet1/ 1” is specified as the uplink port and “GigaEthernet1/ 2” is specified as downlink port.

When the link where the uplink port of Switch B, GigaEthernet1/ 1, is fails, MonitorLink group will forcibly shut down this group's downlink port “GigaEthernet1/ 2”, triggering the link switch of BackupLink group on the DUT.

When the link where the uplink port of Switch B, GigaEthernet1/ 1, is recovers from the failure, the downlink port “GigaEthernet1/ 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. 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 Notes for BackupLink Configuration

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

- Primary port (Ethernet port or aggregate port) can be configured with a BackupLink backup port; moreover, this backup port and primary port cannot be the same port;
- A port can only belong to one BackupLink group; a backup port can only taken as the backup port of one primary port; one primary port can not belong to other BackupLink groups;
- Any port within the BackupLink group cannot be a member of the aggregate ports. Aggregate port and physical port, physical port and physical ports, aggregate port and aggregate port can become the members of BackupLink group.
- BackupLink primary port and backup port may be different in type; they may be Fast Ethernet ports, Gigabit ports or aggregate ports, but both must have similar features. Thus, When the primary port fails, the backup port can forward its data traffic in similar way;
- VLAN load balancing and BackupLink preemption functions cannot be used simultaneously.

### 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 BackupLink Group

Configure BackupLink group according to the following steps.

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

**Note:**

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

**Note:**

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

### 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# <b>config</b>	Enter switch configuration mode.
Switch_config# <b>backup-link-group</b> <i>id</i> { <b>preemption-mode</b> [ <b>forced</b>   <b>bandwidth</b> ] { <b>delay</b> <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
Switch# <b>config</b>	Enter switch configuration mode.
Switch_config# <b>interface</b> <i>interface-type interface-number</i>	Enter port configuration mode
Switch_config_g1/2# <b>share-load vlan</b> <i>vlanmap</i>	Configure load balancing for VLAN. <i>vlanmap</i> : vlan value
Switch_config_g1/2# <b>exit</b>	Exit from the port configuration mode.
Switch_config#	

Note:

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

**Note:**

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

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

**Note:**

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

### 2.3.5 Configuring MonitorLink Group

Configure MonitorLink group according to the following steps.

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

---

**Note:**

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

---

---

**Note:**

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

---



# EAPS 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 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

MY COMPANY 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.

Remark:

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

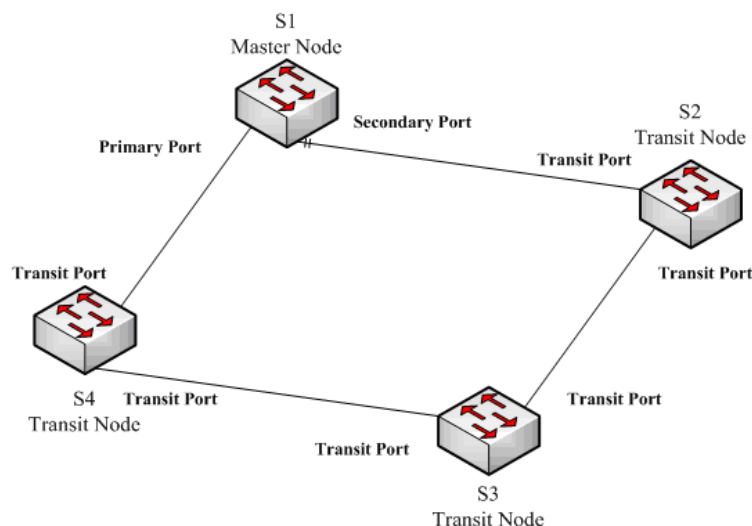


Figure 1.1 EAPS Ethernet ring

### 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.

---

**Remark:**

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.

The VLANs except the control VLAN are all data VLANs, which are used to transmit the packets of normal services or the management packets.

**Note:**

The data VLAN can be used for normal L2/L3 communication. For example, you can establish a VLAN port corresponding to data VLAN and configure dynamic routing protocols.

### 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	Remarks
Loopback detection (HEALTH)	It is transmitted by the master node to detect whether the topology of the ring network is complete.
LINK-DOWN	Indicates that link interruption happens in the ring. This kinds of packets are transmitted by the transit node.
RING-DOWN-FLUSH-FDB	It is transmitted by the master node after interruption of the ring network is detected and the packets show the MAC address aging table of the transit node.

RING-UP-FLUSH-FDB	It is transmitted by the master node after interruption of the ring network is resumed and the packets show the MAC address aging table of the transit node.
-------------------	--

## 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 bpdu-terminal** to keep the ring node from forwarding BPDU, which leads to the storm.

See the following table:

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

Spanning tree protocol	<b>spanning-tree mode rstp</b>
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. 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 MY COMPANYswitch 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# <b>config</b>	Enters the switch configuration mode.
Switch_config# <b>ether-ring id</b>	Sets a node and enters the node configuration mode. id: Instance ID
Switch_config_ring# <b>control-vlan vlan-id</b>	Configures the control VLAN. Vlan-id: ID of the control VLAN
Switch_config_ring# <b>master-node</b>	Configures the node type to be a master node.
Switch_config_ring# <b>hello-time value</b>	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# <b>fail-time value</b>	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# <b>exit</b>	Saves the current settings and exits the node

	configuration mode.
--	---------------------

**Remark:**

The **no ether-ring id** command is used to delete the node settings and port settings of the Ethernet ring.

## 2.4.2 Configuring the Transit Node

Configure a switch to be the transit node of a ring network according to the following steps:

Command	Purpose
Switch# <b>config</b>	Enters the switch configuration mode.
Switch_config# <b>ether-ring id</b>	Sets a node and enters the node configuration mode.  id: Instance ID
Switch_config_ring# <b>control-vlan vlan-id</b>	Configures the control VLAN.  Vlan-id: ID of the control VLAN
Switch_config_ring# <b>transit-node</b>	Configures the node type to be a transit node.
Switch_config_ring# <b>pre-forward-time value</b>	This step is optional. Configures the time of maintaining the pre-forward state on the transit port.  Value: It is a time value ranging from 3 to 30 seconds and the default value is 3 second.
Switch_config_ring# <b>exit</b>	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# <b>config</b>	Enters the switch configuration mode.
Switch_config# <b>interface intf-name</b>	Enters the interface configuration mode.  intf-name: Stands for the name of an interface.
Switch_config_intf# <b>ether-ring id {primary-port   secondary-port   transit-port }</b>	Configures the type of the port of Ethernet ring.  ID of the node of Ethernet ring
Switch_config_intf# <b>exit</b>	Exits from interface configuration mode.

**Remark:**

The **no ether-ring id primary-port { secondary-port | transit-port }** command can be used to cancel the port settings of Ethernet ring.

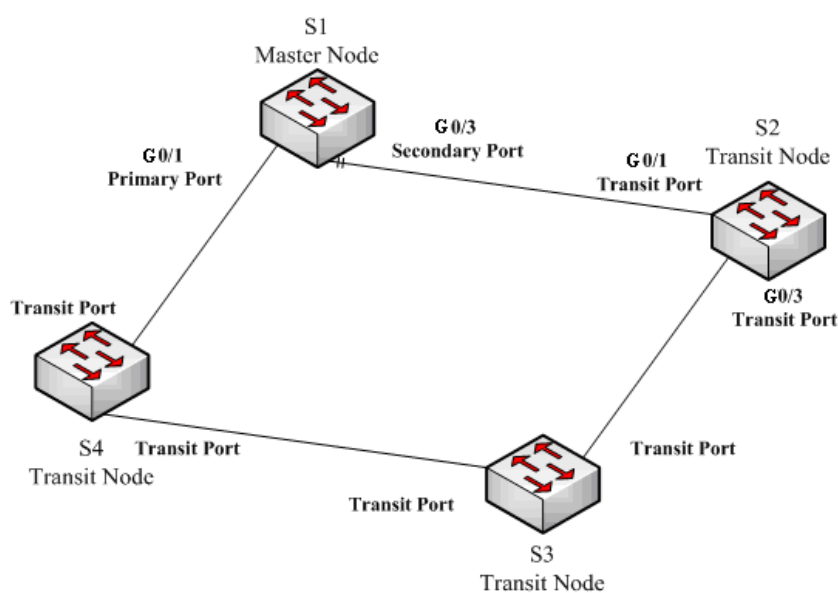
## 2.4.4 Browsing the State of the Ring Protection Protocol

Run the following command to browse the state of the ring protection protocol:

Command	Purpose
<b>show ether-ring <i>id</i></b>	Browes the summary information about the ring protection protocol and the port of Ethernet ring.  id: ID of Ethernet ring
<b>show ether-ring <i>id</i> detail</b>	Browes the detailed information about the ring protection protocol and the port of Ethernet ring.
<b>show ether-ring <i>id</i> interface <i>intf-name</i></b>	Browes the state of the Ether-ring port or that of the common port.

## 2.5 MEAPS configuration

### 2.5.1 Configuration Example



MEAPS configuration

As shown in figure 2.1, master node S1 and transit node S2 are configured as follows. As to the settings of other nodes, they are same to S2's settings.

#### Configuring switch S1:

Shuts down STP and configures the Ether-ring node:

```

S1_config#no spanning-tree
S1_config#ether-ring 1
S1_config_ring1#control-vlan 2
  
```

```
S1_config_ring1#master-node
```

The following commands are used to set the time related parameters:

```
S1_config_ring1#hello-time 2
```

```
S1_config_ring1#fail-time 6
```

Exits from the node configuration mode:

```
S1_config_ring1#exit
```

Configures the primary port and the secondary port:

```
S1_config#interface gigaEthernet 0/1
```

```
S1_config_g0/1#ether-ring 1 primary-port
```

```
S1_config_g0/1#exit
```

```
S1_config#interface gigaEthernet 0/3
```

```
S1_config_g0/3#ether-ring 1 secondary-port
```

```
S1_config_g0/3#exit
```

Establishes the control VLAN:

```
S1_config#vlan 2
```

```
S1_config_vlan2#exit
```

```
S1_config#interface range g0/1 , 3
```

```
S1_config_if_range#switchport mode trunk
```

```
S1_config_if_range#exit
```

### **Configuring switch S2:**

```
S1_config#no spanning-tree
```

```
S1_config#ether-ring 1
```

```
S1_config_ring1#control-vlan 2
```

```
S1_config_ring1#transit-node
```

```
S1_config_ring1#pre-forward-time 8
```

```
S1_config_ring1#exit
```

```
S1_config#interface gigaEthernet 0/1
```

```
S1_config_g0/1#ether-ring 1 transit-port
```

```
S1_config_g0/1#exit
```

```
S1_config#interface gigaEthernet 0/3
```

```
S1_config_g0/3#ether-ring 1 transit-port
```

```
S1_config_g0/3#exit
```

```
S1_config#vlan 2
```

```
S1_config_vlan2#exit
```

```
S1_config#interface range gigaEthernet 0/1 , 3
```

```
S1_config_if_range#switchport mode trunk
```

```
S1_config_if_range#exit
```

# 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.....	4
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 MEAPS Configuration Tasks.....	18
2.2 Fast Ethernet Ring Protection Configuration.....	18
2.2.1 Configuring the Master Node.....	18
2.2.2 Configuring the Transit Node.....	19
2.2.3 Configuring the Edge Node and the Assistant Node.....	20
2.2.4 Configuring Sub-ring Networking Mode.....	21
2.2.5 Configuring the Ring Port.....	21
2.2.6 Browsing the State of the Ring Protection Protocol.....	22
Chapter 3 Appendix.....	23
3.1 Working Procedure of MEAPS.....	23
3.1.1 Complete State.....	23
3.1.2 Link-Down.....	24
3.1.3 Recovery.....	25
3.2 MEAPS Configuration Examples.....	27
3.2.1 Configuration Examples.....	27
3.3 Unfinished Configurations (to be continued).....	33

## Chapter 1 MEAPS Introduction

### 1.1 MEAPS Overview

EAPS is a protocol specially applied on the link layer of the Ethernet ring. When the Ethernet ring is complete, you should prevent the broadcast storm from occurring on the data loopback. But when a link of an Ethernet ring is broken, you should enable the backup link rapidly to resume the communication of different nodes in the ring. The role of switch is specified by you through configuration.

MEAPS, an expansion on the basis of EAPS, can support not only the single ring but also the level-2 multi-ring structure. The later structure consists of the aggregation layer in the middle, constructed by aggregation equipment through the Ethernet ring for fast switching, and the access layer at the outside, connected by the access equipment. Different levels of rings are connected through the tangency or intersection mode. See the specific topology in the following figure:

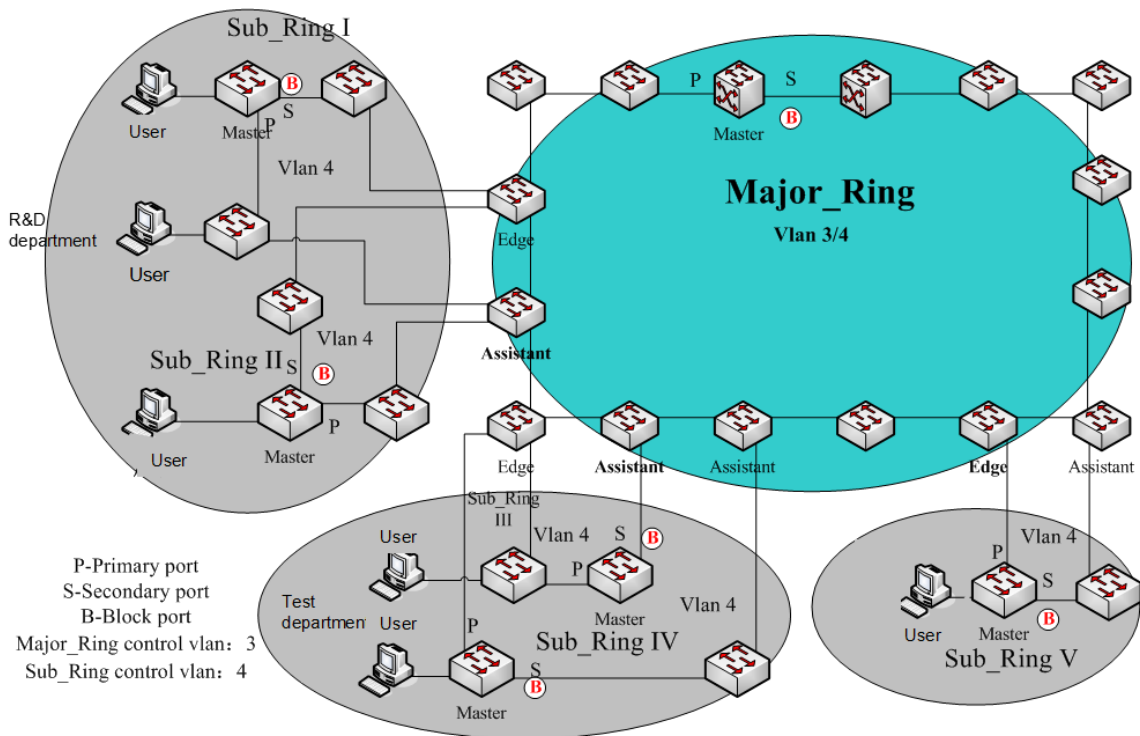


Figure 1 MEAPS Structure

The ring protection protocol and STP are both used for topology control on the link layer. STP is suitable for all kinds of complicated networks, which transmits the change of network topology hop by hop. The ring protection protocol is used for ring topology and adopts the pervasion mechanism to transmit the change of network topology. Therefore, the convergence of the ring protection protocol in the ring network is better than STP. In a sound network, the ring protection protocol can resume network communication within less than 50ms.

## 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 Figure-2.

One MEAPS domain has the following factors: MEAPS ring, control VLAN, master node, transit node, edge node and assistant edge node.

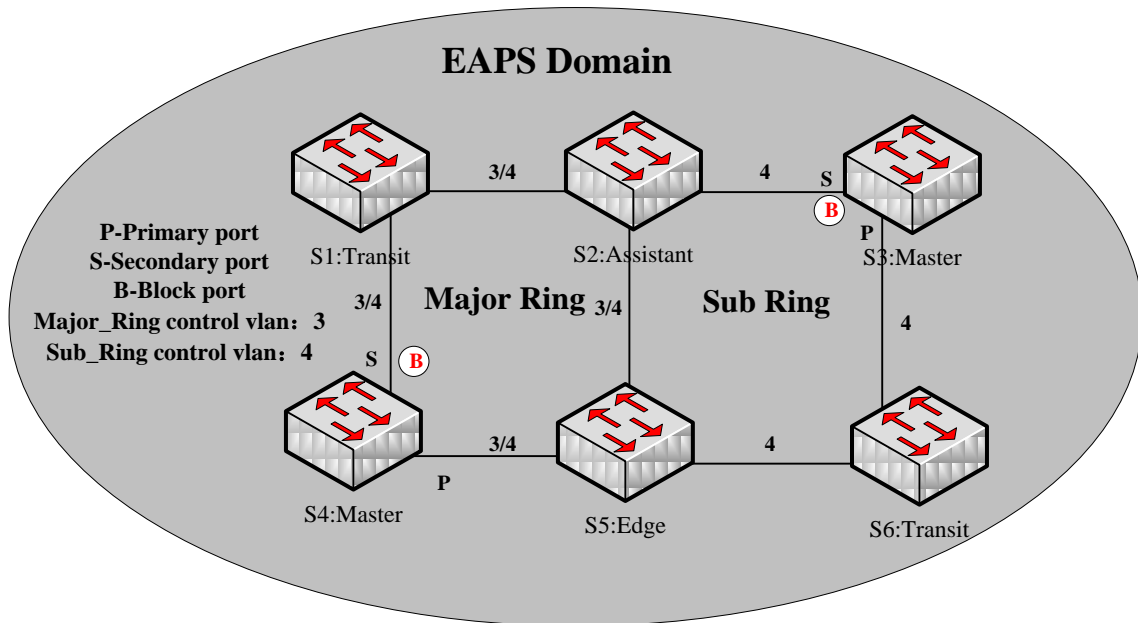


Figure-2 Simple MEAPS model



## 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, the included rings except the major ring are called as sub rings. The primary and secondary ports of each node on the major ring should be added into the main control VLAN and the sub control VLAN at the same time. See Figure-2.

## 1.2.4 Sub Ring

When a domain includes many rings, you should choose one ring from them as a major ring. The primary and secondary ports of each node on the sub ring should be added into the sub control VLAN. See Figure-2.

## 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 Edge Preforwarding state. If the edge port is in forwarding state and the main-ring port that the edge port corresponds to has not received the edge-hello packets, the state of the edge port is changed into the EdgePreforwarding state, and it only receives and forwards the control packets and blocks the data VLAN until the corresponding main-ring port receives the Edge-hello packets again.

The edge port of the edge node and the assistant node is to help detect the completeness of the major ring. For more details, see the channel status checkup mechanism of the sub-ring protocol packets on the major ring in the following chapter.

---

Note:

Each port can be set as the only edge port of a node and it cannot be configured again; the common port can be borne only on a port of the major ring and it cannot be configured on a port without a corresponding main-ring port.

---

### 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. 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

Table 1.1 Types of EAPS packets

Type of the packet	Description
Ring Detection (HEALTH)	It is transmitted by the master node to detect whether the topology of the ring network is complete.
link interruption (LINK-DOWN)	Indicates that link interruption happens in the ring. This kinds of packets are transmitted by the transit node.
MAC address aging table of the transit node (RING-DOWN-FLUSH-FDB)	It is transmitted by the master node after interruption of the ring network is detected and the packets show the MAC address aging table of the transit node.
Ring resume aging address table (RING-UP-FLUSH-FDB)	It is transmitted by the master node after interruption of the ring network is resumed and the packets show the MAC address aging table of the transit node.
Ring completeness detection (EDGE-HELLO)	It is decided by the edge port of the edge node, transmitted by the main-ring port that the edge node corresponds to, and detects whether the major ring is complete.

## 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.

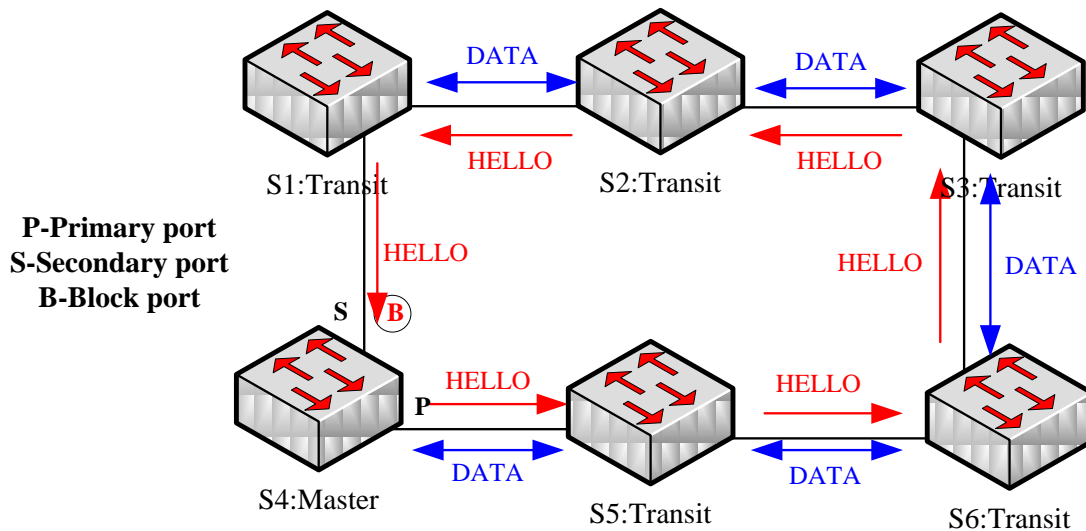


Figure 3 Polling mechanism

**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

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.

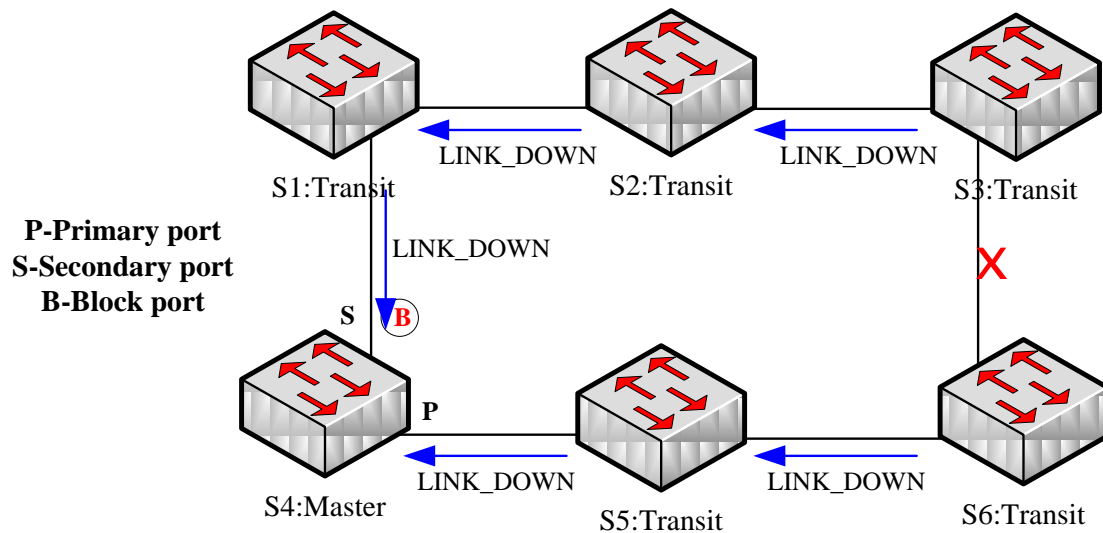


Figure 4 Link status change's notification

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 receive the notification of aging address table from the master node, it thinks that the link connecting the master node is already out of effect, and the transit node will automatically set the pre-forwarding port to be a forwarding one.

---

Note:

You can configure the related commands through the pre-forward-time node to modify the time for the transit port to keep the pre-forwarding state.

---

### 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:

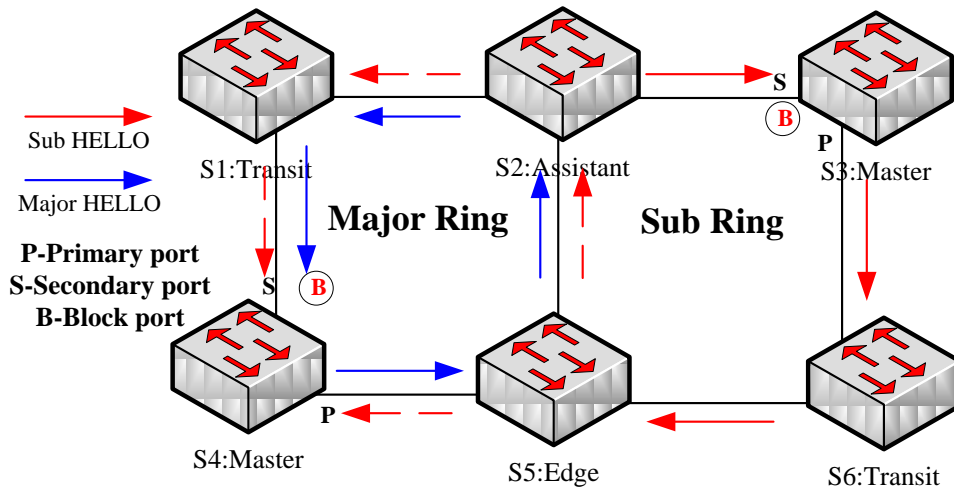


Figure 5 Intersection of the major ring and the sub ring

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.

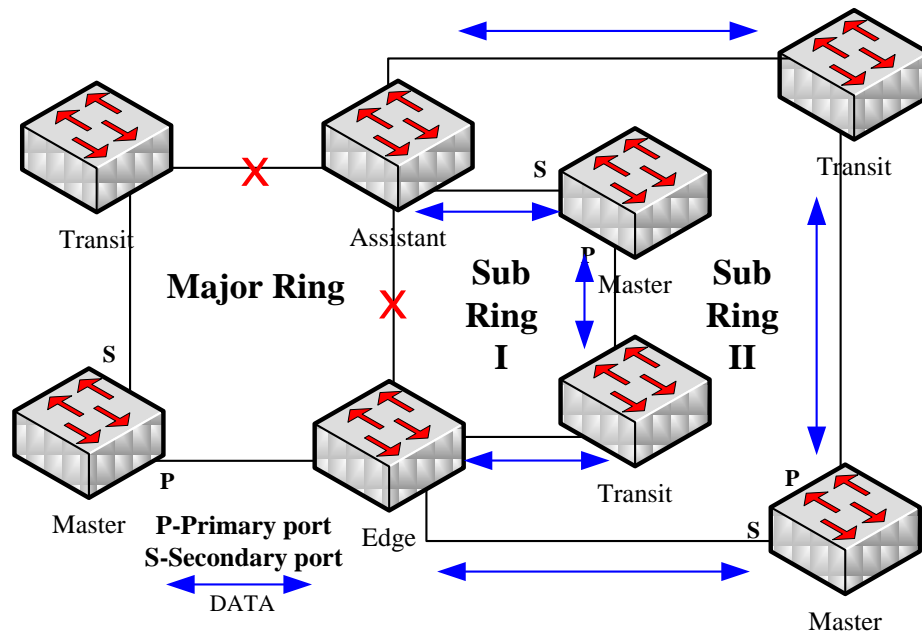


Figure 6 Broadcast storm triggered by the dual homing networking mode

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:



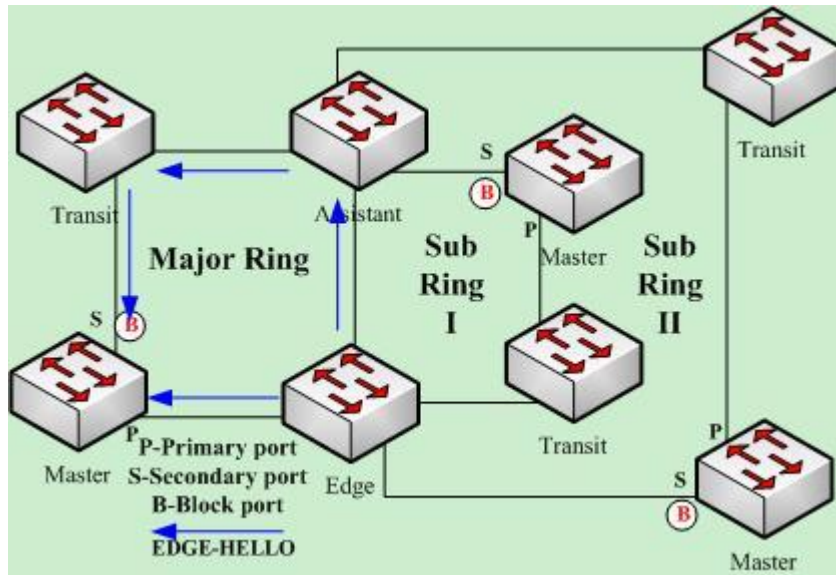


Figure 8 Checking the channel status on the major ring between the edge node and the assistant node

2. The edge node blocks the edge port at the interruption of the channel.

If the assistant node cannot receive the edge-hello packet during Edge Fail Time, the assistant holds that the channel of the sub-ring protocol packet—the edge-hello packet—is interrupted, changes its edge port's status into the Edge-Preforwarding status instantly, blocks the forwarding of the data packets (though still receives and forwards the control packet), and immediately transmits the LINK-DOWN packet to the master node for the master node to open the secondary port to avoid communication interruption among all nodes on the ring.

---

**Note:**

In order to guarantee that the edge port first changes into the edge-preforwarding status and then the master node opens the secondary port, you shall be sure that the cycle for the edge node to transmit the edge-hello packet, Edge Hello Time, is smaller than the cycle for the master node to transmit the Hello packet, Hello Time; similarly, the Edge Fail Time of the assistant node should be smaller than Fail Time. At the same time, Fail Time is generally the triple of Hello Time, and Edge Fail Time is also the triple of Edge Hello Time.

---

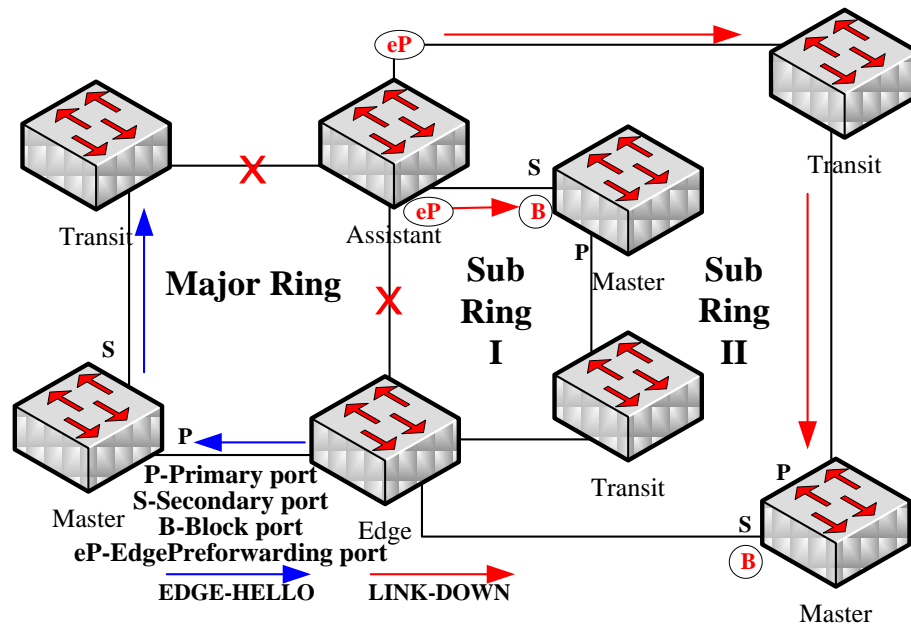


Figure 9 The edge port being blocked by the edge node at the interruption of the channel

### 3. Channel recovery

When the link of the major ring and the communication between the edge node and the assistant node resumes, the channel of the sub-ring protocol packet resumes to the normal function. In this case, the master node of the sub ring receives the Hello packet again, which is transmitted by the master node itself, and therefore it switches to the Complete status, blocks the secondary port and transmits the RING-UP-FLUSH-FDB packet to the ring. At the same time, the status of the edge port of the assistant node changes from Edge-Preforwarding to Forwarding, guaranteeing a smooth communication among all nodes on the ring. The following figure shows that the channel is resumed and then the communication on the ring is also resumed.

#### Note:

Before the edge node opens the blocked edge port, the secondary port of the master node on the sub ring should be blocked to prevent the broadcast storm from happening.

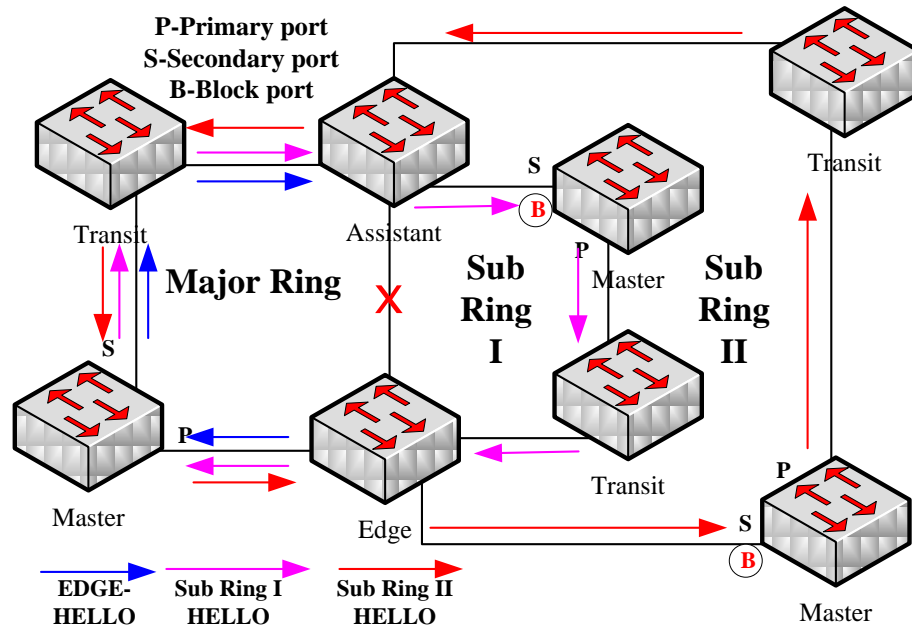


Figure 10 Channel recovery

## Chapter 2 Fast Ethernet Ring Protection Configuration

### Requisites Before Configuration

Before configuring MEAPS, please read the following items carefully:

- One of important functions of the ring protection protocol is to stop the broadcast storm, so please make sure that before the ring link is reconnected all ring nodes are configured. For example, when EAPS is configured, after the master node and all transit nodes are configured, connect the network cable and the secondary port of the master node; when configuring ERPS, please keep at least one link disconnected until all ring nodes are configured.
- Enable the ring protection protocol to be compatible with the STP of a switch through relative configurations. The users are allowed to set “no spanning-tree”, SSTP, RSTP PVST or MSTP mode.
- After an instance of the ring's node is set, users are forbidden to change the basic information of the node (excluding the time parameters) unless the current ring's node is deleted and then reset.
- If you run show to browse the configured node and find its **state** is **init**, it shows that the node's configuration is unfinished and therefore the node cannot be started. In this case, you are required to change or add basic information to complete the configuration of the node.
- The ring protection protocol supports a switch to configure multiple ring networks.
- The configuration of the control VLAN of the ring automatically leads to the establishment of the corresponding VLAN without requiring users' manual configuration.
- The port of each ring can forward the packets from the control VLAN of the ring, while other ports, even in the Trunk mode, cannot forward the packets from the control VLAN.
- By default, Fail-time of the master node is triple longer than Hello-time, so that packet delay is avoided from shocking the ring protection protocol. After Hello-time is modified, Fail-time need be modified accordingly.
- By default, Pre-Forward-Time of the transit node is triple longer than Hello-time of the master node so that it is ensured that the master node can detect the recovery of the ring network before the transit port enters the pre-forwarding state. If Hello-time configured on the master node is longer than Pre-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.

## 2.1 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

## 2.2 Fast Ethernet Ring Protection Configuration

### 2.2.1 Configuring the Master Node

Configure a switch to be the master node of a ring network according to the following steps:

Command	Purpose
Switch# <b>config</b>	Enters the switch configuration mode.
Switch_config# <b>mether-ring id1 domain id2</b>	Sets a node and enters the node configuration mode. id1: instance ID of a node id2: instance ID of a domain (omitted when it is 0)
Switch_config_ring1# <b>master-node</b>	Compulsory. Configures the node type to be a master node.
Switch_config_ring1# <b>major-ring[sub-ring]</b>	Compulsory. Sets the node's level to be one of the major or sub ring node.
Switch_config_ring1# <b>control-vlan vlan-id</b>	Compulsory. Sets the control VLAN and establishes VLAN "id" and VLAN "id+1".



	<i>vlan-id</i> : control vlan ID
Switch_config_ring1# <b>hello-time</b> <i>value</i>	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# <b>fail-time</b> <i>value</i>	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# <b>exit</b>	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*.

## 2.2.2 Configuring the Transit Node

Configure a switch to be the transit node of a ring network according to the following steps:

Command	Purpose
<b>Switch# config</b>	Enters the switch configuration mode.
Switch_config# <b>mether-ring</b> <i>id1</i> <b>domain</b> <i>id2</i>	Sets a node and enters the node configuration mode.  <i>id1</i> : ID of the node; <i>id2</i> : instance ID of a domain (omitted when it is 0)
Switch_config_ring1# <b>transit -node</b>	Compulsory. Configures the node type to be a transit node.
Switch_config_ring1# <b>major-ring</b> [ <b>sub-ring</b> ]	Compulsory. Sets the node's level to be one of the major or sub ring node.

Switch_config_ring1# <b>control-vlan</b> <i>vlan-id</i>	Compulsory. Sets the control VLAN and establishes VLAN “id” and VLAN “id+1” .  <i>vlan-id</i> : control vlan ID
Switch_config_ring1# <b>pre-forward-time</b> <i>value</i>	Optional. Configures the time of maintaining the pre-forward state on the transit port.  Value: It is a time value ranging from 3 to 30 seconds and the default value is 9 seconds.
<b>Switch_config_ring#exit</b>	Saves the current settings and exits the node configuration mode.
<b>Switch_config#</b>	

### 2.2.3 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# <b>config</b>	Enters the switch configuration mode.
Switch_config# <b>mether-ring</b> <i>id1</i> <b>domain</b> <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 (omitted when it is 0)
Switch_config_ring1# <b>edge-node</b> [ <b>assistant-node</b> ]	Compulsory. Sets the node type to be an edge node.
Switch_config_ring1# <b>sub-ring</b>	This step can be omitted. The edge node must be the sub-ring node.
Switch_config_ring1# <b>control-vlan</b> <i>vlan-id</i>	Compulsory. Sets the control VLAN and establishes VLAN “id” and VLAN “id+1” .  <i>vlan-id</i> : control vlan ID.
Switch_config_ring1# <b>pre-forward-time</b> <i>value</i>	Optional. Configures the time of maintaining the pre-forwarding state of the edge port.  Value: It is a time value ranging from 3 to 30 seconds and the default value is 9 seconds.
Switch_config_ring1# <b>exit</b>	Saves the current settings and exits the node configuration mode.
Switch_config#	

## 2.2.4 Configuring Sub-ring Networking Mode

Configure a switch to be the master node of a ring network according to the following steps:

Command	Purpose
Switch# <b>config</b>	Enters the switch configuration mode.
Switch_config# <b>mether-ring</b> <i>id1</i> <b>domain</b> <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 (omitted when it is 0)
Switch_config_ring1# <b>edge-node</b> [ <b>assistant-node</b> ]	Compulsory. Sets the node type to be an edge node.
Switch_config_ring1# <b>sub-ring</b>	This step can be omitted.The edge node must be the sub-ring node.
Switch_config_ring1# <b>control-vlan</b> <i>vlan-id</i>	Compulsory. Sets the control VLAN and establishes VLAN "id" and VLAN "id+1".  <i>vlan-id</i> : control vlan ID
Switch _config_ring2# <b>single-subring-mode</b>	Compulsory. The ring configuration can be finished without configuring the command, but the sub-ring networking mode is not available. In the sub-ring networking mode, the sub-ring protocol packet channel detection mechanism cannot work on the major ring and there must no dual homing networking. The command is effective only for the edge node and the assistant node.
Switch_config_ring1# <b>pre-forward-time</b> <i>value</i>	Optional. Configures the time of maintaining the pre-forwarding state of the edge port.  Value: It is a time value ranging from 3 to 30 seconds and the default value is 9 seconds.
Switch_config_ring1# <b>exit</b>	Saves the current settings and exits the node configuration mode.
Switch_config#	

## 2.2.5 Configuring the Ring Port

Configure a port of a switch to be the port of Ethernet ring according to the following steps:

Command	Purpose
<b>Switch# config</b>	Enters the switch configuration mode.
<b>Switch_config#interface</b> <i>intf-name</i>	Enters the interface configuration mode.

<b>Switch_config_intf#mether-ring</b> <i>id1 domain id2</i> <b>primary-port [ secondary-port   transit-port  </b> <b>common-port   edge-port ]</b>	Configures the type of the port of Ethernet ring.  id1: instance ID of a node id2: instance ID of a domain (omitted when it is 0)
<b>Switch_config_intf#exit</b>	Exits from interface configuration mode.

**Note:**

Run **no mether-ring** *id1 domain id2* **primary-port [ secondary-port | transit-port | common-port | edge-port ]** to delete the ring port configuration.

## 2.2.6 Browsing the State of the Ring Protection Protocol

Run the following command to browse the state of the ring protection protocol:

Command	Purpose
<b>show mether-ring</b>	Browses the summary information about the ring protection protocol and the ports of ring.
<b>show mether-ring</b> <i>id1 domain id2</i>	Browses the summary information about the designated ring protection protocol and the ports of ring.  id1: instance ID of a node id2: instance ID of a domain (omitted when it is 0)
<b>show mether-ring</b> <i>id1 domain id2 detail</i>	Browses the detailed information about the designated ring protection protocol and the port of Ethernet ring.
<b>show mether-ring</b> <i>id1 domain id2 interface intf-name</i>	Browses 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 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.

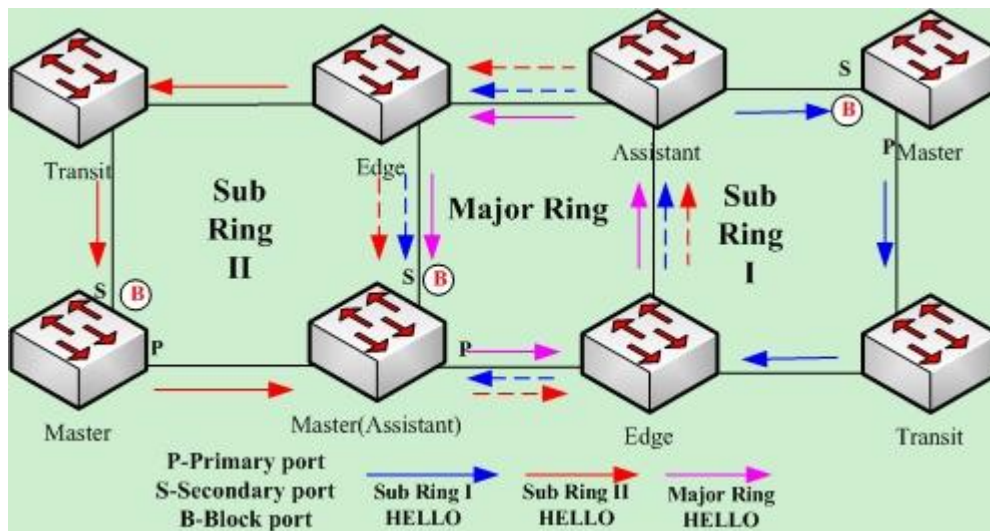


Figure 11 Complete state

### 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.

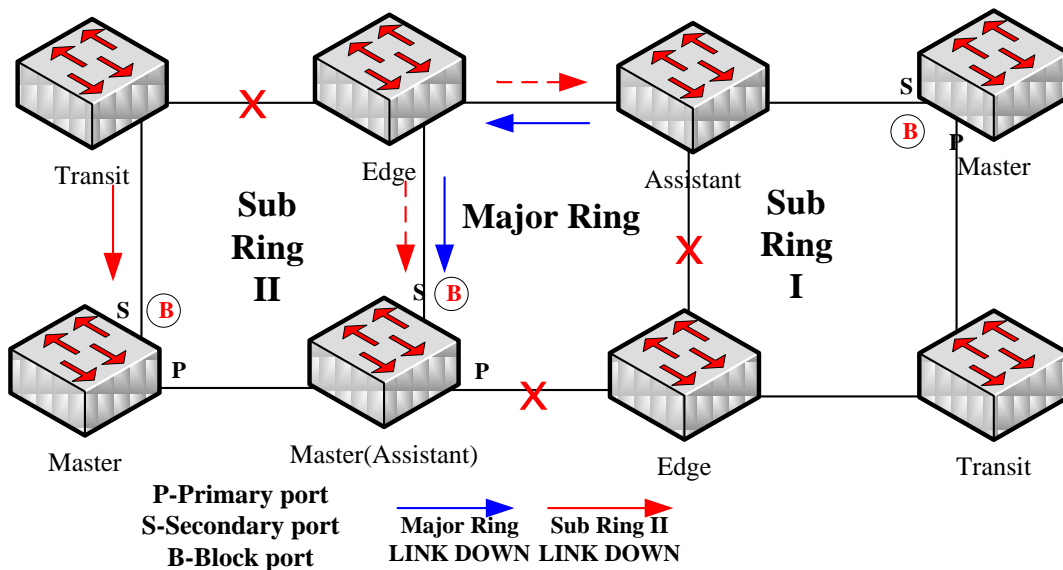


Figure 12 Ring transmitting the trouble and notifying the master node

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.

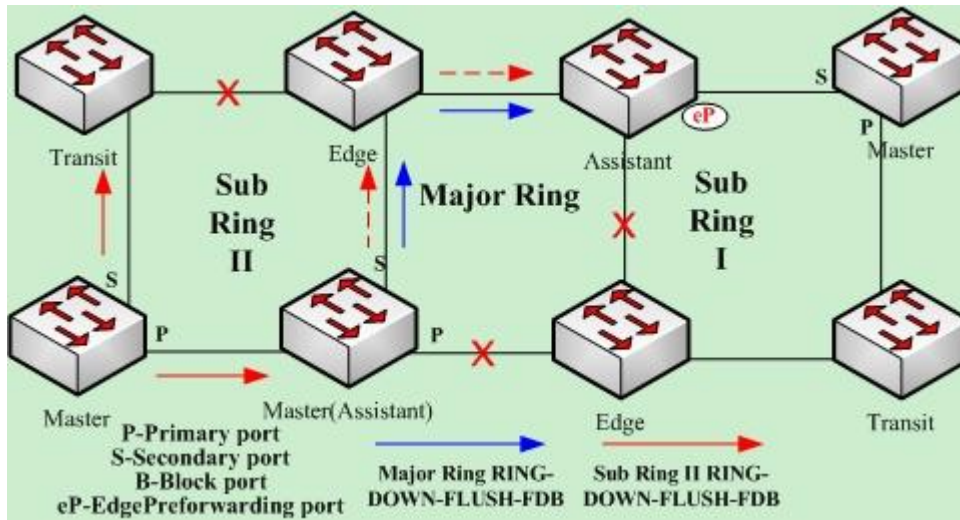


Figure 13 Ring transmitting troubles and refreshing FDB

### 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.

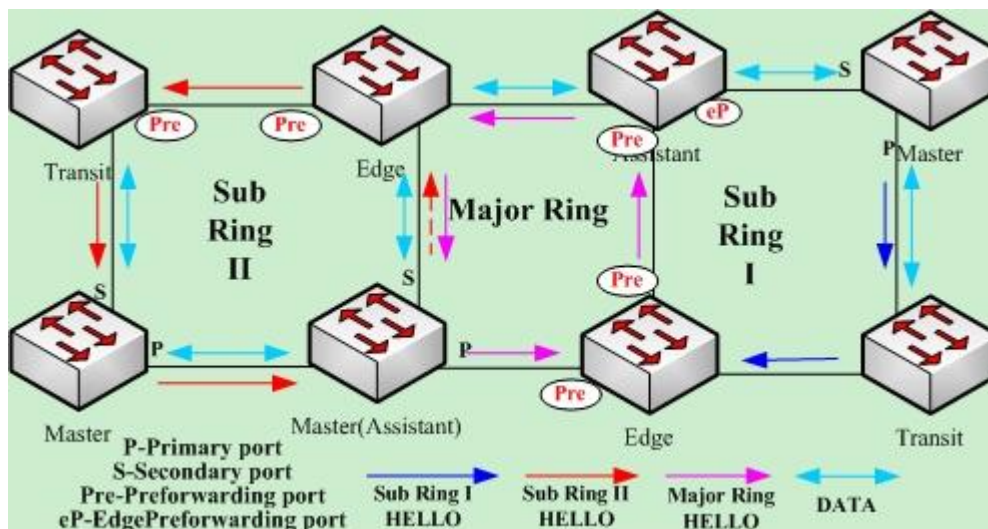


Figure 14 Recovery of the ring's link and the shift of the transit node to preforwarding

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.

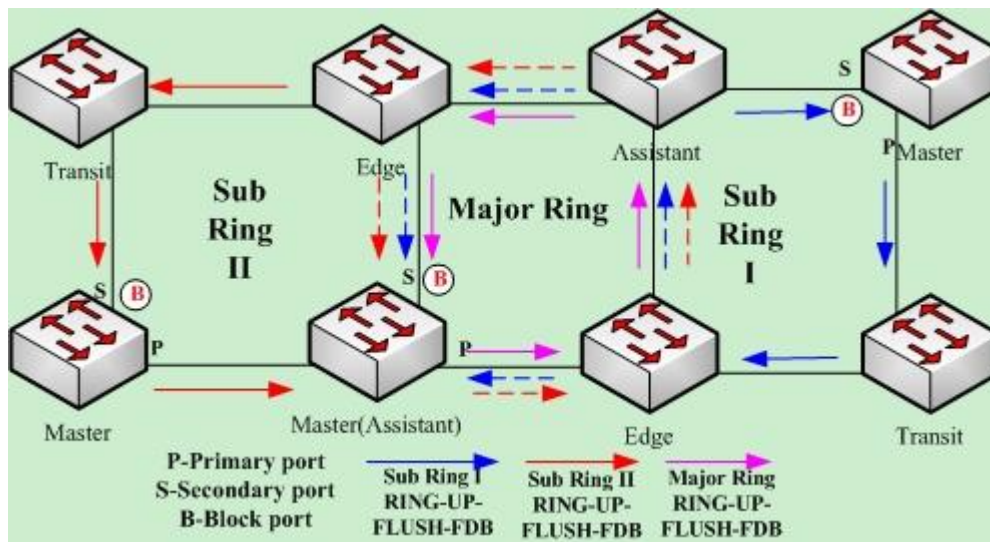


Figure 15 Recovery of the ring

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 Examples

### 3.2.1 Configuration Examples

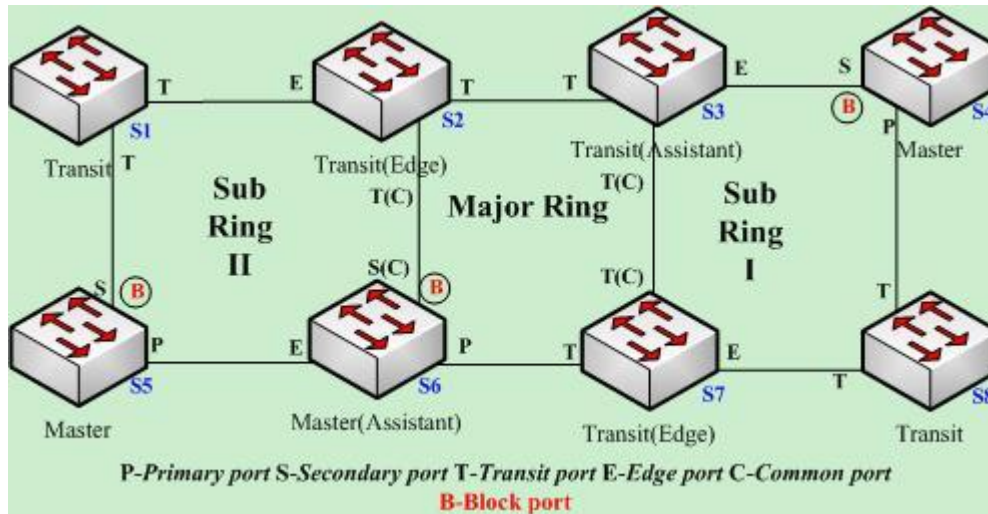


Figure 2.1 MEAPS Configuration Examples

As shown in figure 2.1, master node S1 and transit node S2 are configured as follows. As to the settings of other nodes, they are same to S2's settings.

#### Configuring switch S1:

The following commands are used to set the sub-ring transit node, node 2:

```
Switch_config#mether-ring 2 domain 1
Switch_config_ring2#transit-node
Switch_config_ring2#sub-ring
Switch_config_ring2#control-vlan 2
```

The following commands are used to set the time parameter:

```
Switch_config_ring2#pre-forward-time 12
```

Exits from the node configuration mode:

```
Switch_config_ring2#quit
```

The following commands are used to set the transit port of node 2:

```
Switch_config#interface gigaEthernet 0/1
Switch_config_g0/1#mether-ring 2 domain 1 transit-port
Switch_config_g0/1#switchport mode trunk
```

```
Switch_config_g0/1#quit
Switch_config#interface gigaEthernet 0/2
Switch_config_g0/2#mether-ring 2 domain 1 transit-port
Switch_config_g0/2#switchport mode trunk
Switch_config_g0/2#quit
```

**Configuring switch S2:**

The following commands are used to set the major-ring transit node, node 1:

```
Switch_config#mether-ring 1 domain 1
Switch_config_ring1#transit-node
Switch_config_ring1#major-ring
Switch_config_ring1#control-vlan 2
```

The following commands are used to set the time related parameters:

```
Switch_config_ring1#pre-forward-time 12
```

Exits from the node configuration mode:

```
Switch_config_ring1#quit
```

The following commands are used to set the transit port of node 1:

```
Switch_config#interface gigaEthernet 0/1
Switch_config_g0/1#mether-ring 1 domain 1 transit-port
Switch_config_g0/1#switchport mode trunk
Switch_config_g0/1#quit
Switch_config#interface gigaEthernet 0/2
Switch_config_g0/2#mether-ring 1 domain 1 transit-port
Switch_config_g0/2#switchport mode trunk
Switch_config_g0/2#quit
```

The following commands are used to set the sub-ring edge node, node 2:

```
Switch_config#mether-ring 2 domain 1
Switch_config_ring2#edge-node
Switch_config_ring2#sub-ring (This step can be omitted.)
Switch_config_ring2#control-vlan 2
```

The following commands are used to set the time related parameters:

```
Switch_config_ring2#pre-forward-time 12
```

Exits from the node configuration mode:

```
Switch_config_ring2#quit
```

The following commands are used to set the common port and edge port of node 2:

```
Switch_config#interface gigaEthernet 0/2
Switch_config_g0/2#mether-ring 2 domain 1 common-port
```

```
Switch_config_g0/2#quit
Switch_config#interface gigaEthernet 0/3
Switch_config_g0/3#mether-ring 2 domain 1 edge-port
Switch_config_g0/3#switchport mode trunk
Switch_config_g0/3#quit
```

**Configuring switch S3:**

The following commands are used to set the transit port of node 1:

```
Switch_config#mether-ring 1 domain 1
Switch_config_ring1#transit-node
Switch_config_ring1#major-ring
Switch_config_ring1#control-vlan 2
```

The following commands are used to set the time related parameters:

```
Switch_config_ring1#pre-forward-time 12
```

Exits from the node configuration mode:

```
Switch_config_ring1#quit
```

The following commands are used to set the transit port of node 1:

```
Switch_config#interface gigaEthernet 0/1
Switch_config_g0/1#mether-ring 1 domain 1 transit-port
Switch_config_g0/1#switchport mode trunk
Switch_config_g0/1#quit
Switch_config#interface gigaEthernet 0/2
Switch_config_g0/2#mether-ring 1 domain 1 transit-port
Switch_config_g0/2#switchport mode trunk
Switch_config_g0/2#quit
```

The following commands are used to set the sub-ring assistant node, node 4:

```
Switch_config#mether-ring 4 domain 1
Switch_config_ring4#assistant-node
Switch_config_ring4#sub-ring (This step can be omitted.)
Switch_config_ring4#control-vlan 2
```

The following commands are used to set the time related parameters:

```
Switch_config_ring4#pre-forward-time 12
```

Exits from the node configuration mode:

```
Switch_config_ring4#quit
```

The following commands are used to set the common port and edge port of node 2:

```
Switch_config#interface gigaEthernet 0/2
Switch_config_g0/2#mether-ring 4 domain 1 common-port
```

```
Switch_config_g0/2#quit
Switch_config#interface gigaEthernet 0/3
Switch_config_g0/3#mether-ring 4 domain 1 edge-port
Switch_config_g0/3#switchport mode trunk
Switch_config_g0/3#quit
```

#### **Configuring switch S4:**

The following commands are used to set the sub-ring master node, node 4:

```
Switch_config#mether-ring 4 domain 1
Switch_config_ring4#master-node
Switch_config_ring4#sub-ring
Switch_config_ring4#control-vlan 2
```

The following commands are used to set the time related parameters:

```
Switch_config_ring4#hello-time 4
Switch_config_ring4#fail-time 12
```

Exits from the node configuration mode:

```
Switch_config_ring4#quit
```

The following commands are used to set the primary port and secondary port of node 4:

```
Switch_config#interface gigaEthernet 0/1
Switch_config_g0/1#mether-ring 4 domain 1 primary-port
Switch_config_g0/1#switchport mode trunk
Switch_config_g0/1#quit
Switch_config#interface gigaEthernet 0/2
Switch_config_g0/2#mether-ring 4 domain 1 secondary-port
Switch_config_g0/2#switchport mode trunk
Switch_config_g0/2#quit
```

#### **Configuring switch S5:**

The following commands are used to set the sub-ring master node, node 2:

```
Switch_config#mether-ring 2 domain 1
Switch_config_ring2#master-node
Switch_config_ring2#sub-ring
Switch_config_ring2#control-vlan 2
```

The following commands are used to set the time related parameters:

```
Switch_config_ring2#hello-time 4
Switch_config_ring2#fail-time 12
```

Exits from the node configuration mode:

```
Switch_config_ring2#quit
```

The following commands are used to set the primary port and secondary port of node 2:

```
Switch_config#interface gigaEthernet 0/1
Switch_config_g0/1#mether-ring 2 domain 1 primary-port
Switch_config_g0/1#switchport mode trunk
Switch_config_g0/1#quit
Switch_config#interface gigaEthernet 0/2
Switch_config_g0/2#mether-ring 2 domain 1 secondary-port
Switch_config_g0/2#switchport mode trunk
Switch_config_g0/2#quit
```

#### **Configuring switch S6:**

The following commands are used to set the major-ring master node, node 1:

```
Switch_config#mether-ring 1 domain 1
Switch_config_ring1#master-node
Switch_config_ring1#major-ring
Switch_config_ring1#control-vlan 2
```

The following commands are used to set the time related parameters:

```
Switch_config_ring1#hello-time 4
Switch_config_ring1#fail-time 12
```

Exits from the node configuration mode:

```
Switch_config_ring1#quit
```

The following commands are used to set the transit port of node 1:

```
Switch_config#interface gigaEthernet 0/1
Switch_config_g0/1#mether-ring 1 domain 1 primary-port
Switch_config_g0/1#switchport mode trunk
Switch_config_g0/1#quit
Switch_config#interface gigaEthernet 0/2
Switch_config_g0/2#mether-ring 1 domain 1 secondary-port
Switch_config_g0/2#switchport mode trunk
Switch_config_g0/2#quit
```

The following commands are used to set the sub-ring assistant node, node 2:

```
Switch_config#mether-ring 2 domain 1
Switch_config_ring2#assistant-node
Switch_config_ring2#sub-ring (This step can be omitted.)
Switch_config_ring2#control-vlan 2
```

The following commands are used to set the time related parameters:

```
Switch_config_ring2#pre-forward-time 12
```

Exits from the node configuration mode:

```
Switch_config_ring2#quit
```

The following commands are used to set the common port and edge port of node 2:

```
Switch_config#interface gigaEthernet 0/2
Switch_config_g0/2#mether-ring 2 domain 1 common-port
Switch_config_g0/2#quit
Switch_config#interface gigaEthernet 0/3
Switch_config_g0/3#mether-ring 2 domain 1 edge-port
Switch_config_g0/3#switchport mode trunk
Switch_config_g0/3#quit
```

### **Configuring switch S7:**

The following commands are used to set the major-ring transit node, node 1:

```
Switch_config#mether-ring 1 domain 1
Switch_config_ring1#transit-node
Switch_config_ring1#major-ring
Switch_config_ring1#control-vlan 2
```

The following commands are used to set the time related parameters:

```
Switch_config_ring1#pre-forward-time 12
```

Exits from the node configuration mode:

```
Switch_config_ring1#quit
```

The following commands are used to set the transit port of node 1:

```
Switch_config#interface gigaEthernet 0/1
Switch_config_g0/1#mether-ring 1 domain 1 transit-port
Switch_config_g0/1#switchport mode trunk
Switch_config_g0/1#quit
Switch_config#interface gigaEthernet 0/2
Switch_config_g0/2#mether-ring 1 domain 1 transit-port
Switch_config_g0/2#switchport mode trunk
Switch_config_g0/2#quit
```

The following commands are used to set the secondary port of node 4:

```
Switch_config#mether-ring 4 domain 1
Switch_config_ring4#edge-node
Switch_config_ring4#sub-ring (This step can be omitted.)
Switch_config_ring4#control-vlan 2
```

The following commands are used to set the time related parameters:

```
Switch_config_ring4#pre-forward-time 12
```

Exits from the node configuration mode:

```
Switch_config_ring4#quit
```

The following commands are used to set the common port and edge port of node 2:

```
Switch_config#interface gigaEthernet 0/2
Switch_config_g0/2#mether-ring 4 domain 1 common-port
Switch_config_g0/2#quit
Switch_config#interface gigaEthernet 0/3
Switch_config_g0/3#mether-ring 4 domain 1 edge-port
Switch_config_g0/3#switchport mode trunk
Switch_config_g0/3#quit
```

### Configuring switch S8:

The following commands are used to set the sub-ring transit node, node 4:

```
Switch_config#mether-ring 4 domain 1
Switch_config_ring4# transit -node
Switch_config_ring4#sub-ring
Switch_config_ring4#control-vlan 2
```

The following commands are used to set the time related parameters:

```
Switch_config_ring4#pre-forward-time 12
```

Exits from the node configuration mode:

```
Switch_config_ring4#quit
```

The following commands are used to set the transit port of node 4:

```
Switch_config#interface gigaEthernet 0/1
Switch_config_g0/1#mether-ring 4 domain 1 transit -port
Switch_config_g0/1#switchport mode trunk
Switch_config_g0/1#quit
Switch_config#interface gigaEthernet 0/2
Switch_config_g0/2#mether-ring 4 domain 1 transit -port
Switch_config_g0/2#switchport mode trunk
Switch_config_g0/2#quit
```

## 3.3 Unfinished Configurations (to be continued)

- Unfinished basic information configuration: there is one of the ring's role, the ring's grade and the control VLAN unset. One exceptional case is that when a node's role has configured to be the edge node or assistant node, the default ring's grade is sub-ring.

- Contradiction of basic information: When a node's role is edge-node or assistant-node, the default ring's grade is sub-ring; when the ring's grade is major-ring, prompt information will appear.
- Sub ring having no corresponding major-ring node: When a node's role is edge-node or assistant-node, this node is borne on the major-ring node; if there is no corresponding major-ring node to compulsorily create the sub-ring edge node or sub-ring assistant node, prompt information will appear (in this case, you can use the show command to browse the MEAPS state; if you find the basic information is complete but the state is init, it indicates that the configuration of the ring's node has not finished).
- Conflicts arising during control VLAN configuration: If the control VLAN, which is configured by a node, conflicts with other configured nodes, prompt information will appear (in this case, you can use the show command to browse the MEAPS state; if you find the basic information is complete but the state is init, it indicates that the configuration of the ring's node has not finished).
- When configuring the sub-ring node according to the major ring node, the id of the sub-ring node must be greater than the ID of the major ring node. Otherwise, here pops up a prompt.



# TMRP Protection Configuration

# Table of Contents

- Chapter 1 TMRP Protection Introduction ..... 1
  - 1.1 General ..... 1
- Chapter 2 TMRP Protocol ..... 2
  - 2.1 TMRP Configuration task ..... 2
    - 2.1.1 Create/delete the TMRP example of the switch ..... 2
    - 2.1.2 Configure the bridge priority ..... 2
    - 2.1.3 Configure Forward Time ..... 2
    - 2.1.4 Configure Hello Time ..... 3
    - 2.1.5 Configure Max Age ..... 3
    - 2.1.6 Configure the ring net port ..... 3
    - 2.1.7 Configure the port path cost ..... 4
    - 2.1.8 Configure the port priority ..... 4
  - 2.2 TMRP configuration example ..... 5
    - 2.2.1 Configuration example ..... 5

# Chapter 1 TMRP Protection Introduction

## 1.1 General

TMRP designates one recovery protocol with the ring topology structure as the basis. TMRP is designed to be able to reflect accurately one single internal switch link or switch fault inside the network.

One compatible network should have the ring topology structure with several nodes.

In TMRP, one node is considered as the root or root node. As for each ring net, there is one node port responsible for the data transfer from this segment to the root node. This port is considered as the designated port for this local area network segment while the node where the port is located is considered as the designated bridge of this local area network. The root node is the designated bridge of all the ring nets connected with it. In the port of each ring net, the port which is closest to the root node is the root port of this root node and only the root port and the designated port (if any) are under the transmitting status; there is any kind of ports which are not closed down but they are not root ports or designated ports and this kind of ports are spare ones.

The following parameters decide the structure of active topology after being stable:

- (1) The single identification for each node.
- (2) Path cost of each port.
- (3) Port identification of each port of the node.

The node with the highest priority (the value of identifier is the minimum) is selected as the root node. The port of each node in the ring net has one root path cost attribute, i.e. the minimum value of the sum of the path cost of all ports experienced from the root node to this node. The designated port of each ring net is the port connected to this segment with the minimum root path cost; when several ports (connected to different nodes of the same ring net) has the same root path cost, then firstly the identification of nodes where they are located shall be compared, and then their port identification shall be compared. With this method, each port has one designated port and each node has only one root port.

The ring net topology makes there is no ring circuit in the network, ensuring the stability of the network and the ability to recover from fault. When there is fault in the node, node port or ring net segment in the ring net, TMRP realizes the rapid convergence of the network topology. The new root port on the node can enter immediately the transmitting status for work. At the meantime, the direct recognition among nodes can make the designated port also perform transmitting at once.

## Chapter 2 TMRP Protocol

### 2.1. TMRP Configuration task

#### 2.1.1. Create/delete the TMRP example of the switch

Make following configuration in global configuration mode

Command	Purpose
<b>TMRP</b> <i>id</i>	Configure example of TMRP ring net nodes and enter the node configuration mode.  Id: Number of actual ring net example, range is 0-7.
<b>no TMRP</b> <i>id</i>	Delete the example of TMRP ring net node

#### 2.1.2. Configure the bridge priority

Make following configuration in the TMRP node configuration mode

Command	Purpose
<b>priority</b> <i>value</i>	Configure the node priority

The size of node priority decides whether the node can be selected as the root of the whole ring net. Certain node can be the root of the ring net by configuration of the smaller priority.

What is worth noting is that if the whole ring net adopts several nodes of highest priority, then the node with the smallest MAC address is selected as the root. In the normal condition of ring net, if the priority of certain node is changed, then re-calculation of the root may be caused.

The priority of the node in default condition is 32768.

#### 2.1.3. Configure Forward Time

Make following configuration in configuration mode of TMRP node :

Command	Purpose
<b>forward-time</b> <i>value</i>	Configure Forward Delay.

The link fault will lead to the re-calculation of TMRP ring net. However, the new configuration message obtained from re-calculation can not pass to the whole network immediately. If the newly selected root port and designated port start immediately to transmit the data, it may lead to the temporary loopback. To this end, one state transition mechanism is adopted by the protocol. One middle state has to be experienced before the root port and designated port start again to transmit the data.

The middle state can enter the transmitting state only after the delay of Forward Delay, which makes sure that the new configuration message spreads to all the network. The Forward Delay characteristic of the bridge is related to the network diameter of the switch network. Generally the large the network diameter, the longer the configuration time for Forward Delay.

It is worth noting that when the Forward Delay is configured too small, the network will have temporary redundant path; if it is configured too large, it is possible for the network not to recover the connection for longer time. It is recommended that the user use the default value.

The Forward Delay of the node in default situation is 15 seconds.

#### 2.1.4. Configure Hello Time

Make following configuration in the TMRP node configuration mode

Command	Purpose
<b>hello-time</b> <i>value</i>	Configure Hello Time .

Proper time value of Hello Time can make sure the node is able to detect immediately the link fault in the ring net while not taking too much network resource.

It is worth noting that when the value of Hello Time is too long, the node can not receive the Hello message due to the package loss of the line, then the node will consider that the link has fault and start to re-calculate the root node. If the Hello Time is too short, the node will send frequently the configuration message which occupies the network bandwidth, increasing the network load and CPU load. It is recommended that the user use the default value.

The Hello Time for the node in the default situation is 4 seconds.

#### 2.1.5. Configure Max Age

Make following configuration in configuration mode of TMRP node:

Command	Purpose
<b>max-age</b> <i>value</i>	Configure Max Age.

Max Age is the parameter used to judge whether the configuration message is outdated. The user can make configuration depending on the actual network situation.

Link fault, reducing the self-adaptability of the network. It is recommended that the user use the default value. What is worth noting is that if the Max Age is configured too small, it will be frequent for the ring net to re-calculate the root, and it is possible to mistake the network congestion as the link failure. If the Max Age is configured too large, it is probable that it can not be detected immediately.

The Max Age of the node in the default situation is 20 seconds.

#### 2.1.6. Configure the ring net port

Make the following configuration in the port configuration mode:

## TMRP Protection Configuration

Command	Purpose
<b>tmrp id [primary   secondary]</b>	Configure the ring net port.  Id: Number of actual ring net example, range is 0-7.
<b>no tmrp id [primary   secondary]</b>	Delete the ring net port.  Id: Number of actual ring net example, range is 0-7.

Each ring net has two ring net ports configured: primary port and secondary port.

## 2.1.7. Configure the port path cost

Please make following configuration in the port configuration mode:

Command	Purpose
<b>tmrp id cost value</b>	Configure the value of Path Cost of the port.  Id: Number of actual ring net example, range is 0-7.
<b>no tmrp id cost</b>	Recover the Path Cost of the port to be the default value.  Id: Number of actual ring net example, range is 0-7.

The path cost of the Ethernet port is related to the link rate of this port. The bigger the link rate, the smaller the configured parameter. When the parameter is configured to be the default value, the TMRP protocol can check automatically the link rate of the port of the current Ethernet and convert it to relevant path cost.

What is worth noting is that the configuration of path cost of the Ethernet port will cause the ring net to re-calculate the root. It is recommended that the user use the default value and let the TMRP protocol itself calculate the path cost of the port of the current Ethernet.

The Path Cost of all the ring net ports of the node in default situation is 2000000 when the port rate is 10Mbps, and 200000 when the port rate is 100Mbps.

## 2.1.8. Configure the port priority

Make following configuration in the port configuration mode:

Command	Purpose
<b>tmrp id port-priority value</b>	Configure the priority value of the port.  Id: Number of actual ring net example, range is 0-7.
<b>no tmrp id port-priority</b>	Recover the priority value of the ring net to be

## TMRP Protection Configuration

	the default value. Id: Number of actual ring net example, range is 0-7.
--	--

Special Ethernet port can be designated to be included in the spanning tree by setting the priority of the port. Generally the smaller the value configured, the higher the priority of the port and it is more likely for the Ethernet port to be included in the spanning tree. If all the Ethernet ports of the bridge adopt the same priority parameter value, then the priority of the Ethernet port depends on the index number of the Ethernet port.

It is worth noting that the change of the priority of the Ethernet port will lead to the re-calculation of the spanning tree.

The priority of all the Ethernet ports in the default situation is 128.

## 2.2. TMRP configuration example

### 2.2.1. Configuration example

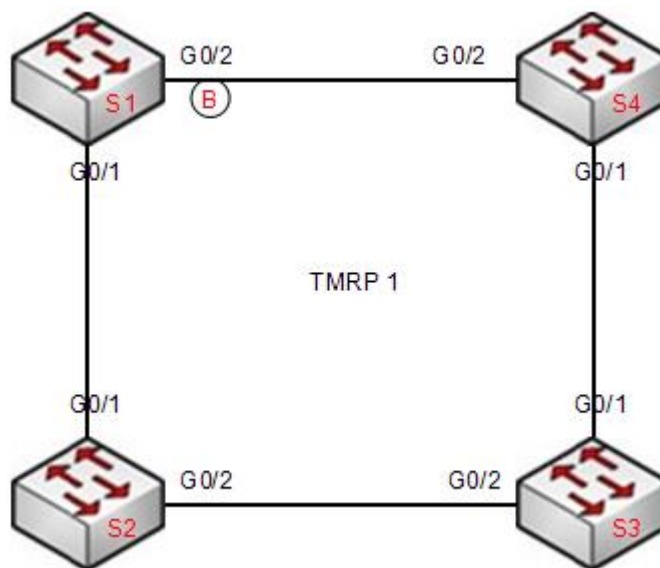


Figure 5.1 TMRP configuration

As shown in figure 5.1, the configuration of [S1](#), [S2](#), [S3](#) and [S4](#) is as follows:

#### 2.2.1.1. The configuration of S1, S2, S3 and S4 of the switch is as follows:

Configure the ring net nodes:

```
Switch_config#tmrp 1
```

```
Switch_config_tmrp1#exit
```

## TMRP Protection Configuration

```

Switch_config#
Configure the primary port:
Switch_config# interface g0/1
Switch_config_g0/1# tmrp 1 primary-port

Configure the secondary port:
Switch_config# interface g0/2
Switch_config_g0/2# tmrp 1 secondary-port

```

## 2.2.1.2. Show the tmrp of the switch S1:

```

Switch_config# show tmrp

TMRP

ring 1
  Root ID   Priority   32768
           Address   00E0.0FE9.E000
           This bridge is the root
           Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID Priority   32768
           Address   00E0.0FE9.E000
           Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface      Role Sts Cost      Pri.Nbr Type
-----
G0/1           Root FWD 200000    128.8  P2p
G0/2           Disa BLK 200000    128.4  P2p

```



# IGMP-SNOOPING Configuration

## Table of Contents

Chapter 1 IGMP-snooping Configuration.....	1
1.1 IGMP-snooping Configuration Task.....	1
1.1.1 Enabling/Disabling IGMP-Snooping of VLAN .....	1
1.1.2 Adding/Deleting Static Multicast Address of VLAN .....	2
1.1.3 Configuring immediate-leave of VLAN .....	2
1.1.4 Configuring Static Routing Interface of VLAN .....	3
1.1.5 Configuring IPACL of Generating Multicast Forward Table .....	3
1.1.6 Configuring Layer-2 Switch Translation Function.....	3
1.1.7 Configuring the Function to Filter Multicast Message Without Registered Destination Addresss.....	4
1.1.8 Configuring Router Age Timer of IGMP-snooping .....	4
1.1.9 Configuring Response Time Timer of IGMP-Snooping.....	4
1.1.10 Configuring Querier of IGMP-Snooping .....	5
1.1.11 Configuring IGMP-snooping's Querier Time Timer .....	5
1.1.12 Configuring data forwarding of IGMP-snooping's forward-l3-to-mrouter to router port .....	6
1.1.13 Configuring sensitive mode and value for IGMP-snooping .....	6
1.1.14 Configuring IGMP-snooping's v3-leave-check function.....	7
1.1.15 Configuring IGMP-snooping's forward-wrongiif-within-vlan function .....	7
1.1.16 Configuring IGMP-snooping's IPACL function at port .....	8
1.1.17 Configuring maximum multicast IP address quantity function at IGMP-snooping's port.....	8
1.1.18 Configuring MACACL at IGMP-snooping port.....	8
1.1.19 Monitoring and Maintaining IGMP-Snooping.....	8
1.1.20 IGMP-Snooping Configuration Example .....	11

## Chapter 1 IGMP-snooping Configuration

### 1.1 IGMP-snooping Configuration Task

The task of IGMP-snooping is to maintain the relationships between VLAN and group address and to update simultaneously with the multicast changes, enabling layer-2 switches 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 static multicast address of VLAN
- Configuring immediate-leave of VLAN
- Configuring the function to filter multicast message without registered destination address
- Configuring the **Router Age** timer of IGMP-snooping
- Configuring the **Response Time** timer of IGMP-snooping
- Configuring IGMP Querier of IGMP-snooping
- Monitoring and maintaining IGMP-snooping
- IGMP-snooping configuration example

#### 1.1.1 Enabling/Disabling IGMP-Snooping of VLAN

Perform the following configuration in global configuration mode:

Command	Description

<b>ip igmp-snooping</b> [vlan <i>vlan_id</i> ]	Enables IGMP-snooping of VLAN.
<b>no ip igmp-snooping</b> [vlan <i>vlan_id</i> ]	Resumes the default configuration.

If *vlan* is not specified, all vlans in the system, including vlans created later, can be enabled or disabled.

In the default configuration, IGMP-snooping of all VLANs is enabled, just as the **ip igmp-snooping** command is configured.

**Note:** IGMP-snooping can run on up to 16 VLANs.

To enable IGMP-snooping on VLAN3, you must first run **no ip IGMP-snooping** to disable IGMP-snooping of all VLANs, then configure **ip IGMP-snooping VLAN 3** and save configuration.

### 1.1.2 Adding/Deleting Static Multicast Address of VLAN

Hosts that do not support IGMP can receive corresponding multicast message by configuring the static multicast address.

Perform the following configuration in global configuration mode:

Command	Description
<b>ip igmp-snooping vlan</b> <i>vlan_id</i> <b>static</b> <i>A.B.C.D</i> <b>interface</b> <i>intf</i>	Adds static multicast address of VLAN.
<b>no ip igmp-snooping vlan</b> <i>vlan_id</i> <b>static</b> <i>A.B.C.D</i> <b>interface</b> <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.

Perform the following configuration in global configuration mode:

Command	Description
<b>ip igmp-snooping vlan</b> <i>vlan_id</i> <b>immediate-leave</b>	Configures the <b>immediate-leave</b> function of the VLAN.
<b>no ip igmp-snooping vlan</b> <i>vlan_id</i> <b>immediate-leave</b>	Sets immediate-leave of VLAN to its default value.

The **immediate-leave** characteristic of VLAN is disabled by default.

### 1.1.4 Configuring Static Routing Interface of VLAN

Configure the static routing interface and send the multicast packet to the routing port. The switch will send the multicast report packets to all routing ports in vlan.

Run following commands in the global configuration mode:

Command	Purpose
<b>ip igmp-snooping vlan</b> <i>vlan_id</i> <b>mrouter interface</b> <i>intf</i>	Add the static routing port of VLAN.
<b>no ip igmp-snooping vlan</b> <i>vlan_id</i> <b>mrouter interface</b> <i>intf</i>	Delete the static routing port of VLAN.

### 1.1.5 Configuring IPACL 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
<b>ip igmp-snooping policy</b> <i>word</i>	Adds IPACL in generating multicast forwarding table.
<b>no ip igmp-snooping policy</b>	Deletes IPACL in generating multicast forwarding table.

### 1.1.6 Configuring Layer-2 Switch Translation Function

Modify vlantag for the downlink protocol packet and modify vlantag for the uplink protocol according to the MACACL rule.

Command	Purpose
<b>ip igmp-snooping translate</b> <b>host-vlan</b> <i>vlan-id</i>	Modify vlan-id of packets sending to host port
<b>ip igmp-snooping translate</b> <b>router-vlan</b> <i>vlan-id</i>	Modify vlan-id of packets sending to router port
<b>no ip igmp-snooping translate</b> <b>host-vlan</b>	Modify translation configuration of packets sending to host port
<b>no ip igmp-snooping translate</b> <b>router-vlan</b>	Delete translation configuration of packets sending to router port

**Note:**

Translation function cannot be configured when enabling MVC.

### 1.1.7 Configuring the Function to Filter Multicast Message Without Registered Destination Addresses

When multicast message target fails to be found ( DLF, the destination address is not registered in the switch chip through igmp-snooping), the default process method is to send message on all ports of VLAN. Through configuration, you can change the process method and all multicast messages whose destination addresses are not registered to any port will be dropped.

Command	Description
<b>ip igmp-snooping dlf-drop</b>	Drops multicast message whose destination fails to be found.
<b>no ip igmp-snooping dlf-drop</b>	Resumes the fault configuration (forward).

**Note:**

- (1) The attribute is configured for all VLANs.
- 1) The default method for the switch to handle this type of message is forward (message of this type will be broadcasted within VLAN).

### 1.1.8 Configuring Router Age Timer of IGMP-snooping

The **Router Age** timer is used to monitor whether the IGMP inquirer exists. IGMP inquirers maintains multicast addresses by sending **query** message. IGMP-snooping works through communication between IGMP inquirer and host.

Perform the following configuration in global configuration mode:

Command	Description
<b>ip igmp-snooping timer router-age <i>timer_value</i></b>	Configures the value of Router Age of IGMP-snooping.
<b>no ip igmp-snooping timer router-age</b>	Resumes the default value of Router Age of IGMP-snooping.

**Note:**

For how to configure the timer, refer to the query period setup of IGMP inquirer. The timer cannot be set to be smaller than query period. It is recommended that the timer is set to three times of the query period.

The default value of Router Age of IGMP-snooping is 260 seconds.

### 1.1.9 Configuring Response Time Timer of IGMP-Snooping.

The **response time** timer is the upper limit time that the host reports the multicast after IGMP inquirer sends the **query** message. If the **report** message is not received after the timer ages, the switch will delete the multicast address.

Perform the following configuration in global configuration mode:

Command	Description
---------	-------------

<b>ip igmp-snooping timer response-time</b> <i>timer_value</i>	Configures the value of Response Time of IGMP-snooping.
<b>no ip igmp-snooping timer response-time</b>	Resumes the default value of Response Time of IGMP-snooping.

**Note:**

The timer value cannot be too small. Otherwise, the multicast communication will be unstable.

The value of Response Time of IGMP-snooping is set to 15 seconds.

### 1.1.10 Configuring Querier of IGMP-Snooping

If the multicast router does not exist in VLAN where IGMP-snooping is activated, the **querier** function of IGMP-snooping can be used to imitate the multicast router to regularly send IGMP **query** message. (The function is global, that is, it can be enabled or disabled in VLAN where IGMP-snooping is globally enabled)

When the multicast router does not exist in LAN and multicast flow does not need routing, the automatic query function of the switch can be activated through IGMP snooping, enabling IGMP snooping to work properly.

Perform the following configuration in global configuration mode:

Command	Description
<b>[no] ip igmp-snooping querier</b> <b>[address</b> <i>[ip_addr]</i>	Configures the querier of IGMP-snooping. The optional parameter <b>address</b> is the source IP address of <b>query</b> 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.

### 1.1.11 Configuring IGMP-snooping's Querier Time Timer

Querier Time Timer is the time interval when switch as local IGMP querier sends messages. Timer broadcasts query message within VLAN after aging.

Configure as following under global configuration mode:

Command	Operation
<b>ip igmp-snooping querier</b> <b>querier-timer</b> <i>timer_value</i>	Configuring the value of IGMP-snooping's Querier Time
<b>no ip igmp-snooping querier</b> <b>querier-timer</b>	Recovering IGMP-snooping's Querier Time as default

By default IGMP-snooping querier is shut down. The default time interval of Query messages is 200 seconds.

**Notice:**

If Querier function is initiated, querier-timer should not be set as too long. In subnet if there are other switches with querier initiated, long querier-timer (longer than other switch's router-age) would lead to the instablization of querier selection in subnet.

### 1.1.12 Configuring data forwarding of IGMP-snooping's forward-l3-to-mrouter to router port

If L3 multicast feature is initiated and igmp-snooping does not join messages to downstream port, only downstream vlan port can be learnt by multicast route. If forward-l3-to-mrouter function is initiated, all the downstream router ports can be learnt. Data messages could be sent to multicast router port registered by PIM-SM message not broadcasting messages to all downstream physical port. The command is mainly used under the following conditions.

When multiple switches initiate L3 multicast cascadingly, the upstream device can only learn downstream vlan ports by multicast router protocol. The upstream and downstream devices do not have interactive igmp messages, therefore, the upstream devices' snooping cannot learn the specific physical ports connected with downstream devices. When upstream devices forward multicast flows, they would send them to all physical port in vlan. When this function is initiated, messages could be forwarded to physical ports which connect with downstream devices, and messages would not be broadcasted in downstream vlan.

Configure as following under global configuration mode:

Command	Operation
[no] ip igmp-snooping forward-l3-to-mrouter	Configuring IGMP-snooping's forward-l3-to-mrouter function.

Under default condition, IGMP-snooping forward-l3-to-mrouter is shut down

**Notice:**

**This command could forward data messages to multicast router port, but switching chip has restraining function on source data port. Therefore, messages would not be forwarded to source data port, but only to downstream router port registered by PIM-SM.**

### 1.1.13 Configuring sensitive mode and value for IGMP-snooping

If IGMP-snooping's sensitive mode is enabled, when port at trunk mode is shut down, set router-age time of mrouter at active status as sensitive value, and send out query message quickly.

Configure as following under global configuration mode:



Command	Operation
[no] ip igmp-snooping sensitive [value [3-30] ]	Configuring IGMP-snooping's sensitive and value could be router-age time of currently active mrouter.

By default IGMP-snooping sensitive is disabled.

**Notice:**

When it is sensitive mode, sensitive value is used to update router-age aiming at current one time period. Next time, route-age is recovered as configured time router-age time.

### 1.1.14 Configuring IGMP-snooping's v3-leave-check function

If IGMP-snooping's v3-leave-check feature is enabled, send special query message after receiving v3's leave message. Otherwise, no operation is processed.

Configure as following under global configuration mode:

Command	Operation
[no] ip igmp-snooping v3-leave-check	Configuring IGMP-snooping's v3-leave-check. Send special query message after receiving v3 leave message..

### 1.1.15 Configuring IGMP-snooping's forward-wrongiif-within-vlan function

If IGMP-snooping's forward-wrongiif-within-vlan function is enabled, do L2 forwarding of the multicast data message received from wrong vlan interface port within source vlan. Forward messages to the group member ports in the vlan. Otherwise, drop messages.

Configure as following under global configuration mode:

Command	Operation
[no] ip igmp-snooping forward-wrongiif- within-vlan	Configuring IGMP-snooping's forward-wrongiif-within-vlan and forwarding relative group member ports within the vlan

By default IGMP-snooping forward-wrongiif-within-vlan is enabled.

**Notice:**

Command ip igmp-snooping forward-wrongiif-within-vlan is only meaningful when L3 multicast is enabled.

### 1.1.16 Configuring IGMP-snooping's IPACL function at port

If IGMP-snooping's IPACL function at port is enabled, use IPACL at port to assign whether messages of some multicast IP address need to be dealt with or ignored.

Configure as following under physical port configuration mode:

Command	Operation
<b>ip igmp-snooping policy</b> <i>word</i>	Adding multicast message's IPACL which need to be dealt with port.
<b>no ip igmp-snooping policy</b>	Deleteding multicast message's IPACL which need to be dealt with port.

### 1.1.17 Configuring maximum multicast IP address quantity function at IGMP-snooping's port

If configuring the maximum multicast IP address quantity at IGMP-snooping port, the quantity of applied groups at the port would be judged whether it is beyond the configured maximum quantity when IGMP-snooping generates forwarding entry. If it is beyond the maximum quantity, the port's entry would not be generated.

Configure as following under physical port configuration mode:

Command	Operation
<b>[no] ip igmp-snooping limit</b> [value [1-2048] ]	configuring the maximum multicast IP address quantity at IGMP-snooping port

By default the maximum quantity is 2048 at IGMP-snooping.

### 1.1.18 Configuring MACACL at IGMP-snooping port

If MACACL function at IGMP-snooping is enabled, use MACAL at port to assign some message whether need to be dealt with or ignored.

Configure as following under physical port configuration mode:

Command	Operation
<b>ip igmp-snooping mac-policy</b> <i>word</i>	Adding multicast message's MACACL which need to be handled by port
<b>no ip igmp-snooping mac-policy</b>	Deleting multicast message's MACACL which has been configured at port

### 1.1.19 Monitoring and Maintaining IGMP-Snooping

Perform the following operations in management mode:

Command	Description
<b>show ip igmp-snooping</b>	Displays IGMP-snooping configuration information.
<b>show ip igmp-snooping timer</b>	Displays the clock information of IGMP-snooping.
<b>show ip igmp-snooping groups</b>	Displays information about the multicast group of IGMP-snooping.
<b>show ip igmp-snooping statistics</b>	Displays statistics information about IGMP-snooping.
<b>[ no ] debug ip igmp-snooping [ packet   timer   event   error ]</b>	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);
```

Display 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
```

Display IGMP-snooping timer:

```
switch#show ip igmp-snooping timers
vlan 1 router age : 251 Indicating the timeout time of the router age timer
vlan 1 multicast address 0100.5e00.0809 response time : 1 Indicating the period from when the
last multicast group query message is received to the current time; if no host on the port
respond when the timer times out, the port will be deleted..
```

Display IGMP-snooping statistics:

```
switch#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  General query of the packet number
special_query_packets:0  Special query of the packet number
join_packets:6     Number of report packets
leave_packets:0    Number of Leave packets
send_query_packets:0  Rserveed statistics option
err_packets:0     Number of incorrect packets
```

Debug the message timer of IGMP-snooping:

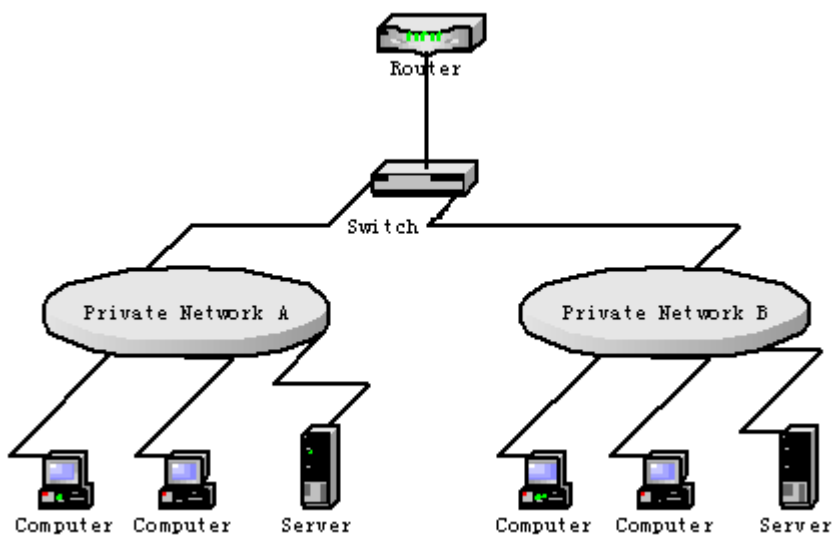
```
switch#debug ip igmp-snooping packet
Jan  1 02:22:28 IGMP-snooping: Receive IGMPv3 report from F0/1, vlan 1:
Jan  1 02:22:28 IGMP-snooping: Flood packet from F0/1 to vlan 1 rc = 0.
Jan  1 02:22:29 IGMP-snooping: Receive IGMPv3 report from F0/1, vlan 1:
Jan  1 02:22:29 IGMP-snooping: Flood packet from F0/1 to vlan 1 rc = 0.
Jan  1 02:22:38 IGMP-snooping: Receive IGMPv3 report from F0/1, vlan 1:
Jan  1 02:22:38 IGMP-snooping: Flood packet from F0/1 to vlan 1 rc = 0.
Jan  1 02:22:39 IGMP-snooping: Receive IGMPv3 report from F0/1, vlan 1:
Jan  1 02:22:39 IGMP-snooping: Flood packet from F0/1 to vlan 1 rc = 0.
Jan  1 02:23:11 IGMP-snooping: Receive IGMPv3 report from F0/1, vlan 1:
Jan  1 02:23:11 IGMP-snooping: Flood packet from F0/1 to vlan 1 rc = 0.
Jan  1 02:23:12 IGMP-snooping: Receive IGMPv3 report from F0/1, vlan 1:
Jan  1 02:23:12 IGMP-snooping: Flood packet from F0/1 to vlan 1 rc = 0.
```

Debug the message timer of IGMP-snooping:

```
switch#debug ip igmp-snooping timer
Jan  1 02:30:36 IGMP-snooping: Vlan 1 router on interface (null) expiry.
Jan  1 02:30:36 IGMP-snooping: Vlan 100 router on interface (null) expiry.
Jan  1 02:30:36 IGMP-snooping: Vlan 200 router on interface (null) expiry.
Jan  1 02:30:36 IGMP-snooping: Vlan 400 router on interface (null) expiry.
Jan  1 02:30:36 IGMP-snooping: Vlan 500 router on interface (null) expiry. Inquering the
response timer expiry
```

### 1.1.20 IGMP-Snooping Configuration Example

Figure 1 shows network connection of the example.



#### 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 Enabling Remote OAM Loopback ..... 5
    - 1.3.3 Configuring OAM Link Monitoring ..... 6
    - 1.3.4 Configuring the Trouble Notification from Remote OAM Entity ..... 8
    - 1.3.5 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

- Supporting Ethernet OAM devices and OAM attributes

The Ethernet OAM connection process is called as the Discovery phase when the OAM entity finds the OAM entity of the remote device and a stable session will be established. During the phase, the connected Ethernet OAM entities report their OAM mode, Ethernet OAM configuration information and local-node-supported Ethernet OAM capacity to each other by interacting the information OAM PDU. If the loopback configuration, unidirectional link detection configuration and link-event configuration have been passed on the Ethernet OAM of the two terminals, the Ethernet OAM protocol will start working on the link layer.

- Link monitoring

The Ethernet OAM conducts the link monitoring through Event Notification OAM PDU. If the link has troubles and the local link monitors the troubles, the local link will transmit 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 the peer terminal must be in active mode.	Yes
Allowing to transmit specified OAM PDU	Yes	Yes

After the Ethernet OAM connection is established, the OAM entities at two terminals maintain connection by transmitting the Information OAM PDU packets. If the Information OAM PDU packet from the peer OAM entity is not received in five seconds, the connection times out and a new OAM connection then requires to be established.

### 1.1.3 Components of the OAM Packet

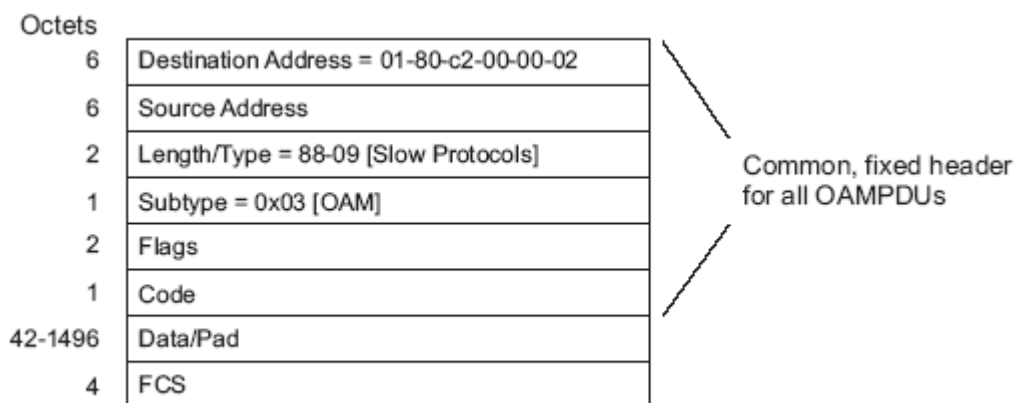


Figure 57-9—OAMPDU frame structure

Figure 1 Components of the OAM packet

The following are the meanings of the fields of the OAM packet:

- Destination address: means the destination MAC address of the Ethernet OAM packet.
- Source address: Source MAC address of the Ethernet OAM packet  
It is the MAC address of the transmitter terminal's port and also a unicast MAC address.
- Length/Type: Always adopts the Type encoding. The protocol type of the Ethernet OAM packet is 0x8809.
- Subtype: The subtype of the protocol for Ethernet OAM packets is 0x03.
- Flags: a domain where the state of Ethernet OAM entity is shown
- Code: a domain where the type of the OAMPDU packet is shown
- Data/Pad: a domain including the OAMPDU data and pad values
- FCS: checksum of the frame

Table 3 Type of the CODE domain

CODE	OAMPDU
00	Information
01	Event Notification
02	Variable Request
03	Variable Response
04	Loopback Control
05-FD	Reserved
FE	Organization Specific
FF	Reserved

The Information OAM PDU packet is used to transmit the information about the state of the OAM entity to the remote OAM entity to maintain the OAM connection.

The Event Notification OAMPDU packet is used to monitor the link and report the troubles occurred on the link between the local and remote OAM entities.

The Loopback control OAMPDU packet is mainly used to control the remote loopback, including the state of the OAM loopback from the remote device. The packet contains the information to enable or disable the loopback function. You can open or shut down the remote loopback according to the contained information.

## 1.2 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
<b>Step1</b>	<b>config</b>	Enters the global configuration mode.
<b>Step2</b>	<b>interface</b> intf-type intf-id	Enters the interface configuration mode.
<b>Step3</b>	<b>ethernet oam</b>	Enables Ethernet OAM on an interface.
<b>Step4</b>	<b>ethernet oam</b> [max-rate oampdus   min-rate seconds   mode {active   passive}   timeout seconds]	Configures optional OAM parameters: <ul style="list-style-type: none"> <li>● The <b>max-rate</b> 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.</li> <li>● The <b>min-rate</b> 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.</li> <li>● The <b>mode {active   passive}</b> 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.</li> <li>● The <b>timeout</b> parameter is used to set the timeout time of the OAM connection. It ranges between 1 and 30 seconds and its default value is 1 second.</li> </ul>

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 Enabling Remote OAM Loopback

The procedure to enable remote loopback on an interface is shown in the following table:

Procedure	Command	Purpose
<b>Step1</b>	<b>config</b>	Enters the global configuration mode.
<b>Step2</b>	<b>interface</b> intf-type intf-id	Enters the interface configuration mode.
<b>Step3</b>	<b>ethernet oam remote-loopback</b>	Configures optional loopback parameters from the

	{supported   timeout seconds}	remote OAM: <ul style="list-style-type: none"> <li>The <b>supported</b> parameter is used to enable an interface to support the remote loopback of Ethernet OAM. Remote loopback is not supported by default.</li> <li>The <b>timeout</b> parameter is used to configure the timeout time of remote loopback. It ranges between 1 and 10 and its default value is 2.</li> </ul>
Step4	exit	Exits from interface configuration mode.
Step5	exit	Exits from the global configuration mode.
Step6	ethernet oam remote-loopback {start   stop} interface intf-type intf-id	Enables or disables remote loopback on an interface.

The remote OAM loopback cannot be enabled on the physical interface that belongs to the aggregation interface.

### 1.3.3 Configuring OAM Link Monitoring

You can configure the low threshold and the high threshold of OAM link monitoring.

The procedure to configure the OAM link monitoring on an interface is shown in the following table:

Procedure	Command	Purpose
Step1	config	Enters the global configuration mode.
Step2	interface intf-type intf-id	Enters the interface configuration mode.
Step3	ethernet oam link-monitor negotiation-supported	Enables link monitoring on an interface. The link monitoring is supported by default.
Step4	ethernet oam link-monitor symbol-period {threshold {high { symbols  none}   low {symbols}}   window symbols}	<p>Sets the high and low threshold of the periodical event of the error signal, which triggers the error link events.</p> <p>The <b>threshold high</b> parameter is used to configure the high threshold. Its unit is signal number. It ranges between 1 and 65535 and its default value is <b>none</b>.</p> <p>The <b>threshold low</b> 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 <b>window</b> 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}	Sets the high and low thresholds of the error frame event, which triggers the link events of error frame.

		<p>The <b>threshold high</b> parameter is used to configure the high threshold. Its unit is signal number. It ranges between 1 and 65535 and its default value is <b>none</b>.</p> <p>The <b>threshold high</b> parameter is used to configure the low threshold. Its unit is signal number. It ranges between 0 and 65535 and its default value is <b>1</b>.</p> <p>The <b>window</b> 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 <b>1</b>.</p>
Step6	<pre>ethernet oam link-monitor frame-period {threshold {high { symbols  none}   low {symbols}}   window symbols}</pre>	<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 <b>threshold high</b> parameter is used to configure the high threshold. Its unit is signal number. It ranges between 1 and 65535 and its default value is <b>none</b>.</p> <p>The <b>threshold high</b> parameter is used to configure the low threshold. Its unit is signal number. It ranges between 0 and 65535 and its default value is <b>1</b>.</p> <p>The <b>window</b> parameter is used to configure the window size of the round-query period. The unit of the window size is the number of the 14881 frames. The window size ranges between 100 and 6000 on a 1000M Ethernet interface and its default value is 100 in this case, while the window size ranges between 10 and 600 on a 100M Ethernet interface and its default value is 10 in this case.</p>
Step7	<pre>ethernet oam link-monitor frame-seconds {threshold {high { symbols  none}   low {symbols}}   window symbols}</pre>	<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 <b>threshold high</b> parameter is used to configure the high threshold. Its unit is signal number. It ranges between 1 and 900 and its default value is <b>none</b>.</p> <p>The <b>threshold low</b> parameter is used to configure the low threshold. Its unit is signal number. It ranges between 0 and 900 and its default value is <b>1</b>.</p> <p>The <b>window</b> 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 <b>60</b>.</p>
Step8	<pre>ethernet oam link-monitor receive-crc {threshold {high { symbols  none}   low {symbols}}   window symbols}</pre>	<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 <b>threshold high</b> parameter is used to configure the high threshold. Its unit is signal number. It ranges between 1 and 65535 and its default value is <b>none</b>.</p> <p>The <b>threshold high</b> parameter is used to configure the low threshold. Its unit is signal number. It ranges</p>

		between 0 and 65535 and its default value is 1.  The <b>window</b> 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.
--	--	---

### 1.3.4 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
<b>Step1</b>	<b>config</b>	Enters the global configuration mode.
<b>Step2</b>	<b>interface</b> intf-type intf-id	Enters the interface configuration mode.
<b>Step3</b>	<b>ethernet oam remote-failure</b> <b>{critical-event   dying-gasp  </b> <b>link-fault} action</b> <b>error-disable-interface</b>	Configures the trigger action of a remote OAM trouble on an interface: <ul style="list-style-type: none"> <li>● The <b>critical-event</b> parameter is used to enable an interface to enter the <b>errdisabled</b> state when an undesignated critical event occurs.</li> <li>● The <b>dying-gasp</b> parameter is used to enable the local interface to enter the <b>errdisabled</b> 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 <b>errdisabled</b> state or if the OAM function on the remote interface which connects the local interface is shut down by the administrator.</li> <li>● The <b>link-fault</b> parameter is used to enable an interface to enter the <b>errdisabled</b> state when the receiver detects signal loss.</li> </ul>

Our switch cannot generate the LINK FAULT packets and the Critical Event packets. However, these packets will be handled if they are received from the remote terminal. Our router can transmit and receive the Dying Gasp packet. When the local port enters the **errdisabled** state or is closed by the administrator or the OAM function of the local port is closed by the manager, the Dying Gasp packet will be transmitted to the remote terminal that connects the local port.

### 1.3.5 Displaying the Information About OAM Protocol

Table 4 Displaying the information about OAM protocol

Command	Purpose
<b>show ethernet oam discovery interface</b> <b>[intf-type intf-id]</b>	Displays the OAM discovery information on all interfaces or

	a designated interface.
<b>show ethernet oam statistics {pdu   link-monitor   remote-failure} interface [intf-type intf-id]</b>	Displays the OAM statistics information on all interfaces or a designated interface. <ul style="list-style-type: none"> <li>• The <b>pdu</b> parameter is used to classify and count the OAM packets according to the code-domain value of the OAM packet.</li> <li>• The <b>link-monitor</b> parameter is used to display the detailed statistics information of normal link events.</li> <li>• The <b>remote-failure</b> parameter is to display the detailed statistics information about the remote trouble.</li> </ul>
<b>show ethernet oam configuration interface [intf-type intf-id]</b>	Displays the OAM configuration information on all interfaces or a designated interface.
<b>show ethernet oam runtime interface [intf-type intf-id]</b>	Displays the OAM running information on all interfaces or a designated interface.

## 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 A:

```
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 B:

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.

# IEEE1588 Transparent Clock Configuration

## Table of Contents

Chapter 1	Configuring IEEE1588 Transparent Clock .....	1
1.1	Task List for IEEE1588 Transparent Clock Configuration .....	1
1.2	Tasks for IEEE1588 Transparent Clock Configuration .....	1
1.2.1	Enabling the Transparent Clock.....	1
1.2.2	Creating the Transparent Clock Port .....	2
1.2.3	Configuring the Link Delay Calculation Mode.....	2
1.2.4	Configuring the Forwarding Mode of Sync Packets.....	2
1.2.5	Configuring the Domain Filtration Function .....	3
1.2.6	Setting the Transmission Interval of Pdelay_Req Packets .....	3
1.3	PTP TC Configuration Example .....	4

# Chapter 1 Configuring IEEE1588 Transparent Clock

## 1.1 Task List for IEEE1588 Transparent Clock Configuration

Enabling the Transparent Clock

Creating the Transparent Clock Port

Configuring the Link Delay Calculation Mode

Configuring the Forwarding Mode of Sync Packets

Configuring the Domain Filtration Function

Setting the Transmission Interval of Pdelay\_Req Packets

## 1.2 Tasks for IEEE1588 Transparent Clock Configuration

### 1.2.1 Enabling the Transparent Clock

The IEEE1588 transparent clock is an intermediate device to connect the master and slave clocks. The IEEE1588 transparent clock can effectively reduce time synchronization interference caused by switch's delay processing and ensure ns-level time synchronization by verifying the dwell time when sync packets pass through the transparent clock.

In global configuration mode, run the following command to enable the transparent clock:

Command	Purpose
<b>ptp enable</b>	Enables the PTP transparent clock.

In global configuration mode, run the following command to shut down the transparent clock and delete all already added PTP ports:

Command	Purpose
<b>no ptp enable</b>	Closes the PTP transparent clock.

The IEEE1588 clock synchronization protocol is independent from the underneath level protocols. It is based on either Ethernet or IPv4/UDP. To enable the transparent clock to transmit and receive IPv4- or UDP-based packets, you have to enable PTP in L3 port mode.

Run the following command in L3 port mode to enable PTP:

Command	Purpose
<b>ptp enable</b>	Enables the PTP transparent clock.

## 1.2.2 Creating the Transparent Clock Port

The transparent clock can include multiple PTP ports to connect the master and slave clock respectively.

Run the following commands in port configuration mode to create the PTP ports:

Command	Purpose
<b>ptp start I2</b>	Creates the PTP L2 port.
<b>Ptp start I3</b>	Creates the PTP L3 port.

Run the following command in port configuration mode to delete the PTP ports:

Command	Purpose
<b>no ptp start</b>	Delete the PTP port.

## 1.2.3 Configuring the Link Delay Calculation Mode

The PTP transparent clock supports two link delay modes (E2E and P2P) to help the master and slave clocks switch between the two modes, among which P2P is the default mode. In E2E mode, TC can process **Delay\_Req,Delay\_Resp** packets; In P2P mode, the path-delay mechanism is running on each PTP port, the Pdelay\_Req packets are transmitted periodically, and the **Pdelay\_Resp** and **Pdelay\_Resp\_Follow\_Up** packets are responded to. The two modes are incompatible with each other. For example, if it is in P2P mode, the **Delay\_Req** packets received from the clock will be dropped.

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

Command	Purpose
<b>ptp delay-mechanism e2e</b>	Sets TC to work in E2E mode.

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

Command	Purpose
<b>ptp delay-mechanism p2p</b>	Sets TC to work in P2P mode.

## 1.2.4 Configuring the Forwarding Mode of Sync Packets

There are two ways to forward Sync packets: straight forwarding and store-forward.

In straight forwarding mode, the PTP port immediately forwards after receiving Sync packets, re-encapsulates the Follow\_UP packets after receiving them and then forwards them out from the corresponding port.

In store-forward mode, the PTP port shall not forward Sync packets after receiving them but store them first, receive corresponding Follow\_up packets and then forward the two kinds of packets together.

The straight forwarding mode is the default one. In this mode, the time to handle Sync packets is apparently less than the time to handle Follow\_up packets and hence in case of multi-level TC cascading the risk of packet disorder arises.

That's why the store-forward mode is recommended in case of multi-level TC cascading. However, in normal cases, we recommend the straight forwarding mode for it can lessen the residence time of Sync packets at the maximum level and reduce its impact on time synchronization.

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

Command	Purpose
<b>ptp sync-mechanism store-forward</b>	Sets the forwarding method of <b>Sync</b> packets to <b>store-forward</b> .

To switch the forwarding mode over to straight forwarding, run the following command in global configuration mode:

Command	Purpose
<b>ptp sync-mechanism straight-forward</b>	Sets the forwarding method of <b>Sync</b> packets to <b>store-forward</b> .

### 1.2.5 Configuring the Domain Filtration Function

PTP devices can be classified through their domains for only PTP clocks in the same domain can exchange PTP synchronization packets and PTP devices in different domains cannot conduct time synchronization. After the domain filtration function is enabled, the PTP packets in other domains are dropped; if domain filtration is disabled, TC will not conduct the domain checkup.

Before domain filtration, you have to set the domain in which the PTP port is located. Run the following command in port mode:

Command	Purpose
<b>ptp domain <i>number</i></b>	Sets the domain to which the PTP port belongs. The default domain of this port is domain0.

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

Command	Purpose
<b>ptp domain-filter</b>	Enables domain filtration, which is enabled by default.

Run the following command in global mode to shut down domain filtration:

Command	Purpose
<b>no ptp domain-filter</b>	Closes domain filtration.

### 1.2.6 Setting the Transmission Interval of Pdelay\_Req Packets

During the path-delay process, you can set the transmission interval of Pdelay\_Req packets.

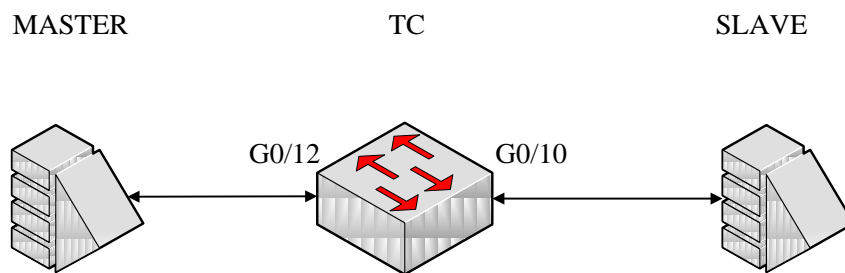


Run the following command to configure the transmission frequency.

Command	Purpose
<code>ptp pdelay-interval <i>time</i></code>	<b>time</b> stands for the transmission interval, which ranges from -4 to 4. The actual transmission interval is <i>time</i> powers of 2. For example, if <i>time</i> is 0, the actual transmission interval is 1 second.

### 1.3 PTP TC Configuration Example

See the following figure:



**MASTER** here stands for the master clock, which is a L2 PTP device. **SLAVE** here stands for the master clock, which is a L3 PTP device. TC stands for a switch that supports transparent clock. The master clock connects port g0/12 of the switch, while the slave clock connects port g0/10 of the switch. MASTER, TC and SLAVE are all working in P2P mode. Ports g0/10 and G0/12 belong to VLAN1.

#### Global configuration

```
ptp enable
ptp delay-mechanism p2p
```

#### Configuration of L3 port

```
Ip add 192.168.0.2 255.0.0.0
ptp enable
```

#### Configuration of port g0/10

```
ptp start I2
```

#### Configuration of port g0/12

```
ptp start I3
```

## Layer 2 Tunnel Protocol Configuration

# Table of Contents

Chapter 1 Configuring Layer 2 Protocol Tunnel .....	1
1.1 Introduction.....	1
1.2 Configuring Layer 2 Protocol Tunnel .....	1
1.3 Configuration Example of Layer 2 Protocol Tunnel .....	1

## Chapter 1 Configuring Layer 2 Protocol Tunnel

### 1.1 Introduction

Layer 2 protocol tunnel allows users between two sides of the switch to transmit the specified layer 2 protocol on their own network without being influenced by the relevant layer 2 software module of the switch. The switch is a transparent media for users.

### 1.2 Configuring Layer 2 Protocol Tunnel

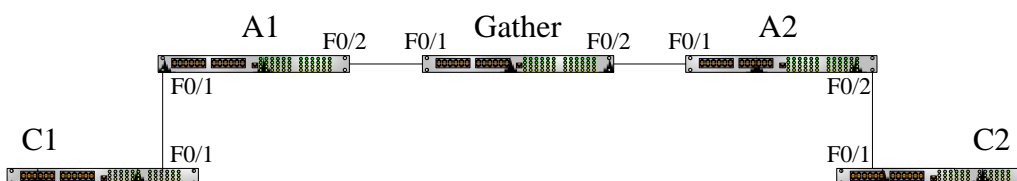
Use command line on the interface of the switch to configure tunnel function of the layer 2 protocol. The configuration steps are as follows:

command	description
<b>config</b>	Enters global configuration mode.
<b>interface</b> <intf_name>	Enters interface configuration mode of the switch. Only the switch port supports layer 2 protocol tunnel (including physical port and aggregation port).
[no] <b>l2protocol-tunnel</b> [stp]	Enables layer 2 protocol of the tunnel function. Currently we only support tunnel function of stp protocol.
<b>no spanning-tree</b>	Disables the spanning tree protocol on the port
<b>exit</b>	Returns to the global mode

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 Configuration Example of Layer 2 Protocol Tunnel

Network environment is as follows:



A1/A2/Gather belong to core network, C1/C2 are switches distributed in two places. Customer wants to combine two of its network to one , that is, the core network is a transparent transmission channel for the customer. If user wants to realize the transparent transmission of STP, then the following configurations should be configured on each switch:

- (1) The g0/2 of Switch A1, g0/1 and g0/2 of Gather, g0/1 of A2 should be configured to trunk mode.
- (2) The f0/1 of switch A1, f0/2 of A2 should be configured to Access, and enables tunnel function of the STP protocol.

# Loopback Detection Configuration

## Table of Contents

Chapter 1 Setting Loopback Detection .....	1
1.1 Intro of Loopback Detection.....	1
1.1.1 Format of Loopback Detection Packet.....	1
1.2 Loopback Detection Configuration Tasks .....	2
1.3 Setting Loopback Detection.....	2
1.3.1 Configuring Loopback Detection Globally.....	2
1.3.2 Configuring Port Loop Check .....	3
1.3.3 Configuring a Port to Conduct Loopback Detection in Specified VLAN .....	3
1.3.4 Configuring the Loopback Detection Interval of Port (Packet transmission interval, controlled port recovery time) .....	3
1.3.5 Configuring Port Control.....	4
1.3.6 Configuring the Destination MAC Address of Loopback Detection Packet .....	4
1.3.7 Configuring Loopback to Exist on a Port by Default.....	4
1.3.8 Displaying the Configuration of Global Loopback Detection.....	5
1.3.9 Displaying the Configuration of Port Loopback Detection .....	5
1.4 Configuration Example .....	5

# Chapter 1 Setting Loopback Detection

## 1.1 Intro of Loopback Detection

The loopback in a network may trigger the repeated transmission of broadcast, multicast or unicast packets, wasting network resources and even leaving network breakdown. To avoid the above-mentioned troubles, it is necessary to provide a detection mechanism to promptly notify users of detecting network connection and configuration at the occurrence of loopback and to take troubled ports under control. Loopback detection can check whether loopback happens on a port of a to-be-tested device by transmitting a detection packet from this port and checking whether this packet can be received still on this port. When the device finds that loopback exists on its port, it can transmit alarm promptly to the network management system for administrators to detect network problems in time; thus, long time of network disconnection can be prevented. Moreover, loopback detection is capable of having ports under control. You can opt for port block, port MAC-learning forbidding or error-disable according to actual requirements to make corresponding ports under control and lessen the loopback's network influence to the minimum level.

Our switches support loopback detection in the following aspects:

- Supporting to set loopback detection on the port
- Supporting to set the destination MAC address for loopback detection packets
- Supporting to conduct loopback detection to at most 10 specified ports
- Supporting to set the transmission interval of loopback detection packets and the recovery time of controlled port
- Supporting to control port, including port block, port MAC-learn forbidding, and error-disable
- Supporting to set whether loopback exists on a port by default

### 1.1.1 Format of Loopback Detection Packet

Field	Length/Byte	Value
DMAC	6	0x0180C2B0000A (default value, configurable)
SMAC	6	MAC address of the switch
TPID	2	0x8100, VLAN tag type
TCI	2	Specific value of the VLAN tag, priority,



		VLAN ID
TYPE	2	Protocol type, which ranges from 0 to 9001
CODE	2	Protocol sub-type, which represents loopback detection and is 0x0001
VERSION	2	0x0000 (currently reserved)
Length	2	0x0008, length of the header of loopback detection packet
RESERVE	2	Reserved field
SYSMAC	6	MAC address of the switch
SEQUENCE	4	Sequence ID of packet, which is generated randomly by the system before the packet is transmitted
DiID	4	Port ID, which is the ID of the global port of 85 Series
End	2	0x0000, end character

## 1.2 Loopback Detection Configuration Tasks

- Configuring Loopback Detection Globally
- Configuring Port Loopback Detection
- Setting a Port to Perform Loopback Detection toward Specified VLAN
- Configuring the Loopback Detection Interval on a Port
- Setting a Port under Control
- Setting Loopback to Exist on a Port by Default
- Displaying the Configuration of Global Loopback Detection
- Displaying the Information about the Loopback Detection Port

## 1.3 Setting Loopback Detection

### 1.3.1 Configuring Loopback Detection Globally

Enabling or disabling loopback detection globally means enabling or disabling loopback detection on all physical ports. Global configuration is just like a switch. Only when this switch is opened can enabled loopback detection on a port take effect.

Command	Purpose
<b>[no] loopback-detection</b>	Sets loopback detection globally.

### 1.3.2 Configuring Port Loop Check

If you want to enable or disable loopback detection on a specified port, you should first enable loopback detection globally.

Command	Purpose
<b>[no] loopback-detection enable</b>	Configures port loopback detection.

### 1.3.3 Configuring a Port to Conduct Loopback Detection in Specified VLAN

If you set loopback detection in a specified VLAN, a port shall transmit multiple detection packets with specified VLAN tag regularly and the port can transmit up to 10 detection packets with specified VLAN tag.

One point to be noted is that the port must exist in the specified VLAN, or the configuration takes no effect. If loopback detection happens in VLAN2 to VLAN8, ports are configured to be in trunk mode, and trunk vlan-allowed is vlans 5-8, the packets with tags 2-4 transmitted by the switch cannot pass through this port and the configuration hence takes no effect.

Command	Purpose
<b>[no] loopback-detection vlan-control <i>vlanlist</i></b>	Configures a port to conduct loopback detection in specified VLAN.

### 1.3.4 Configuring the Loopback Detection Interval of Port (Packet transmission interval, controlled port recovery time)

Command	Purpose
<b>[no] loopback-detection hello-time <i>time</i></b>	Configures the transmission interval of port loopback detection packets.

Because a network is always changeable, loopback detection is a continuous process. The port will transmit loopback detection packets in a regular time. This regular time is called as the transmission interval of loopback detection packets. The default transmission interval of the system is 3 seconds.

Command	Purpose
<b>[no] loopback-detection recovery-time <i>time</i></b>	Configures the transmission interval of port loopback detection packets.

This command above is used to set the automatic recovery time of a port when loopback disappears. In default settings, if a port has not received the already transmitted loopback detection packet within 10 seconds, it is regarded that loopback vanishes. It is recommended to set the recovery time to be triple of the packet transmission time; if the transmission time is set to be a very small value, you'd better set the recovery time to be at least 10 seconds longer than the transmission time.

### 1.3.5 Configuring Port Control

Command	Purpose
<b>[no] loopback-detection control</b> <b>{block learning shutdown}</b>	Configures port control.

When a port detects that loopback exists in its network, you can set port control to manage this port. The control state of a port can be **block**, **nolearn**, **shutdown** or **trap**. When any control state is set and loopback exists on a port, the trap alarm message will be transmitted. It is not configured by default.

When loopback detection is enabled globally, a loopback detection packet is transmitted from a port, on which loopback detection is enabled, and received again by this port, the port may get the following four control actions:

**Block:** When loopback is found, this port is then isolated from other ports. Hence the packets entering this port cannot be forwarded to other ports. The port is then in protocol down state and its MAC address table list ages.

**Nolearn:** means to forbid the port to learn MAC addresses. When loopback is detected, the port will not conduct MAC address learning any more and at the same time the MAC address table of this port ages.

**shutdown:** Means to close the port. When loopback is detected, except that trap message will be transmitted and the port's MAC address table ages, the port will be automatically closed and it cannot forward packets any more until the err-disable-recover time.

**Trap:** It means that the port only reports alarm. When loopback is detected, the port only reports alarm and ages its MAC address table without any further action.

When the port is in block state, it cannot forward incoming packets and at the same time it transmits loopback detection packets continuously. When loopback disappears, the port will recover automatically. In default settings, if a port has not received the already transmitted loopback detection packet within 10 seconds, it is regarded that loopback vanishes.

In block state, the port protocol is down; in shutdown state, the port's link is down directly.

### 1.3.6 Configuring the Destination MAC Address of Loopback Detection Packet

Command	Purpose
<b>[no] loopback-detection dest-mac</b> <i>Mac-address</i>	Configures the destination MAC address of loopback detection packet.

The default destination MAC address of loopback detection packet is **01-80-C2-00-00-0a**. If you have set other destination MAC, it will be used as the destination MAC address of loopback detection packet.

### 1.3.7 Configuring Loopback to Exist on a Port by Default

Command	Purpose
<b>[no] loopback-detection existence</b>	Configures loopback to exist on a port by default.

When a port is up and port loopback detection takes effect, the command above is used to set whether loopback exists on this port. When a port is in shutdown state, this

port is not suitable to set to have loopback, for the port in shutdown state cannot forward packets. The default settings is that loopback does not exist in a port.

### 1.3.8 Displaying the Configuration of Global Loopback Detection

Command	Purpose
<b>show loopback-detection</b>	Displays the configuration of global loopback detection.

This command is used to display the information about global loopback detection configuration, including global configuration, whether loopback exists on each port, and some ports' configurations.

### 1.3.9 Displaying the Configuration of Port Loopback Detection

Command	Purpose
<b>show loopback-detection interface <i>intf</i></b>	Displays the configuration of port loopback detection.

This command is mainly used to display port loopback detection, including the port timer and the information about transmitted and received packets.

## 1.4 Configuration Example

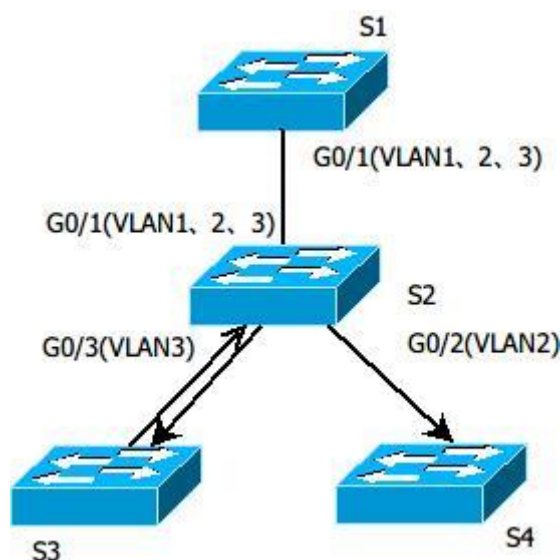


Figure 1.1 Loopback detection configuration

As shown in figure 1.1, the port of S1 conducts loopback detection to specified VLANs 1, 2 and 3. The corresponding configurations on all switches are shown below:

Switch S1:

Configuration of 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:
Configuration of interface GigaEthernet0/1:
  switchport mode trunk
Configuration of interface GigaEthernet0/2:
  switchport mode trunk
Configuration of interface GigaEthernet0/3:
  switchport mode trunk
Global Configuration
vlan1-3
```

```
Switch S3:
Configuration of interface GigaEthernet0/1:
  switchport pvid 3
```

If loopback exists in the network that S3 connects and the PVID of the interface, on which loopback exists, is 3, the packets will be transmitted to interface g0/1 of S1 and S1 will block interface g0/1 after finding loopback.

# 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 Network Interface .....	2
1.3.2 Configuring Multiple IP Addresses on 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 Introduction .....	7
2.1.1 DHCP Applications .....	7
2.1.2 DHCP Advantages .....	7
2.1.3 DHCP Terminology .....	8
2.2 Configuring DHCP Client .....	8
2.2.1 DHCP Client Configuration Tasks .....	8
2.2.2 DHCP Client Configuration Tasks .....	8
2.2.3 DHCP Client Configuration Example .....	10
Chapter 3 IP Service Configuration .....	11
3.1 Configuring IP Service .....	11
3.1.1 Managing IP Connection .....	11
3.1.2 Configuring Performance Parameters .....	13
3.1.3 Detecting and Maintaining IP Network .....	13
3.2 Configuring Access List .....	15
3.2.1 Filtering IP Message .....	15
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 .....	17
3.3 Configuring IP Access List Based on Physical Port .....	18
3.3.1 Filtering IP Message .....	18
3.3.2 Creating Standard and Extensible IP Access List .....	18
3.3.3 Applying the Access List to the Interface .....	19
3.3.4 Extensible Access List Example .....	20

# Chapter 1 Configuring IP Addressing

## 1.1 IP Introduction

### 1.1.1 IP

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

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

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

## 1.2 Configuring IP Address Task List

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

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

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

Followed is an IP address configuration task list:

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



## 1.3 Configuring IP Address

### 1.3.1 Configuring IP Address at Network Interface

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

Type	Address or Range	State
A	0.0.0.0	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	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:

Run...	To...
<b>ip address</b> <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 switches only support masks which are continuously set from the highest byte according to the network character order.

### 1.3.2 Configuring Multiple IP Addresses on Network Interface

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

- If IP addresses in a network segment are insufficient.

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

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

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

**Note:**

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

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

Run...	To...
<b>ip address</b> <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 826 and 1027 respectively.

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

- Defining a static ARP cache

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

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

Run one of the following commands in global configuration mode:

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

Run the following command in interface configuration mode:

Run...	To...
<b>arp timeout</b> <i>seconds</i>	Set the timeout time of the ARP cache item in the ARP cache.
<b>arp dynamic</b>	Set arp dynamic learning on 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 items 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:

Run...	To...
--------	-------

<b>arp send-gratuitous</b>	Start up free ARP message transmission on the interface.
<b>arp send-gratuitous interval</b> <i>value</i>	Set the interval for sending free ARP message on the interface. The default value is 120 seconds.

- Sets the maximum retransmissions of the Re-Detect packets.

To ensure the accuracy of the hardware subnet routing information, the ARP entries (tagged with G) need to be re-detect. The greater the retransmissions, the more likely the re-detection succeeds.

Run...	To...
<b>arp max-gw-retries</b> <i>number</i>	To set the maximum retransmissions of the Re-Detect packets. The default is 3.

- To set whether to carry on redetection at the aging of ARP entries (not just meaning the gateway-related ARP entries), run the following command:

Run...	To...
<b>arp retry-allarp</b>	To set whether to re-detect all ARP entries in aging.

## 2. Mapping host name to IP address

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

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

Run...	To...
<b>ip host</b> <i>name address</i>	Statically map the host name to the IP address.

### 1.3.4 Detecting and Maintaining IP Addressing

Perform the following operations to detect and maintain the network:

#### 1. Clearing cache, list and database

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

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

Run...	To...
<b>clear arp-cache</b>	Clear the IP ARP cache.

## 2. Displaying statistics data about system and network

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

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

Run the following commands in management mode:

Run...	To...
<b>show arp</b>	Display content in the ARP table.
<b>show hosts</b>	Display the cache table about hostname-to-IP mapping.
<b>show ip interface</b> [ <i>type number</i> ]	Display the interface state.
<b>ping</b> { <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 VLAN 11.

```
interface vlan 11
ip address 202.96.2.3 255.255.255.0
```

## Chapter 2 Configuring DHCP

### 2.1 Introduction

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

- Automatic distribution

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

- Dynamic distribution

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

- Manual distribution

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

#### 2.1.1 DHCP Applications

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

- You can distribute IP address, network segment and related sources (such as relevant gateway) to an Ethernet interface by configuring the DHCP client.
- When a switch that can access DHCP connects multiple hosts, the switch can obtain an IP address from the DHCP server through the DHCP relay and then distribute the address to the hosts.

#### 2.1.2 DHCP Advantages

In current software version, the DHCP client or the DHCP client on the Ethernet interface is supported. The function to support the DHCP client has the following advantages:

- Reducing the configuration time
- Reducing configuration faults
- Controlling IP addresses of some device ports through the DHCP server

### 2.1.3 DHCP Terminology

DHCP is based on the Server/Client model. The DHCP-server and DHCP-client exist in the DHCP running conditions.

- DHCP-Server

It is a device to distribute and recycle the DHCP-related sources such as IP addresses and lease time.

- DHCP-Client

It is a device to obtain information from the DHCP server for devices of the local system to use, such as IP address information.

As described above, the lease time is a concept appearing in the procedure of DHCP dynamic distribution.

- Lease time—an effective period of an IP address since its distribution. When the effective period is over, the IP address is to be recycled by the DHCP server. To continuously use the IP address, the DHCP client requires re-applying the IP address.

## 2.2 Configuring DHCP Client

### 2.2.1 DHCP Client Configuration Tasks

- 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.

Run...	To...
<b>ip address dhcp</b>	Specify the DHCP protocol to configure the IP address of the Ethernet interface.

## 2. Specifying an address for DHCP server

If the addresses of some DHCP servers are known, you can specify the addresses for these DHCP servers on the switch to reduce protocol interaction time. Run the following command in global configuration mode:

Run...	To...
<b>ip dhcp-server</b> <i>ip-address</i>	Specify the IP address of the DHCP server.

The command is optional when you perform operations to obtain an IP address.

## 3. Configuring DHCP parameters

You can adjust the parameters for the DHCP protocol interaction according to requirements. Run the following commands in global configuration mode:

Run...	To...
<b>ip dhcp client minlease</b> <i>seconds</i>	Specify the minimum lease time.
<b>ip dhcp client retransmit</b> <i>count</i>	Specify the times of resending protocol message.
<b>ip dhcp client select</b> <i>seconds</i>	Specify the interval for SELECT.
<b>ip dhcp client class_identifier</b> <i>WORD</i>	Specify the provider code number.
<b>ip dhcp client client_identifier</b> <i>hrd_ether</i>	Specify the Ethernet type as the client ID.
<b>ip dhcp client timeout_shut</b>	Specify the timeout of the client.
<b>ip dhcp client bootfileaddmac</b>	Enable DHCP file name to add MAC of the client.
<b>ip dhcp client tftpdnload</b>	Enable TFTP download function.
<b>ip dhcp client retry_interval</b> <i>minutes</i>	Configure the retransmission interval of the protocol packets.

The command is optional when you perform operations to obtain an IP address.

## 4. Monitoring DHCP

To check information about DHCP-server currently found by switch, run the following command in management mode:

Run...	To...
<b>show dhcp server</b>	Display information about the DHCP server known by the routing switch.

Run the following command in management mode to check the IP address currently used by the routing switch:

Run...	To...
<b>show dhcp lease</b>	Display the IP address resources currently used by the routing switch and relevant information.



Additionally, if the DHCP protocol is used to distribute an IP address for an Ethernet interface, you can run **show interface** to check whether the IP address required by the Ethernet interface is successfully obtained.

### 2.2.3 DHCP Client Configuration Example

#### 1. Obtaining an IP address

The following example shows Ethernet1/1 obtains an IP address through DHCP.

```
!  
interface vlan 11  
ip address dhcp
```

## Chapter 3 IP Service Configuration

It is to describe how to configure optional IP service. For the details of the IP service commands, refer to section "IP Service Commands".

### 3.1 Configuring IP Service

Optional IP service configuration tasks are listed as follows:

- Managing IP connection
- Configuring performance parameters
- Configuring default gateway
- Detecting and maintaining IP network

The above operations are not mandatory. You can perform the operations according to your requirements.

#### 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.

Run...	To...
<b>ip unreachable</b>	Enable the function to send an ICMP-unreachable message.

##### 2. Sending ICMP mask response message

Sometimes the host must know the network mask. To get the information, the host can send the ICMP mask request message. If the routing switch can confirm the mask of

the host, it will respond with the ICMP mask response message. By default, the routing switch can send the ICMP mask response message.

To send the ICMP mask request message, run the following command in interface configuration mode:

Run...	To...
ip mask-reply	Send the ICMP mask response message.

### 3. 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.

### 4. Setting IP maximum transmission unit

All interfaces have a default IP maximum transmission unit (MTU), that is, the transmissible maximum IP message length. If the IP message length exceeds MTU, the routing switch segments the message.

Changing the MTU value of the interface is to affect the IP MTU value. If IP MTU equals to MTU, IP MTU will automatically adjust itself to be the same as new MTU as MTU changes. The change of IP MTU, however, does not affect MTU. IP MTU cannot bigger than MTU configured on the current interface. Only when all devices connecting the same physical media must have the same MTU protocol can normal communication be created.

To set IP MTU on special interface, run the following command in interface configuration mode:

Run...	To...
ip mtu <i>bytes</i>	Set IP MTU of the interface.

## 5. Authorizing IP source route

The routing switch checks the IP header of every message. The routing switch supports the IP header options defined by RFC 791: strict source route, relax source route, record route and time stamp. If the switch detects that an option is incorrectly selected, it will send message about the ICMP parameter problem to the source host and drop the message. If problems occur in the source route, the routing switch will send ICMP unreachable message (source route fails) to the source host.

IP permits the source host to specify the route of the IP network for the message. The specified route is called as the source route. You can specify it by selecting the source route in the IP header option. The routing switch has to forward the IP message according to the option, or drop the message according to security requirements. The routing switch then sends ICMP unreachable message to the source host. The routing switch supports the source route by default.

If the IP source route is disabled, run the following command in global configuration mode to authorize the IP source route:

Run...	To...
ip source-route	Authorizing IP source route.

### 3.1.2 Configuring Performance Parameters

#### 1. Setting the wait time for TCP connection

When the routing switch performs TCP connection, it considers that the TCP connection fails if the TCP connection is not created during the wait time. The routing switch then notifies the upper-level program of the failed TCP connection. You can set the wait time for TCP connection. The default value of the system is 75 seconds. The previous configuration has no impact on TCP connections that the switch forwards. It only affects TCP connections that are created by the switch itself.

Run the following command in global configuration mode to set the wait time for TCP connections:

Run...	To...
ip tcp synwait-time <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:

Run...	To...
ip tcp window-size <i>bytes</i>	Set the size of TCP windows.

### 3.1.3 Detecting and Maintaining IP Network

### 1. Clearing cache, list and database

You can clear all content in a cache, list or database. Incorrect data in a cache, list or database need be cleared.

Run the following command to clear incorrect data:

Run...	To...
<b>clear tcp statistics</b>	Clear TCP statistics data.

### 2. Clearing TCP connection

To disconnect a TCP connection, run the following command:

Run...	To...
<b>clear tcp</b> { <b>local</b> host-name port <b>remote</b> host-name port   <b>tcb</b> address}	Clear the designated TCP connection. TCB refers to TCP control block.

### 3. Displaying statistics data about system and network

The system can display the content in the cache, list and database. These statistics data can help you know the usage of systematic sources and solve network problems.

Run the following commands in management mode. For details, refer to "IP Service Command".

Run...	To...
<b>show ip access-lists</b> <i>name</i>	Display the content of one or all access lists.
<b>show ip sockets</b>	Display all socket information about the routing switch.
<b>show ip traffic</b>	Display statistics data about IP protocol.
<b>show tcp</b>	Display information about all TCP connection states.
<b>show tcp brief</b>	Briefly display information about TCP connection states.
<b>show tcp statistics</b>	Display TCP statistics data.
<b>show tcp tcb</b>	Display information about the designated TCP connection state.

### 4. Displaying debugging information

When problem occurs on the network, you can run **debug** to display the debugging information.

Run the following command in management mode. For details, refer to "IP Service Command".

Run...	To...
--------	-------

<b>debug arp</b>	Display the interaction information about ARP.
<b>debug ip icmp</b>	Display the interaction information about ICMP.
<b>debug ip raw</b>	Display the information about received/transmitted IP message.
<b>debug ip packet</b>	Display the interaction information about IP.
<b>debug ip tcp</b>	Display the interaction information about TCP.
<b>debug ip udp</b>	Display the interaction information about UDP.

## 3.2 Configuring Access List

### 3.2.1 Filtering IP Message

Filtering message helps control the movement of packet in the network. The control can limit network transmission and network usage through a certain user or device. To make packets valid or invalid through the crossly designated interface, our routing switch provides the access list. The access list can be used in the following modes:

- Controlling packet transmission on the interface
- Controlling virtual terminal line access
- Limiting route update content

The section describes how to create IP access lists and how to use them.

The IP access list is an orderly set of the **permit/forbid** conditions for applying IP addresses. The ROS software of our switch tests the address one by one in the access list according to regulations. The first match determines whether the ROS accepts or declines the address. After the first match, the ROS software terminates the match regulations. The order of the conditions is, therefore, important. If no regulations match, the address is declined.

Use the access list by following the following steps:

- (1) Create the access list by designating the access list name and conditions.
- (2) Apply the access list to the interface.

### 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:

Run...	To...
<b>ip access-list standard</b> <i>name</i>	Use a name to define a standard access list.
<b>deny</b> { <i>source [source-mask]   any</i> }[ <b>log</b> ] or <b>permit</b> { <i>source [source-mask]   any</i> }[ <b>log</b> ]	Designate one or multiple <b>permit/deny</b> conditions in standard access list configuration mode. The previous setting decides whether the packet is approved or disapproved.
Exit	Log out from the access list configuration mode.

Run the following command in global configuration mode to create an extensible access list.

Run...	To...
<b>ip access-list extended</b> <i>name</i>	Use a name to define an extensible IP access list.
{ <b>deny</b>   <b>permit</b> } <i>protocol source source-mask destination destination-mask [precedence precedence] [tos tos] [established] [log]{deny   permit} protocol any any</i>	Designate one or multiple <b>permit/deny</b> conditions in extensible access list configuration mode. The previous setting decides whether the packet is approved or disapproved.  <b>precedence</b> means the priority of the IP packet; <b>TOS</b> 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.

Run...	To...
<b>ip access-group</b> <i>name</i> { <b>in</b>   <b>out</b> }	Apply the access list to the interface.

The access list can be used on the **in** interfaces and the **out** interfaces. For the standard access list of the **in** interface, the source address of the packet is to be

checked according to the access list after the packet is received. For the extensible access list, the routing switch also checks the destination. If the access list permits the address, the software goes on processing the packet. If the access list does not permit the address, the software drops the packet and returns an ICMP unreachable message.

For the standard access list of the **out** interfaces, after a packet is received or routed to the control interface, the software checks the source address of the packet according to the access list. For the extensible access list, the routing switch also checks the access list of the receiving side. If the access list permits the address, the software will send the packet. If the access list does not permit the address, the software drops the packet and returns an ICMP unreachable message.

If the designated access list does not exist, all packets allows to pass.

### 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.

During the connection period, the same two port numbers are used. The mail packet from the Internet has a destination port, that is, port 25. The outgoing packet has a contrary port number. In fact, the security system behind the routing switch always receives mails from port 25. That is the exact reason why the incoming service and the outgoing service can be uniquely controlled. The access list can be configured as the outgoing service or the incoming service.

In the following case, the Ethernet is a B-type network with the address 130.20.0.0. The address of the mail host is 130.20.1.2. The keyword **established** is only used for the TCP protocol, meaning a connection is created. If TCP data has the ACK or RST digit to be set, the match occurs, meaning that the packet belongs to an existing connection.

```
ip access-list aaa
permit tcp any 130.20.0.0 255.255.0.0 established
permit tcp any 130.20.1.2 255.255.255.255 eq 25
interface vlan 10
ip access-group aaa in
```



## 3.3 Configuring IP Access List Based on Physical Port

### 3.3.1 Filtering IP Message

Filtering message helps control the movement of packet in the network. The control can limit network transmission and network usage through a certain user or device. To make packets valid or invalid through the crossly designated interface, our routing switch provides the access list. The access list can be used in the following modes:

- Controlling packet transmission on the interface
- Controlling virtual terminal line access
- Limiting route update content

The section describes how to create IP access lists and how to use them.

The IP access list is an orderly set of the **permit/forbid** conditions for applying IP addresses. The ROS software of our switch tests the address one by one in the access list according to regulations. The first match determines whether the ROS accepts or declines the address. After the first match, the ROS software terminates the match regulations. The order of the conditions is, therefore, important. If no regulations match, the address is declined.

Use the access list by following the following steps:

- (1) Create the access list by designating the access list name and conditions.
- (2) Apply the access list to the interface.

### 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:

Run...	To...
<b>ip access-list standard</b> <i>name</i>	Use a name to define a standard access list.
<b>deny</b> { <i>source [source-mask]   any</i> } or <b>permit</b> { <i>source [source-mask]   any</i> }	Designate one or multiple <b>permit/deny</b> conditions in standard access list configuration mode. The previous setting decides whether the packet is approved or disapproved.
Exit	Log out from the access list configuration mode.

Run the following command in global configuration mode to create an extensible access list.

Run...	To...
<b>ip access-list extended</b> <i>name</i>	Use a name to define an extensible IP access list.
<b>{deny   permit}</b> <i>protocol source source-mask destination destination-mask [precedence precedence] [tos tos]</i> <b>{deny   permit}</b> <i>protocol any any</i>	Designate one or multiple <b>permit/deny</b> conditions in extensible access list configuration mode. The previous setting decides whether the packet is approved or disapproved.  <b>precedence</b> means the priority of the IP packet; <b>TOS</b> 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 3.2.3 “Applying the Access List to the Interface”.

### 3.3.3 Applying the Access List to the Interface

After the access list is created, you can apply it to one or multiple interfaces including the **in** interfaces and **out** interfaces.

Run the following command in interface configuration mode.

Run...	To...
<b>ip access-group</b> <i>name</i>	Apply the access list to the interface.

The access list can be used on the **in** interfaces and the **out** interfaces. For the standard access list of the **in** interface, the source address of the packet is to be checked according to the access list after the packet is received. For the extensible access list, the routing switch also checks the destination. If the access list permits the address, the software goes on processing the packet. If the access list does not permit the address, the software drops the packet and returns an ICMP unreachable message.

For the standard access list of the **out** interfaces, after a packet is received or routed to the control interface, the software checks the source address of the packet according to the access list. For the extensible access list, the routing switch also checks the access list of the receiving side. If the access list permits the address, the software will send the packet. If the access list does not permit the address, the software drops the packet and returns an ICMP unreachable message.

If the designated access list does not exist, all packets allows to pass.

### 3.3.4 Extensible Access List Example

#### 1. Port-based IP access list supporting TCP/UDP port filtration

```
{deny | permit} {tcp | udp}
source source-mask [ { [src_porrange begin-port end-port] | [ {gt | lt } port ] } ]
destination destination-mask [ { [dst_porrange begin-port end-port] | [ {gt | lt } port ] } ]
[precedence precedence] [tos tos]
```

If you configure the access list by defining the port range, pay attention to the following:

- If you use the method of designating the port range to configure the access list at the source side and the destination side, some configuration may fail because of massive resource consumption. In this case, you need to use the fashion of designating the port range at one side, and use the fashion of designating the port at another side.
- When the port range filtration is performed, too many resources will be occupied. If the port range filtration is used too much, the access list cannot support other programs as well as before.

#### 2. Port-based IP access list supporting TCP/UDP designated port filtration

In the following example, the first line allows any new TCP to connect the SMTP port of host 130.2.1.2.

```
ip access-list extended aaa
permit tcp any 130.2.1.2 255.255.255.255 eq 25
interface f0/10
ip access-group aaa
```

# Physical Port IP Access List Configuration

# Table of Contents

- Chapter 1 Configuring Physical Port-based IP Access List..... 1
  - 1.1 Filtering IP Message..... 1
  - 1.2 Creating Standard and Extensible IP Access List ..... 1
  - 1.3 Applying the Access List to Port ..... 2
  - 1.4 Extensible Access List Example ..... 2
    - 1.4.1 Port-Based IP Access List Supporting Filtration on TCP/UDP Ports ..... 2
    - 1.4.2 Port-Based IP Access List Supporting Filtration of Port-Based IP Access List Supporting Filtration of TCP/UDP-Specified Ports ..... 3

# Chapter 1 Configuring Physical Port-based IP Access List

## 1.1 Filtering IP Message

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

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

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

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

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

- (1) Create the IP access list by specifying the access list name and access conditions.
- (1) Apply the IP access list to the port.

## 1.2 Creating Standard and Extensible IP Access List

Use a character string to create an IP access list.

### Note:

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

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

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

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

Run...	To...
--------	-------

## Physical Port IP Access List Configuration

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

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

**Note:**

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

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

## 1.3 Applying the Access List to Port

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

Run the following command in port configuration mode:

Run...	To...
<b>ip access-group name</b>	Apply the access list to the port.

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

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

## 1.4 Extensible Access List Example

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

The example is shown as follows:

```
{deny | permit} {tcp | udp}
source source-mask [ { [src_portrange begin-port end-port] | [ {gt | lt } port ] ]
destination destination-mask [ { [dst_portrange begin-port end-port] | [ {gt | lt } port ] ] }
```

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

In this case, port I4 of TCP and UDP can be controlled through the access list. Pay attention to the following problems when you configure the access list by defining the port range:

- (1) If the access list is configured at the source and destination by specifying the port range, some configuration may fail because lots of sources are occupied during configuration. To solve the problem, you are recommended to specify the port range at one side and the port at the other side.
- (2) Using the port range filtration needs a lot of resources. The access list cannot provide strong support to other applications because the port range filtration is used too much.

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

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

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



# NTP Configuration

## Table of Contents

Chapter 1 Abstract.....	1
1.1 Conventions .....	1
1.1.1 Command Line Format Convention .....	1
Chapter 2 NTP Configurations.....	2
2.1 Abstract .....	2
2.2 NTP Configurations .....	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 Abstract

### 1.1 Conventions

#### 1.1.1 Command Line Format Convention

Format	Connotation
<b>Bold</b>	Keywords (text that remains unchanged and must be entered without modifications) in command lines are in bold.
<i>{Italic}</i>	Parameters (the part that must be replaced with actual values) in command lines are italic in "{}".
< <i>Italic</i> >	Parameters (the part that must be replaced with actual values) in command lines are italic in "<>".
[]	Content in "[]" is optional during command configuration.
{ x   y   ... }	Choose one from two or more options.
[ x   y   ... ]	Choose one or reject to choose any one from two or more options.
{ x   y   ... } *	Choose at least one from two or more options, but cannot exceed the total options.
[ x   y   ... ] *	Choose several options or reject to choose any one from two or more options.
&<1-n>	Parameters preceding the symbol "&" can be repetitively entered for 1 to n times.
#	Lines started with "#" are comment lines.

## Chapter 2 NTP Configurations

### 2.1 Abstract

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 Configurations

#### 2.2.1 Configure the Equipment As an NTP Server

[Configuration mode] Global configuration mode

Command	Purpose
<b>ntp master primary</b>	In the event that the equipment does not have an upper-level NTP server, configure the equipment as the original NTP server (stratum = 1).
<b>ntp master secondary</b>	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 configuration mode

Command	Purpose
<b>ntp authentication enable</b>	Open the authentication function (closed by default).
<b>ntp authentication key</b> <i>keyid md5 password</i>	Configure NTP md5 authentication keyid and corresponding keys.
<b>ntp authentication trusted-key</b> <i>keyid</i>	Configure the keyid corresponding key as the trusted key.

### 2.2.3 Configure NTP Association

[Configuration mode] Global configuration mode

Command	Purpose
<b>ntp server</b> <i>ip-address</i> [ <b>version</b> <i>number</i>   <b>key</b> <i>keyed</i>   <b>vrf</b> <i>vrf-name</i> ]*	Configure the IP address of NTP server; the version number, key number, and vrf instance can be designated.
<b>ntp peer</b> <i>ip-address</i> [ <b>version</b> <i>number</i>   <b>key</b> <i>keyid</i>   <b>vrf</b> <i>vrf-name</i> ]*	Configure the IP address of equipment NTP peer; the version number, key number, and vrf instance can be designated.

#### 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.

# Cluster Management Configuration

# Table of Contents

- Chapter 1 Cluster Management Configuration ..... 1
  - 1.1 Overview ..... 1
  - 1.2 Cluster Management Configuration Task List..... 1
  - 1.3 Cluster Management Configuration Task ..... 1
    - 1.3.1 Planning Cluster ..... 1
    - 1.3.2 Creating Cluster ..... 2
    - 1.3.3 Configuring Cluster ..... 2
    - 1.3.4 Monitoring the State of Standby Group ..... 4
    - 1.3.5 Using SNMP to Manage Cluster ..... 4

# Chapter 1 Cluster Management Configuration

## 1.1 Overview

The switch cluster is a group of switches which can be managed as a single entity. In the cluster, there must be a switch worked as the command switch, which allows up to 253 switches simultaneously to join the cluster as member switches. As the single access node in the cluster, the command switch is used to configure, manage and monitor member switches. One switch belongs to only one cluster at a certain moment.

## 1.2 Cluster Management Configuration Task List

- Planning cluster
- Creating cluster
- Configuring cluster
- Monitoring the state of standby group
- Using SNMP to manage cluster
- Using Web to manage cluster

## 1.3 Cluster Management Configuration Task

### 1.3.1 Planning Cluster

#### 1. VLAN

To manage the switch through the cluster, the command switch, the member switch and candidate switch of a cluster must have the default VLAN. The interface of the default VLAN of these switches has already existed.

#### 2. Automatically discovering member switches and candidate switches

The command switch uses the BDP protocol to find the member switch, candidate switch and other clusters. The command switch also uses the BDP protocol to find the network topology. Therefore, you need to run the BDP protocol on the member switch, candidate switch and other clusters and activate BDP on the interconnected interfaces.



### 3. IP address

If the management station accesses the cluster through the TCP/IP management mode, such as telnet, http and snmp, you need configure the IP address of the command switch that the management station can access. You need not configure the IP address for the member switch of the cluster.

After the member switch joins in the cluster, the command switch distributes an IP address to each member switch. These IP addresses are selected from the IP pool of the cluster configured on the command switch. When planning the address pool, pay attention that the service addresses cannot be the same as those in the address pool; note that the address number in the address pool cannot be smaller than the maximum number of member switches in the cluster (including the command switch).

## 1.3.2 Creating Cluster

### 1. Activating command switch

Run the following command in global configuration mode to set the current switch to the command switch:

Command	Description
<b>cluster mode commander</b> <i>cluster-name</i>	Sets the current switch to the command switch.

### 2. Activating standby switch

Run the following command in global configuration mode to set the current switch to the standby switch:

Command	Description
<b>cluster mode member</b>	Sets the current switch to the standby switch.

### 3. Adding member switch

Run the following command in global configuration mode to add the standby switch with the designated MAC address to the cluster:

Command	Description
<b>cluster member</b> [ <i>id member-id</i> ] <b>mac-address</b> <i>H.H.H</i> [ <b>password</b> <i>enable-password</i> ]	Adds member switch.

## 1.3.3 Configuring Cluster

### 1. Configuring IP pool

Run the following command in global configuration mode to configure the IP address pool for cluster management:

Command	Description
---------	-------------

<b>cluster address-pool</b> <i>A.B.C.D A.B.C.D</i>	Configures the IP address pool.
--	---------------------------------

## 2. Configuring hellotime

You can modify the interval to send the handshake message between the command switch and the member switch by configuring hellotime (unit:second).

Run the following command in global configuration mode to configure the cluster's hellotime:

Command	Description
<b>cluster hellotime</b> <i>&lt;1-300&gt;</i>	Configures the interval of sending hello message between the command switch and the member switch.

## 3. Configuring holdtime

If the member switch and the command switch do not receive the handshake message from the peer in an interval, they think the peer is in **down** state. You can configure **holdtime** to change the interval value

Run the following command in global configuration mode to configure the cluster's holdtime:

Command	Description
<b>cluster holdtime</b> <i>&lt;1-300&gt;</i>	Configures the interval of sending handshake message between the command switch and the member switch.

## 4. Configuring hop number of the discovery protocol

The cluster uses the hop number to measure the distance of switches in the cluster. The hop number of the discovery protocol configured on the command switch equals the distance between the cluster verge and the candidate switch which is farthest to the cluster verge.

Run the following command in global configuration mode to configure the hop number of the discovery protocol for the cluster:

Command	Description
<b>cluster discovery</b> <i>hop-count&lt;1-7&gt;</i>	Configures the PDP hop number of the discovery protocol.

## 5. Configuring the applied discovery protocol

The cluster uses the discovery protocol to acquire the neighbor information. Run the following command in global configuration mode to configure the neighbor discovery protocol.

Command	Description
<b>cluster discovery mode</b> <i>{pdp lldp}</i>	Configures the discovery protocol.

## 6. Configuring the management VLAN

For communication, the cluster requires the VLAN in the switch and the members must be the same. Run the following command to configure the cluster management VLAN before enable the cluster function:

Command	Description
<b>cluster management-vlan</b> <1-4094>	Configures the cluster management VLAN.

### 1.3.4 Monitoring the State of Standby Group

Run the following command in privileged mode to monitor the configuration and state of cluster:

Command	Description
<b>show cluster</b>	Monitors the state of the standby group.
<b>show cluster</b> <i>member</i>	Checks the cluster member.
<b>show cluster candidate</b>	Checks the cluster candidate.
<b>show cluster topo</b>	Checks the cluster topology.
<b>show address-pool</b>	Checks the address pool the cluster.

### 1.3.5 Using SNMP to Manage Cluster

After the cluster is created, the snmp message can be transmitted between the member switch and the snmp application through the command switch. The detailed process is shown as follows:

To access No. N member switch in snmp mode, specify the destination IP address as the address of the switch in an snmp application.

Set **community string** to **community string + @esN**, which belongs to the corresponding right of the command switch. If **community string** on the command switch is **public**, **community string** of No.6 member switch is **public@es6**.

# IEC61850Server Configuration

# Contents

- Chapter 1 IEC61850Server Configuration ..... 1
  - 1.1 IEC61850 General ..... 1
  - 1.2 IEC61850Server Configuration Task Table..... 2
  - 1.3 IEC61850Server Configuration ..... 3
    - 1.3.1 Configure IEC61850Server function ..... 3
    - 1.3.2 Configure IEC61850Server authentication password ..... 3
    - 1.3.3 Configure renewal cycle for data attribute of IEC61850Server ..... 3
    - 1.3.4 Configure the IP address interface for IEC61850Server ..... 3
    - 1.3.5 Show the quantity of connection of the client ends for IEC61850Server ..... 3
    - 1.3.6 Show the data attribute information of IEC61850Server ..... 4

# Chapter 1 IEC61850Server Configuration

## 1.1 IEC61850 General

IEC 61850 standards, as international ones, are issued by International Eelectrotechnical Commission in 2004 and applied to communication network and systems of substations. They define the communication and relevant system requirements among intelligent electronic device (IED) inside the substations.

Define the interactive abstract models among the service customers

Define the abstract communication service interfaces

Define specific communication service mapping

IEC 61850 characteristics:

IEC 61850 uses the modeling technology oriented to the objects, defines the data model based on the structure of client machine/server. Each IED includes one or several servers, each server itself includes one or several logic equipment, the logic equipment includes logic nodes and the logic node includes data object. The data object is the named example of public data consisting of data attributes. From the perspective of communication, IED also plays the role of client end at the same time. Any client end can be accessed by abstract communication server interface (ACSI) or the relevant data objects in the data model of the server end can be modified to subscribe the relevant report of the server end (RCB) (table 1). Therefore, the client end can be noticed immediately when the corresponding variables are changed; or some variables are observed when the server end is set so that the customer can be prompted immediately when such value is changed.

Note: our switch includes one server, this server includes one logic device and one logic device includes several logic nodes.

The data information models supported by our switch are:

Logical device

Logical node

Data

Data set

Reporting

Unbuffered report control

The service models supported by our switch are:

Table 1 List of service models of the device

Service	
Server (chapter 6)	
Server Directory	Server Directory
Application association (chapter 7)	
Associate	Associate
Abort	Abort

Release	Release
Logical device (chapter 8)	
LogicalDeviceDirectory	Logical Device Directory
Logical node (chapter 9)	
LogicalNodeDirectory	Logical Node Directory
GetAllDataValues	Get All Data Values
Data (chapter 10)	
GetDataValues	Get Data Values
SetDataValues	Set Data Values
GetDataDirectory	Get Data Directory
GetDataDefinition	Get Data Definition
Data set (chapter 11)	
GetDataSetValues	Get Data Set Values
SetDataSetValues	Set Data Set Values
CreateDataSet	Create Data Set
DeleteDataSet	Delete Data Set
GetDataSetDirectory	Get Data Set Directory
Reporting (chapter 14)	
Unbuffered report control block	URCB Unbuffered report control block
Report	Report
data-change	dchg data change
qchg-change	qchg quality change
GetURCBValues	get URCB Values
SetURCBValues	Set URCB Values

## 1.2 IEC61850Server Configuration Task Table

Configure IEC61850Server function

Configure IEC61850Server authentication password

- Configure renewal cycle of data attribute
- Configure the IP address interfaces of IEC61850Server
- Show the quantity of connection of client ends of IEC61850Server
- Show the data attribute information of IEC61850Server

## 1.3 IEC61850Server Configuration

### 1.3.1 Configure IEC61850Server function

Open or close globally the function of IEC61850Server. After the function of IEC61850Server is started, the server end starts to monitor the connection of client ends. Our server supports at most the connection of two client ends and it is able to respond to different kinds of service request of the client ends after the connection is established.

Command	Purpose
[no] iec61850-server enable	Configure the function to start and close the iec61850-server.

### 1.3.2 Configure IEC61850Server authentication password

Configure globally the password safety authentication function for IEC61850Server. After the configuration, the client end has to include the password which is the same as this password authentication in the message of establishing the connection request before successful connection with the server end.

Command	Purpose
[no] iec61850-server authentication password {0 7} password	Configure the safety authentication password for iec61850Server, 0 is the clear text and 7 is the cipher text.

### 1.3.3 Configure renewal cycle for data attribute of IEC61850Server

Configure globally the renewal cycle for data attribute of IEC61850Server. The default is 2s with the value range of 2-60S. IEC61850Server will update the value of data attribute in each cycle.

Command	Purpose
[no] iec61850-server mmsDAupdateTime time	Configure the renewal cycle for data attribute of iec61850Server.

### 1.3.4 Configure the IP address interface for IEC61850Server

Configure globally the IP address interface vlan for IEC61850Server. The default is vlan 1.

Command	Purpose
[no] iec61850-server config-vlan-id vlan-id	Configure the interface vlan for getting IP address for iec61850Server

### 1.3.5 Show the quantity of connection of the client ends for IEC61850Server

It is mainly used to show the quantity of connected client ends of iec61850Server.



Configuration

Command	Purpose
show iec61850-server client-connection-count	Show the quantity of connected client ends of iec61850Server

1.3.6 Show the data attribute information of IEC61850Server

It is mainly used to show the data attribute information for iec61850Server. See appendix A for detailed data attribute and logic device, logic node, data object and restraint function.

Command	Purpose
show iec61850-server DA-valueread DA-name	Show the information of data attribute of iec61850Server.

# ZTP Configuration

---

# Contents

**CHAPTER 1 ZTP CONFIGURATION .....1**

    1.1 GENERAL ..... 1

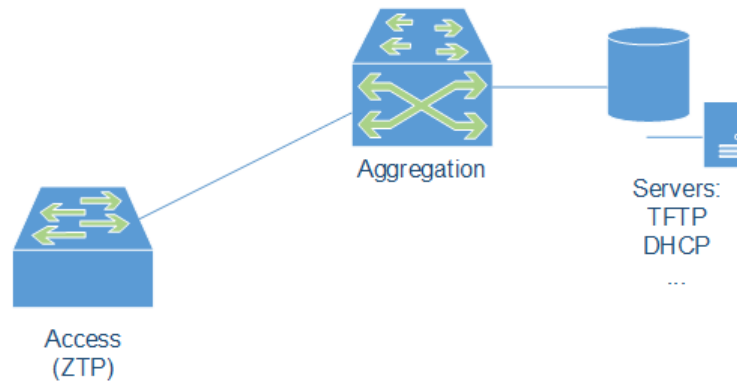
    1.2 ZTP CONFIGURATION ..... 1

        1.2.1 *Factory default configuration* ..... 1

# Chapter 1 ZTP Configuration

## 1.1 General

The function of Zero Touch Provisioning is used to simplify the deployment and configuration of equipment on site environment. The operation environment of one ZTP is shown in following figure.



ZTP includes the following function modules and steps.

- Ex-factory default configuration. There are default configuration files at the ex-factory of the equipment. The necessary functions of ZTP that have to be used in the default configuration documents: LLDP and DIM.
- LLDP. The device Access receives the LLDP-MED message sent by the device Aggregation. The message carries Network Policy TLV, among which the VLAN ID will be used as new management VLAN by the device Access.
- Dynamic Interface Manager(DIM). DIM is based on new management VLAN to create three layers of management interface (VLAN Interface) and start the DHCP client end.
- DHCP Client. Operated on the newly created VLAN port. Obtain the management IP address from DHCP server, store the IP address of TFTP server of device configuration files and the name of configuration files to be downloaded.
- TFTP Client. Download the site configuration files from TFTP server address obtained from DHCP client end.
- Site configuration files loaded by device

Note: ZTP function supports IPv6, and it can only work on the device supporting IPv6.

## 1.2 ZTP configuration

### 1.2.1 Factory default configuration

To use the ZTP function, the device must have the default configuration files with following configuration information during ex factory.

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

ZTP  
Configuration

<b>lldp run</b>	Enable globally LLDP function.
<b>dim enable</b>	Enable globally DIM function. If only ZTP based on IPv6 is needed, this command can not be configured.
<b>dim enable ipv6</b>	Enable the DIM function based on IPv6. This configuration can only be used on device supporting IPv6. If only ZTP based on IPv4 is needed, this command can not be configured.

# IPv6 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.

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.

Kind	Referred Format	Remarks
Unicast address	2001:0:0:0:0DB8:800:200C:417A/64	<b>2001:0:0:0:0DB8:800:200C:417A</b> stands for a unicast address, while <b>64</b> stands for the length of the prefix of this address.
Multicast address	FF01:0:0:0:0:0:0:101	All multicast addresses begin with FF.
Any address	2002:0:0:0:0DB8:800:200C:417A/64	The format of this address is the same as that of the unicast address. Different VLAN interfaces can be set to have the same address, no matter it is a unicast/broadcast/multicast address.

For the further details of the IPv6 address, see RFC 4291.

In order to enable IPv6, users must set a unicast address in VLAN interface configuration mode. The set unicast address must be one or multiple addresses of the following type:

- IPv6 link-local address



- Global IPv6 address

To set an IPv6 link-local address in VLAN interface configuration mode, run the following commands.

Command	Purpose
ipv6 enable	Sets a link-local address automatically.
ipv6 address fe80::x link-local	Sets a link-local address manually.

**Note:**

- The link-local address must begin with fe80. The default length of the prefix is 64 bit. At manual settings only the values at the last 64 bits can be designated.
- On a VLAN interface can only one link-local address be set.
- After IPv6 is enabled through the configuration of the link-local address, IPv6 only takes effect on the local link.

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   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. (Refer to RFC 4007 for the range of the IPv6 address.)
- 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 the transmission frequency of the ICMPv6 packet
- (3) Setting IPv6 destination unreachability
- (4) Setting IPv6 ACL

##### 1. Setting the MTU of IPv6

All interfaces have a default IPv6 MTU. If the length of an IPv6 packet exceeds MTU, the router will fragment this IPv6 packet.

To set IPv6 MTU on a specific interface, run the following command in interface configuration mode:

Command	Purpose
ipv6 mtu bytes	Sets IPv6 MTU on an interface.

##### 2. Setting IPv6 redirection

Sometimes, the route selected by the host is not the best one. In this case, when a switch receives a packet from this route, the switch will transmit, according to the routing table, the packet from the interface where the packet is received, and forward it to another router which belongs to the same network segment with the host. Under this condition, the switch will notify the source host of sending the packets with the same destination address to another router directly, not by way of the switch itself. The redirection packet demands the source host to replace the original route with the more direct route contained in the redirection packet. The operating system of many hosts will add a host route to the routing table. However, the switch more trusts the information getting from the routing protocol and so the host route will not be added according to this information.

IPv6 redirection is opened by default. However, if a hot standby router protocol is configured on an interface, IPv6 redirection is automatically closed. If the hot standby router protocol is canceled, this function will not automatically opened.

To open IPv6 redirection, run the following command:

Command	Purpose
ipv6 redirects	Allows IPv6 to transmit the redirection packets.

## 5. 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	Allows IPv6 to transmit the destination unreachable packets.

## 6. Setting IPv6 ACL

Users can use ACL to control the reception and transmission of packets on a VLAN interface. If you introduce ACL on a VLAN interface in global configuration mode and designate the filtration's direction, the IPv6 packets will be filtered on this VLAN interface.

To filter the IPv6 packets, run the following command in interface configuration mode.

Command	Purpose
ipv6 access-group WORD	Filters the IPv6 packets in the reception direction on a VLAN interface.

# ND Configuration

# Table of Contents

Chapter 1 ND Configuration ..... 1

    1.1 ND Overview ..... 1

        1.1.1 Address Resolution ..... 1

        1.1.2 ND Configuration..... 2

# Chapter 1 ND Configuration

## 1.1 ND Overview

A node (host and router) uses ND (Neighbor Discovery protocol) to determine the link-layer addresses of the connected neighbors and to delete invalid cache rapidly. The host also uses the neighbor to discover the packet-forwarding neighboring routers. Additionally, the node uses the ND mechanism to positively trace which neighbors are reachable or unreachable and to test the changed link-layer address. When a router or the path to a router has trouble, the host positively looks for another working router or another path.

IPv6 ND corresponds to IPv4 ARP, ICMP router discovery and ICMP redirect.

ND supports the following link types: P2P, multicast, NBMA, shared media, changeable MTU and asymmetric reachability. The ND mechanism has the following functions:

- (1) To discover routers: how the host to locate the routers on the connected links.
- (2) To discover prefixes: how the host to find a group of address prefixes, defining which destinations are on-link on the connected links.
- (3) To discover parameters: how the node to know the link-related or network-related parameters of the transmission interface.
- (4) To automatically set addresses: how the node to set the address of an interface automatically.
- (5) Address solution: When the IP of a destination is given, how a node determines the link-layer address of the on-link destination.
- (6) To determine the next hop: it is an algorithm to map the IP address of a destination to the neighboring IP. The next hop can be a router or destination.
- (7) To test unreachable neighbors: how a node to determine unreachable neighbors; if neighbor is a router, the default router can be used.
- (8) To test repeated address: how a node to determine whether a to-be-used address is not used by another node.
- (9) Redirect: how a router to notify the host of the best next hop.

### 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
<b>ipv6 neighbor</b> ipv6address vlan vlanid hardware-address	Sets a static ND cache and translates IPv6 address into a link-layer address.

### 1.1.2 ND Configuration

The ND protocol is used not only for address resolution but for other functions such as neighbor solicitation, neighbor advertisement, router solicitation, router advertisement and redirect.

The following commands are all run in port configuration mode:

- Setting the number of transmitted NSs when ND performs DAD on a local port

Before the IPv6 port is started, it should send the NS information to the local machine to find if there is any duplicate IPv6 address existing on links through DAD.

Command	Purpose
<b>ipv6 nd dad attempts</b> num	Sets the number of transmitted NSs when the local port performs DAD.

- Setting the M flag in the RA message transmitted by the local port

The M flag indicates that the RA message host should obtain addresses through on-status automatic configuration. To set the M flag in the RA message transmitted by the local port to 1, run the following command.

Command	Purpose
<b>ipv6 nd managed-flag</b>	Sets the M flag in the RA message transmitted by the local port.

- Setting the NS transmission interval of the local port and the **retrans-timer** field in the RA message

This command can be used to set the NS transmission interval of the local switch on the local port and at the same time the **retrans-timer** field in the RA message on the local port.

The host sets its **retrans-timer** variable according to the retrans-timer field in RA.

Command	Purpose
<b>ipv6 nd ns-interval</b> milliseconds	Means the NS retransmission interval in the local port and the retrans-timer field in the RA message. Its default value is 1000ms.

- Setting the O flag in the RA message transmitted by the local port

The O flag indicates that the RA message host should obtain other information through on-status automatic configuration. To set the O flag in the RA message transmitted by the local port to 1, run the following command:

Command	Purpose
<b>ipv6 nd other-flag</b>	Sets the O flag in the RA message transmitted by the local port.

- Setting the prefix of the RA message

The router releases address prefixes to the network host via RA message. The address prefix plus the host address is the entire unicast address. The prefix option is carried by the RA message, and the host obtains the IPv6 address prefix and related parameter from this option.

Command	Purpose
<b>ipv6 nd prefix</b> {ipv6-prefix/prefix-length   <b>default</b> } [ <b>no-advertise</b>   [valid-lifetime preferred-lifetime <b>[off-link</b>   <b>no-autoconfig]]</b> ]	Means that the local port transmits the prefix option's content in the RA message.

- Setting the RA transmission interval

The following command is used to set the range of RA transmission interval. The RA transmission interval is in general an indefinite value but a random value in a fixed range, which can avoid abrupt flow surge in the network.

Command	Purpose
<b>ipv6 nd ra-interval-range</b> max min	Sets the range of RA transmission interval. The maximum RA transmission interval is 600s and the minimum RA transmission interval is 200s.

The interval for the local port to transmit the first three messages cannot be more than 16 seconds, while that to transmit the following messages varies between the maximum interval (600 seconds) and the minimum interval (200 seconds).

- Setting a specific RA transmission interval

RA packets are transmitted in an interval configured by **ra-interval-range**, but if users want to use a specific transmission interval, they can set this value through the following command:

Command	Purpose
<b>ipv6 nd ra-interval</b> interval	Sets a specific RA transmission interval, which is not set by default.

- Setting the router-lifetime field in the RA message transmitted by the local port

The **router-lifetime** field in the RA message is the triple of the maximum value of **ipv6 nd ra-interval-range**.

Command	Purpose
<b>ipv6 nd ra-lifetime</b> seconds	Sets the router-lifetime field in the RA message transmitted by the local port.

- Setting the reachable-time field of the RA message

**reachable-time** means the time to reach a neighbor, which is 0 by default.



Command	Purpose
<b>ipv6 nd reachable-time</b> milliseconds	Sets the <b>reachable-time</b> field in the RA message transmitted by the local port. Its default value is 0ms.

- Setting the value of the router preference in the RA message

**router-preference** means the router's priority, which accounts for two bits in the **flags** domain in the RA message. The router's priority can be high, medium and low. The medium priority is the default settings.

Command	Purpose
<b>ipv6 nd router-preference</b> preference	Sets the <b>router-preference</b> field in the RA message transmitted by the local port. It is medium by default.

- Stopping a port to be the notification port of a switch

Only the notification port can transmit RA packets. The notification port supports multicast and is set to have at least one unicast IP address. Its AdvSendAdvertisement flag is TRUE in value.

The configuration of **ipv6 nd suppress-ra** in the VLAN port means shutdown the notification port. This command is not set by default.

Command	Purpose
<b>ipv6 nd suppress-ra</b>	Means the value of the AdvSendAdvertisement flag on the local port. 0

# Ethernet Ring Network (G8032-201003) Protection Configuration

## Contents

Chapter 1 Introduction of Fast Ethernet Ring Network Protection .....	1
1.1 Overview .....	1
1.2 ERPS-Related Concepts .....	2
1.2.1 Ring Network Level.....	2
1.2.2 Ring Network Node Role .....	2
1.2.3 Ring Network Port Role .....	3
1.2.4 ERPS & CFM.....	3
1.2.5 Ring Network Interconnection Mode Using R-APS Virtual Channel .....	4
1.2.6 R-APS Transmission VLAN .....	5
1.2.7 Revertive Mode.....	5
1.3 Type of ERPS Packets.....	5
1.4 ERPS Ring Network Protection Mechanism.....	6
1.4.1 Stable State.....	6
1.4.2 Local Link Failure Processing.....	6
1.4.3 Local Link Recovery Processing .....	6
1.4.4 Protection Switching—Link Recovery.....	7
1.4.5 Protection Switching—Manual Switching .....	7
1.4.6 Protection Switching— Forced Switching.....	8
1.4.7 Switching Recovery Processing .....	9
Chapter 2 ERPS Configuration .....	10
2.1 ERPS Configuration Instructions .....	10
2.2 ERPS Configuration Tasks.....	10
2.2.1 Configuring the Ring Network Nodes .....	10
2.2.2 Configuring the Ring Network Ports.....	12
2.2.3 Ring Network Control Commands .....	13
2.2.4 Checking Ring Network Protection Protocol Status.....	13
2.3 ERPS Configuration Instance .....	14
2.3.1 Configuration Instance 1 — ERPS Single Ring Configuration .....	14
2.3.2 Configuration Instance 2 — ERPS Multiple-ring Configuration .....	18

# Chapter 1 Introduction of Fast Ethernet Ring Network Protection

## 1.1 Overview

Fast Ethernet ring protection protocol is a special kind of link layer protocol, which is used to construct the ring Ethernet topology. The Ethernet protection protocol blocks a link in the case that the ring topology is complete, preventing the data loop against forming the broadcast storm. In case of link interruption, the protocol quickly enables the link to be restored to the status before link interruption so that the communication between the nodes of the loop can be restored.

Fast ring network protection protocol can ensure through controlling the aging of MAC address table for the switch that the data packets can be sent to the correct link when the topology takes change. Under normal circumstances, the aging time of the MAC address in the address table is 300 seconds. The ring network protection protocol can control the aging of the MAC address table for the switch in a very short period of time.

Ring network protection protocol and spanning tree protocol are both used for link layer topology control. The spanning tree protocol is suitable for all kinds of complex networks, which uses the hop-by-hop method to transmit the change in the network topology. The ring network protection protocol is dedicated to the ring topology, which uses the diffusion method to transmit the topological change. Therefore, in the ring network, the convergence performance of the ring protection protocol is better than that of the spanning tree protocol. In the case of good network condition, the ring network protection protocol can restore network communication within less than 50 ms.

---

**Note:**

Ring network protection protocol supports a switch configured as the node of multiple physical ring networks to form a tangent ring. It does not support the intersecting rings with public links.

---

## 1.2 ERPS-Related Concepts

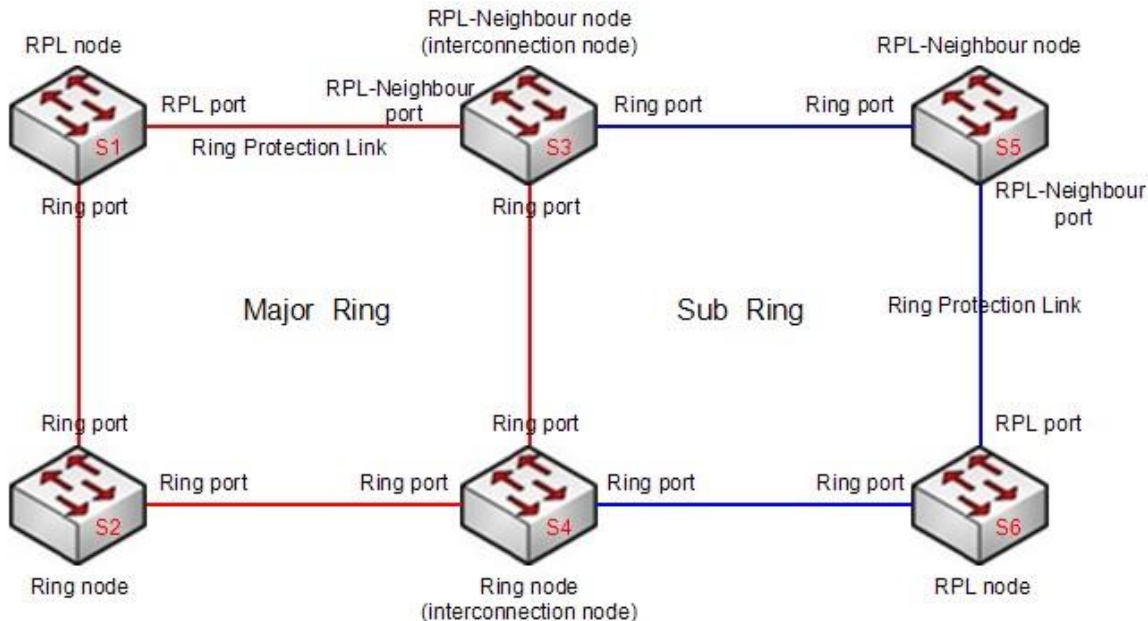


Figure 1 Diagram of ERPS Ethernet

### 1.2.1 Ring Network Level

ERPS supports multiple-ring or hierarchical transport network topology, as is shown in Figure 1. The major ring is a complete single ring; the sub-ring is connected to major ring (or sub-ring) through two interconnection-nodes. In Figure 1, red lines constitute a major ring, including Node S1, Link S1-S2, Node S2, Link S2-S4, Node S4, Link S4-S3, Node S3, Link S3-S1. Blue lines constitute a sub-ring, including Node S3, link, Link S3-S5, Node S5, Link S5-S6, Node S6, Link S6-S4, Node S4, but not including Link S4-S3.

### 1.2.2 Ring Network Node Role

Each switch constituting the ring network is a ring network node. The ring network node role falls into four kinds: RPL protection node, RPL neighbor node, interconnection node and ordinary node. A physical link is selected from each single ring as RPL protection link; one of two switches directly connected to this link is taken as RPL protection node and the other is taken as RPL neighbor node; and the remaining switches are used as ordinary nodes. The interconnection nodes are two intersecting nodes when the sub-ring is connected to major ring (or sub-ring).

As is shown in Figure 1, in the major ring, S1 is a RPL protection node; S3 is a RPL neighbor node, S4 and S2 are ordinary nodes; in the sub-ring, S6 is a RPL protection node, S5 is a RPL neighbor node, they are connected to the major ring through Interconnection Node: S4 and S3.

---

### Ethernet Ring Network (G8032-201003) Protection Configuration

---

The node type of the ERPS protocol is determined by the port role, but the node type of the interconnection node needs to be determined in the configuration; by default, the node is not the interconnection-node.

For the ring network nodes, their functions are basically the same: detecting the status of local ring network port and sending a notification when the link fails. Differently, under normal circumstances, the RPL protection node and the RPL neighbor node block the RPL link, but the ordinary node does not block the RPL link. For the interconnection node, there is only one ring network port connected to the sub ring, and this node must also be a node in the other main ring (or sub ring).

#### 1.2.3 Ring Network Port Role

The ERPS protocol requires that each node has two ports that are connected to the RING network. Each port is called "Ring Port". In addition, in each single ring, there is also a ring network port as the ring network protection link (RPL). For the interconnection node, although only the ring port is connected to the sub-ring, there is also a virtual port to detect the connectivity between two interconnection nodes. This point will be discussed in the later part.

Under normal circumstances, all the ring network ports but the RPL link in the ring network are in the forwarding state. RPL ports of the RPL protection node and the RPL neighbor node are blocked to avoid the loop. In the case of the failure in the ring network link, the RPL protection node and RPL neighbor nodes don't block the RPL port any more, restoring the network communication.

In one switch, each ring network node instance can only be configured with one RPL port.

---

Note :

ERPS protocol supports the configuration of the aggregated port as ring network port.

---

#### 1.2.4 ERPS & CFM

In the ERPS port, MEP is configured to monitor the ring network link. The ring network port monitors the status of its ring network link through "Down MEP"; meanwhile, the ring network port where the interconnection node is connected to the sub-ring is configured with "Up MEP" to monitor the connectivity of the major ring, as is shown in Figure 2.

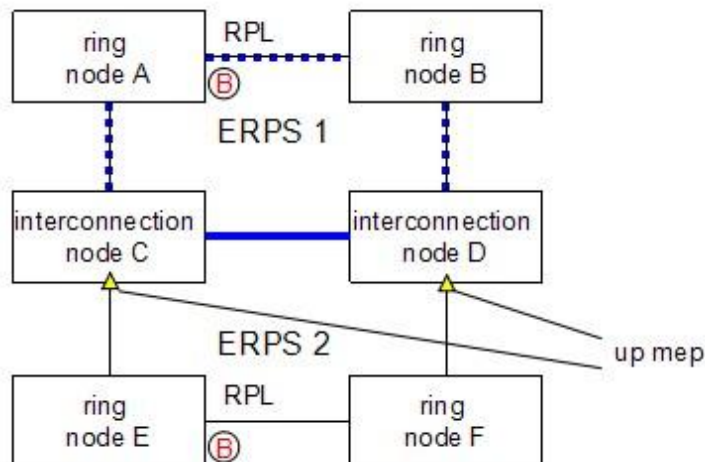


Figure 2 Virtual ports for interconnection nodes configured on the “Up MEP” port

In Figure 2, all the ERPS ring network ports are configured with “Down Mep” to monitor the ring network link through “Down MEP”. For example, Ring Link A-C is later monitored as a ring network port of Node A and Node C is configured with “Down Mep”; when the link fails or restores from the failure, it will send the corresponding notice to ERPS control module; meanwhile, the “Down Mep” is responsible for receiving and sending R-APS messages. The “Up MEP” is only configured on the ring network port where the interconnection node is connected to the sub-ring to monitor the connectivity of major ring. When the major ring between the interconnection nodes is blocked or restored to smooth communication, it sends the corresponding notification to the ERPS control module. In addition, the ring network port where the interconnection node is connected to the sub-ring is not only configured with “Up MEP”, but also “Down MEP”.

**Note:**

The ring network port where the interconnection node is connected to the sub-ring is configured with “Up Mep” to monitor the connectivity of major ring; at this time, it means that the virtual port of major ring link is monitored.

### 1.2.5 Ring Network Interconnection Mode Using R-APS Virtual Channel

For the sub-rings, the interconnection node is a node that connects the sub rings and other networks. For example, in Figure 1, the major ring is connected. The “Up MEP” port of interconnection node monitors the connectivity of the major ring, which is called the R-APS virtual channel. Through the R-APS virtual channel, two interconnection nodes can conduct R-APS communication via other networks.

The sub-ring transmits R-APS information to the network (and receives R-APS message from the network) through the R-APS virtual channel; meanwhile, the R-APS information can be transmitted in the network as data stream. Of course, the R-APS information should be separated from the ordinary data stream; so for different ERPS ring networks, different “control VLANs” are used to carry the R-APS information.

Of course, when the interconnection node is connecting the sub-ring with other networks, the R-APS channel is not used, which is in the forwarding state.

## 1.2.6 R-APS Transmission VLAN

As R-APS packets are transmitted in the R-APS channel, a VLAN must be set up for R-APS channel. Different nodes have different VLANs, but for some node, other nodes' VLANs can be used as VLAN for ordinary data stream transmission.

When configuring R-APS's VLAN, if the VLAN has not been created, the ERPS system will automatically create the VLAN.

The state of the ERPS ring network port in the R-APS channel is consistent with that of ordinary data stream. But the sub-ring without using the R-APS virtual channel is an exception. The R-APS channel of interconnection node in this sub-ring is suspended, so the nodes on the sub-ring of the R-APS virtual channel are not used, and their R-APS channels are in the forwarding state.

---

Note:

The VLAN for the MEP port on the ERPS port is consistent with R-APS Transmission VLAN.

---

## 1.2.7 Revertive Mode

In some ring networks, under normal circumstances, the network resources of the link channel for data stream transmission would be better; but the channel of RPL is only used for backup; so the revertive mode is used in the switching clearance to return the data stream to the channel with better network resources. For some ring networks, as they don't have high requirements for network resources, they needn't immediately return to the original link channel after the switching is restored. So, the non-returning mode is adopted so that the times of returning to switching can be reduced.

In the operation of returning mode, when a switch is cleared, the data stream will return to the original channel, blocking RPL. In the case of fault clearance, the data stream returns under the premise of the timeout of the WTR timer, avoiding protection switching in the case of intermittent faults. In the case of clearing manual switching or forced switch commands, there is need to wait for the WTB timer. In the operation of non-revertive mode, when a switching is cleared, the data stream still remains in RPL channel as long as there is no fault in the RPL channel.

---

Note:

WTR timer and WTB timer are valid only in revertive mode.

---

## 1.3 Type of ERPS Packets

The type of packet used by the ERPS protocol is shown in table 2.1.

Table 4.1 ERPS Ring Network Protection Protocol Packet Type

Type of packet	Description
Forced Switch (FS)	Ring network node (including RPL node) notifies other nodes after the forced switching command.
Signal Fail (SF)	Ring network node (including RPL node) notifies other nodes after finding the local link failure in the detection.



## Ethernet Ring Network (G8032-201003) Protection Configuration

Manual Switch (MS)	Ring network node (including RPL node) notifies other nodes after manual switching commands.
No Request (NR)	Ring network node notifies other nodes after finding all the local ring network links are recovered in the detection.
No Request, RPL Blocked (NR-RB)	Ring network protection node notifies other nodes of the recovery of ring network protection switching.

## 1.4 ERPS Ring Network Protection Mechanism

### 1.4.1 Stable State

In the stable state, the RPL port is blocked by the ring network protection node, which continuously sending the NR-RB protocol message with a configurable cycle.

For all the ordinary nodes that receive NR-RB packets, the local ring network port is set as the forwarding state. In the stable state, ordinary nodes do not send protocol packets.

The protection node is modified by configuring the command through the “send-time” node to send the cycle of the NR-RB packet.

### 1.4.2 Local Link Failure Processing

When a ring network node detects the local link failure, the blocking state of the enabled local port (including the RPL port or the ordinary ring port which has not yet entered the forwarding state) is immediately eliminated, and then the SF protocol message begins to be sent and the aging of local MAC address table begins.

For all other nodes receiving SF packets, the local packet sending first stops, and then the blocking state of the local enabled port is relieved and the address table aging starts.

The disabled node for the link continuously sends the SF packet taking the configured “send-time” as the cycle. In this process, if the port for another node recovers from the failure state, this node will restore the state of port as the forwarding state after receiving SF packets.

### 1.4.3 Local Link Recovery Processing

When the ring network node finds that the local ring network port recovers from the failure state in the detection, it will keep the port still in the blocking state and begins to continue to send NR packets.

In the process of sending NR packet, if the node receives the SF packet from other nodes, it indicates that there are other disabled links in the network; the local node stops sending the NR packet and sets the recovered port to be in the forwarding state.

If local node does not receive new SF packet, it will start switching recovery timer after the ring network protection node (RPL node) receives the NR packet; and after the timer timeout, RPL node blocks the RPL port once again and sends NR-RB packet and

then starts the address table aging. The network communication recovers to the initial stable state.

#### 1.4.4 Protection Switching—Link Recovery

When the ring network node finds that the local ring network port recovers from the failure state in the detection, it will keep the port still in the blocking state and begins to continue to send NR packets.

In the process of sending NR packet, if the node receives the SF packet from other nodes, it indicates that there are other disabled links in the network; the local node stops sending the NR packet and sets the recovered port to be in the forwarding state.

If local node does not receive new SF packet, it will recover the link after the ring network protection node (RPL node) receives the NR packet. But when the link is recovered, the revertive mode and non-revertive mode are not consistent in behavior and function.

##### 1.4.4.1 Revertive mode

In revertive mode, the ring network link will be recovered. After RPL node receives the NR packet, it will start switching recovery timer; after the timer timeout, RPL node blocks the RPL port once again and sends the NR-RB packet; and then the address table aging starts, the network communication is recovered to the initial stable state.

##### 1.4.4.2 Non-revertive mode

In the non-revertive mode, the ring network link is not automatically recovered. After receiving the NR packet, the RPL node does not make any response; after other ring network nodes receive the NR packets, they don't do any action. Only when the RPL node receives the "Clear" command, the RPL node blocks the RPL link and continues to send RB NR packets to two ring network ports, and then execute Flush FDB. After the disabled node receives the RB NR packet, it relieves the blocking state of the port. After receiving the RB NR packet, the ring network node executes Flush FDB.

#### 1.4.5 Protection Switching—Manual Switching

In the normal ring network state, after the ring network node receives a manual switching command, it blocks data stream channel and the R-APS channel (Blocking a data stream channel and R-APS channel port) and opens other ring network ports and continues to send MS packets to two ring network ports, and then execute Flush FDB. After other ring network nodes receive the MS packet, they open RPL data stream channel and R-APS channel. After receiving the MS packet, the ring network node sending MS packet stops sending MS packet. After receiving the MS packet, the ring network nodes execute Flush FDB.

The above action completes an operation of manual switching; in order to keep switching operation normal, there are several points deserving our attention:

(1) When a manual switching command has existed in the ring network, the later manual switching commands are invalid. The node receiving new switching command must refuse new switching command and give notice that the manual switching is rejected.

(2) For the node which has generated manual switching command locally, if receiving MS packets of different node IDs, this node should remove the local manual switching command and send the NR packet. At the same time, the node continues to block the ring network port blocked by previous manual switching commands.

(3) For the node which has generated manual switching command locally, if receiving higher priority of local request or packet, this node shall remove manual switching requests and execute the higher priority of requests.

For the node which generates manual switching command, after receiving the “Clear” command, it removes manual switch command. The node continues to block the ring network port blocked by previous manual switching commands and sends NR packets to two ring network ports. But when the link is recovered, the revertive mode and non-revertive mode are not consistent in behavior and function.

#### 1.4.5.1 Revertive mode

In revertive mode, the ring network link will be recovered. After the RPL node receives the NR packet, it starts the WTB timer. After the timeout of the WTB timer, the RPL node will block the RPL link and send the RB NR packet, and then execute FDB Flush. After other ring network nodes receive the RB NR packet, they eliminate the blocking state of all non-RPL links, and then execute FDB Flush.

#### 1.4.5.2 Non-revertive mode

In the non-revertive mode, the ring network link is not automatically recovered. After receiving the NR packet, the RPL node does not make any response; after other ring network nodes receive the NR packets, they don't do any action. Only when the RPL node receives the “Clear” command, the RPL node blocks the RPL link and continues to send NR RB packets to two ring network ports, and then execute Flush FDB. After other ring network nodes receive the NR RB packet, they eliminate the blocking state of non-RPL link and execute Flush FDB.

### 1.4.6 Protection Switching— Forced Switching

In the normal ring network state, after the ring network node receives a forced switching command, it blocks data stream channel and the R-APS channel (Blocking a data stream channel and R-APS channel port) and opens other ring network ports and continues to send FS packets to two ring network ports, and then execute Flush FDB. After other ring network nodes receive the FS packet, they open RPL data stream channel and R-APS channel. After receiving the FS packet, the ring network node sending FS packet stops sending FS packet. After receiving the FS packet, the ring network nodes execute Flush FDB.

The above action completes an operation of forced switching; in order to keep switching operation normal, there is one point deserving our attention:

When a forced switching command has existed in the ring network, the later forced switching commands are acceptable unless this node has accepted a forced switching request in advance. At the same time, the node receiving new switching command must execute forced switching once again, block the port and send FS packets. Of course, the repeated execution of forced switching command will segment the ring network, so it is appropriate to avoid such adverse situation.

For the node which generates forced switching command, after receiving the “Clear” command, it removes forced switching command. The node continues to block the ring network port blocked by previous forced switching commands and sends NR packets to two ring network ports. But when the link is recovered, the revertive mode and non-revertive mode are not consistent in behavior and function.

#### 1.4.6.1 Revertive mode

In revertive mode, the ring network link will be recovered. After the RPL node receives the NR packet, it starts the WTB timer. After the timeout of the WTB timer, the RPL node will block the RPL link and send the RB NR packet, and then execute FDB Flush. After other ring network nodes receive the NR RB packet, they eliminate the blocking state of all non-RPL links, and then execute FDB Flush.

#### 1.4.6.2 Non-revertive mode

In the non-revertive mode, the ring network link is not automatically recovered. After receiving the NR packet, the RPL node does not make any response; after other ring network nodes receive the NR packets, they don't do any action. Only when the RPL node receives the “Clear” command, the RPL node blocks the RPL link and continues to send NR RB packets to two ring network ports, and then execute Flush FDB. After other ring network nodes receive the NR RB packet, they eliminate the blocking state of all non-RPL links and execute Flush FDB.

### 1.4.7 Switching Recovery Processing

The ring network protection node (RPL owner) realizes the ring network switching recovery through the WTR timer (Wait-to-Restore timer) and the WTB timer (Wait-to-Block timer). The WTR timer and WTB timer can be used to avoid frequent switching on the ring network.

The WTR timer is only valid in the revertive mode; in the non-revertive mode, after the fault recovery of the ring network from the protection state, the ring network doesn't recover, so there is no need to start the WTR timer. In the revertive mode, after the RPL node receives the NR message from other nodes, it starts the WTR timer; after the timeout of timer, the RPL node maintains the forwarding state of the RPL port, and it does not send the ring network recovery notification. If the RPL node receives the SF message, it indicates that the ring network has not been fully recovered; at this time, the node stop sthe WTR timer. After the timeout of WTR timer, the RPL node will re-block the RPL port.

The WTB timer is effective only in the revertive mode, which is used at the time of clearing the forced and manual switching command. When the forced switching command is cleared repeatedly, the WTB timer must ensure that a single forced switching command does not make RPL blocked repeatedly. When a manual switching command is cleared, the WTB timer must prevent RPL node against causing a closed ring because of receiving an outdated remote MS request in the recovery process.

The WTB timer must ensure that there is sufficient time to receive the remote SF, FS and MS packets, so the time of defining the WTB timer is 5 seconds longer than that of defining the Guard timer. This period of time is enough for one ring network node sending the packet to send 2 R-APS packets and allow the entire ring network to confirm each situation.

## Chapter 2 ERPS Configuration

### 2.1 ERPS Configuration Instructions

Please read the following instructions before configuring the ERPS ring network protection protocol:

- The ERPS port must be carried on the MEP port of the CFM; the MEP information must be configured to match with the MEP port for the ERPS port; after the configuration is successful, the ERPS port can be enabled normally.
- It must be configured that the default VLANs (or control VLANs) of all ring network ports are consistent , ensuring that the ERPS packet can be forwarded normally.
- In the case that the ERPS and EAPS protocols are used simultaneously, the default VLAN and control VLAN for ERPS ring network port cannot be the same as control VLAN for EAPS. The control VLAN for EAPS cannot forward the ERPS protocol packet.
- One port cannot be simultaneously used as the ring network port of ERPS and EAPS protocols.
- The ERPS protocol supports the configuration of physical port or aggregate port as the ring network port. However, the physical port that has been configured with the link aggregation, 802.1X authentication or port security cannot be configured as a ERPS ring network port.

### 2.2 ERPS Configuration Tasks

- [Configuring the ring network nodes](#)
- [Configuring the ring network ports](#)
- [Checking ring network protection protocol status](#)

#### 2.2.1 Configuring the Ring Network Nodes

In the global configuration mode, the switch is configured as ERPS node according to the following steps.

Command	Purpose
Switch_config# <b>erps</b> <i>id</i>	Configure ERPS ring network node instance and enter the node configuration mode.  id: Ring network instance number; Range 0-7.
Switch_config_ring# <b>control-vlan</b> <i>value</i>	Mandatory. Configure the control VLAN of the local node. No control VLAN: Delete the control

## Ethernet Ring Network (G8032-201003) Protection Configuration

	<p>VLAN of the local node. After the normal operation of the node, the change shall not be allowed.</p> <p>Value : Range: 1-4094. By default, no control-vlan.</p>
Switch_config_ring# <b>interconnection-node</b>	<p>Mandatory. Configure the local node as the interconnection node. No interconnection-node: Configure that the local node is not the interconnection node. After the normal operation of the node, the change shall not be allowed.</p> <p>By default, the local node is not the interconnection node.</p>
Switch_config_ring# <b>raps-virtual-channel</b>	<p>Mandatory. Configure that the local node uses the R-APS virtual channel. No Raps-virtual-channel: Configure that the local node doesn't use the R-APS virtual channel. After the normal operation of the node, the change shall not be allowed.</p> <p>By default, the local node uses the R-APS virtual channel.</p>
Switch_config_ring# <b>revertive-mode</b>	<p>Mandatory. Configure that the revertive mode of local node is the revertive mode. No revertive-mode: Configure that the revertive mode of local node is not the revertive mode. After the normal operation of the node, the change shall not be allowed.</p> <p>By default, the local node is the revertive mode.</p>
Switch_config_ring# <b>version value</b>	<p>Configure the local node's version.</p> <p>value: By default, 1; range: 0-2.</p>
Switch_config_ring# <b>wtr-time value</b>	<p>Configure the timeout value of WTR timer.</p> <p>Value: Timeout value: by default, 20 seconds; range: 10-720 seconds.</p>
Switch_config_ring# <b>guard-time value</b>	<p>Configure the timeout value of Guard Timer.</p> <p>When a port is recovered from the failure state, the Guard timer is prohibited to handle the received protocol packets in a short period of time to avoid the wrong protocol action caused by receiving the outdated packet.</p> <p>Value: 1 ms as the unit; 500 as the default value; range of 10-2000; step size of 10ms.</p>
Switch_config_ring# <b>send-time value</b>	<p>Configure the protocol packet sending cycle.</p> <p>value : Packet sending cycle: by default, 5 seconds; range: 1-10.</p>

## Ethernet Ring Network (G8032-201003) Protection Configuration

Switch_config_ring# <b>exit</b>	Exit from node configuration mode and enable the node.

**Note:**

1. Use the “**no erps id**” command to delete the ring network node configuration and node port configuration.
2. The “interconnection-node” “raps-virtual-channel” “revertive-mode” commands are mandatory, but they all have their default configuration, so when the local node is created, these commands can be omitted if the default values needn’t be amended.

## 2.2.2 Configuring the Ring Network Ports

The switch port is configured as the ring network port according to the following steps.

Command	Purpose
Switch_config# <b>interface</b> <i>interface-type</i> <i>interface-number</i>	Enter the port configuration mode. intf-name: Port name.
Switch_config_intf# <b>erps id ring-port</b>	Configure the port as a ordinary ring network port for the specified node. id: Ring network instance number.
Switch_config_intf# <b>erps id rpl</b>	Configure the port as a ring network protection link for the specified node. In the case of automatically discovering enabling, the function of this command is equivalent to the change of a priority value to 0. id: Ring network instance number.
Switch_config_intf# <b>erps id neighbour</b>	Configure the port as a RPL neighbor port of the specified node; meanwhile, this port must be connected to the RPL port and must be configured as a RPL neighbor port. id: Ring network instance number.
Switch_config_intf# <b>erps id mep [up   down] md</b> <i>md-WORD</i> <b>ma</b> <i>ma-WORD</i> <b>level</b> <i>level-id</i> <b>local</b> <i>local-id</i> <b>remote</b> <i>remote-id</i>	Bind ERPS port with MEP port. id: Ring network instance number. md-WORD: MEP maintenance domain information. ma-WORD: MEP maintenance link information. level-id: MEP level information. local-id: MEP local ID information. remote-id: MEP remote ID information.

## Ethernet Ring Network (G8032-201003) Protection Configuration

Switch_config_intf# <b>exit</b>	Exit from port configuration mode.
---------------------------------	------------------------------------

**Note:**

1. Configure the command through the “**no erps id rpl**” port, and change the RPL port into ordinary ring network port.
2. Configure the command through the “**no erps id ring-port(neighbor)**” port, delete the ordinary ring network port (RPL neighbor port) or RPL port configuration.
3. In the case that the ring network node is not configured globally, use the command “**erps id ring-port (neighbor)**” and “**rpl**” to simultaneously create the ring network nodes.
4. “up mep” is only configured in the interconnection-node, and the interconnection-node can only be configured with one ring network port.

### 2.2.3 Ring Network Control Commands

In the management mode, use the following commands to control the ring network status.

Command	Purpose
<b>erps id ForcedSwitch interface</b> <i>interface-type</i> <i>interface-number</i>	For the node, execute the forced switching to the port “interface-type interface-number”.  id: Ring network instance number.
<b>erps id ManualSwitch interface</b> <i>interface-type</i> <i>interface-number</i>	For the node, execute the manual switching to the port “interface-type interface-number”.  id: Ring network instance number.
<b>erps id Clear</b>	Clear the switching command of the node.  id: Ring network instance number.

### 2.2.4 Checking Ring Network Protection Protocol Status

Use the following commands to check the ring network protection protocol status.

Command	Purpose
<b>show erps id</b>	Check the summary information of ring network protection protocol and ring network port.  id: Ring network instance number.
<b>show erps id detail</b>	Check the detailed information of ring network protection protocol and port.
<b>show erps interface</b> <i>interface-type</i> <i>interface-number</i>	Check the status information of ring network port.



## 2.3 ERPS Configuration Instance

### 2.3.1 Configuration Instance 1 — ERPS Single Ring Configuration

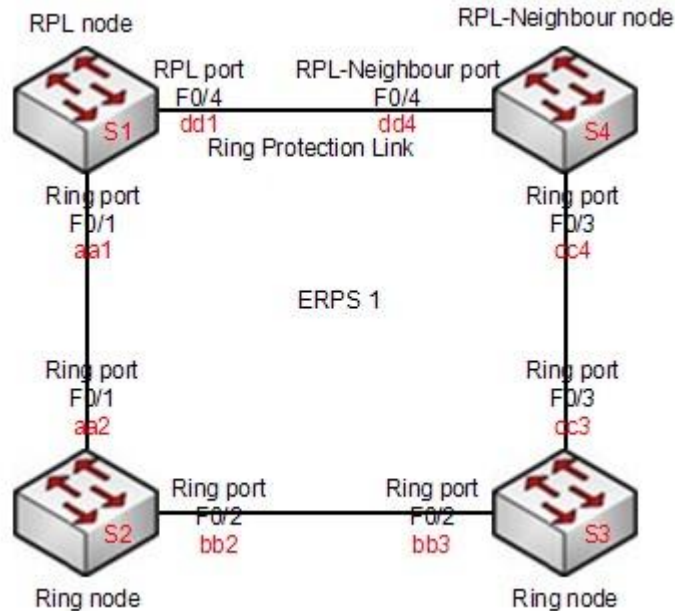


Figure 5.1 ERPS single ring configuration

As is shown in Figure 5.1, the configuration of [S1](#), [S2](#), [S3](#) and [S4](#) is as follows:

#### 2.2.1.1 Configuring Switch 1 (S1)

Configure the CFM function:

```
Switch# config
Switch_config# ethernet cfm ENABLE
Switch_config# ethernet cfm md mdnf STRING mdn a level 4
Switch_config_cfm# ma manf STRING man a meps 1-2 vlan 2
Switch_config_cfm#exit
Switch_config# ethernet cfm md mdnf STRING mdn d level 4
Switch_config_cfm# ma manf STRING man d meps 1,4 vlan 2
Switch_config_cfm#exit
Switch_config#interface f0/1
Switch_config_f0/1# ethernet cfm ENABLE
Switch_config_f0/1# ethernet cfm mep add mdnf STRING mdn a manf STRING man a mepid 1
Switch_config_f0/1# ethernet cfm mep ENABLE mdnf STRING mdn a manf STRING man a mepid 1
Switch_config_f0/1# ethernet cfm mep cci-ENABLE mdnf STRING mdn a manf STRING man a mepid 1
```

## Ethernet Ring Network (G8032-201003) Protection Configuration

```

Switch_config_f0/1# interface f0/4
Switch_config_f0/4# ethernet cfm ENABLE
Switch_config_f0/4# ethernet cfm mep add mdnf STRING mdn d manf STRING man d mepid 1
Switch_config_f0/4# ethernet cfm mep ENABLE mdnf STRING mdn d manf STRING man d mepid 1
Switch_config_f0/4# ethernet cfm mep cci-ENABLE mdnf STRING mdn d manf STRING man d mepid 1

```

Configure the ring network node:

```

Switch_config#erps 1
Switch_config_ring1#control-vlan 2
Switch_config_ring1#exit
Switch_config#

```

Configure the ordinary port:

```

Switch_config# interface f0/1
Switch_config_f0/1# erps 1 ring-port
Switch_config_f0/1# erps 1 mep down md a ma a level 4 local 1 remote 2

```

Configure the RPLport:

```

Switch_config# interface f0/4
Switch_config_f0/4# erps 1 rpl
Switch_config_f0/4# erps 1 mep down md d ma d level 4 local 1 remote 4

```

### 2.2.1.2 Configuring Switch 2 (S2)

Configure the CFM function:

```

Switch# config
Switch_config# ethernet cfm ENABLE
Switch_config# ethernet cfm md mdnf STRING mdn a level 4
Switch_config_cfm# ma manf STRING man a meps 1-2 vlan 2
Switch_config_cfm#exit
Switch_config# ethernet cfm md mdnf STRING mdn b level 4
Switch_config_cfm# ma manf STRING man b meps 2-3 vlan 2
Switch_config_cfm#exit
Switch_config#interface f0/1
Switch_config_f0/1# ethernet cfm ENABLE
Switch_config_f0/1# ethernet cfm mep add mdnf STRING mdn a manf STRING man a mepid 2
Switch_config_f0/1# ethernet cfm mep ENABLE mdnf STRING mdn a manf STRING man a mepid 2
Switch_config_f0/1# ethernet cfm mep cci-ENABLE mdnf STRING mdn a manf STRING man a mepid 2
Switch_config_f0/1# interface f0/2
Switch_config_f0/2# ethernet cfm ENABLE
Switch_config_f0/2# ethernet cfm mep add mdnf STRING mdn b manf STRING man b mepid 2

```

---

 Ethernet Ring Network (G8032-201003) Protection Configuration
 

---

```
Switch_config_f0/2# ethernet cfm mep ENABLE mdnf STRING mdn b manf STRING man b
mepid 2
```

```
Switch_config_f0/2# ethernet cfm mep cci-ENABLE mdnf STRING mdn b manf STRING man b
mepid 2
```

Configure the ring network node:

```
Switch_config#erps 1
Switch_config_ring1#control-vlan 2
Switch_config_ring1#exit
Switch_config#
```

Configure the ordinary port:

```
Switch_config# interface f0/1
Switch_config_f0/1# erps 1 ring-port
Switch_config_f0/1# erps 1 mep down md a ma a level 4 local 2 remote 1
Switch_config_f0/1# interface f0/2
Switch_config_f0/2# erps 1 ring-port
Switch_config_f0/2# erps 1 mep down md b ma b level 4 local 2 remote 3
```

### 2.2.1.3 Configuring Switch 3 (S3)

Configure the CFM function:

```
Switch# config
Switch_config# ethernet cfm ENABLE
Switch_config# ethernet cfm md mdnf STRING mdn b level 4
Switch_config_cfm# ma manf STRING man b meps 2-3 vlan 2
Switch_config_cfm#exit
Switch_config# ethernet cfm md mdnf STRING mdn c level 4
Switch_config_cfm# ma manf STRING man c meps 3-4 vlan 2
Switch_config_cfm#exit
Switch_config#interface f0/2
Switch_config_f0/2# ethernet cfm ENABLE
Switch_config_f0/2# ethernet cfm mep add mdnf STRING mdn b manf STRING man b mepid 3
Switch_config_f0/2# ethernet cfm mep ENABLE mdnf STRING mdn b manf STRING man b
mepid 3
Switch_config_f0/2# ethernet cfm mep cci-ENABLE mdnf STRING mdn b manf STRING man b
mepid 3
Switch_config_f0/2# interface f0/3
Switch_config_f0/3# ethernet cfm ENABLE
Switch_config_f0/3# ethernet cfm mep add mdnf STRING mdn c manf STRING man c mepid 3
Switch_config_f0/3# ethernet cfm mep ENABLE mdnf STRING mdn c manf STRING man c
mepid 3
Switch_config_f0/3# ethernet cfm mep cci-ENABLE mdnf STRING mdn c manf STRING man c
mepid 3
```

Configure the ring network node:

```
Switch_config#erps 1
```

## Ethernet Ring Network (G8032-201003) Protection Configuration

```

Switch_config_ring1#control-vlan 2
Switch_config_ring1#exit
Switch_config#

Configure the ordinary port:

Switch_config# interface f0/2
Switch_config_f0/2# erps 1 ring-port
Switch_config_f0/2# erps 1 mep down md b ma b level 4 local 3 remote 2
Switch_config_f0/2# interface f0/3
Switch_config_f0/3# erps 1 ring-port
Switch_config_f0/3# erps 1 mep down md c ma c level 4 local 3 remote 4

```

## 2.2.1.4 Configuring Switch 4 (S4)

Configure the CFM function:

```

Switch# config
Switch_config# ethernet cfm ENABLE
Switch_config# ethernet cfm md mdnf STRING mdn c level 4
Switch_config_cfm# ma manf STRING man c meps 3-4 vlan 2
Switch_config_cfm#exit
Switch_config# ethernet cfm md mdnf STRING mdn d level 4
Switch_config_cfm# ma manf STRING man d meps 1,4 vlan 2
Switch_config_cfm#exit
Switch_config#interface f0/3
Switch_config_f0/3# ethernet cfm ENABLE
Switch_config_f0/3# ethernet cfm mep add mdnf STRING mdn c manf STRING man c mepid 4
Switch_config_f0/3# ethernet cfm mep ENABLE mdnf STRING mdn c manf STRING man c
mepid 4
Switch_config_f0/3# ethernet cfm mep cci-ENABLE mdnf STRING mdn c manf STRING man c
mepid 4
Switch_config_f0/3#interface f0/4
Switch_config_f0/4# ethernet cfm ENABLE
Switch_config_f0/4# ethernet cfm mep add mdnf STRING mdn d manf STRING man d mepid 4
Switch_config_f0/4# ethernet cfm mep ENABLE mdnf STRING mdn d manf STRING man d
mepid 4
Switch_config_f0/4# ethernet cfm mep cci-ENABLE mdnf STRING mdn d manf STRING man d
mepid 4

```

Configure the ring network node:

```

Switch_config#erps 1
Switch_config_ring1#control-vlan 2
Switch_config_ring1#exit
Switch_config#

Configure the ordinary port:

Switch_config# interface f0/3
Switch_config_f0/3# erps 1 ring-port
Switch_config_f0/3# erps 1 mep down md c ma c level 4 local 4 remote 3

```

## Ethernet Ring Network (G8032-201003) Protection Configuration

Configure the RPL neighbor port:

```
Switch_config# interface f0/4
Switch_config_f0/4# erps 1 neighbour
Switch_config_f0/4# erps 1 mep down md d ma d level 4 local 4 remote 1
```

### 2.3.2 Configuration Instance 2 — ERPS Multiple-ring Configuration

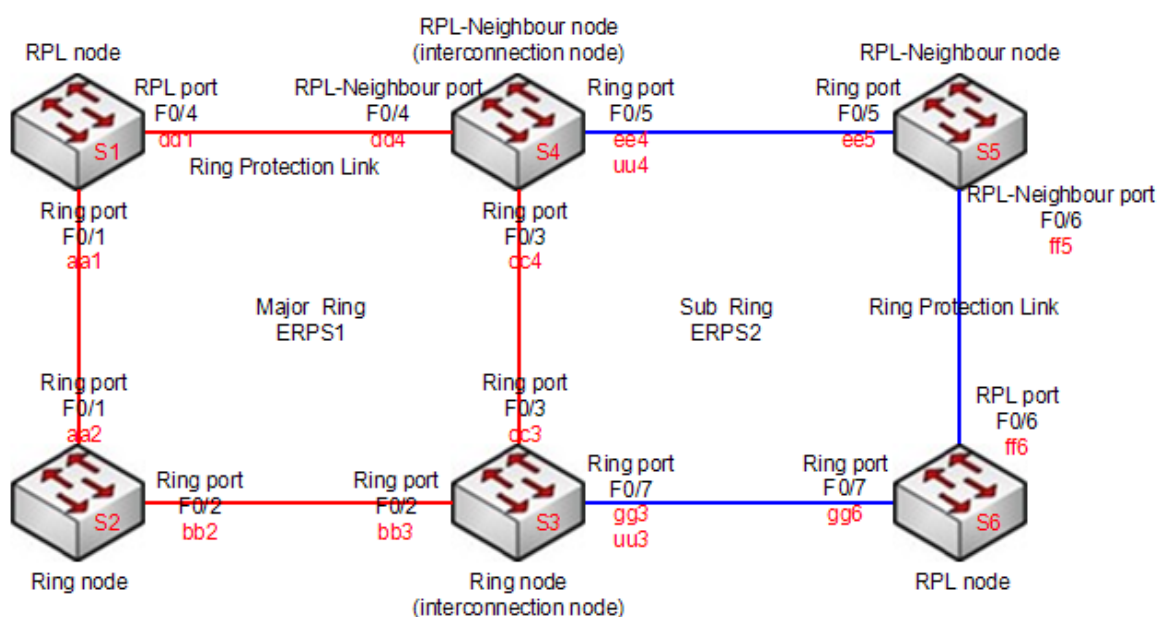


Figure 5.2 ERPS multiple-ring configuration

As is shown in Figure 5.2, the configuration of Interconnection Node [S3](#) and [S4](#) is as follows; the configuration of other nodes is omitted.

#### 2.3.2.1 Configuring Switch 3 (S3)

Configure the CFM function:

```
Switch# config
Switch_config# ethernet cfm ENABLE
Switch_config# ethernet cfm md mdnf STRING mdn b level 4
Switch_config_cfm# ma manf STRING man b meps 2-3 vlan 2
Switch_config_cfm#exit
Switch_config# ethernet cfm md mdnf STRING mdn c level 4
Switch_config_cfm# ma manf STRING man c meps 3-4 vlan 2
Switch_config_cfm#exit
Switch_config# ethernet cfm md mdnf STRING mdn g level 4
Switch_config_cfm# ma manf STRING man g meps 3,6 vlan 3
Switch_config_cfm#exit
Switch_config# ethernet cfm md mdnf STRING mdn u level 5
Switch_config_cfm# ma manf STRING man u meps 3-4 vlan 3
```

## Ethernet Ring Network (G8032-201003) Protection Configuration

```

Switch_config_cfm#exit
Switch_config#interface f0/2
Switch_config_f0/2# ethernet cfm ENABLE
Switch_config_f0/2# ethernet cfm mep add mdnf STRING mdn b manf STRING man b mepid 3
Switch_config_f0/2# ethernet cfm mep ENABLE mdnf STRING mdn b manf STRING man b
mepid 3
Switch_config_f0/2# ethernet cfm mep cci-ENABLE mdnf STRING mdn b manf STRING man b
mepid 3
Switch_config_f0/2# interface f0/3
Switch_config_f0/3# ethernet cfm ENABLE
Switch_config_f0/3# ethernet cfm mep add mdnf STRING mdn c manf STRING man c mepid 3
Switch_config_f0/3# ethernet cfm mep ENABLE mdnf STRING mdn c manf STRING man c
mepid 3
Switch_config_f0/3# ethernet cfm mep cci-ENABLE mdnf STRING mdn c manf STRING man c
mepid 3
Switch_config_f0/3# interface f0/7
Switch_config_f0/7# ethernet cfm ENABLE
Switch_config_f0/7# ethernet cfm mep add mdnf STRING mdn g manf STRING man g mepid 3
Switch_config_f0/7# ethernet cfm mep ENABLE mdnf STRING mdn g manf STRING man g
mepid 3
Switch_config_f0/7# ethernet cfm mep cci-ENABLE mdnf STRING mdn g manf STRING man g
mepid 3
Switch_config_f0/7# ethernet cfm mep add mdnf STRING mdn u manf STRING man u mepid 3
direction up
Switch_config_f0/7# ethernet cfm mep ENABLE mdnf STRING mdn u manf STRING man u
mepid 3
Switch_config_f0/7# ethernet cfm mep cci-ENABLE mdnf STRING mdn u manf STRING man u
mepid 3

```

Configure the ring network node:

```

Switch_config#erps 1
Switch_config_ring1#control-vlan 2
Switch_config_ring1#exit
Switch_config#
Switch_config#erps 2
Switch_config_ring1#control-vlan 3
Switch_config_ring1#interconnection-node
Switch_config_ring1#exit
Switch_config#

```

Configure the ordinary port of ERPS1:

```

Switch_config# interface f0/2
Switch_config_f0/2# erps 1 ring-port
Switch_config_f0/2# erps 1 mep down md b ma b level 4 local 3 remote 2
Switch_config_f0/2# interface f0/3
Switch_config_f0/3# erps 1 ring-port
Switch_config_f0/3# erps 1 mep down md c ma c level 4 local 3 remote 4

```

Configure the ordinary port of ERPS2:

## Ethernet Ring Network (G8032-201003) Protection Configuration

```

Switch_config_f0/3# interface f0/7
Switch_config_f0/7# erps 2 ring-port
Switch_config_f0/7# erps 2 mep down md g ma g level 4 local 3 remote 6
Switch_config_f0/7# erps 2 mep down md u ma u level 5 local 3 remote 4

```

## 2.3.2.2 Configuring Switch 4 (S4)

Configure the CFM function:

```

Switch# config
Switch_config# ethernet cfm ENABLE
Switch_config# ethernet cfm md mdnf STRING mdn c level 4
Switch_config_cfm# ma manf STRING man c meps 3-4 vlan 2
Switch_config_cfm#exit
Switch_config# ethernet cfm md mdnf STRING mdn d level 4
Switch_config_cfm# ma manf STRING man d meps 1,4 vlan 2
Switch_config_cfm#exit
Switch_config# ethernet cfm md mdnf STRING mdn e level 4
Switch_config_cfm# ma manf STRING man e meps 4-5 vlan 3
Switch_config_cfm#exit
Switch_config# ethernet cfm md mdnf STRING mdn u level 5
Switch_config_cfm# ma manf STRING man u meps 3-4 vlan 3
Switch_config_cfm#exit
Switch_config#interface f0/3
Switch_config_f0/3# ethernet cfm ENABLE
Switch_config_f0/3# ethernet cfm mep add mdnf STRING mdn c manf STRING man c mepid 4
Switch_config_f0/3# ethernet cfm mep ENABLE mdnf STRING mdn c manf STRING man c mepid 4
Switch_config_f0/3# ethernet cfm mep cci-ENABLE mdnf STRING mdn c manf STRING man c mepid 4
Switch_config_f0/3#interface f0/4
Switch_config_f0/4# ethernet cfm ENABLE
Switch_config_f0/4# ethernet cfm mep add mdnf STRING mdn d manf STRING man d mepid 4
Switch_config_f0/4# ethernet cfm mep ENABLE mdnf STRING mdn d manf STRING man d mepid 4
Switch_config_f0/4# ethernet cfm mep cci-ENABLE mdnf STRING mdn d manf STRING man d mepid 4
Switch_config_f0/4# interface f0/5
Switch_config_f0/5# ethernet cfm ENABLE
Switch_config_f0/5# ethernet cfm mep add mdnf STRING mdn e manf STRING man e mepid 4
Switch_config_f0/5# ethernet cfm mep ENABLE mdnf STRING mdn e manf STRING man e mepid 4
Switch_config_f0/5# ethernet cfm mep cci-ENABLE mdnf STRING mdn e manf STRING man e mepid 4
Switch_config_f0/5# ethernet cfm mep add mdnf STRING mdn u manf STRING man u mepid 4 direction up
Switch_config_f0/5# ethernet cfm mep ENABLE mdnf STRING mdn u manf STRING man u mepid 4

```

---

 Ethernet Ring Network (G8032-201003) Protection Configuration
 

---

```
Switch_config_f0/5# ethernet cfm mep cci-ENABLE mdnf STRING mdn u manf STRING man u
mepid 4
```

Configure the ring network node:

```
Switch_config#erps 1
Switch_config_ring1#control-vlan 2
Switch_config_ring1#exit
Switch_config#
Switch_config#erps 2
Switch_config_ring1#control-vlan 3
Switch_config_ring1#interconnection-node
Switch_config_ring1#exit
Switch_config#
```

Configure the ordinary port of ERPS1:

```
Switch_config# interface f0/3
Switch_config_f0/3# erps 1 ring-port
Switch_config_f0/3# erps 1 mep down md c ma c level 4 local 4 remote 3
```

Configure the RPL neighbour port of ERPS1:

```
Switch_config# interface f0/4
Switch_config_f0/4# erps 1 neighbour
Switch_config_f0/4# erps 1 mep down md d ma d level 4 local 4 remote 1
```

Configure the ordinary port of ERPS2:

```
Switch_config# interface f0/5
Switch_config_f0/5# erps 2 ring-port
Switch_config_f0/5# erps 2 mep down md e ma e level 4 local 4 remote 5
Switch_config_f0/5# erps 2 mep down md u ma u level 5 local 4 remote 3
```

### Show erps of Switch 3 (S3):

```
Switch_config# show erps
```

Ethernet Ring Protection Switching

Ring1

```

RPL Owner   Priority   Unknown
           Address
           This node is the RPL Owner

Node ID     Priority   32770 (priority 32770 id 1)
Address     00E0.0F81.111B
Control Vlan 2
Version     1
RAPS Virtual Channel: True
Revertive Mode: Revertive
State Pending      WTR False
```



Ethernet Ring Network (G8032-201003) Protection Configuration

Signal Fail False Sending NR  
 WTR time 0/20 sec WTB time 0/6 sec  
 Guard time 0/500 ms Send time 1/5 sec

Interface	Role	State	Status	MEP Role
F0/2	Ring-Port	BLK	Link-down	DOWN-MEP
F0/3	Ring-Port	FWD	Link-down	DOWN-MEP

Ring2

RPL Owner Priority Unknown  
 Address

Node ID Priority 32770 (priority 32768 id 2)  
 Address 00E0.0F81.111B  
 Control Vlan 3  
 Version 1

This node is the interconnection node

RAPS Virtual Channel: True  
 Revertive Mode: Revertive  
 State Protection  
 Signal Fail False Sending SF  
 WTR time 0/20 sec WTB time 0/6 sec  
 Guard time 0/500 ms Send time 1/5 sec

Interface	Role	State	Status	MEP Role
F0/7	Ring-Port	FWD	Link-up	DOWN-MEP
F0/7	(up) Ring-Port	BLK	Link-down	UP-MEP

## 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/Canceling 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 .....	2
1.2.6 Setting Querier of MLD-Snooping .....	3
1.2.7 Setting the Port of the Static Multicast Router .....	3
1.2.8 Enabling/Disabling Immediate Leave .....	3
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 solves the above-mentioned problems by monitoring the Query or Report packets of MLD-Snooping, MLD snooping can work normally only when there exists the multicast router.

## 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
<b>ipv6 mld-snooping</b>	Enables MLD snooping multicast.
<b>no ipv6 mld-snooping</b>	Disables MLD snooping.

**Note:**

After MLD-Snooping is enabled and the multicast packets fail to be found, the multicast packets whose destination addresses are not registered are dropped.

### 1.2.2 Enabling/Disabling the Solicitation of Hardware Forward of Multicast Group

Run the following commands in global configuration mode.

Command	Purpose
<b>ipv6 mld-snooping solicitation</b>	Enables the solicitation of hardware forward of multicast group.
<b>no ipv6 mld-snooping solicitation</b>	Disables the solicitation of hardware forward of multicast group.

### 1.2.3 Adding/Canceling the Static Multicast Address of VLAN

Run the following commands in global configuration mode.

Command	Purpose
<b>ipv6 mld-snooping vlan <i>vlan_id</i> static X:X:X:X:X interface <i>intf_name</i></b>	Adds the static multicast address of VLAN.
<b>no ipv6 mld-snooping vlan <i>vlan_id</i> static X:X:X:X:X interface <i>intf_name</i></b>	Removes the static multicast address of VLAN.

### 1.2.4 Setting Router Age Timer of MLD-Snooping

Run the following commands in global configuration mode.

Command	Purpose
<b>ipv6 mld-snooping timer router-age <i>timer_value</i></b>	Sets the router age of MLD-Snooping.
<b>no ipv6 mld-snooping timer router-age</b>	Resumes the default router age of MLD-Snooping.

**Note:**

The settings of this timer shall refer to the query period settings of MLD-Snooping and be larger than the query period. It is recommended to set the router age timer to be triple of the query period.

The default router age of MLD snooping is 260 seconds.

### 1.2.5 Setting Response Time Timer of MLD-Snooping

Run the following commands in global configuration mode.

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

<b>ipv6 mld-snooping timer response-time</b> <i>timer_value</i>	Sets the response time of MLD-Snooping.
<b>no ipv6 mld-snooping timer response-time</b>	Resumes the default response time of MLD-Snooping.

**Note:**

The value of the timer cannot be set too small, or the multicast communication may be unstable.

The default response time of MLD snooping is 10 seconds.

### 1.2.6 Setting Querier of MLD-Snooping

If there is no multicast router in enabling VLAN with MLD-snooping, enable Querier of MLD-snooping module (which acts as a virtualized multicast router) to forward IGMP group query packets regularly. (The function can only be enabled or disabled when all VLANs enable MLD-snooping)

When there is no multicast router in the LAN and the multicast flow has no need for routing, run following command in global configuration mode activate the self-query of the switch:

Command	Purpose
<b>[no] ipv6 mld-snooping querier</b> <b>[address [ip_addr]]</b>	Sets Querier of MLD-snooping. Selects the address of the optional parameter as the source IP of the Query packet.

IGMP-snooping querier is disabled by default. The source IP address of the fake Query packet is FE80::3FF:FEFE:FD00:1.

**Note:**

Enable Querier, if there is a multicast router in the VLAN, the function becomes invalid automatically; if the multicast router is timeout, the function become valid automatically.

### 1.2.7 Setting the Port of the Static Multicast Router

Run the following commands in global configuration mode.

Command	Operation
<b>ipv6 mld-snooping vlan WORD mrouter</b> interface <i>inft_name</i>	Sets the static multicast router's port of MLD snooping in Vlan <b>word</b> .
<b>no ipv6 mld-snooping vlan WORD mrouter</b> interface <i>inft_name</i>	Deletes the static multicast router's port of MLD snooping in Vlan <b>word</b> .

### 1.2.8 Enabling/Disabling Immediate Leave

Run the following commands in global configuration mode.

Command	Purpose
<b>ipv6 mld-snooping vlan WORD immediate-leave</b>	Enables the immediate-leave functionality.
<b>no ipv6 mld-snooping vlan WORD immediate-leave</b>	Resumes the default settings.

### 1.2.9 Monitoring and Maintaining MLD-Snooping Multicast

Run the following commands in EXEC mode:

Command	Operation
<b>show ipv6 mld-snooping</b>	Displays the configuration of MLD-Snooping.
<b>show ipv6 mld-snooping timer</b>	Displays the clock of MLD-Snooping.
<b>show ipv6 mld -snooping groups</b>	Displays the multicast group of MLD-Snooping.
<b>show ipv6 mld-snooping statistics</b>	Displays the statistics information of MLD-Snooping.
<b>show ipv6 mld-snooping vlan</b>	Displays the configuration of MLD-Snooping in VLAN.
<b>show ipv6 mld-snooping mac</b>	Displays the multicast MAC addresses recorded by MLD snooping.

The MLD-Snooping information is displayed below:

```
#show ipv6 mld-snooping
Global MLD snooping configuration:
-----
Globally enable      : Enabled
Querier              : Enabled
Querier address     : FE80::3FF:FEFE:FD00:1
Router age           : 260 s
Response time        : 10 s
Handle Solicitation  : Disabled

Vlan 1:
-----
Running
Routers: SWITCH(querier);
```

The multicast group of MLD-Snooping is displayed below:

```
#show ipv6 mld--snooping groups
Vlan Group          Type Port(s)
-----
1 FF02::1:FF32:1B9B MLD G2/23
```

```

1 FF02::1:FF00:2 MLD G2/23
1 FF02::1:FF00:12 MLD G2/23
1 FF02::1:FF13:647D MLD G2/23
2 FF02::1:FF00:2 MLD G2/22
2 FF02::1:FF61:9901 MLD G2/22

```

The timer of MLD-Snooping is displayed below:

```
#show ipv6 mld-snooping timers
```

```
vlan 1 Querier on port 0 : 251
```

```
#
```

**Querier on port 0:** 251 meaning the router age timer times out.

**vlan 2 multicast address 3333.0000.0005 response time :** This shows the time period from receiving a multicast query packet to the present; if there is no host to respond when the timer times out, the port will be canceled.

The MLD-snooping statistics information is displayed below:

```
#show ipv6 mld-snooping statistics
```

```
vlan 1
```

```

-----
v1_packets:0          quantity of v1 packets
v2_packets:6          quantity of v2 packets
v3_packets:0          quantity of v3 packets
general_query_packets:5  Quantity of general query packets
special_query_packets:0  Quantity of special query packets
listener_packets:6      Quantity of Report packets
done_packets:0         Quantity of Leave packets
err_packets:0          Quantity of error packets

```

The MLD-Snooping proxying is displayed below:

```
#show ipv6 mld-snooping mac
```

```

Vlan Mac                Ref Flags
-----
1 3333:0000:0001         1 2
2 3333:ff61:9901         1 0
   FF02::1:FF61:9901
1 3333:0000:0002         1 2
1 3333:ff00:0002         1 0
   FF02::1:FF00:2
1 3333:ff00:0012         1 0
   FF02::1:FF00:12
1 3333:ff13:647d         1 0
   FF02::1:FF13:647D
1 3333:ff32:1b9b         1 0
   FF02::1:FF32:1B9B
2 3333:ff00:0002         1 0
   FF02::1:FF00:2
1 3333:ff00:0001         1 2

```



1	3333:ff8e:7000	1	2
---	----------------	---	---

## DHCP-SNOOPING Configuration

# Table of Contents

Table of Contents .....	ii
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 Attack Prevention in a VLAN .....	2
1.1.4 Setting an Interface to a DHCP-Trusting Interface .....	2
1.1.5 Enabling or Disabling the Fast Update Function of the Binding Table .....	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 .....	4
1.1.10 Setting DHCP-Snooping Option 82 .....	4
1.1.11 Setting the Policy of DHCP-Snooping Option82 Packets .....	6
1.1.12 Configuring the TFTP Server for Backing up Interface Binding .....	6
1.1.13 Configuring a File Name for Interface Binding Backup .....	7
1.1.14 Configuring the Interval for Checking Interface Binding Backup .....	7
1.1.15 Configures Interface Binding Manually .....	7
1.1.16 Forwarding DHCP Packets .....	8
1.1.17 Multi-vlan Forwarding Dhcp Packets .....	8
1.1.18 Monitoring and Maintaining DHCP-Snooping .....	8
1.1.19 Example of DHCP-Snooping Configuration .....	10

# 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
- Setting an Interface to a DHCP-Trusting Interface
- Enabling DAI in a VLAN
- Setting an Interface to an ARP-Trusting Interface
- Enabling Source IP Address Monitoring in a VLAN
- Setting A Trust Interface for Monitoring Source IP Address
- Binding DHCP Snooping to a Standby TFTP Server
- Configuring a file name for DHCP-snooping binding backup
- Configuring an interval for DHCP-snooping binding backup
- Configuring or adding the binding relationship manually
- Monitoring and Maintaining DHCP-Snooping
- DHCP-Snooping Example

### 1.1.1 Enabling/Disabling DHCP-Snooping

Run the following commands in global configuration mode.

Command	Purpose
<b>ip dhcp-relay snooping</b>	Enables DHCP-snooping.
<b>no ip dhcp-relay snooping</b>	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. The switch will drop the attack packets of DHCP DOS.

Run the following commands in global configuration mode.

Command	Purpose
<b>ip dhcp-relay snooping vlan</b> <i>vlan_id</i>	Enables DHCP-snooping in a VLAN.
<b>no ip dhcp-snooping vlan</b> <i>vlan_id</i>	Disables DHCP-snooping in a VLAN.

### 1.1.3 Enabling DHCP Attack Prevention 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
<b>ip dhcp-relay snooping vlan</b> <i>vlan_id</i> <b>max-client</b> <i>number</i>	Enables DHCP anti-attack in a VLAN.
<b>no ip dhcp-relay snooping vlan</b> <i>vlan_id</i> <b>max-client</b>	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	Purpose
<b>dhcp snooping trust</b>	Sets an interface to a DHCP-trusting interface.
<b>no dhcp snooping trust</b>	Resumes an interface to a DHCP-distrusted interface.

The interface is a distrusted interface by default.

### 1.1.5 Enabling or Disabling the Fast Update Function of the Binding Table

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	Purpose
<b>ip dhcp-relay snooping rapid-refresh-bind</b>	Enables the fast update function of the binding table.
<b>no ip dhcp-relay snooping rapid-refresh-bind</b>	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	Purpose
<b>ip arp inspection vlan <i>vlanid</i></b>	Enables dynamic ARP monitoring on all distrusted ports in a VLAN.
<b>no ip arp inspection vlan <i>vlanid</i></b>	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	Purpose
<b>arp inspection trust</b>	Sets an interface to an ARP-trusting interface.
<b>no arp inspection trust</b>	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	Purpose
<b>ip verify source vlan <i>vlanid</i></b>	Enables source IP address checkup on all distrusted interfaces in a VLAN.
<b>no ip verify source vlan <i>vlanid</i></b>	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 an Interface to the One Which is Trusted by IP Source Address Monitoring

Source address checkup is not enabled on an interface if the interface has a trusted source IP address.

Run the following commands in interface configuration mode.

Command	Purpose
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	Purpose
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	Purpose
ip dhcp-relay snooping information option format {snmp-ifindex/manual/cm-type/hn-type [host]}	Sets the format of option82 that the DHCP packets carry when they are forwarded by DHCP-Snooping. The option is SNMP-IFINDEX, manual configuration, cm or cisco.
no ip dhcp-relay snooping	Sets that option82 is not carried when DHCP-snooping forwards

information option format {snmp-ifindex/manual/cm-type/hn-type [host]}	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	Purpose
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 <b>hex</b> [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 to 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	Purpose
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 <b>hex</b> [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	Purpose
<b>dhcp snooping information vendor-specific string STRING</b>	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 STRING. This command is set on the port that connects the client.
<b>dhcp snooping information vendor-specific hex</b> [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.
<b>no dhcp snooping information vendor-specific</b>	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	Purpose
<b>dhcp snooping information drop</b>	Drops the request packets that contain option82.

“Append” policy: Run the following command in port mode to add the request packets with option82.

Command	Purpose
<b>dhcp snooping information append</b>	Enables the function to add option82 on a port.
<b>dhcp snooping information append first-subop9-param hex</b> [xx-xx-xx-xx-xx-xx]	Stands for the Hex system of the first parameter carried by option82 vendor-specific (suboption9).
<b>dhcp snooping information append second-subop9-param hex</b> [xx-xx-xx-xx-xx-xx]	Stands for the Hex system of the second parameter carried by option82 vendor-specific (suboption9).

### 1.1.12 Configuring the TFTP Server for Backing up Interface Binding

After the switch configuration is rebooted, the previously-configured interface binding will be lost. In this case, there is no binding relationship on this interface. After source IP address monitoring is enabled, the switch rejected forwarding all IP packets. After the TFTP server is configured for interface binding backup, the binding relationship will be backed up to the server through the TFTP protocol. After the switch is restarted, the switch automatically downloads the binding list from the TFTP server, securing the normal running of the network.

Run the following commands in global configuration mode.

Command	Purpose
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>	Cancels the TFTP Server for backing up interface binding.

### 1.1.13 Configuring a File Name for Interface Binding Backup

When backing up the interface binding relationship, the corresponding file name will be saved on the TFTP server. In this way, different switches can back up their own interface binding relationships to the same TFTP server.

Run the following commands in global configuration mode.

Command	Purpose
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	Cancels a file name for interface binding backup.

### 1.1.14 Configuring the Interval for Checking Interface Binding Backup

The MAC-to-IP binding relationship on an interface changes dynamically. Hence, you need check whether the binding relationship updates after a certain interval. If the binding relationship updates, it need be backed up again. The default interval is 30 minutes.

Run the following commands in global configuration mode.

Command	Purpose
ip dhcp-relay snooping write-immediately	Configuring the immediate backup of DHCP Snooping when the binding information changes.
ip dhcp-relay snooping write <i>num</i>	Configures the interval for checking interface binding backup.
no ip dhcp-relay snooping write-time	Resumes the interval of checking interface binding backup to the default settings.

### 1.1.15 Configures 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	Purpose
<code>ip source binding <i>MAC IP</i> interface <i>name</i> [vlan <i>vlan-id</i>]</code>	Configures interface binding manually.
<code>no ip source binding <i>MAC IP</i> vlan <i>vlan-id</i></code>	Cancels an interface binding item.

### 1.1.16 Forwarding DHCP Packets

The following command can be used to forward the DHCP packets to the designated DHCP server to realize DHCP relay. The negative form of this command can be used to shut down DHCP relay.

Note: This command can only be used to enable DHCP relay on L2 switches, while on L3 switches, DHCP relay is realized by the DHCP server.

Run the following commands in global configuration mode.

Command	Purpose
<code>ip dhcp-relay agent</code>	Enables DHCP relay.
<code>ip dhcp-relay helper-address <i>address</i> vlan <i>vlan-id</i></code>	Configures the destination address and VLAN of the relay.

### 1.1.17 Multi-vlan Forwarding Dhcp Packets

The **dhcp vlan remap** forwarding function of layer-2 switch is matching original vlan and **dhcp client mac** address. If the match succeeds, redirects dhcp request to designated vlan and modify vlan tag of the packet simultaneously. The reply packets of the request will also be redirected to the original vlan.

The function can replace **dhcp relay** in condition of loose broadcast isolation requirement. When a same vlan needs to be distributed with different address fields, it can be realized by matching mac address.

Command	Purpose
<code>ip dhcp-relay vlan-remap vlan <i>VLAN</i> mac-acl <i>WORD</i> vlan <i>VLAN</i></code>	Enables dhcp vlan remap function
<code>no ip dhcp-relay vlan-remap vlan <i>VLAN</i> mac-acl <i>WORD</i></code>	Disables dhcp vlan remap function

### 1.1.18 Monitoring and Maintaining DHCP-Snooping

Run the following commands in EXEC mode:

Command	Purpose
<b>show ip dhcp-relay snooping</b>	Displays the information about DHCP-snooping configuration.
<b>show ip dhcp-relay snooping binding</b>	Displays the effective address binding items on an interface.
<b>show ip dhcp-relay snooping binding all</b>	Displays all binding items which are generated by DHCP snooping.
<b>[ no ] debug ip dhcp-relay [ snooping   binding   event   all ]</b>	Enables or disables the switch of DHCP relay snooping binding or event.

The following shows the information about the DHCP snooping configuration.

```
switch#show ip dhcp-relay snooping
ip dhcp-relay snooping vlan 3
ip arp inspection vlan 3
DHCP Snooping trust interface:
  GigaEthernet0/1
ARP Inspect interface:
  GigaEthernet0/11
```

The following shows the binding information about dhcp-relay snooping:

```
switch#show ip dhcp-relay snooping binding
Hardware Address      IP Address      remainder time Type          VLAN  interface
00-e0-0f-26-23-89    192.2.2.101    86400          DHCP_SN          3     GigaEthernet0/3
```

The following shows the binding information about dhcp-relay snooping:

```
switch#show ip dhcp-relay snooping binding all
Hardware Address      IP Address      remainder time Type          VLAN  interface
00-e0-0f-32-1c-59    192.2.2.1      infinite       MANUAL           1     GigaEthernet0/2
00-e0-0f-26-23-89    192.2.2.101    86400          DHCP_SN          3     GigaEthernet0/3
```

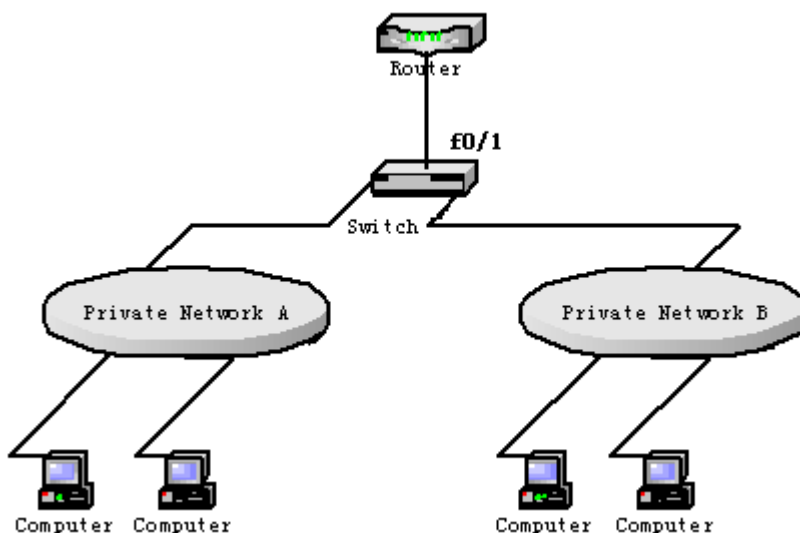
The following shows the information about dhcp-relay snooping.

```
switch#debug ip dhcp-relay all
DHCP: receive l2 packet from vlan 3, diID: 3
DHCP: DHCP packet len 277
DHCP: add binding on interface GigaEthernet0/3
DHCP: send packet continue
DHCP: receive l2 packet from vlan 3, diID: 1
DHCP: DHCP packet len 300
DHCP: send packet continue
DHCP: receive l2 packet from vlan 3, diID: 3
DHCP: DHCP packet len 289
DHCP: send packet continue
DHCP: receive l2 packet from vlan 3, diID: 1
DHCP: DHCP packet len 300
DHCP: update binding on interface GigaEthernet0/3
```

DHCPR: IP address: 192.2.2.101, lease time 86400 seconds  
 DHCPR: send packet continue

### 1.1.19 Example of DHCP-Snooping Configuration

The network topology is shown in figure 1.



Configuring Switch:

- (1) 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
```
- (2) 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
```
- (3) Set the interface which connects the DHCP server to a DHCP-trusting interface.  

```
Switch_config_f0/1#dhcp snooping trust
```
- (4) Set the 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
```

# MAC Access List Configuration

# Table of Contents

Chapter 1 Configuring MAC List.....	1
1.1 MAC List Configuration Task.....	1
1.1.1 Creating MAC List.....	1
1.1.2 Configuring Items of MAC List.....	1
1.1.3 Applying MAC List.....	2



## Chapter 1 Configuring MAC List

### 1.1 MAC List Configuration Task

MAC list configuration task includes

- Creating MAC List
- Configuring Items of MAC List
- Applying MAC List

#### 1.1.1 Creating MAC List

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

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

Command	Purpose
<b>configure</b>	Log in to the global configuration mode.
<b>[no] mac access-list name</b>	Add or delete a MAC list. <b>name</b> means the name of the MAC list.

#### 1.1.2 Configuring Items of MAC List

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

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

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

Command	Purpose
<b>[no] {deny   permit} {any   host src-mac-addr} {any   host dst-mac-addr}[ethertype]</b>	Add/Delete an item of the MAC list. You can rerun the command to add or delete multiple items of the MAC list. <b>any</b> means any MAC address can be compatible; <b>src-mac-addr</b> means the source MAC address; <b>src-mac-mask</b> means source mac mask; <b>dst-mac-addr</b> means the destination MAC address. Arp means matching arp packet; <b>ethertype</b> means the type of matched Ethernet packet.

<b>exit</b>	Log out from the MAC list configuration mode and enter the global configuration mode again.
<b>exit</b>	Enter the management mode again.
<b>write</b>	Save configuration.

### MAC list configuration example

```
Switch_config#mac acce 1
Switch-config-macl#permit host 1.1.1 any
Switch-config-macl#permit host 2.2.2 any
```

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

### 1.1.3 Applying MAC List

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

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

Command	Purpose
<b>configure</b>	Enter the global configuration mode.
<b>interface g0/1</b>	Log in to the port that is to be configured.
<b>[no] mac access-group name</b>	Apply the created MAC list to the port or delete the applied MAC list from the port. <b>name</b> means the name of the MAC list.
<b>exit</b>	Enter the global configuration mode again.
<b>exit</b>	Enter the management mode again.
<b>write</b>	Save configuration.

# 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 ..... 3
  - 2.1 Attack Prevention Configuration Tasks ..... 3
  - 2.2 Attack Prevention Configuration ..... 3
    - 2.2.1 Configuring the Attack Filter Parameters..... 3
    - 2.2.2 Configuring the Attack Prevention Type ..... 4
    - 2.2.3 Enabling the Attack Prevention Function ..... 4
    - 2.2.4 Checking the State of Attack Prevention ..... 4
- Chapter 3 Attack Prevention Configuration Example ..... 6
  - 3.1 Use Filter ARP to Protect the LAN..... 6

# 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 switch will not provide any service to these hosts.

Filter limits the packet from a certain host by blocking the source address. For ARP attack, Filter blocks source MAC address; for IP attacks, such as Ping scan and TCP/UDP scan, Filter blocks source IP address.

## 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# <b>config</b>	Enters the global configuration mode.
Switch_config# <b>filter period</b> <i>time</i>	Sets the attack filter period to time. Its unit is second.
Switch_config# <b>filter threshold</b> [ <b>arp</b>   <b>bpdu</b>   <b>dhcp</b>   <b>igmp</b>   <b>ip</b>   <b>icmp</b> ] <i>value</i>	Sets the attack filter threshold to value.
Switch_config# <b>filter block-time</b> <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# <b>filter polling period</b> <i>time</i>	Sets the filter polling period in Hybrid mode. Its unit is second.
Switch_config# <b>filter polling threshold</b> [ <b>arp</b>   <b>bpdu</b>   <b>dhcp</b>   <b>igmp</b>   <b>ip</b>   <b>icmp</b> ] <i>value</i>	Sets the filter polling threshold in Hybrid mode.
Switch_config# <b>filter polling auto-fit</b>	Sets the corresponding parameters of <b>period</b> and <b>threshold</b> 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

## 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# <b>config</b>	Enters the global configuration mode.
Switch_config# <b>filter dhcp</b>	Enables DHCP packet attack filter in the global configuration mode.
Switch_config# <b>interface intf-name</b>	Enters the interface configuration mode.
Switch_config_intf# <b>filter arp</b>	Enables ARP packet attack filter on the interface.
Switch_config_intf# <b>filter bpdu</b>	Enables BPDU packet attack filter on the interface.
Switch_config_intf# <b>filter dhcp</b>	Enables DHCP packet attack filter on the interface.

---

### Note:

The ARP attack takes the host's MAC address and the source port as the attack source, that is, message from the same MAC address but different ports cannot be calculated together. Both the IGMP attack and IP attack take the host's IP address and source port as the attack source.

### Note:

1. The IGMP attack prevention and the IP attack prevention cannot be started up together.
  2. 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# <b>filter enable</b>	Enables the attack prevention function.
Switch_config# <b>filter mode raw</b>	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
<b>show filter</b>	After attack prevention is started, you can run the following command to check the state of attack prevention:



<b>show filter summary</b>	Checks the parameter configuration and summary information of Filter.
----------------------------	---

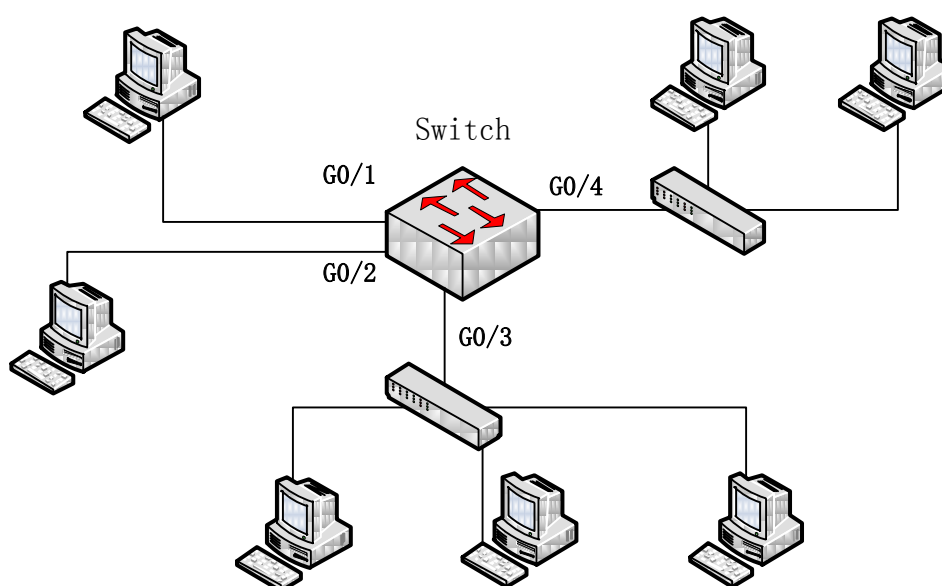
## Chapter 3 Attack Prevention Configuration Example

### Note:

The examples shown in this chapter is only a reference for Filter configuration. Please configure according to your actual network condition.

### 3.1 Use 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
```

# QoS Configuration

## Table of Contents

Chapter 1 QoS Configuration .....	1
1.1 Overview .....	1
1.1.1 QoS Concept .....	1
1.1.2 P2P QoS Model .....	1
1.1.3 Algorithm of QoS Queue of QoS Queue .....	2
1.2 QoS Configuration Task List .....	2
1.3 QoS Configuration Tasks .....	3
1.3.1 Configuring global QoS Priority Queue .....	3
1.3.2 Configuring the Bandwidth of the CoS Priority Queue .....	4
1.3.3 Configuring the Schedule Strategy for the CoS Priority Queue .....	4
1.3.4 Configuring the Default CoS Value of the Port .....	4
1.3.5 Establishing QoS Strategy Mapping .....	5
1.3.6 Configuring Description of QoS Strategy Mapping .....	5
1.3.7 Configuring the Matched Data Flow of the QoS Strategy Mapping .....	6
1.3.8 Configuring Actions for Matched Data Flow of the QoS Strategy Mapping .....	7
1.3.9 Applying the QoS Strategy on the port .....	7
1.3.10 Displaying the QoS Strategy Mapping Table .....	8
1.4 QoS Configuration Example .....	8
1.4.1 Example for Applying QoS Strategy on the Port .....	8

# Chapter 1 QoS Configuration

If you concern how to fully use the bandwidth of your line and effectively use your network resources, you need to configure the service quality.

## 1.1 Overview

### 1.1.1 QoS Concept

The switch is normally in best-effort served mode. In this mode, the switch equally treats all flows and tries its best to forward all flows. In this case, all flows have the same chance to be dropped if congestion occurs. In real network conditions, different flows have different importance. The QoS function of the switch provides different services to different flows according to the importance of the flow, providing more important flows better service.

The current network provides two methods to distinguish the importance of the flow.

- Distinguish the importance based on the tag in the 802.1Q frame. The tag has two bytes. Three bits in the highest byte represent the priority levels. There are eight priority levels, 0 and 7 representing the lowest priority and the highest priority level respectively.
- Distinguish the importance based on the DSCP field in the IP header of the IP message. The DSCP field occupies 6 bits in the TOS domain of the IP header.

In real network application, the verging switches distribute different priorities to different flows according to their importance. Other switches provide different flows different services according to the priority information contained in the flow. The peer-to-peer (P2P) QoS service is realized.

Additionally, you can configure a switch in the network, enabling the switch to specially handle message with special features. The action performed by the switch is called as one-hop action.

The QoS function of the switch makes the network bandwidth effectively use, which greatly improves the performance of the network.

### 1.1.2 P2P QoS Model

The service model describes the capability of the P2P QoS, that is, the capability to send special network communication from one peer to another peer. The QoS software supports two kinds of service models: best-effort served service and differentiated service.

#### a. Best-effort service

It is a single service model. In this mode, the application can send any number of data at

necessary time without applying permission or previous notification of network. For the best-effort service, network can transmit data without concerning reliability, delay range or putthrough. The QoS function of the switch in best-effort service model complies with the “first come, first served” order.

#### b. Differentiated service

For the differentiated service, if the to-be-sent service is special, the corresponding QoS label must be designated in each packet. The designation can be embodied in different modes such as setting IP priority in the IP packet. The switch uses the QoS rule to classify the service and perform intelligent queue. The QoS function of switch provides strict priority, weighted round robin (WRR) and “first come, first served” (FCFS) to send the differentiated service.

### 1.1.3 Algorithm of QoS Queue of QoS Queue

The algorithm of QoS Queue of QoS queue guarantees the QoS realization. Our switches provide the queue algorithm for the strict priority, weighted round robin (WRR) and “first come, first served” (FCFS).

#### a. Strict priority

The queue algorithm of the strict priority means first providing service to a flow with the high priority until the flow with the high priority does not exist. The queue algorithm provides better service for the flows with high priority. Its shortcoming is that the flows with low priority cannot get service and die eventually.

#### b. Weighted round robin

WRR algorithm is an effective way to solve the shortcoming of the queue algorithm of strict priority. A certain bandwidth is distributed to each priority queue. Each priority queue is provided service according to the order from high priority to low priority. When the queue with high priority has already used up all the distributed bandwidth, the WRR algorithm turns to the queue with low priority and provides service to it.

#### c. First come first served

FCFS algorithm strictly follows the order the message reaches the switch to provide service for the flows. The message flow that first reaches the switch is first provided with service.

## 1.2 QoS Configuration Task List

Generally, the switch tries its best to deliver every message. When congestion occurs, all messages have the same chance to be dropped. In fact, different message has different

importance. Important message should be provided with better service. The QoS function provides different message with different priorities for providing different services. Therefore, the network has better performance and can be effectively used.

The section describes how to configure the QoS function of the switch.

The QoS configuration tasks are listed as follows:

- Configuring global CoS priority queue
- Configuring the bandwidth of the CoS priority queue
- Configuring the schedule strategy for the CoS priority queue
- Configuring the schedule standard for the CoS priority queue
- Configuring the default CoS value of the port
- Configuring CoS priority queue of the port
- Establishing QoS strategy mapping
- Configuring the description of QoS strategy mapping
- Configuring the matched data flow of the QoS strategy mapping
- Configuring actions for the matched data flow of the QoS strategy mapping
- Applying the QoS strategy on the port
- Displaying the QoS strategy mapping table
- Configuring the limitation for the port flow rate

## 1.3 QoS Configuration Tasks

### 1.3.1 Configuring global QoS Priority Queue

Configuring QoS priority queue is to map eight CoS values defined by IEEE802.1p to the priority queue. The switch has eight priority queues. The switch adopts the corresponding strategy according to different queues and makes the QoS service realized.

If you configure the CoS priority queue in global configuration mode, the CoS priority mapping at all ports is to be affected. When the priority queue is configured at the layer-2 port, the port will use the priority queue. Otherwise, the global configuration is to be used.

Perform the following operations in privileged mode to configure the global CoS priority queue:

Command	Purpose
<b>configure</b>	Enters the global configuration mode.
<b>[no] cos map <i>quid cos1..cosn (1-8)</i></b>	Set the COS priority queue. <b>quid</b> is the ID of the COS priority. <b>cos1..cosn</b> is the cos value defined in IEEE802.1p.
<b>exit</b>	Returns to the management mode.
<b>write</b>	Saves configuration.

### 1.3.2 Configuring the Bandwidth of the CoS Priority Queue

The bandwidth of the CoS priority queue is the bandwidth distributed for each priority when the schedule strategy of the CoS priority queue is WRR.

Using the command affects the bandwidth of the CoS priority queues on all ports. The command is valid only when the schedule strategy is WRR. The command decides the bandwidth value of the CoS priority queue when the wrr schedule strategy is used.

Perform the following operations in privileged mode to configure the bandwidth of the CoS priority queue:

command	description
<b>configure</b>	Enters global configuration mode.
[no] scheduler weight bandwidth <i>weight1...weightn</i>	Sets the bandwidth of CoS priority queue.  weight1...weightn represent eight CoS CoS priority queue values.
<b>exit</b>	Returns to management configuration mode.
<b>write</b>	Saves configuration.

### 1.3.3 Configuring the Schedule Strategy for the CoS Priority Queue

Each port of the switch has multiple output queues. This series of switches have eight priority queues. The following methods can be used to schedule the output queue:

- SP (Sheer Priority): sheer priority schedule. The packet of low priority queue will be forwarded only when the high priority queue is vacant. If there are packets in the high priority queue, these packets are to be sent first.
- WRR (Weighted Round Robin): It is to distribute a bandwidth value for each queue and the bandwidth is then distributed to each queue according to their value.

Perform the following operations in privileged mode to configure the schedule strategy of the CoS priority queue.

Command	Purpose
<b>configure</b>	Enter the global configuration mode.
[no] scheduler policy { <b>sp</b>   <b>wrr</b> }	Set the schedule strategy for the QoS priority queue.  <b>sp</b> represents the sp schedule strategy. <b>wrr</b> represents the <b>wrr</b> schedule strategy.
<b>exit</b>	Returns to the management mode.
<b>write</b>	Saves configuration.

### 1.3.4 Configuring the Default CoS Value of the Port

If the port receives the frame without label, the switch will add a default COS priority to it.



Configuring the default CoS value is to set the default Cos value to the designated value of the unlabelled frame.

Perform the following operations in privileged mode to the default Cos value on the port.

Command	Purpose
<b>configure</b>	Enter the global configuration mode.
<b>interface g0/1</b>	Logs in to the port that will be configured.
<b>[no] cos default cos</b>	Configures the CoS value for the unlabelled frame. <b>Cos</b> represents the corresponding cos value.
<b>exit</b>	Returns to the global configuration mode.
<b>exit</b>	Returns to the management mode.
<b>write</b>	Saves configuration.

### 1.3.5 Establishing QoS Strategy Mapping

QoS strategy mapping means to adopt certain regulations to distinguish headers of a certain feature, and to perform the designated operations on the headers.

Only one rule can be used to match the IP access list and the MAC access list of the data flow. If not, the configuration will fail. When the action is **permit**, the rule is used to distinguish data flow. When the action is **deny**, the rule is not used to match the data flow. The port number of IP access list must be fixed.

Perform the following operations in privileged mode to create the QoS strategy mapping:

Command	Purpose
<b>configure</b>	Enters the global configuration mode.
<b>[no]policy-map name</b>	Enters the QoS strategy table configuration mode. <b>name</b> represents the strategy name.
<b>exit</b>	Returns to the global configuration mode.
<b>exit</b>	Returns to the management mode.

### 1.3.6 Configuring Description of QoS Strategy Mapping

Perform the following operations in privileged mode to configure the description of QoS strategy mapping:

Command	Purpose
<b>configure</b>	Enters the global configuration mode.

<b>[no]policy-map</b> <i>name</i>	Enters the QoS strategy list configuration mode.  <b>name</b> represents the strategy name.
<b>description</b> <i>description-text</i>	Configures the description of the QoS strategy.  <b>description-text</b> is the text to describe the strategy.
<b>exit</b>	Returns to the global configuration mode.
<b>exit</b>	Returns to the management mode.

### 1.3.7 Configuring the Matched Data Flow of the QoS Strategy Mapping

The classification rule of the QoS data flow is the filtration rule configured by administrator according to requirements.

Perform the following operations in privileged mode to configure the matched data flow of the strategy. The data flow will replace the previous configuration.

Command	Purpose
<b>configure</b>	Enters the global configuration mode.
<b>[no]policy-map</b> <i>name</i>	Enters the QoS strategy list configuration mode.  <b>name</b> represents the strategy name.
<b>description</b> <i>description-text</i>	Configures description of QoS strategy  Description-text is the text of the strategy
<b>classify</b> { <i>any</i>   <i>cos</i> <i>cos</i>   <i>vlan</i> <i>vlanid</i>   <i>precedence</i> <i>precedence-value</i>   <i>dscp</i> <i>dscp-value</i>   <i>tos</i> <i>tos-value</i>   <i>diffserv</i> <i>diffserv-value</i>   <i>ip</i> <i>ip-access-list</i>   <i>sip</i>   <i>smac</i>   <i>ipv6</i> }  <b>no classify</b> { <i>any</i>   <i>cos</i>   <i>icos</i>   <i>vlan</i>   <i>precedence</i>   <i>dscp</i>   <i>tos</i>   <i>diffserv</i>   <i>ip</i>   <i>smac</i>   <i>ip</i>   <i>ipv6</i> }	<i>any</i> means to match any packet.  <i>cos</i> means the matched cos value: 0~7  <i>vlanid</i> means matched VLAN, 1 to 4094  <i>precedence-value</i> is the priority field of tos in ip packets (5-7 of tos), 0-7  <i>dscp-value</i> is dscp field of tos in ip packets (2 -7 of tos),0~63  <i>tos-value</i> means the field of delay, throughput, reliability and cost in the ip packet (1 to 4), 0~15  <i>diffserv-value</i> means the 8 bit of the whole tos field in the IP packet, 0 -255  <i>ip-access-list</i> is the matched ip access list name, 1 to 19  <i>Smac</i> means the matched source MAC address  <i>Sip</i> means the matched source IP address  <i>Ipv6</i> means the matched ipv6 address.

<b>exit</b>	Returns to the global configuration mode.
<b>exit</b>	Returns to the management mode.

### 1.3.8 Configuring Actions for Matched Data Flow of the QoS Strategy Mapping

Defining the action of the data flow means to take corresponding actions according to the data flow that complies with the filtration rule, including limiting bandwidth, dropping message, updating domains.

Perform the following operations in privileged mode to configure actions for the matched data flow:

Command	Purpose
<b>configure</b>	Enters the global configuration mode.
<b>[no]policy-map name</b>	Enters the QoS strategy list configuration mode. <b>name</b> represents the strategy name.
<b>action{bandwidth max-band   cos cos   drop   dscp dscp-value  forward   queue queue-value   redirect interface-id   vlanID vlanid }</b>  <b>no action {bandwidth   cos   drop   dscp   forward   queue   redirect   vlanID}</b>	Configures the matched data flow strategy of the QoS strategy table.  <b>max-band</b> stands for the maximum bandwidth occupied by the data flow.  <b>drop</b> stands for the dropped message.  <b>dscp-value</b> means to set the <b>dscp</b> field of the matched flow to <b>dscp-value</b> .  Forward means to take no action to the matched packets.  queue-value means to set mapping queue, 1 to 8.  <b>interface-id</b> stands for the exit of the redirection match flow.  <b>vlanID</b> means to replace or add outer vlanid, 1 to 4094.
<b>exit</b>	Returns to the global configuration mode.
<b>exit</b>	Returns to the management mode.

### 1.3.9 Applying the QoS Strategy on the port

You can apply the QoS strategy to a port. Multiple strategies can be applied to one port; one strategy can be applied to multiple ports too. To the strategies applied on a port, the strategies that are first applied have high priority. If the message simultaneously configures two strategies and the configuration actions are conflicted, take the action of firstly matched strategy as standard. After the strategy is applied on the port, the switch adds a strategy by default on the port to block the data flow that is not allowed to pass. When all strategies on

the port are deleted, the switch automatically deletes the default strategy from the port. Perform the following operations in privileged mode to apply the QoS strategies:

Command	Purpose
<b>configure</b>	Enters the global configuration mode.
<b>interface g0/1</b>	Logs in to the port that will be configured.
<b>[no] qos policy name { ingress }</b>	Applies the QoS strategy on the port.  <b>name</b> stands for the name of the QoS strategy.  <b>ingress</b> means the QoS strategy has impact on the entrance.
<b>exit</b>	Returns to the global configuration mode.
<b>exit</b>	Returns to the management mode.

### 1.3.10 Displaying the QoS Strategy Mapping Table

You can run the **show** command to display all or the designated QoS strategy mapping table. Perform the following operations in privileged mode to display the QoS strategy mapping table:

Command	Purpose
<b>show policy-map {policy-map-name / interface [interface-id]}</b>	Displays all or designated QoS strategy mapping table.  <b>policy-map-name</b> stands for the name of the strategy mapping table.

## 1.4 QoS Configuration Example

### 1.4.1 Example for Applying QoS Strategy on the Port

Configure the strategy that change the COS value of the message to 2 on the port.

```

policy-map pmap
  classify any
  action cos 2
!
interface g0/2
  qos policy pmap ingress

```