ORIGO

Layer 2 switch

Operation Manual

Catalog

Reader Range

This manual is suitable for the following persons:

- engineering technicians,
- project opening personnel,
- equipment maintenance personnel,
- network manager,
- other people interested in this product.

Content Introduction

Describe the main content of this book, introduce the key points of each chapter, and guide users to use this book in a targeted manner.

Chapter name	Outline
Chapter 1 basic configuration	This chapter introduces the basic configuration of the switch, including device connection, login, basic system configuration, file system configuration, device file upload and download, etc.
Chapter 2 equipment management configuration	This chapter introduces the configuration of equipment management in the switch, including hardware configuration and image configuration, log management and optical information module.
Chapter 3 layer 2 Ethernet configuration	This chapter introduces the basic function configuration of the switch layer 2 Ethernet.
Chapter 4 IP service configuration	This chapter focuses on the IP service configuration and DHCP configuration of the switch.
Chapter 5 QoS configuration	This chapter introduces the basic content, configuration process and configuration examples of QoS in switch, including queue scheduling and congestion control.
Chapter 6 security configuration	This chapter introduces the basic content, configuration process and configuration examples related to security in the switch.
Chapter 7 reliability configuration	This chapter introduces the basic contents of reliability management in switch Capacity, configuration process and configuration examples.
Chapter 8 PoE configuration	This chapter mainly introduces the PoE configuration of switch.
Chapter 9 multicast constraint mechanism configuration	This chapter mainly introduces the configuration of multicast constraint mechanism of switch.
Chapter 10 lldp configuration	This chapter mainly introduces lldp related configuration of the switch.
Chapter 11 UDLD configuration	This chapter mainly introduces the UDLD configuration of the switch.

Chapter 12 operation and maintenance management configuration	This chapter introduces the switch related operation and maintenance management configuration, including SNMP and RMON configuration.
Chapter 13 Loop Guard configuration	This chapter mainly introduces the Loopback-de configuration of the switch.

1. Basic Configuration

1.1 Overview

This chapter mainly introduces the basic configuration operation of the switch. This chapter includes the following topics:

Content	Page number
1.1 Overview	9
1.2 Interface Introduction	9
1.3 Log in to the Switch	10
1.4 Basic Configuration	15
1.5 File System Configuration	22
1.6 System Configuration File Operation	23
1.7 Device File Upload and Download	25

1.2 Interface Introduction

The interface is a unit provided by the switch to the user for operation or configuration, and is mainly used for receiving and sending data. Interfaces can be divided into management interfaces and service interfaces in terms of function, and can be divided into physical interfaces and logical interfaces in terms of physical form.

1.2.1 Management Interface

Background Information

Management interface is a kind of artificial division, mainly relative to business interface. The management interface mainly provides configuration management support for users, that is, users can log in to the switch through this interface and perform configuration and management operations. The management interface does not undertake service transmission.

Operation Process

The switch provides a console management interface, which complies with the EIA / TIA-232 standard, and the interface type is DCE. This interface is connected to the COM serial port of the configuration terminal, which is used to build a field configuration environment.

1.2.2 Physical Interface

Background Information

The physical interface is the actual interface. The physical interfaces are distributed on the switching main control board and circuit board of the switch.

The physical interface includes management interfaces and service interfaces.

Operation Process

The switch currently supports physical interfaces including:

- console port,
- Gigabit Ethernet interface.

1.3 Log in to the Switch

1.3.1 Log in to the Switch through the Console Port

Purpose

This section describes the operation process of using the local PC to log in the switch using the console serial port.

Networking Environment

When users log in to the management switch through the console port, they need to use a serial port line to connect the [console] port on the line card, as shown in Figure 1-1.

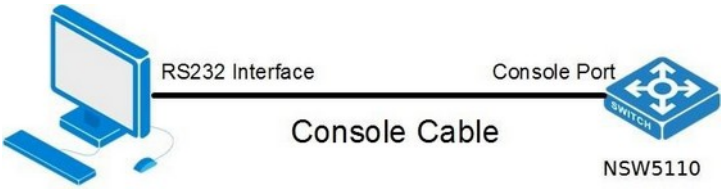
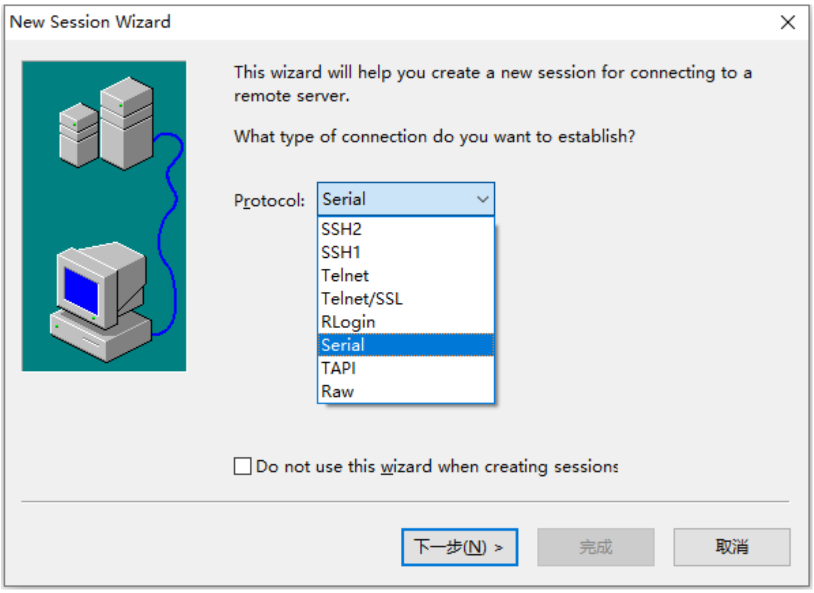


Figure 1-1. Logging in to the switch through the console port.

Process

Taking Secure CRT software as an example, the steps to log in to the switch through the console interface are as follows.

- As shown in Figure 1-1, log in to through console port, and connect PC host and switch with a serial port line.
- Start Secure CRT software on PC.
- After starting CRT, click new session under the left session manager, and then select serial. As shown in Figure 1-2.


New Session Wizard

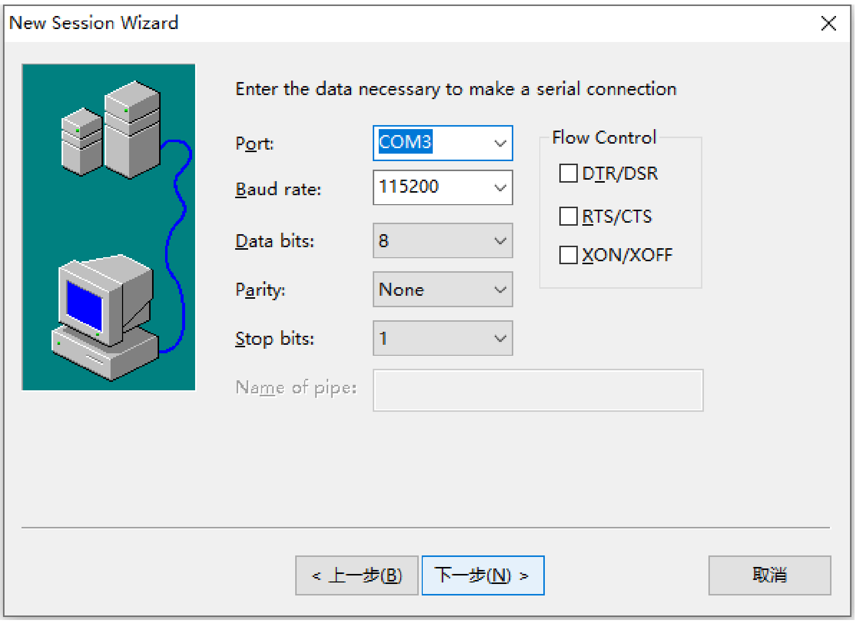
This wizard will help you create a new session for connecting to a remote server.

What type of connection do you want to establish?

Protocol: Serial

□ Do not use this wizard when creating sessions

- Set serial port properties. As shown in Figure 1-3, set the switch serial port properties.



Enter the data necessary to make a serial connection

Port: COM3

Baud rate: 115200

Data bits: 8

Parity: None

Stop bits: 1

Name of pipe:

Flow Control

☐ DTR/DSR

☐ RTS/CTS

☐ XON/XOFF

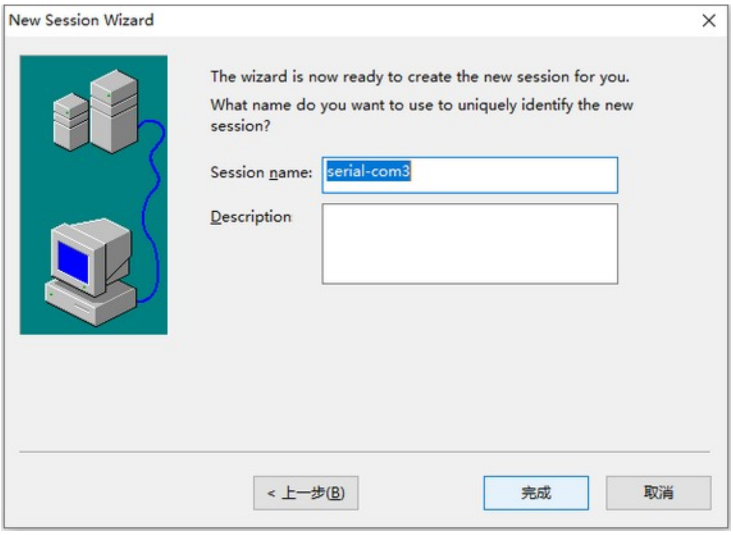
Figure 1-3. Setting up switch serial port.

Please set the parameters as shown in Table 1-1 property parameter description of serial port login switch.

Table 1-1. Attribute parameter description of serial port login switch.

Parameter	Value
Serial port	Serial port pin number on PC
Bits per second	115200
Data bits	8
Parity	-
Stop bit	1

- Click the next button, and the naming session window as shown in Figure 1-4 will pop up, and then click finish.



The wizard is now ready to create the new session for you. What name do you want to use to uniquely identify the new session?

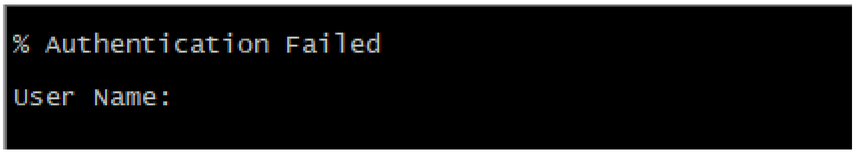
Session name: serial-com3

Description

Figure 1-4. Named session window.

Result

After completing the setup according to the above process, if the device operates normally, the CRT session window will display the interface shown in Figure 1-5 serial port login switch, indicating login to the switch.



```
% Authentication Failed

User Name:
```

Figure 1-5. Serial port login switch.

1.3.2 Telnet Login to the Switch

Purpose

In addition to the console serial port login, the login switch can also log in using telnet mode. The serial port provided by the switch itself is only for daily version upload, upgrade and maintenance.

This section describes the procedures for logging in to the switch using telnet mode with the local PC.

Telnet supports local and remote user login.

Premise

Before using telnet mode to log in the switch, users need to confirm:

- After the device is powered on for the first time and the device is logged in through the serial port, the telnet function of the device is enabled by typing the IP telnet command in the config mode. The local PC can ping the switch.

Networking Environment

When users log in to the switch by Telnet, they need to use the network cable to connect directly or through the hub, as shown in Figure 1-6 telnet to log in to the switch.

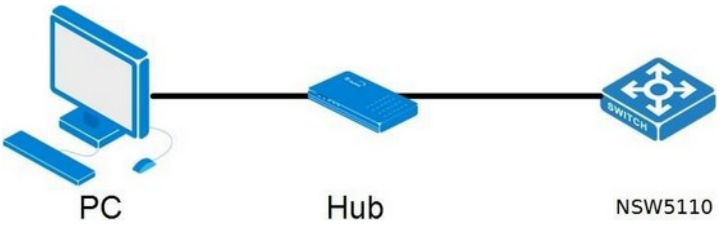
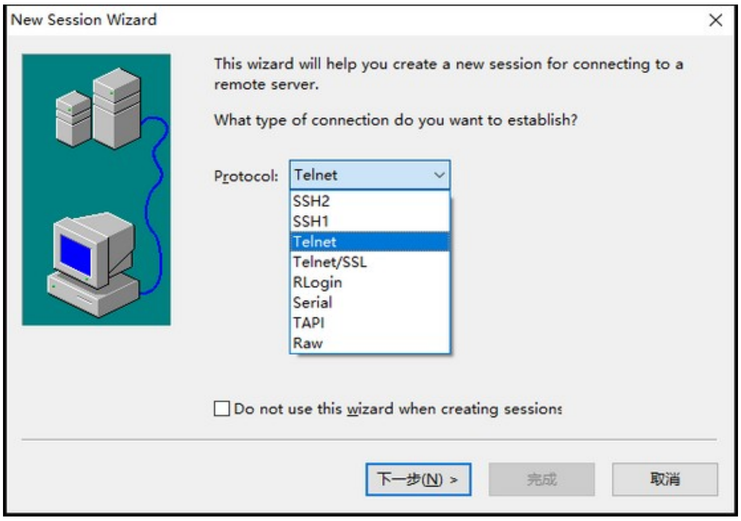


Figure 1-6. Telnet login to nsw5110 switch.

Process

Taking Secure CRT software as an example, the steps to log in to the switch through Telnet are as follows.

1. After starting the CRT, click New Session under the session manager on the left, and then select Serial. As shown in Figure 1-7.


New Session Wizard

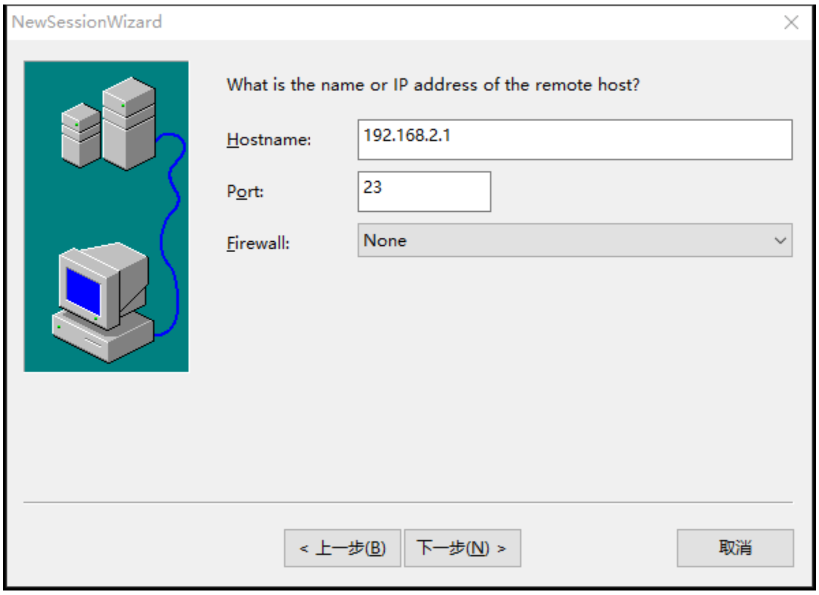
This wizard will help you create a new session for connecting to a remote server.

What type of connection do you want to establish?

Protocol: Telnet

Figure 1-7. Select login method.

2. After selecting the login method, you need to set the IP address of the remotely connected switch, as shown in Figure 1-8.


NewSessionWizard

What is the name or IP address of the remote host?

Hostname: 192.168.2.1

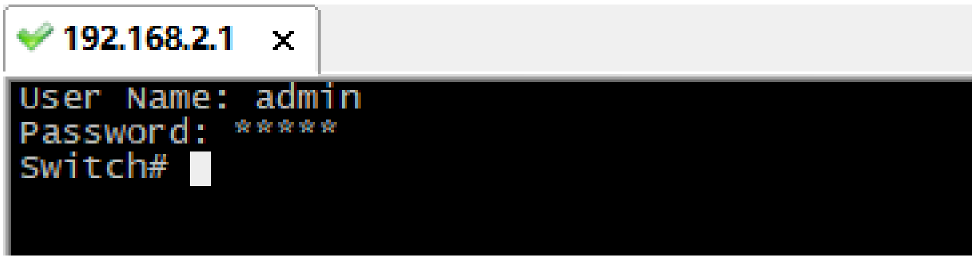
Port: 23

Firewall: None

Figure 1-8. Setting the IP address of the remote switch.

Result

After completing the settings according to the above process, if the device is operating normally, you can enter the user name and password in the session window (the user name and password are both admin), and then the session window displays the interface shown in Figure 1-9 Telnet login to the switch, indicating login switch.



```
User Name: admin
Password: *****
Switch#
```

Figure 1-9. Telnet login success.

1.3.3 SSH Login to the Switch

Purpose

This section describes the procedure for logging in to the switch using SSH using a local PC. Generally, when the user login security requirements are high, use SSH to log in to the switch.

Networking Environment

Refer to Console or Telnet to log in to the switch for networking.

Premise

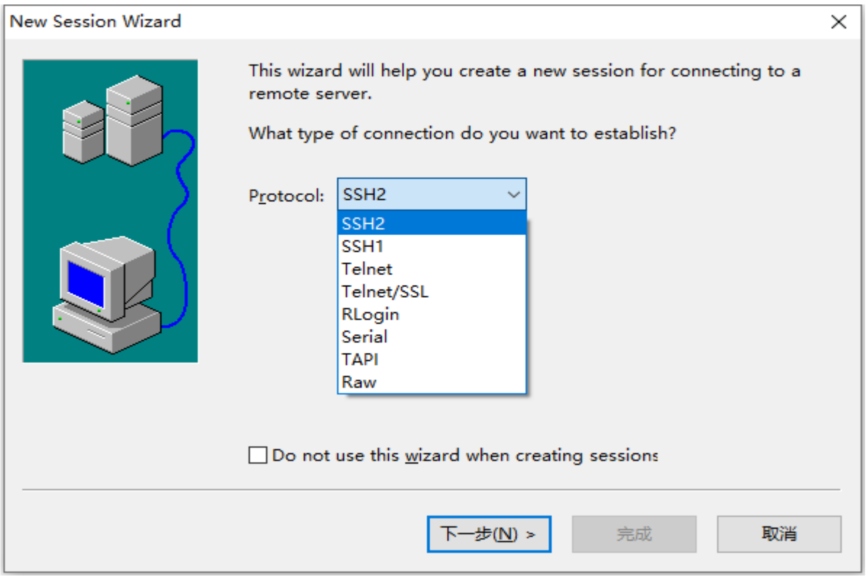
Before logging in to the switch using SSH, users need to confirm:

After the device is powered on for the first time and logged into the device through the serial port, the SSH function of the device has been enabled by typing the ip ssh command in the config mode.

Process

Taking Secure CRT software as an example, the steps to log in to the switch through SSH are as follows.

1. After starting the CRT, click New Session under the session manager on the left, and then select Serial. As shown in Figure 1-10.



New Session Wizard

This wizard will help you create a new session for connecting to a remote server.

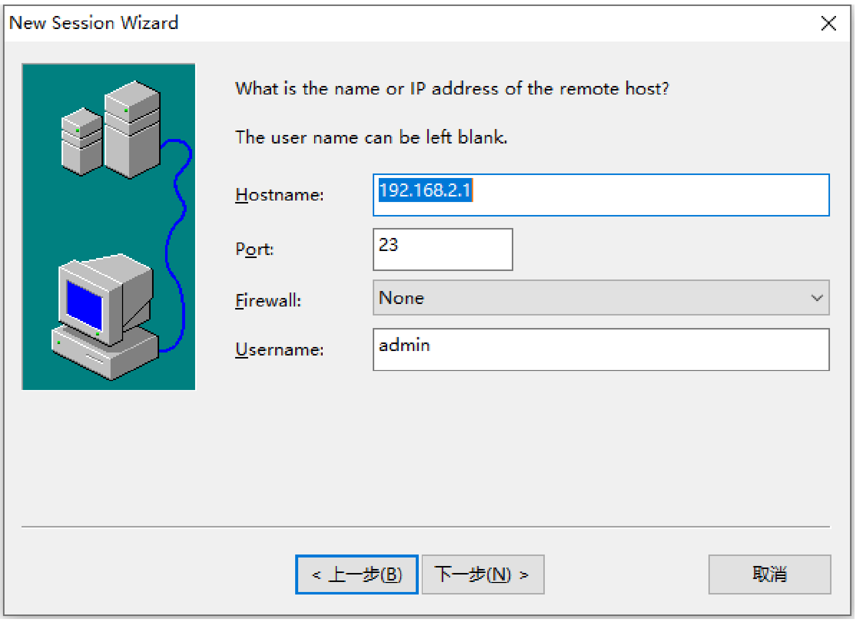
What type of connection do you want to establish?

Protocol: SSH2

□ Do not use this wizard when creating sessions

Figure 1-10. Select login method.

2. After selecting the login method, you need to set the IP address and user name of the remotely connected switch, as shown in Figure 1-1.



New Session Wizard

What is the name or IP address of the remote host?

The user name can be left blank.

Hostname: 192.168.2.1

Port: 23

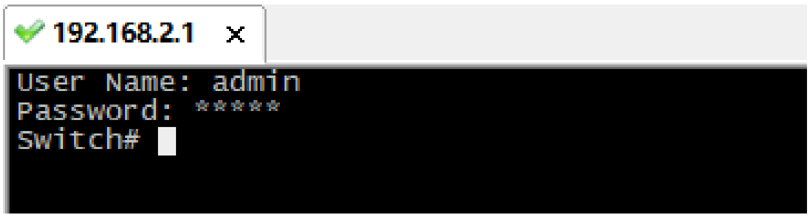
Firewall: None

Username: admin

Figure 1-11. Set the switch IP address and user name.

Result

After completing the settings according to the above process, if the device is operating normally, you can enter the user name and password in the session window (the user name and password are both admin) switch.



```
User Name: admin
Password: *****
Switch#
```

Figure 1-12. Successful SSH login.

1.4 Basic Configuration

1.4.1 Introduction to Basic Configuration

Before configuring services, users often need to perform some basic configuration according to the environment requirements during system operation to meet operation and maintenance requirements.

The basic configuration mainly includes the following two aspects:

- Basic environment configuration of the system: mainly including the configuration of language mode, host name, system time and other system environment.
- Basic user environment configuration: mainly including user terminal, user level switching and other user environment configurations.

1.4.2 Configure Basic Device Management

Purpose

This section describes the operation of equipment management.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
To display system help information.	1. In any configuration view. 2. Execute the command "**?**" to display system help information. 3. End.
To test IP network connectivity.	1. Do not execute any command to keep the current privileged user view. 2. Execute command **ping** *ip-address*; Or execute command **ping** *ip-address* **count** *repetitions* to test the connectivity of IP network. 3. End.
To reboot the device.	1. Do not execute any command to keep the current privileged user view. 2. Execute command **reboot** to restart the device.
To configure the maximum number of hops detected.	1. Do not execute any command to keep the current privileged user view. 2. Execute command **traceroute** *ipv4-address* **max_hop** *max-number* the maximum number of hops to configure the probe.
To configure the control list for access devices.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **management access-list** { **telnet| web | snmp | ssh | ftp | all** } to configure access control lists.

Attached table:

Parameter	Explanation	Value
ip-address	Host IP address to be tested on the network.	Dotted decimal.
repetitions	Number of repetitions.	1 – 999999999
max-number	Specifies the maximum number of hops to probe.	0 – 1000
telnet|web| snmp|ssh|ftp|all	Configures telnet, web, snmp, ssh,ftp or all the above access lists.	-

1.4.3 Configure the Basic Environment of the System

Purpose

This section introduces the operations related to the basic environment of the system.

Process

According to different purposes, perform the corresponding process, see the table below for details. This section introduces the operations related to the basic environment of the system.

Purpose	Process
To configure the host name of the device.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **hostname** *hostname*. The host name is used to configure the device.
To configure the current date and time of the switch.	1. Maintain the current privileged user view without executing any commands. 2. Execute the command **clock set** *HH:MM:SS DD MM YYYY* to set the current date and time of the switch. 3. End.
To configure the name of daylight saving time and the effective start and end time.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **clock summer-time** ACRONYM **date** *start-month start-day start-year start-hour start-minutes end-month end-day end-year end-hour end-minutes* to set the name of the daylight saving time and the effective start and end time. 3. Execute the command **no clock summer-time** to cancel the daylight saving time setting. 4. End.
To configure the local time zone information.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **clock timezone** ACRONYM HOUR-OFFSET[minutes *minutes*] to set the local time zone information. 3. Execute the command **no clock summer-time** to restore the local time zone to the default UTC time zone. 4. End.

Attached table:

Parameter	Explanation	Value
hostname	Specify the device name.	In the form of a string, the length range is 1 – 30 bytes.
HH:MM:SS	Specify the current time of the switch. HH means hours, MM means minutes, SS means seconds.	HH, MM, SS are integer values. The HH range is 0 – 23. The MM range is 0 – 59. The SS range is 0 – 59.
DD	Specify the current day of the switch.	1 – 31

MM	Specify the current month of the switch.	1 – 12
YYYY	Specify the current year of the switch.	2000 – 2035
ACRONYM	Specify time zone name.	1 – 4 characters.
start-month	Specify the start month.	1 – 12
start-day	Specify the start date.	1 – 31
start-year	Specify the start year.	2001 – 2099
start-hour	Specify the start hour.	0 – 23
start-minutes	Specify the start minute.	0 – 59
end-month	Specify the end month.	1 – 12
end-day	Specify the end date.	1 – 31
end-year	Specify the end year.	2001 – 2099
end-hour	Specify the end hour.	0 – 23
end-minutes	Specify the end minute.	0 – 59
ACRONYM	Specify time zone name.	1 – 4 characters.
HOUR-OFFSET	Time difference between hour and UTC.	-12 ~ 13
minutes	Time difference between minutes and UTC	0 – 59

1.4.4 Configure User Terminal Interface

Purpose

This section introduces the configuration of user terminal display and terminal operation.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
To display all available commands in the current configuration view.	1. In any view. 2. Execute an order “**?**” to display all available commands in the current configuration view. 3. End.
To configure no input timeout for virtual terminal.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **line {console|ssh|telnet}**. Enter the corresponding Line configuration view.

	3. Execute the command **exec-timeout** *time* to set the no input timeout time of the virtual terminal. 4. Execute the command **no timeout** to restore the virtual terminal no input timeout time to the default value. 5. End.
To configure the number of display lines on the terminal.	1. Maintain the current privileged user view without executing any commands. 2. Execute the command **terminal length** *terminal-length* to configure the number of terminal display lines. 3. Execute the command **no terminal length** to restore the default configuration. 4. End.
To configure whether debugging information is printed on the screen.	1. Maintain the current privileged user view without executing any commands. 2. Execute the command **terminal monitor** to set the debugging information to be printed on the screen. 3. Execute the command **no terminal monitor** to cancel debugging information printed on the screen. 4. End.

Attached table:

Parameter	Explanation	Value
time	No input timeout.	0 – 65535
terminal-length	Number of lines displayed by the terminal.	0 – 24.

1.4.5 Configure Users and their Permissions

Background Information

The login users are divided into 2 categories, as shown in Table 1-2 User Types. Only users belonging to the Administrator group have permission to add users.

Table 1-2. User types.

User type	Description
Administrators.	Management level: all commands related to the basic operation of the system. It also includes commands for the system support module. These commands provide support for services, including file system, FTP, TFTP, download, user management commands, level setting commands, etc., corresponding to level 15.

Users.	Monitoring level: used for system maintenance, business fault diagnosis, etc., including **logging dbgmsg** debugging command, the corresponding level is 1.

Purpose

This section describes how to manage users and assign user rights after logging in to the device.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
To create a user account to log in to the device.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **username** *username* **nopassword**, or **username** *username* **password** *password*, or **username** *username* **secret** *password* to create a user account for logging in to the device. 3. End.
To modify the current user's password.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **username** *username* **nopassword**, or **username** *username* **nopassword**, or **username** *username* **secret** *password* to modify the current user's password; 3. End.
To modify the specified user's permission group.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **username** *username* **privilege {user|admin} nopassword** or **username** *username* **privilege {user|admin} password** *password* to modify the permission group of the specified user; 3. End.

Attached table:

Parameter	Explanation	Value
username	User name to be created / to be modified.	String form.
password	User password of the user to be created.	String form, the length range is 1 – 64.

1.4.6 Maintenance and Commissioning

Purpose

This section describes related operations for viewing basic configuration information.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
To display the device hardware clock.	1. Do not execute any command to maintain the current privileged user view. 2. Execute the command **show clock** to display the device hardware clock. 3. End.
To display the current CPU utilization of the system.	1. Do not execute any command to maintain the current privileged user view. 2. Execute the command **show cpu utilization** to display the current CPU utilization of the system. 3. End.
To display the history commands used by users.	1. Do not execute any command to maintain the current privileged user view. 2. Execute the command **show history** to display the historical commands used by the user. 3. End.
To display the system's current software and hardware version number, compilation time, device running time and other information.	1. Do not execute any command to maintain the current privileged user view. 2. Execute the command **show version** the current software and hardware version number of the system and other information. 3. End.
To display the attributes of the created local user.	1. Do not execute any command to maintain the current privileged user view. 2. Execute the command **show username** to display the attributes of the created local users. 3. End.
To display the MAC address information in use.	1. Do not execute any command to maintain the current privileged user view. 2. Execute the command **show info** to display what MAC address information is being used. 3. End.
To display the access control list.	1. Do not execute any command to maintain the current privileged user view. 2. Execute the command **show management**

	access-list to display the access control list. 3. End.

1.4.7 Configuration Example

Networking Requirements

A PC is connected to a switch. The user can use the default configuration, or create the user name, password, permission and other parameters of the accessible device according to their actual requirements.

Networking Diagram

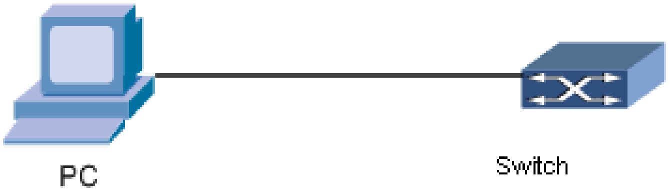


Figure 1-13. Example of user authority configuration.

Configuration Ideas

Log in to the system with the default user name and password, enter the global configuration view, and add a default user whose user name is 123, authority is administrator, and password is 123.

Configuration Process

```
#Configure user name and password
Switch(config)# username
Switch(config)# username 123 privilege admin password 123
#Log out and log in with the user with the configuration number
Switch# exit
Switch> exit
User Name: 123
Password: ***
```

1.5 File System Configuration

1.5.1 Introduction to File System

Configuration Process

In order to facilitate the effective management of flash and other storage devices, the switch provides a file system module. File system provides users with access management functions of files and directories, mainly including the creation, deletion, modification, renaming of files and directories, as well as the display of the contents of files. By default, the file system will prompt the user to confirm the commands that may cause losses to the user (such as deleting files, overwriting files, etc).

According to different operating objects, file system operations can be divided into the following categories:

- directory operation,
- file operation.

File

File is a mechanism for system to store and manage information.

Catalog

Directory is a mechanism to organize the whole file collection. Directory is the logical container of files.

1.5.2 File Operations

Purpose

File operations can delete files, display the contents of files, rename, copy files, and display information about specified files. You can use the following commands to perform the corresponding file operations. The procedure for file operations is as follows.

Process

The procedure for file operations is as follows.

Purpose	Process	Parameter description
To delete files.	1. Do not execute any command to maintain the current privileged user view. 2. Execute the command **delete flash://** *filename* to delete a specific file from flash. 3. End.	The number of characters in a single file name cannot exceed 127.
To copy files.	1. Do not execute any command to maintain the current privileged user view. 2. Execute the command **copy** *srcfile destfile* to copy files, copy the contents of one file to another file. 3. End.	String form.

1.6 System Configuration File Operation

1.6.1 Introduction to Management System Configuration File

Basic Concepts of Configuration Files

The configuration file refers to the configuration items loaded this time or the next time the switch is started.

Basic Concepts of Configuration Files and Current Configuration

Initial configuration: When the switch is powered on, it reads the configuration file from the default storage path to initialize the switch. Therefore, the configuration in this configuration file is called the initial configuration. If there is no configuration file in the default storage path, the switch is initialized with default parameters.

Current configuration: The configuration that is in effect during the operation of the switch is called the current configuration and corresponds to the initial configuration.

The user can modify the current configuration of the switch through the command line interface. In order to make the current configuration the initial configuration when the switch is powered on next time, the current configuration can be saved to the default storage device to form a configuration file.

1.6.2 Configure System Configuration File

Purpose

This section describes operations related to system configuration files.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
To delete the startup configuration file in the storage device.	1. Maintain the current privileged user view without executing any commands. 2. Execute the command **delete startup-config** to empty the boot configuration file in the storage device. 3. End.
To overwrite the current running configuration by backup configuration.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **copy backup-config running-config** to copy the configuration file to the current system configuration. 3. End.
To save the current system configuration to the startupconfiguration file.	1. Do not execute any command to maintain the current privileged user view. 2. Execute the command **copy runing-config startup-config** to write the current system configuration to the startup configuration file. 3. End.

1.6.3 Maintenance and Commissioning

Purpose

This section is used to view system profiles.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
To display the current effective system configuration parameters of the device.	1. Do not execute any command to maintain the current privileged user view. 2. Execute the command **show running-config** to display the current effective system configuration parameters of the device. 3. End.
To display the profile information used by the device when it is powered on next time.	1. Do not execute any command to maintain the current privileged user view. 2. Execute the command **show startup-config** to display the configuration file information used when the

	device is powered on and started next time. 3. End.

1.7 Device File Upload and Download

1.7.1 TFTP Configuration

1.7.1.1 TFTP Introduction

TFTP (Trivial File Transfer Protocol, simple file transfer protocol), originally intended to boot a disk less system (usually a workstation or X terminal), compared to another file transfer protocol FTP, TFTP does not have a complex interactive access interface and authentication control suitable for environments where no complex interaction is required between the client and the server. The TFTP protocol is generally implemented on the basis of UDP.

The TFTP protocol transmission is initiated by the client. When a file needs to be downloaded, the client sends a read request packet to the TFTP server, then receives data from the server, and sends a confirmation to the server; when a file needs to be uploaded, the client sends a write request packet to the TFTP server, and then sends it to the server Data and receive confirmation from the server. The mode of TFTP file transfer is only binary mode.

Before configuring TFTP, the network administrator must first configure the IP addresses of the TFTP client and server, and ensure that the client and server are reachable.

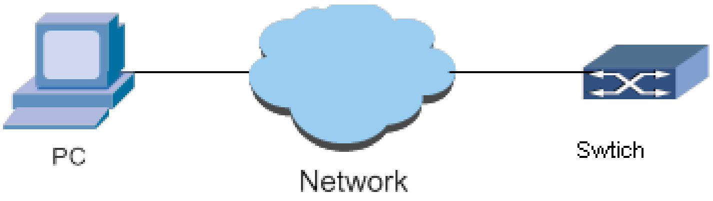


Figure 1-14. TFTP configuration diagram.

1.7.1.2 TFTP Upload Files

⚠ **Note**: it is recommended that users perform this command under the guidance of technical personnel.

Purpose

When the switch needs to upload a file to the TFTP server, the switch acts as a client to send a write request packet to the TFTP server, then sends data to the server, and receives confirmation from the server. You can use the following command to upload files.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
To upload local files to flash. (For IPv4).	1. Maintain the current privileged user view without executing any commands. 2. Execute the command **copy tftp:**//*ipv4-address* **flash:**//*filename* to upload local files to a remote TFTP Server. 3. End.

Attached table:

Parameter	Explanation	Value
ipv4-address	IPv4 address of the host.	Dotted decimal form.
filename	Specify the firmware name or file name on the switch.	String form, the length range is 1 – 63.

1.7.1.3 TFTP Download Files

Note: it is recommended that users perform this command under the guidance of technical personnel.

Purpose

When a file needs to be downloaded, the client sends a read request packet to the TFTP server, then receives data from the server, and sends a confirmation to the server. In the actual operation and maintenance of the device, it is often necessary to download the configuration file or the operating system file from the host to the device to change the configuration or upgrade the system operating system. This command is used to download files to the device.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
To download remote files via tftp and store them locally. (For IPv4).	1. Maintain the current privileged user view without executing any commands. 2. Execute the command **copy flash:**//*filename* **tftp:**//*ipv4-address* to download remote files via TFTP and store them locally. 3. End.

Attached table:

Parameter	Explanation	Value
ipv4-address	IPv4 address of the host.	Dotted decimal form.
filename	Specify the firmware name or file name in the switch flash.	String form, the length range is 1 – 63.

1.7.1.4 TFTP Client Configuration Example

Purpose

Switch as a TFTP Client for configuration file backup and software upgrade configuration example.

Device	Configuration	Default value	Configuration instructions
PC	To start TFTP Server and configure the TFTP working directory.	-	-

Switch	You can directly use TFTP commands to log in to the remote TFTP server to upload or download files.	-	TFTP is suitable for environments where no complex interaction is required between the client and the server. Make sure that the switch and the TFTP server can be pinged.

Networking Requirements

The switch serves as the TFTP client, and the PC serves as the TFTP server. The TFTP working path is configured on the TFTP server. The IP address in the switch band is 192.168.2.1, the port connecting the switch and the PC belongs to this VLAN, and the IP address of the PC is 192.168.2.74. The switch application switch.z is saved on the PC. The switch downloads switch.z from the TFTP server through TFTP, and uploads the configuration file of the switch to the working directory **vrpcfg.txt** of the TFTP server at the same time, to realize the backup of the configuration file.

Network Diagram

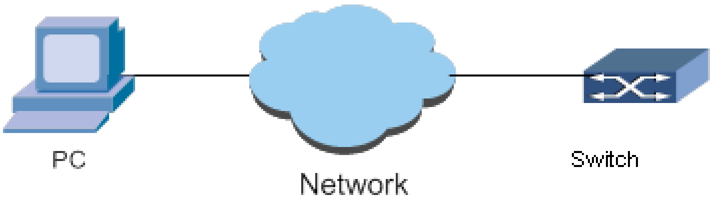


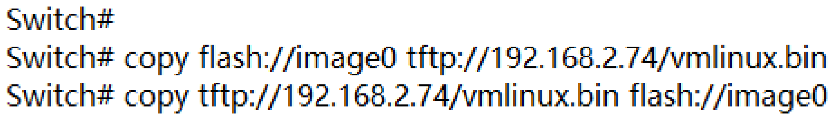
Figure 1-15. TFTP configuration diagram.

Configuration Process

1. Start TFTP Server on the PC and configure the working directory of TFTP Server.

2. Configuration on the switch.

#Users log in to the switch (users can log in to the switch locally through the console port, or remotely log in to the switch through telnet).



```
Switch#
Switch# copy flash://image0 tftp://192.168.2.74/vmlinux.bin
Switch# copy tftp://192.168.2.74/vmlinux.bin flash://image0
```

2. Device Management Configuration

2.1 Overview

This chapter introduces the basic content, configuration process, and configuration examples of device management in the switch, including: line card and hardware configuration, mirror configuration, log management, and device diagnosis.

This chapter includes the following topics:

2.2 Mirror Configuration

2.2.1 Mirror Overview

Mirroring refers to copying the data stream to the mirroring destination port. The mirroring technology is mainly used to realize the monitoring function of the data flow in order to eliminate the network fault.

The observing port of the switch can be set up to 8, but each board port can only be mirrored to at most two observing ports.

2.2.2 Mirror Classification

Layer 2 switches support local port mirroring: also called Local Switched Port Analyzer (SPAN), which means that the source and destination ports of the mirror are on the same switch.

There are also two types of flow mirroring, namely flow mirroring to the CPU and flow mirroring to the port:

- Flow mirroring to CPU: refers to copying a packet that meets the matching requirements on the flow mirroring interface and sends it to the CPU for analysis and diagnosis.
- Flow mirroring to port: means to copy a packet that meets the matching requirements on the flow mirroring interface and sends it to the destination port for analysis and diagnosis.

Description: like port mirroring, flow mirroring is also divided into local flow mirroring and remote flow mirroring.

2.2.3 Configure Mirroring

Purpose

When users need to monitor or analyze the packets flowing through a port on the device, and the mirror source port and mirror destination port are on the same device, you can configure local port mirroring.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
The target port to start the port mirroring session.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **mirror session** *Session ID* **destination interface GigabitEthernet** *interface-number* to start the target interface of the port mirroring session. 3. End.
Cancel the target interface of the port mirroring session.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **no mirror session** *Session ID* **destination interface GigabitEthernet** *interface-number* to cancel the target interface of the port mirroring session. 3. End.
To diaplay the mirroring session configuration.	1. Maintain the current privileged user view without executing any commands. 2. Execute the command **show mirror** to display the mirroring session configuration. 3. End.
Source interface to start port mirroring session.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **mirror session** *Session ID* **source interface {GigabitEthernet|LAG}** *interface-number* to start the source interface of the port mirroring session. 3. End.
Cancel the source interface of the port mirroring session.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **no mirror session** *Session ID* **source interface {GigabitEthernet|LAG}** *interface-number* to cancel the source interface of the port mirroring session. 3. End.

Attached table:

Parameter	Explanation	Value
Session ID	Specify the mirroring session ID.	1 – 4
interface-number	Specify the Ethernet interface number as the observation port.	Integer form, GE interface value range is 1 – 28, LAG interface value range is 1 – 8.

2.2.4 Configuration Example

Network Requirements

Department A and Department B of a group company are connected to SwitchA through interfaces 1/0/1 and 1/0/2, respectively. The data monitoring device is connected to the switch SwitchA through the interface 1/0/3. The local port mirroring function is required to implement the data monitoring device to monitor the packets sent by department A and department B to the switch SwitchA.

Network Diagram

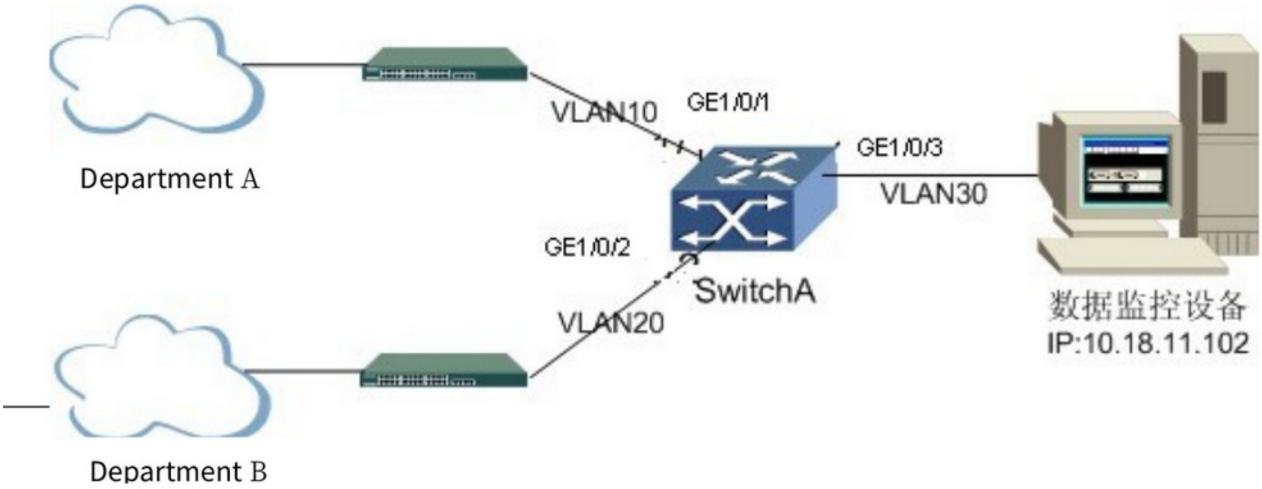


Figure 2-1. Network diagram of local port mirroring configuration.

Configuration Process

1. Configure each interface so that both departments can communicate with data monitoring equipment.

#Create VLAN10, VLAN20, and VLAN30, and add ports 1/0/1, 1/0/2, and 1/0/3 to VLAN10, VLAN20, and VLAN30, respectively.

```
vlan 10,20,30
Switch(config)# interface GigabitEthernet 1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk native vlan 10
SwitchA (config-ge1/0/1)#exit
Switch(config)# interface GigabitEthernet 2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk native vlan 20
SwitchA (config-ge1/0/2)#exit
Switch(config)# interface GigabitEthernet 3
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 10,20,30
SwitchA (config-vlan-3)#exit
SwitchA (config)#
```

2.Create a local mirroring group and its observation port.

#Create local mirroring group 1 on SwitchA and configure its observation port to 1/3.

```
Switch(config)# mirror session 1 destination interface GigabitEthernet 3
```

3. Set the mirroring function of the port on the mirror source port.

#Configure ports 1/0/1 and 1/0/2 on SwitchA as mirror source ports to monitor the data packets sent by department A and department B.

```
Switch(config)# mirror session 1 source interfaces GigabitEthernet 1 rx
Switch(config)# mirror session 1 source interfaces GigabitEthernet 2 rx
```

4. End.

2.3 Log Management Configuration

2.3.1 Introduction to Log Management

In order to track the running status of the system and the current state of the system, the system log recording function can be opened to automatically record the state of the system, so as to grasp the running status of the system and perform corresponding operations. The log file can continuously record 2000 records. When the record exceeds 4000, the record with the oldest date is automatically deleted. Therefore, in order to prevent the system from losing records, it is recommended that users regularly export log files.

2.3.2 Configure Log Management

2.3.2.1 Enable or Disable Log Management Function

Purpose

This operation is used to enable or disable the switch log management function.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process	Parameter Description
To enable the system log service function.	1. Execute the command **configure**. 2. Execute the command **logging**.	-
To disable the system record service function.	1. Execute the command **configure**. 2. Execute the command **no logging**.	
To clear logs in ARM and Flash.	1. Execute the command **configure**. 2. Execute the command **clear logging** {buffered| file }.	Buffered: Buffer logging file: File logging.

2.3.2.2 Configure Log Parameters

Purpose

This operation is used to configure log parameters, including various log output methods supported by the switch and configuration log information. The user can choose to use it according to the actual situation.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process	Parameter Description
To enable logging.	1. Execute the command **configure**. 2. Execute the command **logging {buffered|console |file}**. 3. End.	-
Do not enable logging.	1. Execute the command **configure**. 2. Execute the command **no logging {buffered|console |file}**. 3. End.	

2.3.2.2 Configure Logging Level

Purpose

This operation is used to configure the switch to record different levels of log information, including the following eight different levels of information:

- 0 – > system is unstable,
- 1 – > emergency handling actions,
- 2 – > emergency information,
- 3 – > error message,
- 4 – > warning information,
- 5 – > general information,
- 6 – > details,
- 7 – > debug information.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process	Parameter Description
To configure the log level for system recording.	1. Execute the command **configure**. 2. Execute the command **logging {buffered|console |file} severity** *level*. 3. End.	*level*: specify the log level. The value is an integer; the range is 0 – 7.

2.3.2.4 Configure Remote Server

Purpose

This operation is used to configure Remote Server parameters.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
To configure Remote Server.	1. Execute the command **configure**.

	2. Execute the command **logging host** {*ipv4-address*|*HOSTNAME*} **port** *port* **severity** *level* facility {local0|local1|local2|local3|local4|local5|local6|local7}.
To remove Remote Server.	1. Execute the command **configure**. 2. Execute the command **no logging host** {*ipv4-address*|*HOSTNAME*}.

Attached table:

Parameter	Explanation	Value
ipv4-address	Specify the server IPv4 address.	Dotted decimal.
port	Specify the server port number.	Integer form, the value range is 1 – 65535.
level	Specify the log level.	The value range is 0 – 7.
local0|local1|local2|local3|local4|local5|local6|local7	Local user 1 / local user 2 / local user 3 / local user 4 /local user 5 / local user 6 / local user 7	The value range is 16 – 23.

2.3.2.5 View Log Configuration Information

Purpose

After configuring the log management function and related parameters, if you need to check whether the configuration is correct, you can use the operations described in this section to view related information.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process	Parameter Description
To display the global log configuration.	1. Start the device, enter the user name and password to enter the privileged user view. 2. Execute the command **show logging**. 3. End.	-
To display specified log records.	1. Start the device, enter the user name and password to enter the privileged user view. 2. Execute the command **show logging** {buffered|file }. 3. End.	

2.4 Optical Module Information Reading

Purpose

This section describes how to read optical module information.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process	Parameter Description
To display diagnostic information of the specified interface.	1. Start the device, enter the user name and password to enter the privileged user view. 2. Execute the command **show fiber-transceiver interfaces GigabitEthernet** *interfaces-number*. 3. End.	*interfaces-number*: Refers to the GE interface, the range of values: 1 – 28.

3. Layer 2 Ethernet Configuration

3.1 Overview

This chapter introduces the basic function configuration of Layer 2 Ethernet. This chapter includes the following topics:

3.2 Ethernet Interface Configuration

3.2.1 Ethernet Interface Configuration Overview

Ethernet port configuration includes:

- entering Ethernet port view;
- opening / closing the Ethernet port;
- setting the duplex status of the Ethernet port;
- setting the Ethernet port rate;
- setting Ethernet port flow control;
- setting the suppression function of broadcast / multicast packets on the Ethernet port;
- setting the Ethernet port rate suppression function;
- setting the port priority size;
- setting the maximum transmission unit of the Ethernet port;
- describing the Ethernet port;
- display Ethernet port status.

3.2.2 Ethernet Interface Basic Attribute Configuration

3.2.2.1 Enter Ethernet Port View

Background Information

To configure the Ethernet port, first enter the Ethernet port view.

Perform the following configuration in the global configuration view.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process	Parameter Description
To enter Ethernet port view.	1. Execute the command **configure** to enter the global view. 2. Execute the command **interface** *interface-type port* to enter the configuration view of a specified interface.	*interface-type*: Including 2 types of ports: **LAG**, **GigabitEthernet (GE)**; integer form, the value range of **LAG** interface is 1 – 8; the value range of **GE** interface is 1 – 28.
To exit Ethernet port view.	1. Execute the command exit.	-

3.2.2.2 Open / Close Ethernet port

Background Information

After the relevant parameters and protocols of the port are configured, you can use the no shutdown command to open the port; if you want to prevent a port from forwarding data, you can use the shutdown command to close the port. By default, the port is open.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process	Parameter Description
To shut down the Ethernet port. When the interface is idle, that is, when there is no cable connected to work, use the shutdown command to shut down the interface to prevent the occurrence of interface abnormalities due to interference.	1. Execute the command **configure** to enter the global view. 2. Execute the command **interface** *interface-type port* to enter the configuration view of a specified interface. 3. Execute the command **shutdown** to close the current Ethernet.	*interface-type*: Including 2 types of ports: **LAG**, **GigabitEthernet (GE)**; integer form, the value range of **LAG** interface is 1 – 8; the value range of **GE** interface is 1 – 28.
When the Ethernet port is open and the attribute parameters of the interface are modified, but the new configuration fails to take effect immediately, you can use the shutdown and no shutdown commands to shut down and restart the interface to make the new configuration take effect.	1. Execute the command **configure** to enter the global view. 2. Execute the command **interface** *interface-type port* to enter the configuration view of a specified interface. 3. Execute the command **no shutdown** to open the current Ethernet.	

3.2.2.3 Set the Duplex Status of the Ethernet Port

Background Information

When you want the port to receive data packets while sending data packets, you can set the port to full-duplex attribute; when you want the port to only send data packets or receive data packets at the same time, you can set the port to half-duplex attribute; when the port is set to the auto-negotiation state, the duplex state of the port is determined by the auto negotiation between the local port and the peer port.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process	Parameter Description
To set the Ethernet port to work in full-duplex state.	1. Execute the command **configure** to enter the global view. 2. Execute the command **interface** *interface-type port* to enter the configuration view of a specified interface. 3. Execute the command **duplex full** to enter full-duplex mode.	By default, when an Ethernet interface works in non-auto-negotiation mode, its working mode is full-duplex mode. *interface-type*: Including 2 types of ports: **LAG**, **GigabitEthernet (GE)**; integer form, the value range of **LAG** interface is 1 – 8; the value range of **GE** interface is 1 – 28.
To set the Ethernet port to work in half-duplex state.	1. Execute the command **configure** to enter the global view. 2. Execute the command **interface** *interface-type port* to enter the configuration view of a specified interface. 3. Execute the command **duplex half** to enter half-duplex mode.	

3.2.2.4 Set the Ethernet Port Rate

Background Information

The following commands can be used to set the speed of the Ethernet port. When the port speed is set to the auto-negotiation state, the speed of the port is determined by auto negotiation between the local port and the peer port.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process	Parameter Description
To configure Ethernet interface rate.	1. Execute the command **configure** to enter the global view. 2. Execute the command **interface** *interface-type port* to enter the configuration view of a specified interface. 3. Execute the command **speed 10/100/1000** to set different rates for the interface. They are 10Mbit / s, 100Mbit / s and 1000Mbit / s respectively.	*interface-type*: Including 2 types of ports: **LAG**, **GigabitEthernet (GE)**; integer form, the value range of **LAG** interface is 1 – 8; the value range of **GE** interface is 1 – 28.

3.2.2.5 Set up Port Flow Control

Background Information

After the local and peer switches have enabled the flow control function, if the local switch is congested, it will send a message to the peer switch to notify the peer switch to temporarily stop sending packets; will temporarily stop sending messages to the local end; vice verse. Thereby, avoiding the occurrence of packet loss. You can use the following command to set whether the local Ethernet port has the flow control function turned on. If it is turned off, no flow control frame will be sent.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process	Parameter Description
To turn on Ethernet port flow control.	1. Execute the command **configure** to enter the global view. 2. Execute the command **interface** *interface-type port* to enter the configuration view of a specified interface. 3. Execute the command **flowcontrol on**.	By default, the flow control of the Ethernet interface is turned off. *interface-type*: Including 2 types of ports: **LAG**, **GigabitEthernet (GE)**; integer form, the value range of **LAG** interface is 1 – 8; the value range of **GE** interface is 1 – 28.
To turn off Ethernet port flow control.	1. Execute the command **configure** to enter the global view. 2. Execute the command **interface** *interface-type port* to enter the configuration view of a specified interface. 3. Execute the command **flowcontrol off**.	
Adaptive flow control.	1. Execute the command **configure** to enter the global view. 2. Execute the command **interface** *interface-type port* to enter the configuration view of a specified interface. 3. Execute the command **flowcontrol auto**.	

3.2.2.6 Set the Suppression Function of Broadcast / Multicast Packets on the Ethernet Port

Background Information

To prevent port blocking due to flooding of broadcast and multicast packets, the switch provides the function of suppressing broadcast / multicast packets. Users set the bandwidth value to suppress broadcast messages / multicast / unicast messages.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process	Parameter Description
To configure an Ethernet	1. Execute the command **configure** to enter the global view.	By default, the interface does not limit the rate of broadcast

interface to monitor storm control of broadcast, multicast, or unknown packets.	2. Execute the command **interface** *interface-type port* to enter the configuration view of a specified interface. 3. Execute the command **storm-control { broadcast | unknown-multicast | unknown-unicast} level** *value*.	packets, multicast packets, or unknown unicast packets. **broadcast**: Specifies storm control on broadcast packets. **unknown-multicast**: Specify storm control for multicast packets. **unknown-unicast**: specify storm control for unknown unicast packets. *value*: The granularity of the bandwidth of the passed packet is (bps: 16 – 1000000, pps: 1 – 262143).
To disable the storm control function.	1. Execute the command **configure** to enter the global view. 2. Execute the command **interface** *interface-type port* to enter the configuration view of a specified interface. 3. Execute the command **no storm-control { broadcast | unknown-multicast | unknown-unicast} level**.	

3.2.2.7 Set the Ethernet Port Rate Suppression Function

Background Information

In some occasions, it may be necessary to control the rate of the port in order to provide different bandwidths for different users. The specific granularity of input / output bandwidth control may vary depending on the type of interface.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process	Parameter Description
To configure Ethernet port rate suppression.	1. Execute the command **configure** to enter the global view. 2. Execute the command **interface** *interface-type port* to enter the configuration view of a specified interface. 3. Execute the command **rate-limit** *{ingress| egress} value*.	By default, no bandwidth limit is configured on the interface. *ingress*: Port inbound bandwidth control. *egress*: Port outbound bandwidth control. *value*: The value range is 1 – 1000000.
To disable the Ethernet port rate suppression function.	1. Execute the command **configure** to enter the global view. 2. Execute the command **interface** *interface-type port* to enter the configuration view of a specified interface. 3. Execute the command **no rate-limit** *{ingress| egress}*.	

3.2.2.8 Clear Current Interface Statistics

Purpose

This operation is applicable when a large amount of information in an interface configuration view needs to be cleared.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process	Parameter Description
To clear current interface statistics.	1. Hold the current privileged user view. 2. Execute the command **clear interfaces {GigabitEthernet|LAG}** Value **counters**. 3. End.	Value: Ethernet interface number, integer, LAG interface value range is 1 – 8; GigabitEthernet interface value range is 1 – 28.

3.2.2.9 Describe the Ethernet Port

Purpose

Use the following command to set the port description string to distinguish each port.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process	Parameter Description
To set the Ethernet port description string.	1. Execute the command **configure** to enter the global view. 2. Execute the command **interface** *interface-type port* to enter the configuration view of a specified interface. 3. Execute the command **description** *WORD*.	*WORD*: The value range for the descriptor is 1 – 32 characters.
To delete the Ethernet port description string.	1. Execute the command **configure** to enter the global view. 2. Execute the command **interface** *interface-type port* to enter the configuration view of a specified interface. 3. Execute the command **no description**.	

3.2.3 Ethernet Interface Advanced Attribute Configuration

3.2.3.1 Display Ethernet Port Status

Background Information

Execute the **show** command in user view to display the running status of the configured Ethernet port, and verify the effect of the configuration by viewing the displayed information.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
To display Ethernet port status.	1. Privileged user view. 2. Execute the command **show interface {LAG | GigabitEthernet }** *interface-number* **status**.
To display interface details.	1. Privileged user view. 2. Execute the command **show interfaces brief**.

3.2.3.2 Configure the Automatic Recovery Function Parameters of the Management Status of the Interface

Purpose

If the user hopes that the closed interface can be automatically restored, you can use this section to make the closed interface automatically recover after a delay time.

Process

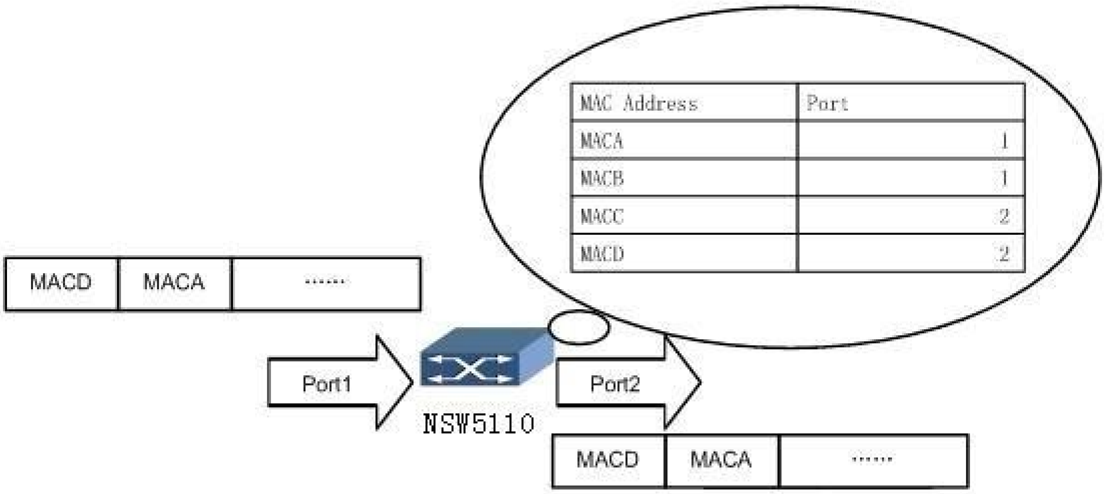
According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
To configure the delay time for the management status of the interface to automatically return to Up.	1. Execute the command **configure** to enter the global view. 2. Execute the command **errdisable recovery interval** <30-86400> to configure the delay time for the management status of the interface to automatically return to Up.
To enable port error disable recovery.	1. Privileged user view. 2. Execute the command **show interfaces brief**.

3.3 MAC Configuration

In order to quickly forward packets, the switch needs to maintain the MAC address table. The entries in the MAC address table include the MAC address of the device connected to the switch and the port number of the switch connected to the device. The dynamic entries (not manually configured) in the MAC address table are learned by the switch. The method for the switch to learn the MAC address is as follows: If a data frame is received from a port (assumed to be port A), the switch analyzes the source MAC address of the data frame (assumed to be MAC-SOURCE) and considers the destination MAC address to be MAC -SOURCE packets can be forwarded by port A; if the MAC address table already contains MAC-SOURCE, the switch will update the corresponding entry, if the MAC address table does not already contain MAC-SOURCE, the switch will use the new MAC address (and The forwarding port corresponding to the MAC address) is added to the MAC address table as a new entry.

For the packets whose destination MAC address can be found in the MAC address table, the system will directly use hardware forwarding; for the packets whose destination MAC address cannot be found in the address table, the system forwards the packets by broadcast. If after the broadcast, the message reaches the network device corresponding to the destination MAC address, the destination network device will reply to the broadcast message, which contains the MAC address of the device, and the switch will add the new MAC address to the MAC through address learning Address forwarding table. Subsequent messages to the same destination MAC address can be directly forwarded using the newly added MAC address entry.



MAC Address	Port
MACA	1
MACB	1
MACC	2
MACD	2

Figure 3-1. The switch uses the forwarding table to forward packets.

Attached table:

Parameter	Explanation	Value
cause	Error disable event.	acl all arp-inspection bpduguard broadcast-flood dhcp-rate-limit psecure-violation selfloop udld unicast-flood unknown-multicast-flood

3.3.1 Set MAC Address Table Entry

Purpose

The administrator can manually add, modify or delete entries in the MAC address table according to the actual situation.

Using a static MAC address to bind the user device to the interface can prevent illegal users with fake identities from cheating on data and improve the security of the device.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process	Parameter Description
To add / modify address table	1. Execute the command	*vlan-number*: VLAN interface number,

entry.	**configure** to enter the global view. 2. Execute the command **mac address-table static** *mac-address* **vlan** *vlan-number* **interfaces{LAG| GigabitEthernet}** *interface-number*.	integer, value range is 1 – 4094. *mac-address*: Static MAC address, the format is AA: BB: CC: DD: EE: FF. Where A | B | C | D |E | F each is a hexadecimal number, can be 0, for example: 00: 01: 02: 03: 04: 05. MAC address cannot be set to FF: FF: FF: FF: FF: FF *interface-number*: It is an integer. The value range of the LAG interface is <1-8>, and the value range of the GigabitEthernet interface is <1-28>.

3.3.2 Set System MAC address Aging Time

Background Information

Setting the appropriate aging time can effectively achieve the MAC address aging function. If the aging time set by the user is too long or too short, it may cause the switch to broadcast a large number of data packets that cannot find the destination MAC address and affect the operation performance of the switch. If the aging time set by the user is too long, the switch may save many outdated MAC address table entries, thus exhausting the MAC address table resources, and causing the switch to fail to update the MAC address table according to network changes. If the aging time set by the user is too short, the switch may delete valid MAC address entries.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process	Parameter Description
To set MAC address aging time.	1. Execute the command **configure** to enter the global view. 2. Execute the command **mac address-table aging-time** *aging-time*.	*aging-time*: Specifies the integer form of the aging time of dynamic MAC address entries, ranging from 10-630, in seconds.

3.3.3 Display Layer 2 MAC Address Table Entries

Purpose

The purpose of this program is to help users quickly locate the relevant information of the specified MAC address entry, so that users can query specific information.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
To display the Layer 2 static forwarding table.	1. Privileged user view. 2. Execute the command **show mac address-table static**.
To show mac entries.	1. Privileged user view. 2. Execute the command **show mac address-table**.

3.3.4 Configure Black Hole MAC

Purpose

The use of black hole MAC address entries can prevent fraudulent users with fake identities from cheating on data and improve the security of the device.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
To add black hole MAC address entry.	1. Execute the command configure to enter the global view. 2. Execute the command **mac address-table static** *mac-address* **vlan** <1-4094> to add black hole MAC address table entry.
To delete black hole MAC address entry.	1. Execute the command configure to enter the global view. 2. Execute the command **no mac address-table static** *mac-address* **vlan** <1-4094>. No black hole MAC address entries are added.
To show mac entries.	1. Maintain privileged user view. 2. Execute the command **show mac address-table static** to display the black hole MAC address table information.

3.3.5 Configure MAC Address Learning Function

Purpose

After the MAC address of the interface is learned, all Ethernet frames sent to the destination MAC address can be directly forwarded to the correct interface according to the entry, avoiding broadcasting.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
To configure MAC address learning limit.	1. Execute the command **interface { LAG | GigabitEthernet }** *interface-number*. Enter the configuration view of the specified interface. 2. Execute the command **port-security address-limit** *(1 – 256)*. Configure MAC address learning limit. 3. End.
To display the configured MAC address learning restriction rules.	1. Maintain privileged user view or execute commands. 2. Execute the command **show port-security interfaces { LAG | GigabitEthernet }** *interface-number*. View the configured MAC address learning restriction rules.

3.4 ARP Configuration

The ARP mapping table can be maintained dynamically or manually. The mapping of IP addresses to MAC addresses manually configured by users is usually called static ARP. Through related manual maintenance commands, users can display, add, and delete mapping entries in the ARP mapping table.

3.4.1 View ARP Information

Purpose

This section describes how to view ARP related information. This section helps users to perform LAN fault detection by viewing the ARP mapping table of the LAN. ARP establishes a correspondence between network addresses and local network hardware addresses. Each corresponding item record is kept in the cache for a period of time, and then discarded.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
To display ARP information.	1. Execute commands in privileged view **show arp**.

3.5 Link Aggregation Configuration

3.5.1 Introduction to Port Aggregation

Port aggregation is the aggregation of multiple ports together to form an aggregation group to achieve load sharing among member ports, while also providing higher connection reliability. Port aggregation can be divided into manual aggregation, dynamic LACP aggregation and static LACP aggregation. The types of ports in the same aggregation group should be consistent, that is, if a port is an electrical / optical port, other ports should also be electrical / optical ports.

Currently, the switch only supports manual aggregation and static LACP aggregation.

3.5.2 Configure Static Aggregation

Background Information

Before changing the working mode of the trunk, make sure that no member interfaces are added to the trunk, otherwise the working mode of the trunk cannot be modified. To delete an existing member interface, execute the command **switchport mode type** in the corresponding interface view.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
To create trunk and enter its configuration view.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **interface LAG** *interface-number*. 3. End.
To add member interfaces to the trunk.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **interface GigabitEthernet** *interface-number* to enter the configuration view of a port. 3. Execute the command **lag** *LAG-number* **mode static**. Configure the working mode to be static aggregation and add member

	interfaces. 4. End.

Attached table:

Parameter	Explanation	Value
interface-number	Specify the Ethernet interface number as the observation port.	The value is an integer. The value range of the GE interface is 1 – 28.
LAG-number	Specify the link aggregation interface number.	It is an integer and the value range is 1 – 8.

3.5.3 Configure LACP Function

Purpose

Through this section, you can configure LACP related operations.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
To enable LACP globally.	1. Execute the command **configure** to enter the global map. 2. Execute the command **lacp enable** to open LACP globally. 3. End.
To configure the corresponding system priority.	1. Execute the command **configure** to enter the global map. 2. Execute the command **lacp system-priority** *priority* to set the corresponding system priority. 3. End
To configure an aggregation group connection.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **lag** *LAG-number* **mode {passive|active}**. 3. End.

Attached table:

Parameter	Explanation	Value
priority	The specified priority size.	1 – 65535
LAG-number	Specify the aggregation group connection number.	1 – 8.

3.5.4 Maintenance and Commissioning

Purpose

When the LACP function is not normal and you need to view, debug, or locate the problem, you can use this section to operate.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
To enable LACP Debugging function.	1. Maintain the current privileged user view without executing any commands. 2. Execute the command **deunish env** to enter debug mode. 3. Execute the command **logging dbgmsg** *lacp-number* to enable debugging lacp function. 4. End.
To disable LACP Debugging function.	1. Maintain the current privileged user view without executing any commands. 2. Execute the command **no logging dbgmsg** *lacp-number* to disable debugging lacp function. 3. End
To display LACP Profile information.	1. Do not execute any command to maintain the current privileged user view. 2. Execute the command **show lacp internal** to display the information of LACP aggregation configuration file. 3. End.
To display all or specified group information of LACP.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **show lacp** *trunk-id* **{counters|internal|neighbor}** to display the status information of the specified LACP aggregation group or all LACP aggregation groups. 3. End.
To display LACP protocol related configuration information.	1. Do not execute any command to maintain the current privileged user view. 2. Execute the command **show lacp status** to display LACP protocol related configuration information. 3. End.

Attached table:

Parameter	Explanation	Value
trunk-id	Link aggregation group interface number.	1 – 8.

3.5.5 Typical Examples of Aggregation Ports

Network requirements

Configure link aggregation groups on two directly connected Switch devices to improve the bandwidth and reliability between the two devices. Specific requirements are as follows:

- The link between the two devices has the capability of redundant backup. When some links fail, the backup link is used to replace the failed link to keep the data transmission uninterrupted.
- The active link has the ability of load sharing.

Network diagram

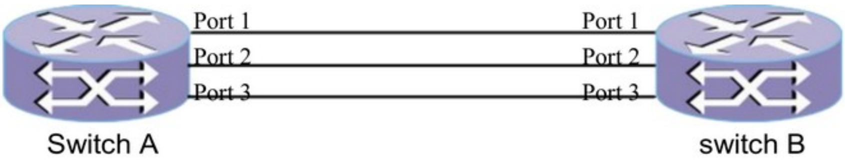
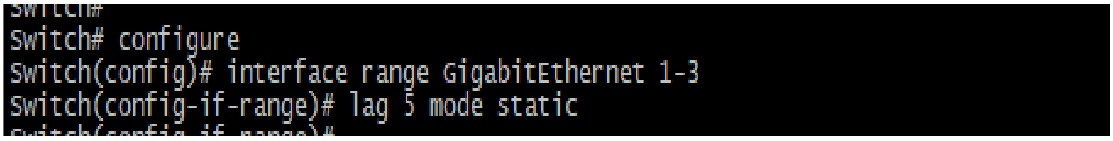


Figure 3-2. LACP configuration topology.

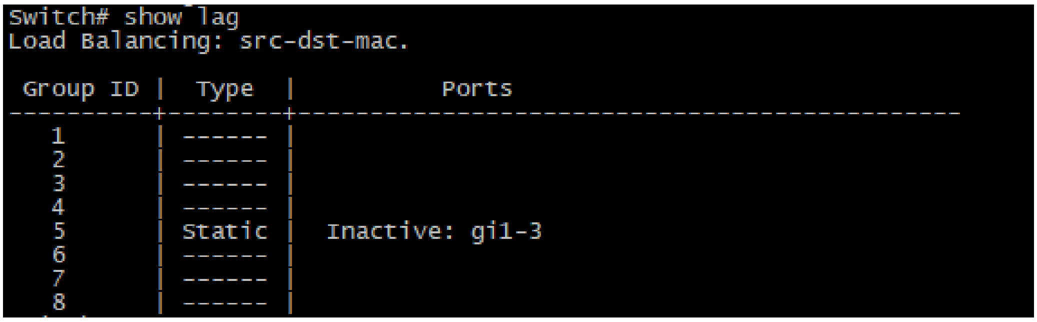
Configuration steps

1. Interfaces 1-3 are added to aggregation group 5.



```
Switch#
Switch# configure
Switch(config)# interface range GigabitEthernet 1-3
Switch(config-if-range)# lag 5 mode static
Switch(config-if-range)#
```

2.Use the show command to view the results.



```
Switch# show lag
Load Balancing: src-dst-mac.

 Group ID |  Type  |          Ports
----------+--------+---------------------------------------------
    1     | ------ |
    2     | ------ |
    3     | ------ |
    4     | ------ |
    5     | Static |  Inactive: gi1-3
    6     | ------ |
    7     | ------ |
    8     | ------ |
```

3.6 VLAN Configuration

3.6.1 VLAN Overview

The meaning of VLAN

Logically, a local area network LAN (Local Area Network) is divided into multiple subsets, and each subset forms its own broadcast domain, that is, virtual local area network VLAN (Virtual Local Area Network).

In short, VLAN is a technology that logically, rather than physically, divides the devices in a LAN into individual network segments, thereby realizing the isolation of broadcast domains in a LAN.

Features of VLAN

- Isolate the broadcast domain, reduce broadcast storms, and enhance security.
- In a large-scale networking environment, VLAN can limit network failures to the VLAN range, enhancing the robustness of the network.

3.6.2 Create VLAN

Purpose

Use this section to create a VLAN. Creating a VLAN is a basic prerequisite for configuring other VLAN functions.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
To create and enter VLAN interface configuration view.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **vlan** *vlan-id1-* [*vlan-id2*] to create one or more VLAN and enter VLAN view. 3. End.
To delete designation VLAN interface.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **no vlan** *vlan-id1-* [*vlan-id2*] to delete one or multiple VLAN in batches. 3. End.

Attached table:

Parameter	Explanation	Value
vlan-id	Specify VLAN number.	1 – 4094

3.6.3 Configure Interface-Based VLAN

Purpose

Use the operations in this section to configure interface-based VLAN.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
To configure the VLAN to which the Hybrid interface belongs.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **interface GigabitEthernet** *interface-number* to enter interface configuration view. 3. Execute the command **switchport hybrid allowed vlan add** *vlan-list* to configure the VLAN to which the Hybrid interface belongs. 4. End.
To configure the default VLAN of the hybrid interface.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **interface GigabitEthernet** *interface-number* to enter interface configuration view.

	3. Execute the command **switchport hybrid allowed vlan remove** *vlan-list*. 4. End.
To configure the link type of the interface, that is, the interface type.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **interface GigabitEthernet** *interface-number* to enter interface configuration view. 3. Execute the command **switchport mode{ access | trunk | hybrid | tunnel }** to configure the link class of the interface. 4. End.
To configure native vlan for trunk interface.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **interface GigabitEthernet** *interface-number* to enter interface configuration view. 3. Execute the command **switchport trunk native vlan** *vlan-id* to configure trunk type interface into VLAN. 4. End.
To configure the VLAN list allowed by the trunk port, add or delete.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **interface GigabitEthernet** *interface-number* to enter interface configuration view. 3. Execute the command **switchport hybrid allowed vlan {add| remove}** *vlan-list*.
To configure pvid for hybird interface.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **interface GigabitEthernet** *interface-number* to enter interface configuration view. 3. Execute the command **switchport hybrid pvid** *vlan-id*. 4. End.

Attached table:

Parameter	Explanation	Value
vlan-id	Specify VLAN number.	1 – 4094
vlan-list	List of VLAN to which the trunk interface belongs.	1 – 4094

3.6.4 Configure VLAN Based on MAC Address

Purpose

Use the operations in this section to configure VLAN division based on MAC addresses.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
To configure permission for the interface to pass MAC-based VLANs.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **interface GigabitEthernet** *interface-number* to enter interface configuration view. 3. Execute the command **vlan mac-vlan group** *group ID* **vlan** *vlan-id* to join VLAN based on MAC address. 4. End.

Attached table:

Parameter	Explanation	Value
interface-number	Interface number.	GE interface: 1 – 28, LAG interface: 1 – 8.
group ID	Mapping group number.	<1 – 2147483647>
vlan-id	Specify the VLAN ID associated with the MAC address.	1 – 4094

3.6.5 Configure VLAN Other Parameters

Purpose

Use this section to configure other VLAN related parameters, and the user can select according to the actual situation.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
To configure VLAN description information.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **vlan** *vlan-id* to create and enter interface configuration view. 3. Execute the command **name** *VLAN name* to configure the description information of the VLAN interface. 4. End.
To configure the label protocol identifier of the outer tag of the current interface.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **interface GigabitEthernet** *interface-number* to enter interface configuration view. 3. Execute the command **switchport vlan tpid {0x8100|0x88A8|0x9100|0x9200}** to configure the label protocol identifier of the outer tag of the current interface. 4. End.

Attached table:

Parameter	Explanation	Value
vlan-id	ID number of the VLAN.	1 – 4094
interface-number	Interface number.	1 – 28
vlan name	Specify the description information of the VLAN interface.	The string length range is 1 – 32.

3.6.6 Maintenance and Commissioning

Purpose

When the VLAN function is abnormal and you need to view, debug, or locate the problem, you can use this section to operate.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
To display the VLAN interface configuration information.	1. Maintain the current privileged user view without executing any commands. 2. Execute the command **show interfaces switchport GigabitEthernet** *interface-number* to display the VLAN interface configuration information. 3. End.
To display information about VLAN.	1. Maintain the current privileged user view without executing any commands. 2. Execute the command **show vlan** to display VLAN related information. 3. End.

Attached table:

Parameter	Explanation	Value
interface-number	Specify interface number.	1 – 28

3.6.7 Configuration Example

Network Requirements

An enterprise user, employee computers and department servers in the R & D department and the market are interconnected using switches SwitchA and SwitchB, respectively. It is now required that employees ’computers in the R & D department can access the department server Server1, and employees’ computers in the marketing department can access the department server Server2.

- According to the requirements, two VLAN need to be divided into VLAN 100 and VLAN 200, and the VLAN descriptors are set to “Development100” and “Market200” respectively.

- The R & D department employee computer and Server1 are divided into VLAN 100.
- The employee computers and Server2 of the marketing department are divided into VLAN 200.

Network Diagram

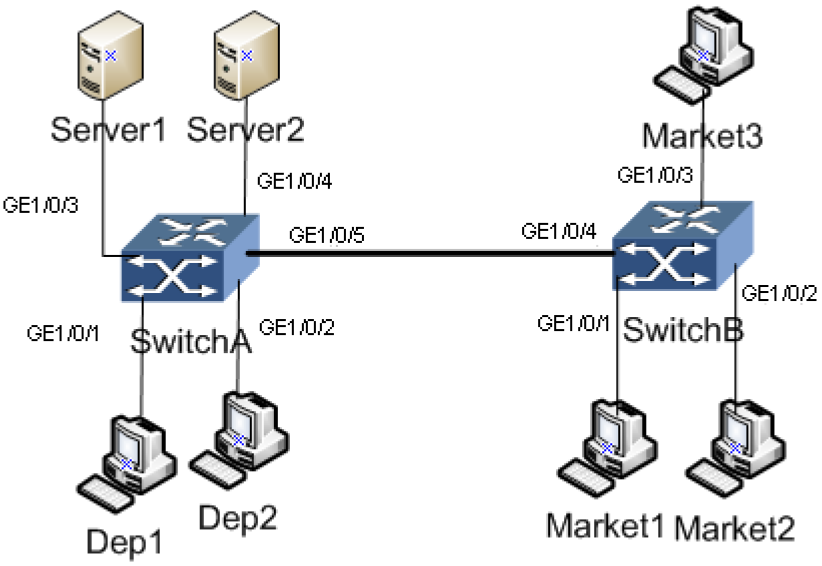


Figure 3-3. VLAN configuration topology.

Configuration Process

1. Configure SwitchA.

//Create VLAN100.

```
Switch(config)# vlan 100

Switch(config-vlan)# exit
```

//Configure the description information of

VLAN100 as Development100.

```
Switch(config-vlan)# name Development100
```

//Add ports Ge1/0/1,Ge1/0/2 and Ge1/0/3 to VLAN100, and set VLAN100 as the port The native-vlan values of Ge1/0/,Ge1/0/2, and Ge1/0/3.

```
Switch(config)# interface range GigabitEthernet 1-3
Switch(config-if-range)# switchport mode trunk
Switch(config-if-range)# switchport trunk native vlan 100
```

//Create VLAN200.

```
Switch(config)# vlan 200

Switch(config-vlan)# exit
```

//Configure the description information of

VLAN200 as Market200.

```
Switch(config-vlan)# name Market200
```

Add ports Ge1/0/4,Ge1/0/5 to VLAN200, and set VLAN200 to ports Ge1/0/4,Ge1/0/5 PVID value.

```
Switch(config)# interface range GigabitEthernet 4-5
Switch(config-if-range)# switchport mode trunk
Switch(config-if-range)# switchport trunk native vlan 200
```

2. Configure SwitchB.
//Create VLAN200.

```
Switch(config)# vlan 200

Switch(config-vlan)# exit
```

//Configure the description information of
VLAN200 as Market200.

```
Switch(config-vlan)# name Market200
```

//Add ports Ge1/0/,Ge1/0/2,Ge1/0/3, and Ge1/0/4 to VLAN200, and set VLAN200 to ports Ge1/0/1,Ge1/0/2,Ge1/0/3 and the native-vlan value of Ge1/0/4.

```
Switch(config)# interface range GigabitEthernet 1-4
Switch(config-if-range)# switchport mode trunk
Switch(config-if-range)# switchport trunk native vlan 20
```

3.7 Voice VLAN Configuration

3.7.1 Voice VLAN Overview

With the development of voice technology, IP telephony and IAD (Integrated Access Device) are becoming more and more widely used, especially in broadband communities. There are often two types of traffic: voice data and service data. Voice data needs to have a higher priority than service data during transmission to reduce possible delays and packet loss during transmission. The traditional processing method to improve the priority of voice data transmission is to use ACL to distinguish voice data and use QoS to ensure the transmission quality.

When the source MAC address of the packet matches the OUI address of the voice device, the data will be regarded as voice data, and the priority of the packet will be automatically modified and forwarded to the corresponding Voice VLAN to ensure the call quality.

The main feature of Voice VLAN is that it can automatically identify voice traffic through the source MAC address of the packet and distribute the voice traffic to a specific VLAN (Voice VLAN) for transmission.

When configuring Voice VLAN on a port, users can choose from the following two application modes:

Automatic mode: When a port configured in automatic mode receives a voice packet, it will automatically modify the priority of the packet and forward it to the corresponding Voice VLAN, and use the aging mechanism to maintain the ports in the Voice VLAN. Before the aging time arrives, if the port does not receive data from this MAC address again, the MAC address will automatically exit from the Voice VLAN.

Manual mode: The user needs to use the command to configure the default vid of the port as the vid of the voice VLAN.

3.7.2 Voice VLAN Related Operation Configuration

Purpose

Use the operations in this section to set Voice VLAN related configurations.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process	Parameter Description
To enable or disable global Voice VLAN function.	1. Execute the command **config** to enter the global view. 2. Execute the **voice-vlan** enable command; execute the **no voice-vlan** not enable command.	-
To enable or disable Voice VLAN function on the port.	1. Execute the command **config** to enter the global view. 2. Execute the command **interface {LAG| GigabitEthernet}** *interface-number* to enter the interface configuration view. 3. Execute the **voice-vlan** enable command; execute the **no voice-vlan** not enable command. 4. End.	*interface-number*: The specified interface number, the GE interface number ranges from 1 – 28; the LAG interface number ranges from 1 – 8.
To configure Voice VLAN id.	1. Execute the command **config** to enter the global view. 2. Execute the command **voice-vlan vlan** *vlan-id*.	*vlan-id*: The specified VLAN id number, the value range is 2 – 4094.
To configure cos value of voice VLAN.	1. Execute the command **config** to enter the global view. 2. Execute the command **voice-vlan cos** *cos-number*.	*cos-number*: The value range is 0 – 7.
To configure the COS attribute of Voice VLAN on the interface.	1. Execute the command **config** to enter the global view. 2. Execute the command **interface {LAG| GigabitEthernet}** *interface-number* to enter the interface configuration view. 3. Execute the command **voice-vlan cos {src| all }**. 4. End.	-
To configure Voice VLAN mode on the interface.	1. Execute the command **config** to enter the global view. 2. Execute the command **interface {LAG| GigabitEthernet}** *interface-number* to enter the interface configuration view. 3. Execute the command **voice-vlan mode**	-

	{ manual|auto }.	
To configure aging time of Voice VLAN.	1. Execute the command **config** to enter the global view. 2. Execute the command **voice-vlan aging-time** *old-time*. 3. End.	*old-time*: The specified aging time value range is 30 – 65535.
To configure MAC address on Voice VLAN.	1. Execute the command **config** to enter the global view. 2. Execute the command **voice-vlan oui-table** *mac-address [description]**. 3. End.	*mac-address*: The first three bits of the specified MAC address in the format AA: BB: CC.

3.7.3 Debug Voice VLAN Information

Purpose

When the Voice VLAN function is abnormal and you need to view, debug, or locate the problem, you can use this section to operate.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process	Parameter Description
To display Voice VLAN status.	1. Keep the current privileged view. 2. Execute the command **show voice-vlan**. 3. End.	-
To display the Voice VLAN configuration on the interface.	1. Execute the command **config** to enter the global view. 2. Execute the command **show voice-vlan interfaces {LAG|GigabitEthernet}** *interface-number*. 3. End.	*interface-number*: The specified interface number, the GE interface number ranges from 1 – 28; the LAG interface number ranges from 1 – 8.
To enable Voice VLAN debugging.	1. Keep the current privileged view. 2. Execute the command **deunish env** to enter debug mode. 3. Execute the command **logging dbgmsg** *id* to enable the debugging function.	*id*: Refers to the sequence number of the Voice VLAN in the debug view. The value range is 0 – 200.
To disable Voice VLAN debugging.	1. Keep the current privileged view. 2. Execute the command **deunish env** to enter debug mode. 3. Execute the command **logging dbgmsg** *id* to disable the debugging function.	

3.8 GVRP Configuration

3.8.1 Overview

GARP (Generic Attribute Registration Protocol) provides a set of mechanisms for registration, cancellation and transfer of general attributes. According to the different attributes of the content of the GARP protocol packet, different upper layer protocol applications can be supported.

GVRP (GARP VLAN Registration Protocol) is an application of GARP that implements the functions of dynamic registration, logout and attribute transfer of VLAN. The GARP protocol distinguishes different applications by the destination MAC of the protocol message. The destination MAC used by GVRP is 01-80-c2-00-00-21. GVRP can only be configured on trunk mode ports.

3.8.2 GVRP Related Operation Configuration

Purpose

Use this section to configure and learn the dynamic VLAN supported by the peer switch port.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process	Parameter Description
To enable GVRP function.	1. Execute the command **configure**. 2. Execute the command **gvrp**.	*interface-number*: The specified GE interface number ranges from 1 – 28.
To enable interface GVRP function.	1. Execute the command **configure**. 2. Execute the command **interface GigabitEthernet** *interface-number* to enter the interface configuration view. 3. Execute the command **switchport mode trunk** to change the interface mode to trunk. 4. Execute the command **gvrp**.	
To set the GVRP registration mode of the interface.	1. Execute the command **configure**. 2. Execute the command **interface GigabitEthernet** *interface-number* to enter the interface configuration view. 3. Execute the command **gvrp registration-mode {fixed|forbidden | normal }**.	
To enable or disable dynamic learning of VLANs under the interface.	1. Execute the command **config** to enter the global view. 2. Execute the command **interface GigabitEthernet** *interface-number* to enter the interface configuration view. 3. Execute the command **gvrp vlan-creation-forbid** Vlan-create-ban without enabling the interface; execute the command **no gvrp vlan-creation-forbid** to enable dynamic learning of	-

	VLAN under the interface. 4. End.	

3.8.3 Debug GVRP Information

Purpose

When the GVRP function is not normal and you need to view, debug, or locate the problem, you can use this section.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
To clear statistics or error statistics.	1. Keep the current privileged view. 2. Execute the command **clear gvrp {error-statistics|statistics }**. 3. End.
To display statistics or error statistics.	1. Keep the current privileged view. 2. Execute the command **show gvrp {error-statistics|statistics }**. 3. End.
To display GVRP global information.	1. Keep the current privileged view. 2. Execute the command **show gvrp**. 3. End.
To display the GVRP configuration of a port.	1. Keep the current privileged view. 2. Execute the command **show gvrp configuration**. 3. End.
To enable GVRP debugging function.	1. Keep the current privileged view. 2. Execute the command **deunish env** to enter debug mode. 3. Execute the command **logging dbgmsg** *id* to enable debugging.
To disable GVRP debugging function.	1. Keep the current privileged view. 2. Execute the command **deunish env** to enter debug mode. 3. Execute the command **no logging dbgmsg** *id* to disable debugging.

Attached table:

Parameter	Explanation	Value
id	Serial number of GVRP in debug view.	0 – 200

3.9 QinQ Configuration

QinQ refers to encapsulating a user's private network VLAN Tag in a public network VLAN Tag, so that a packet carries a two-layer VLAN Tag across the operator's backbone network (public network). In the public network, packets are only propagated according to the outer VLAN Tag (that is, the public network VLAN Tag, and the user's private network VLAN Tag is blocked).

QinQ can mainly solve the following problems:

- To alleviate the problem of increasingly scarce public network VLAN ID resources.
- Users can plan their own private network VLAN ID without conflicting with public network VLAN ID.
- Provide a relatively simple Layer 2 VPN solution for small metropolitan area networks or enterprise networks.

3.9.1 QinQ Introduction

QinQ (802.1Q-in-802.1Q) protocol is a Layer 2 tunneling protocol based on IEEE 802.1Q technology. Since the frames transmitted in the public network have two layers of 802.1Q tags (one public network tag and one private network tag), it is called QinQ protocol.

The core idea of QinQ is to encapsulate user private network VLAN tags in public network VLAN tags, and the packets carry two layers of tags across the backbone network of the network operator, thus providing users with a relatively simple layer 2 VPN tunnel.

The QinQ function is directly configured on the port. This is different from the old VLAN translation module which first creates a VLAN translation entry, and then binds the entry to the port. QinQ can only add VLAN tags, but cannot modify or delete VLAN tags.

3.9.2 Configure QinQ for the Interface

Purpose

This section describes configuring the QinQ enable of the interface.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process	Parameter Description
To enable QinQ.	1. Execute the command **configure** to enter the global view. 2. Execute the command **interface GigabitEthernet** *interface-number* to enter the configuration view of a specified interface. 3. Execute the command **switchport mode trunk** uplink.	*interface-number*: The specified GE interface number ranges from 1 – 28.
To disable QinQ.	1. Execute the command **configure** to enter the global view. 2. Execute the command **interface GigabitEthernet** *interface-number* to enter the configuration view of a specified interface. 3. Execute the command **no switchport mode**.	

3.9.3 Configuration Example

Network Diagram

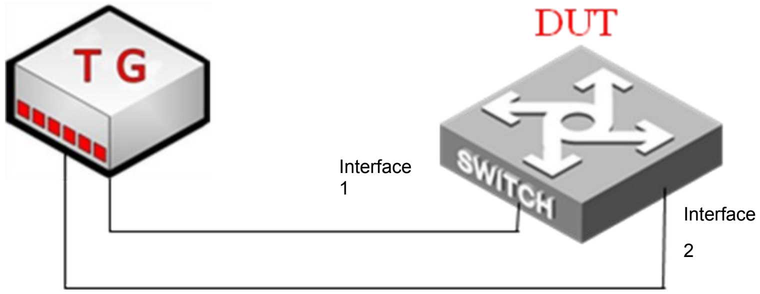


Figure 3-5. QinQ configuration topology.

Configuration steps

1. Add interface 1 and interface 2 to vlan 100 and vlan 200 by tag.

2. Configure QinQ entries on interface 1.

3. Capture packets on the interface to view the VLAN translation results to determine whether the entry is valid.

The configuration example is as follows:

First create vlan, vlan 100,200:

```
Switch# configure
Switch(config)# vlan 100
Switch(config-vlan)# exit
Switch(config)# vlan 200
Switch(config-vlan)# exit
```

The software sends a message interface, interface 1 configuration:

```
Switch(config)# interface GigabitEthernet 1
Switch(config-if)# switchport mode trunk uplink
Switch(config-if)# switchport vlan tpid 0x9100
Switch(config-if)# switchport trunk allowed vlan add 100,200
```

Receive message interface 2 configuration:

```
Switch(config)# interface GigabitEthernet 2
Switch(config-if)# switchport mode trunk uplink
Switch(config-if)# switchport vlan tpid 0x9100
Switch(config-if)# switchport trunk allowed vlan add 100,20
```

4. IP Service Configuration

4.1 Overview

This chapter focuses on the IP service of the switch. This chapter includes the following topics:

4.2 IPv4 Configuration

4.2.1 Ethernet Interface Configuration Overview

Purpose

This section describes how to configure the IP address of the current device.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process	Parameter Description
To configure the IP address of the switch.	1. Execute the command **configure** to enter the global view. 2. Execute the command **iip address** *ip-address* **mask** *Netmask*.	*ip-address*: Value range of style a.b.c.d: (A / B / C / D = 0 ~ 255). *Netmask*: the subnet mask.

4.2.2 View System IP Interface Information

Purpose

This section describes how to view system IP interface information.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
To display system IP interface information.	1. Keep the current privileged view. 2. Execute the command **show ip**.

4.3 DHCP Configuration

4.3.1 DHCP Brief Introduction

DHCP Background

A computer connected to the Internet needs to know its IP address and other information, such as the gateway address, sub net mask used, and domain name server address before sending or receiving data grams. The computer can obtain this information through the BOOTP protocol. The BOOTP protocol (Bootstrap Protocol) is an earlier remote boot protocol. It communicates with a remote server to obtain the necessary information for communication. It is mainly used for disk less clients to obtain their own IP addresses and server IP address, boot image file name, gateway IP address, etc.

BOOTP is designed for relatively static environments, each host has a permanent network connection. The administrator creates a BOOTP configuration file, which defines a set of BOOTP parameters for each host. Since the configuration usually remains the same, this file will not change often. Typically, the configuration will remain unchanged for several weeks.

As the network scale continues to expand and the complexity of the network increases, it is often the case that the number of computers exceeds the available IP addresses for allocation. At the same time, with the widespread use of portable computers and wireless networks, the location of computers often changes, and the corresponding IP addresses must also be updated frequently, resulting in more and more complicated network configurations. DHCP (Dynamic Host Configuration Protocol) is developed to meet these needs. DHCP adopts the client / server communication mode. The client submits a configuration application to the server, and the server returns the corresponding configuration information such as the IP address to implement dynamic configuration of the IP address and other information.

DHCP Related Terms

✧ DHCP server

The DHCP service provider interacts with the DHCP client through DHCP messages to assign appropriate IP addresses to various types of clients, and can assign other network parameters to the clients as needed.

✧ DHCP client

It is the trigger and driver of the entire DHCP process, and interacts with the DHCP server through the DHCP message to obtain the IP address and other network parameters.

✧ DHCP Relay

Relay forwarder of DHCP messages. It undertakes the relay service between the DHCP client and the server between different network segments, and solves the problem that the DHCP client and the DHCP server must be on the same network segment.

✧ DHCP Snooping

Layer 2 monitoring function of DHCP service. Use this function to record the user's IP address and MAC address information.

DHCP Related Terms

In order to be compatible with BOOTP, DHCP retains the BOOTP message format. The difference between DHCP and BOOTP messages is mainly reflected in the Option field. The functions added by DHCP on the basis of BOOTP are implemented through the Option field.

DHCP uses the Option field to transfer control information and network configuration parameters to achieve dynamic address allocation and provide clients with richer network configuration information.

Common DHCP options are:

✧ Option 3:Router option, used to specify the gateway address assigned to the client.

✧ Option 6:DNS server option, used to specify the DNS server address assigned to the client.

✧ Option 51:IP address lease options.

✧ Option 53:DHCP message type option, which identifies the type of DHCP message.

✧ Option 55:Request parameter list options. The client uses this option to specify which network configuration parameters need to be obtained from the server. The option content is the option value corresponding to the parameter requested by the client.

✧ Option 66:TFTP server name option, used to specify the domain name of the TFTP server assigned to the client.

✧ Option 67:Start up file name option, used to specify the start up file name assigned to the client.

✧ Option 150:The TFTP server address option is used to specify the address of the TFTP server assigned to the client.

✧ Option 121 : No classification routing option. This option contains a set of unclassified static routes (that is, the mask of the destination address is any value, and the sub net can be divided by the mask). After receiving this option, the client will add these static routes to the routing table.

✧ Option 33:Static routing options. This option contains a set of classified static routes (that is, the mask of the destination address is fixed as a natural mask and cannot be divided into sub nets). After receiving this option, the client will add these static routes to the routing table. If Option 121 exists, the option is ignored.

Advantages and Disadvantages of DHCP

DHCP adopts the client / server communication mode. All IP network configuration parameters are centrally managed by the DHCP server and are responsible for handling the client's DHCP request; the client uses the IP network parameters assigned by the server for communication.

According to the different needs of clients, DHCP provides three IP address allocation strategies. Administrators can choose which strategy DHCP uses to respond to each network or each host.

✧ Manual address assignment: The administrator statically binds a fixed IP address to a few specific clients (such as WWW server, etc.), and sends the configured fixed IP address to the client through DHCP.

✧ Automatic address allocation: DHCP allocates IP addresses with unlimited lease duration to clients.

✧ Dynamic address assignment: DHCP assigns an IP address with a valid period to the client. After the use period is reached, the client needs to apply for an address again.

DHCP expands BOOTP in two ways:

✧ DHCP allows computers to quickly and dynamically obtain IP addresses. To use DHCP's dynamic address allocation mechanism, the administrator must configure the DHCP server so that it can provide a set of IP addresses, called an address pool. Whenever a new computer is connected to the network, the computer contacts the server and applies for an IP address. The server selects an address from the configured address pool and assigns it to the computer.

✧ Compared with BOOTP, DHCP can provide clients with richer network configuration information.

DHCP has the following disadvantages:

✧ When there are multiple DHCP servers on the network, one DHCP server cannot find out the IP addresses that have been leased by other servers.

✧ The DHCP server cannot communicate with clients across network segments unless

forwarding packets through a DHCP relay.

4.3.2 Configure DHCP Function

Purpose

Configure DHCP to implement the DHCP server to assign IP addresses to users.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
To enable DHCP function on the device globally.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **ip dncp** to enable the DHCP client function globally.

5. QoS Configuration

5.1 Overview

This chapter introduces the basic content, configuration process and configuration examples of QoS. This chapter includes the following topics:

5.2 Traffic Policing and Traffic Shaping Configuration

Flow-based traffic policing refers to rate limiting traffic that meets the flow classification after flow classification on the device. By monitoring the rate of this type of traffic entering the device and discarding the part that exceeds the rate limit, this type of traffic entering the device is restricted to a reasonable range, thereby protecting network resources and the interests of operators. Flow-based traffic policing uses dual token bucket technology.

Specify the rate limit rules through Meter, including CIR, CBS, PIR, and PBS, and then specify the flow type through ACL and associate it with Meter. ACL can be enabled on physical interfaces (including trunks) or VLAN interfaces can.

The switch supports two types of traffic shaping: port shaping and port queue shaping, which can be configured as required. When the two types of traffic shaping coexist, you need to ensure that the port shaping committed information rate (CIR) is greater than or equal to the sum of the port queue shaping CIR; otherwise, traffic shaping will exhibit anomalies (such as low priority queues seizing the bandwidth of high priority queues).

This command is used to configure the QOS CAR profile (CIR, CBS, PIR, PBS) and apply it to the outbound and inbound directions of the port. After QoS CAR is applied to a physical interface or an Eth-Trunk interface, the system limits all upstream packets on the physical interface or Eth-Trunk interface.

The priority of the QoS CAR on the interface is higher than that of the VLAN. Therefore, if QoS CAR is applied on the interface and the VLAN, the system prefers the QoS CAR on the interface.
cir-value:

Specify the committed information rate, which is the average rate that is guaranteed to pass.

The value is an integer that ranges from 64 to 4294967295, in kbit / s.

cbs-value:

Specify the committed burst size, that is, the committed burst traffic that can pass in an instant.
The value is an integer that ranges from 10000 to 4294967295, and the unit is byte.

pir-value:

Specify peak information rate.

The value is an integer that ranges from 64 to 4294967295, in kbit / s. pir-value must be greater than or equal to cir-value. pir-value must be greater than or equal to cir-value, the default is equal to cir-value. If the specified pir-value is equal to cir-value, pbs-value defaults to 0 byte; otherwise, pbs-value defaults to 125 times pir-value.

pbs-value

Specify the peak burst size.

The value is an integer that ranges from 10000 to 4294967295, in bytes. pbs-value must be greater than or equal to cbs-value.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process	Parameter Description
To configure outgoing rate of the specified interface.	1. Execute the command **configure** to enter the global view. 2. Execute the command **interface GigabitEthernet** *interface-number* to enter the configuration view of a specified interface. 3. Execute the command **rate-limit egress** <0-1000000>.	*interface-number*: The specified GE interface number ranges from 1 – 28.
To configure the specified interface inflow rate.	1. Execute the command **configure** to enter the global view. 2. Execute the command **interface GigabitEthernet** *interface-number* to enter the configuration view of a specified interface. 3. Execute the command **rate-limit egress** <0-1000000>.	
To display the configured rate limit.	1. Keep current view as privileged view. 2. Execute the command **show running-config** to display information about system operation. 3. End.	

5.3 Queue Scheduling and Congestion Control Configuration

5.3.1 Queue Scheduling and Congestion Control Overview

Congestion Impact

The so-called congestion refers to a phenomenon in which the forwarding rate drops and additional delay is introduced due to the relative shortage of supply resources.

The bottleneck of the link bandwidth can cause congestion. Any lack of resources for normal forwarding processing, such as insufficient processor time, buffers, and memory resources, can cause congestion. In the current complex network environment of mulch service applications, congestion is extremely common.

Congestion may cause a series of negative effects:

- Congestion increases the delay and shake of packet transmission. Excessive delay will cause packet re-transmission.
- Congestion reduces the effective throughput of the network, resulting in a reduction in the utilization of network resources.

- Increased congestion will consume a lot of network resources (especially storage resources), and unreasonable resource allocation may even cause the system to fall into a resource deadlock and crash.

Queue Technology

Central content of congestion management: how to formulate a resource scheduling strategy when congestion occurs and decide the processing order of packet forwarding. For congestion management, queue technology is generally used, and a queue algorithm is used to classify the traffic, and then a certain priority algorithm is used to send the traffic out. Each queuing algorithm is used to solve specific network traffic problems and has a very important impact on bandwidth resource allocation, delay, and shake.

Queue Scheduling Algorithm Supported by Switch

- SP strict priority queue

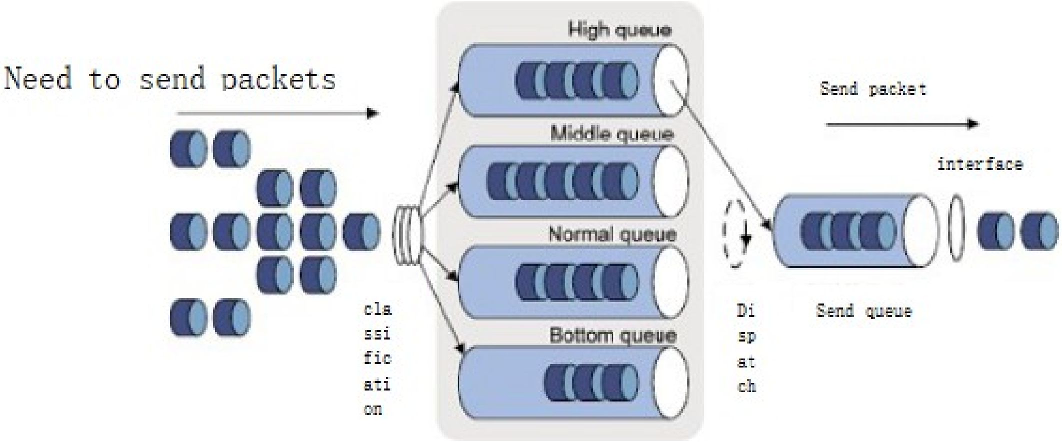


Figure 5-1. SP queue scheduling.

When scheduling in the SP (STRICT PRIORITY) queue, strictly in the order of priority from high to low, the packets in the higher priority queue are preferentially sent. When the higher priority queue is empty, it is sent to the lower priority queue Grouping.

Putting critical business packets into higher priority queues and placing non-critical business packets into lower priority queues can ensure that critical business packets are transmitted preferentially. Non-critical business packets are processing critical business data. The idle gap is transmitted. Generally, the switch chip supports a maximum of 8 queues.

5.3.2 Qos Module Configuration

Purpose

This section describes how to set the scheduling method and the settings for queue mapping.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
To enable or disable qos.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the **qos** enable command; execute the **no qos** not enable command.

	3. End.
To configure the cos value on the interface.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **interface {GigabitEthernet|LAG}** *interface-number* to enter the interface configuration view. 3. Execute the command **qos cos** *cos-number*.
To configure cos map queue operation.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **qos map cos-queue cos** *[cos]** **to** *queue*.
To enable the marking feature on the interface.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **interface {GigabitEthernet|LAG}** *interface-number* to enter the interface configuration view. 3. Execute the command **qos remark {precedence|qos|dhcp}**.
To configure change qos basic mode trust type.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **qos trust {cos | cos-dscp | dscp | precedence}**.
To enable or disable qos trust on the interface.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **interface {GigabitEthernet|LAG}** *interface-number* to enter the interface configuration view. 3. Execute the **qos trust** enable command; execute the **no qos trust** not enable command.

Attached table:

Parameter	Explanation	Value
interface-number	Specify interface number.	GE interface value range is 1 – 28; LAG interface value range is 1 – 8.
cos-number	Specify COS value.	0 – 7
queue	Specify queue number.	1 – 8

5.3.3 Maintenance and Commissioning

Purpose

When the queue scheduling and congestion control functions are not normal and you need to view, debug or locate the problem, you can use this section to operate.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
To display interface QoS configuration information.	1. Maintain the current privileged user view without executing any commands. 2. Execute the command **show qos interface {LAG| GigabitEthernet}** *interface-number* to display interface QoS configuration information.
To display interface queue and priority mapping relationship.	1. Maintain the current privileged user view without executing any commands. 2. Execute the command **show qos map**. 3. End.

Attached table:

Parameter	Explanation	Value
interface-number	Specify interface number.	Integer form, value range of the GE interface is 1 – 28.

6. Security Configuration

6.1 Overview

This chapter introduces the basic security content, configuration examples in the switch. This chapter includes the following topics:

6.2 ACL Configuration

6.2.1 ACL Overview

ACL Function

By configuring ACL (Access Control List) rules and actions to determine what kind of data packets can pass, what kind of data packets should be rejected, etc., so as to realize the transmission of control data, improve network performance, and ensure business security.

ACL is a series of sequential rules and actions composed of Layer 2 MAC and Layer 3 IP. These rules filter packets based on the source address, destination address, and port number of the packet. ACL classifies the data packets through these rules. These rules are applied to the switch. The switch determines which data packets can be received, which data packets need to be rejected, and other actions based on these rules.

Supported ACL Classification

The switch supports Layer 2 ACL and Layer 3 ACL.

✧ Layer 2 ACL: mainly based on the source MAC address, destination MAC address, VLAN, priority, protocol type, rate limit template, time period template and other information to classify and define data packets.

✧ Layer 3 ACL: mainly based on the source IP address, destination IP address, source port number, destination port number, protocol type, priority, fragmentation, time-to-live, rate limit template, time period template, etc. The definition of classification.

6.2.2 Configure Layer 2 ACL

Background Information

An ACL is a series of lists composed of several rules and actions. Several rule lists form an ACL.

Before configuring the rules of the Layer 2 ACL, you first need to create a Layer 2 ACL and specify the ACL type label number as 1 – 1000.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
To create a Layer 2 ACL.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **mac acl** *acl-name* to create a Layer 2 ACL (access control list) and enter the Layer 2 ACL configuration view. 3. End.
To configure Layer 2 ACL rules.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **mac acl** *acl-name* to enter the Layer 2 ACL configuration view. 3. Execute the command: **sequence** *sequence-number* **permit** {*src-mac-address/M*| **any**} {*dst-mac-address/M* |**any**} **vlan** {*VLAN ID*|**any**} **cos** {*cos-src cos-dst*|**any**} **ethtype** {*ethtype-number*|**any**} **sequence** *sequence-number* **deny** {*src-mac-address/M*| **any**} {*dst-mac-address/M* |**any**| **any**} **vlan** {*VLAN ID*|**any**} **cos** {*cos-src cos-dst*| **any**} **ethtype** {*ethtype-number*|**any**} **sequence** *sequence-number* **deny** {*src-mac-address/M*| **any**} {*dst-mac-address/M* |**any**| **any**} **vlan** {*VLAN ID*|**any**} **cos** {*cos-src cos-dst*| **any**} **ethtype** {*ethtype-number*|**any**} **shutdown**
To bind Layer 2 ACL.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **interface GigabitEthernet** *interface-number* to enter the interface configuration view; execute the command **mac acl** *acl-name* to apply ACL to physical ports. 3. End.
To unbind the port that is globally bound to the ACL.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **interface GigabitEthernet** *interface-number* to enter the interface configuration view; execute the command **no mac acl** *acl-name* to cancel applying ACL to physical ports. 3. End.

Attached table:

Parameter	Explanation	Value
acl-name	Specify the name of the access control list.	Integer form, value range is 1 – 16.
sequence-number	Specify the priority number of the rule.	1 – 2147483647

src-mac-address/ M| **any**	Source MAC address information of the specified ACL rule.	*M* is an integer and the range is 1 – 48. **any** represents any source MAC address.
dst-mac-address/M |**any**	The destination MAC address information of the specified ACL rule.	*M* is an integer and the range is 1 – 48. **any** represents any source MAC address.
VLAN ID|**any**	VLAN number.	1 – 4094
cos-src cos-dst|**any**	Cos value.	0 – 7, **any** means all.
ethtype-number| **any**	Type of data frame.	Value range is 0x600-0xffff; **any** means all.

6.2.3 Configure Layer 3 ACL

ACL Function

An ACL is a series of lists composed of several rules and actions. Several rule lists form an ACL.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
To create a Layer 3 ACL (IPv4).	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **ip acl** *acl-name* to create a Layer 3 ACL (access control list) and enter the Layer 3 ACL configuration view. 3. End.
To configure three-tier ACL rules (IPv4).	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **ip acl** *acl-name* to enter the Layer 3 ACL configuration view. 3. Execute the following command to configure matching ACL rules: **sequence** *sequence-number* **{deny|permit} ip** { *src-mac-address/M*| **any**} {*dst-mac-address/M* |**any**} {**any|dscp |precedence**} *value-number* **sequence** *sequence-number* **{deny|permit} ICMP** {src-ipv6-address/M| **any**} {*dst-mac-address/M* |**any**} {**any** |*code*} {**any** | number} (list only commonly used configurations) 4. End.
To create a three-tier ACL (IPv6).	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **ipv6 acl** *acl-name* to create a three-layer

	ACL (access control list) with the number and enter the three-layer ACL configuration view. 3. End.
To configure three-tier ACL rules (IPv6).	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **ipv6 acl** *acl-name* to enter the Layer 3 ACL configuration view. 3. Execute the following command to configure matching ACL rules: **sequence** *sequence-number* **{deny|permit} ICMP** { *src-ipv6-address/M*| **any** } {*dst-ipv6-address/M*|**any**} {**any** |*icmp-type-define*} {**any**|*icmp-code-define*}**{dscp |precedence}** {**any**|*value-number*}
To bind to Layer 3 ACL.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **interface GigabitEthernet** *interface-number* to enter the interface configuration view. 3. Execute the command **ip acl** *acl-name* (IPv4) or **ipv6 acl** *acl-name* (IPv6) to apply ACL to the interface. 4. End.
To remove the ACL applied to the connection.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **interface GigabitEthernet** *interface-number* to enter the interface configuration view. 3. Execute the command **no ip acl** (IPv4) or **no ipv6 acl** (IPv6) to remove the ACL applied to the connection. 4. End.

Attached table:

Parameter	Explanation	Value
acl-name	Access control list name.	String form.
sequence-number	The priority number of the rule.	1 – 2147483647
value-number	The priority value.	DSCP: 0 – 63 or ip: 0 – 7.
src-ip-address/M | **any**	Source IP of the specified ACL rule address information.	*src-ip-address* is in dotted decimal form; *M*: 1 – 32. **any** represents any source IP address.
dst-ip-address/M | **any**	The purpose of the specified ACL rule IP address information.	*dst-ip-address* is in dotted decimal form; *M*: 1 – 32. **any** represents any source IP address.

type	ICMP type.	-
code	ICMP code.	0 – 255
interface-number	Interface number.	1 – 28
src-ipv6-address/M **any**	Source IPv6 of the specified ACL rule address information.	*src-ip-address* is in dotted decimal form; *M*: 1 – 32. **any** represents any source IPv6 address.
dst-ipv6-address/M |**any**	The purpose of the specified ACL rule IPv6 address information.	*dst-ip-address* is in dotted decimal form; *M*: 1 – 128. **any** represents any source IP address.
cmp-type-define	Number of type messages.	0 – 255
icmp-code-define	ICMP code.	0 – 255

6.2.4 Maintenance and Commissioning

Purpose

When the ACL function is not normal and you need to view, debug or locate the problem, you can use this section to operate.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
To delete ACL.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **no mac acl** *acl-name* or **no ip acl** *acl-name*, or **no ipv6 acl** *acl-name* to delete the corresponding ACL. 3. End.
To delete ACL rule.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **mac acl** *acl-name* or **ip acl** *acl-name*, or **ipv6 acl** *acl-name* to enter ACL configuration view. 3. Execute the command **no sequence** *sequence-number* to delete the corresponding ACL rules. 4. End.
To display access control list configuration information.	1. Keep in privileged user view. 2. Execute the command **show acl** to display the global configuration of the access control list. 3. End.

To enable ACL debugging.	1. Keep in privileged user view. 2. Execute the command **deunish env** to enter the debug mode. 3. Execute the command **logging dbgmsg** ACL-ID(Sequence number of ACL) to enable ACL debugging. 4. End.
To enable ACL debugging.	1. Keep in privileged user view. 2. Execute the command **deunish env** to enter the debug mode. 3. Execute the command **logging dbgmsg** ACL-ID(Sequence number of ACL) to enable ACL debugging. 4. End.
To disable ACL debugging.	1. Keep in privileged user view. 2. Execute the command **deunish env** to enter the debug mode. 3. Execute the command **no logging dbgmsg** ACL-ID(Sequence number of ACL) to disable ACL debugging. 4. End.

Attached table:

Parameter	Explanation	Value
acl-name	Access control list name.	String form.
sequence-number	The priority number of the rule.	1 – 2147483647

6.2.5 Configuration Example

6.2.5.1 Example of Configuring Layer 2 ACL

Network Requirements

As a gateway device, the Switch is connected to the user's PC. It is required to configure ACL to prohibit the packets with source MAC address 0001-0203-0405 and destination MAC address 0102-0304-0506 from passing through.

Network Diagram

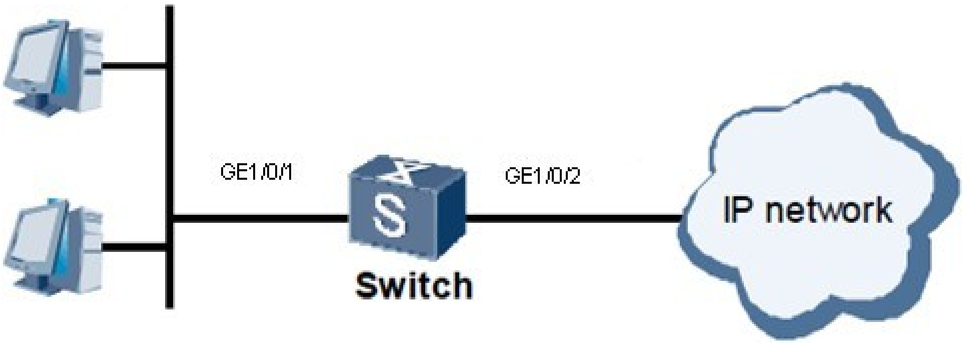
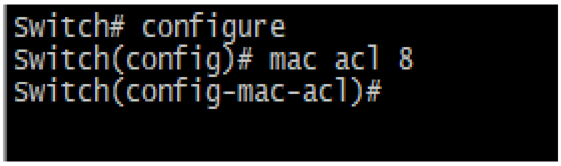


Figure 6-1. Layer 2 ACL example.

Configuration Process

1.Create a Layer 2 acl.

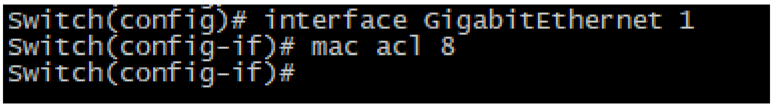


```
Switch# configure
Switch(config)# mac acl 8
Switch(config-mac-acl)#
```

2.Configure Layer 2 ACL actions and rules.

Switch(config-mac-acl)#sequence 1 deny 00:01:02:03:04:05/FF:FF:FF:FF:FF:FF 01:01:02:03:04:06/FF:FF:FF:FF:FF:FF

3.Port binding ACL.



```
Switch(config)# interface GigabitEthernet 1
Switch(config-if)# mac acl 8
Switch(config-if)#
```

6.2.5.2 Example of Configuring Layer 3 ACL

Network Requirements

The company enterprise network realizes the interconnection between various departments through the Switch. It is required to configure the IPv4 ACL correctly, prohibit the R & D department from accessing the salary query server (IP address is 10.164.9.9), and the president ’s office is not restricted and can be accessed at any time.

Network Diagram

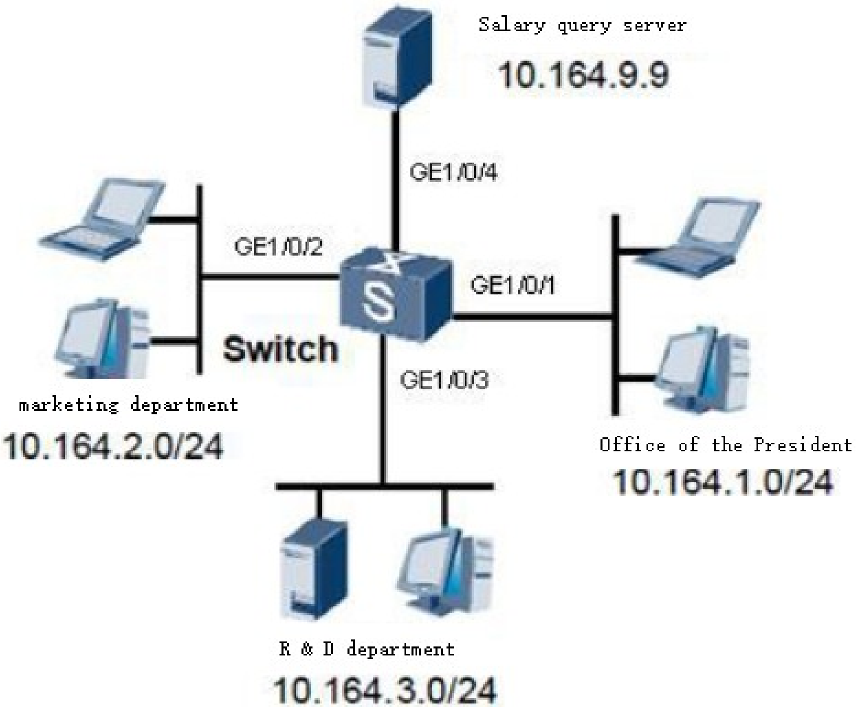


Figure 6-2. Three layer ACL example

Configuration Process

1.Configure the ACL of the president's office to allow access to the payroll query server.

Switch# configure

Switch(config)# ip acl 2

Switch(config-ip-acl)#

```
Switch(config-ip-acl)# sequence 1 permit ip
10.164.1.0/255.255.255.0
10.164.9.9/255.255.255.255
```

2.Configure the ACL of salary query server that R & D department is forbidden to access.

```
Switch# configure
Switch(config)# ip acl 3
Switch(config-ip-acl)#
Switch(config-ip-acl)# sequence 1 deny ip 10.164.3.0/255.255.255.0
10.164.9.9/255.255.255.255
```

3.Apply ACL to port.

```
Switch(config)#interface GigabitEthernet 1
Switch(config-if)# ip acl 2
Switch(config-if)# exit
Switch(config)#interface GigabitEthernet 2
Switch(config-if)# ip acl 3
Switch(config-if)# exit
```

6.3 DHCP Snooping Configuration

6.3.1 Introduction to DHCP Snooping

DHCP snooping is designed to enhance the security of DHCP.

DHCP snooping divides switch ports into two types:

✧ Non trust port: usually the port connecting the terminal equipment, such as PC, network printer, etc;

✧ Trust port: connect to the port of legal DHCP server or the uplink port of convergence switch.

By intercepting and processing the DHCP messages between DHCP client and DHCP server, the switch with DHCP snooping enabled can filter the distrust DHCP messages and establish and maintain a DHCP snooping binding table entry. This table item includes the client IP address, MAC address, port number and VLAN ID of the distrust port.

By turning on the DHCP snooping function, the switch restricts the user port (distrust port) to send only DHCP requests and discards all other DHCP messages from the user port, such as DHCP offer messages. At the same time, the switch will also compare the source MAC address of the DHCP request message with the hardware address of the DHCP client (i.e. **chaddr** field). Only the same request message of the two will be forwarded, otherwise it will be discarded. This prevents DHCP exhaustion attacks. The trust port can receive all DHCP messages. By setting the port that the switch connects to the legitimate DHCP server as the trust port and the other port as the distrust port, users can be prevented from forging the DHCP server to attack the network.

Before the relay agent forwards the DHCP message of the client to the DHCP server, it can insert some option information, so that the DHCP server can know the information of the client more accurately, and can allocate IP address and other parameters more flexibly according to corresponding policies. This option is called: DHCP relay agent information option. The option number is 82, so it is also called option 82. The related standard document is rfc3046.

Option 82 is an extended application of the DHCP option. Option 82 is only an application extension. Whether to carry option 82 will not affect the original application of DHCP. Also see if the DHCP server supports option 82. The DHCP server that does not support option 82 receives the message with option 82 inserted, or the DHCP server that supports option 82 receives the message without option 82 inserted, neither of which will affect the original basic DHCP service. To support the extended application brought by option 82, the DHCP server itself must support option 82 and the received DHCP message must be inserted with option 82 information.

Option 82 can identify different users, and the server can assign different users different options according to Option 82.

- IP address to realize QoS and Option82 field configuration.

DHCP Snooping Features Supported by the Switch

- **Trusted/distrust** Interface configuration.
- Statically add user binding entry function.
- MAC address detection function.
- Safety management.
- Address to realize QoS, Option82 field configuration.

6.3.2 Configure to Prevent DHCP Server Phishing Attacks

Background Information

The counterfeit DHCP Server in the network will respond to the DHCP Client counterfeit information, so that the DHCP Client cannot access the network normally or cannot access the correct network. To avoid being attacked by the counterfeiters of DHCP Server, DHCP Snooping provides Trusted / distrust working mode. Configure the network-side interface to Trusted mode and the user-side interface to distrust mode. All DHCP Relay messages received from the distrust interface are discarded.

Prerequisites

The DHCP server has been configured on the network.

Purpose

In order to prevent DHCP server phishers from attacking and locating DHCP server phishers, you can use the DHCP Snooping Trusted / distrust working mode and the DHCP Server detection function.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
To enable DHCP Snooping globally.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **ip dhcp snooping** to enable DHCP Snooping globally.
To configure trusted / distrust interface.	1. Execute the command **configure** to enter the global configuration view.

	2. Execute the command **interface GigabitEthernet** *interface-number* to enter the interface configuration view. 3. Execute the command **ip dhcp snooping trust** to configure the corresponding interface as a trusted interface; execute the command **no ip dhcp snooping trust** to configure the corresponding interface as an distrust interface.
To disable global DHCP snooping.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **no ip dhcp snooping** to disable the DHCP Snooping function. 3. End.

Attached table:

Parameter	Explanation	Value
interface-number	GE interface number.	Integer format, GE interface value range is 1 – 28.

6.3.3 Configure to Prevent DoS Attacks that Change the CHADDR Value

Background Information

If the attacker on the network does not change the source MAC address of the data frame header, but constantly changes the CHADDR (Client Hardware Address) value in the DHCP message to continuously apply for an IP address, the device only judges this based on the source MAC of the data frame header. The message is considered legal. Such attack packets can still be forwarded normally.

Prerequisites

The DHCP Server and DHCP Relay have been configured on the network.

Purpose

To prevent an attacker from attacking the DHCP server by changing the CHADDR value, you can perform the operation in this section to configure the DHCP Snooping function to check the CHADDR field in the DHCP Request message (this field is consistent with the source MAC of the data frame header, and then forward this message; if it is not , Then discard this message).

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
To enable DHCP Snooping globally.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **ip dhcp snooping** to enable DHCP Snooping globally. 3. End.
To enable the function to check whether the	1. Execute the command **configure** to enter the global configuration view.

MAC address in the request packet sent by the DHCP user is legal.	2. Execute the command **interface GigabitEthernet** *interface-number* to enter the interface configuration view. 3. Execute the command **ip dhcp snooping verify mac-address**. 4. End.

Attached table:

Parameter	Explanation	Value
interface-number	GE interface number.	Integer format, GE interface value range is 1 – 28.

6.3.4 Configure Option

Purpose

Use the operations in this section to set option related configurations.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
(Optional.) To enable / disable Option82 function under the interface.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **interface GigabitEthernet** *interface-number* to enter the interface configuration view. 3. Execute the command **ip dhcp snooping option** to enable Option82 on the interface; execute the command **no ip dhcp snooping option** to disable Option82 function.
To enable DHCP Snooping globally.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **ip dhcp Snooping** to enable DHCP Snooping globally.
To configure Option82.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **interface GigabitEthernet** *interface-number* to enter the interface configuration view. 3. Execute the command **ip dhcp snooping option circuit-id** *circuit-id* to configure the circuit-id content of Option82. 4. Execute the command **ip dhcp snooping option remote-id** *remote-id* to configure the remote-id content of Option82. 5. End.
To remove Option82 Circuit-ID content.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **interface GigabitEthernet** *interface-number* to enter the interface configuration view. 3. Execute the command **no ip dhcp snooping option circuit-id *circuit-id*** to delete the Circuit-ID content of Option82. 4. End.

To delete Option82 Remote-ID content.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **no ip dhcp snooping option remote-id** ***remote-id*** to delete the Remote-ID content of Option82. 3. End.
To configure Option82's strategy.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **interface GigabitEthernet** *interface-number* to enter the interface configuration view. 3. Execute the command **ip dhcp snooping option action { drop | keep | append }** to enable Option82 on the interface; execute the command **no ip dhcp snooping option** to configure Option82 strategy. 4. End.

Attached table:

Parameter	Explanation	Value
interface-number	GE interface number.	1 – 28
circuit-id	Circuit ID number.	1 – 63
remote-id	Remote ID number.	1 – 63

6.3.5 Maintenance and Commissioning

Purpose

When the DHCP Snooping function is not normal and you need to view, debug, or locate the problem, you can use this section.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
To enable DHCP Snooping debugging.	1. Maintain the current privileged user view without executing any commands. 2. Execute the command **deunish env** to enter debug view. 3. Execute the command **logging dbgmsg** *DHCP-id* to enable DHCP Snooping debugging.
To disable DHCP Snooping debugging.	1. Maintain the current privileged user view without executing any commands. 2. Execute the command **no logging dbgmsg** *DHCP-id* to disable DHCP Snooping debugging.
To clear DHCP Snooping statistics.	1. Maintain the current privileged user view without executing any commands. 2. Execute the command **clear ip dhcp snooping database statistics** to clear the DHCP Snoop statistical count.

	3. End.
To display DHCP Snooping configuration information.	1. Maintain the current privileged user view without executing any commands. 2. Execute the command **show ip dhcp snooping** to display the configuration information of DHCP Snooping protocol. 3. End.
To display binding configuration information of DHCP Snooping protocol.	1. Maintain the current privileged user view without executing any commands. 2. Execute the command **show ip dhcp snooping binding** to display user binding configuration information of DHCP Snooping protocol. 3. End.
To display user interface configuration statistics under DHCP Snooping protocol.	1. Maintain the current privileged user view without executing any commands. 2. Execute the command **show ip dhcp snooping interfaces GigabitEthernet** *interface-number* to display user interface configuration information under DHCP Snooping protocol. 3. End.

Attached table:

Parameter	Explanation	Value
DHCP-id	Number of options in the specified debug view.	0 – 200
interface-number	Specify the GE interface.	1 – 28

6.3.6 Configuration Example

Networking Requirements

A company's office area includes three groups group1, group2, and group3, which are independently distributed in three rooms. The company manages IP addresses through a DHCP server and assigns different groups of addresses in different ranges.

The specific requirements are as follows:

✧ The DHCP server assigns addresses of the 192.168.1.0/24 network segment to office equipment, and the validity period is 12 hours, and specifies the DNS and WINS server addresses as 192.168.10.2 and 192.168.10.3, respectively.

✧ The three groups group1, group2, and group3 connect to the DHCP snooping device through ports Ethernet1 / 0/1, Ethernet1 / 0/2, and Ethernet1 / 3, respectively, and communicate with the DHCP server through the DHCP snooping device.

✧ The DHCP server allocates addresses between 192.168.1.2 and 192.168.1.30 for users in group1; addresses between 192.168.1.100 and 192.168.1.200 for users in group2; and addresses between 192.168.1.200 and 192.168.1.250 for users in group3 Address.

Network Diagram

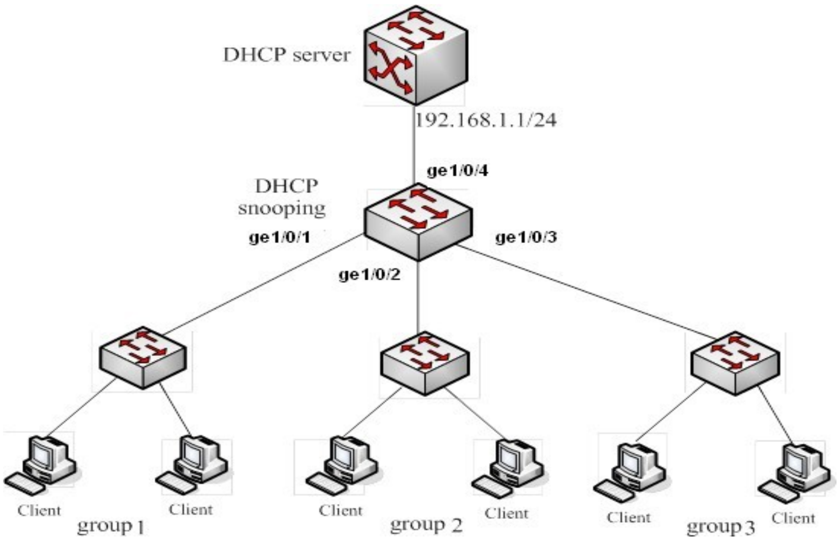


Figure 6-3. IGMP configuration topology.

Configuration Ideas

✧ Enable Option 82 on the DHCP snooping device.

✧ You can configure Option 82 sub-option content through the command line, so that users in different groups carry different Option 82 information. This can be achieved by user-defined Circuit ID sub-option content.

✧ The DHCP server allocates addresses between 192.168.1.2 and 192.168.1.30 for users in group1; addresses between 192.168.1.100 and 192.168.1.200 for users in group2; and addresses between 192.168.1.200 and 192.168.1.250 for users in group3 Address.

Configuration Ideas

1. Enable DHCP Snooping globally.

```
Switch#configure
Switch(config)#ip dhcp snooping
```

2. Configure port gigaethernet1 / 0/4 as a trusted port.

```
Switch(config)#interface GigabitEthernet 4
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)# exit
Switch(config)#
```

3.Enable Option 82 on port gigaethernet1 / 0/1.

```
Switch(config)#interface GigabitEthernet 1
Switch(config-if)# ip dhcp snooping option
```

4.Configure the circuit ID of Option 82 on port gigaethernet1 / 0/1 to be filled with group1.

```
Switch(config-if)# ip dhcp snooping option circuit-id group1
```

5.Enable Option82 on port gigaethernet1 / 0/2.

```
Switch(config)#interface GigabitEthernet 2
Switch(config-if)# ip dhcp snooping option
```

6.Configure the circuit ID of Option 82 on port gigaethernet1 / 0/2 and fill it with group2.

```
Switch(config-if)# ip dhcp snooping option circuit-id group2
Switch(config-if)# exit
Switch(config)#
```

7.Enable Option 82 on port gigaethernet1 / 0/3.

```
Switch(config)#interface GigabitEthernet 3
Switch(config-if)# ip dhcp snooping option
```

8.On port gigaethernet1 / 0/3, configure the Circuit ID of Option 82 to be filled with group3.

```
Switch(config-if)# ip dhcp snooping option circuit-id group3
```

9.Check the configuration effect.

```
Swich#show running-config
!
ip dhcp snooping
!
interface gi1
ip dhcp snooping option
ip dhcp snooping option circuit-id "group1"
!
interface gi2
ip dhcp snooping option
ip dhcp snooping option circuit-id "group2"
!
interface gi3
ip dhcp snooping option
ip dhcp snooping option circuit-id
"group3"
!
interface gi4
ip dhcp snooping trust
!
```

6.4 Dynamic ARP Protection

6.4.1 Dynamic ARP Protection Related Configuration

Purpose

This section describes how to configure dynamic arp protection and related modules.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
To enable or disable the dynamic arp check function.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **ip arp inspection** to enable the dynamic arp check function; execute the command **no ip arp inspection** to disable the dynamic arp check function. 3. End.
To enable or disable the VLAN dynamic arp check function.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **ip arp inspection vlan** *vlan-id* to enable the VLAN dynamic arp check function; execute the command **no ip arp inspection vlan** *vlan-id* to disable this function. 3. End.
To configure the arp rate limit on the interface.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **interface {LAG|GigabitEthernet}** *interface-number* to enter the interface configuration view. 3. Execute the command **ip arp inspection rate-limit** *rate*. 4. End.

Attached table:

Parameter	Explanation	Value
vlan-id	VLAN ID.	1 – 4094
rate	Specify arp rate.	1 – 50, Unit pps.

6.4.2 Maintenance and Commissioning

Purpose

This section describes how to display arp related configuration information.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process	Parameter Description
To display the arp check settings.	1. Maintain the privileged user view. 2. Execute the command **show ip arp inspection** to verify the arp check settings. 3. End.	-
To display the arp rate of the interface.	1. Maintain the privileged user view. 2. Execute the command **show ip arp inspection interfaces {LAG| GigabitEthernet}** *interface-number* .	*interface-number*: The specified GE interface number ranges from 1 – 28. LAG interface number ranges 1 – 8.

6.5 IP Source Guard Configuration

6.5.1 Introduction to IP Source Guard

6.5.1.1 Technical Background

There are many ways to steal IP addresses, and the common methods are as follows:

1. Statically modify the IP address For any TCP / IP implementation, the IP address is a mandatory option for its user configuration. If the user uses an IP address that is not authorized to be assigned when configuring TCP / IP or modifying TCP / IP configuration, IP address theft is formed. Since the IP address is a logical address, users cannot limit the static modification of the IP address of their host.

2. Modify the IP and MAC address in pairs. For the problem of statically modifying the IP address, many units now use IP and MAC binding technology to solve it. For the binding technology, the IP theft technology has a new development, that is, modify the IP and MAC address in pairs. For some compatible network cards, the MAC address can be modified using the network card configuration program. If you change the IP address and MAC address of a computer to the IP address and MAC address of another legal host, it can also access the network.
In addition, for those network cards whose MAC addresses cannot be directly modified, users can also use software to modify the MAC address, that is, by modifying the underlying network software to deceive the upper network software.

3. Dynamically modify the IP address Some attack programs send and receive data packets on the network, you can bypass the upper layer network software and dynamically modify your own IP address (or IP and MAC address pair) to achieve IP spoofing.

The IPSG feature is a Layer 2 interface feature that provides a detection mechanism to ensure that packets received by a single interface can be accepted by each interface. If the check is successfully passed, the data packet will be permitted; otherwise, activities that violate the policy will occur. IPSG can not only ensure that the IP addresses of terminal devices in the second layer network are not hijacked, but also ensure that unauthorized devices cannot access the network or cause the network to crash and paralyze by specifying the IP address.

By configuring IPSG, when the link is up, only DHCP packets are allowed to pass. Once the DHCP server has assigned an IP address, the DHCP binding table will be updated. IPSG then automatically loads the port-based ACL on the interface. The above process can limit the client traffic to the source IP address configured in the binding table. They will filter the traffic from the host port of the source IP address other than the source IP binding. The filtering can restrict the host from The neighboring host seizes the IP address to realize the function of network attack.

IP Source Guard is a port traffic filtering technology based on IP / MAC, which can prevent IP address spoofing attacks in the LAN. There is an IP source binding table inside the switch as the detection standard for the data packets received by each port. Only in two cases, the switch will forward the data-or the received IP packet meets the port / IP in the IP source binding table The corresponding relationship of / MAC, or received DHCP packets, the rest of the packets will be discarded by the switch. The IP source binding table can be statically configured by the user on the switch, or it can be automatically learned by the switch from DHCP Snooping. Static configuration is a simple and fixed method with poor flexibility. Therefore, it is recommended that users use IP Source Guard in conjunction with DHCP Snooping. The IP source binding table is generated by DHCP Snooping Binding Database.

6.5.1.2 Basic Concept

IP Source Guard

IP source protection is equivalent to adding an ACL entry to the port, and by default filtering all IP packets (except DHCP packets) sent by all users on the port. After the user interactively applies for an IP address through DHCP, a filter entry is added to the port to allow the user to use the address for IP packet communication, and other users still prohibit communication.

DHCP Snooping

It means DHCP snooping. By snooping the DHCP interactive messages between the client and the server, users can be monitored. At the same time, DHCP snooping functions as a DHCP message filtering function, and can filter illegal servers through reasonable configuration.

IP Source Binding Table

The IP source binding table can be added statically by the user on the switch, or the switch can listen to the binding table from DHCP (DHCP Snooping Binding Table) automatically learned and obtained. Static configuration is a simple and fixed method, but the flexibility is very poor. Therefore, it is recommended that users use IP Source Guard in conjunction with DHCP Snooping technology. The DHCP source monitors the binding table to generate the IP source binding table.

ACL

The access control list is a list of instructions applied to the router interface. These instruction lists are used to tell the router which data packets can be received and which data packets need to be rejected. As for whether the data packet is received or rejected, it can be determined by specific indication conditions like source address, destination address, port number, protocol and so on.

6.5.1.3 Features

The functional characteristics of IP Source Guard are shown in Table 6-1:

Table 6-1. IP Source Guard features.

Serial number	Function name	Function description
1	Source IP + PORT filtering	Filter IP traffic based on source IP address and port, and only allow traffic if the flow matches the binding entry. When a port creates, modifies, or deletes a new IP source binding entry, the IP source address filter will change. In order to reflect the change of IP source binding, the port ACL will be modified and reapplied to the port. By default, if the port has IP source protection enabled without an IP source binding entry, the default ACL will reject all traffic on the port (actually all IP traffic except DHCP messages).
2	Source IP + PORT + MAC filtering	Same as above.

3	Source IP + PORT + VLAN filtering	Same as above.
4	Source IP + PORT + MAC + VLAN filtering	Same as above.

6.5.1.4 System Features

The features of IP source guard system are as follows:

- IP + port + MAC + VLAN multiple combination binding to filter IP traffic.
- It can be used in combination with the dynamic table items of dhcp snooping, or it can play a role independently.
- The configuration priority of IP source guard is higher than that of dhcp snooping.
- source guard and dhcp snooping share the upper limit of configuration.
- With powerful DEBUG function.

6.5.2 Configure IP Source Guard Function

Purpose

IP Source Guard source protection is equivalent to adding an ACL entry on the port, and by default filtering all IP packets (except DHCP packets) sent by all users on the port. After the user interactively applies for an IP address through DHCP, a filter entry is added to the port to allow the user to use the address for IP packet communication, and other users still prohibit communication.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
To enable IP source protection on the interface. Use this command to check whether the IP packet matches the binding table to decide whether to forward it.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **interface GigabitEthernet** *interface-number* to enter the interface configuration view. 3. Execute the command **ip source verify** to enable interface IP packet inspection function. 4. End.
To disable IP source protection on the interface.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **interface GigabitEthernet** *interface-number* to enter the interface configuration view. 3. Execute the command **no ip source verify** to disable interface IP packet inspection function.
To configure the IP packet check option to IP plus MAC.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **interface GigabitEthernet** *interface-number* to enter the interface configuration view. 3. Execute the command **ip source verify mac-and-ip** to

	configure inspection options for IP packets (see the table below for parameter descriptions). 4. End.
To restore IP packet inspection options to default options.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **interface GigabitEthernet** *interface-number* to enter the interface configuration view. 3. Execute the command **no ip source verify** to restore IP packet inspection options to default options (see the table below for parameter descriptions). 4. End.
To configure static binding entries.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **ip source binding [A:B:C:D:E:F] vlan** *vlan-id ipv4-address Netmask* **interface GigabitEthernet** *interface-number* to configure static binding entries (see the table below for parameter descriptions).
To delete static binding entries.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **no ip source binding [A:B:C:D:E:F] vlan** *vlan-id ipv4-address Netmask* **interface GigabitEthernet** *interface-number* to delete static binding entries (see the table below for parameter descriptions). 3. End.

Attached table:

Parameter	Explanation	Value
ip-address	Checking whether the IPv4 address of the IP packet matches the binding entry.	-
mac-address	Checking whether the MAC address of the IP packet matches the binding entry.	-
vlan	Checking whether the VLAN of the IP packet matches the binding entry.	-
interface-number	GE interface number.	1 – 28
A:B:C:D:E:F	MAC address information.	**A:B:C:D:E:F**: It is in dotted decimal form; each letter is in integer form, the range is 1 – 48.

vlan-id	Specifies the VID entry where the user is located.	1 – 4094
ipv4-address	IP address to be bound.	ip-address IPv4: Address dotted decimal form.
Netmask	Subnet mask corresponding to the IP address.	-

6.5.3 Maintenance and Commissioning

Purpose

When the IP Source Guard function is abnormal and you need to view, debug, or locate the problem, you can use this section to operate.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
To enable IP Source Guard debugging.	1. Maintain the current privileged user view. 2. Execute the command **deunish env** to enter the debug view. 3. Execute the command **logging dbgmsg id** to enable the IP Source Guard debugging function. 4. End.
To disable IP Source Guard debugging.	1. Maintain the current privileged user view. 2. Execute the command **deunish env** to enter the debug view. 3. Execute the command **no logging dbgmsg id** to disable the IP Source Guard debugging function. 4. End.
To display ip source protection settings of the interface.	1. Maintain the current privileged user view. 2. Execute the command **show ip source interfaces GigabitEthernet** *interface-number* to display ip source protection settings of the interface. 3. End.
To display binding entries protected by ip source.	1. Maintain the current privileged user view. 2. Execute the command **show ip source binding {static| dynamic }** to display the binding entry of ip source protection. 3. End.

Attached table:

Parameter	Explanation	Value
id	Specify the sequence number of IP Source Guard in debug view.	**Id=9**

interface-number	GE interface number.	1 – 28.

6.5.4 Configuration Example

Network Requirements

As shown in Figure 6-4, hosts A and B are connected to the switch through interfaces ge 1/0/1 and ge 1/0/2, respectively, to ensure that host B cannot spoof the server by spoofing A's IP and MAC, and that host A's The text can be sent normally.

Network Requirements

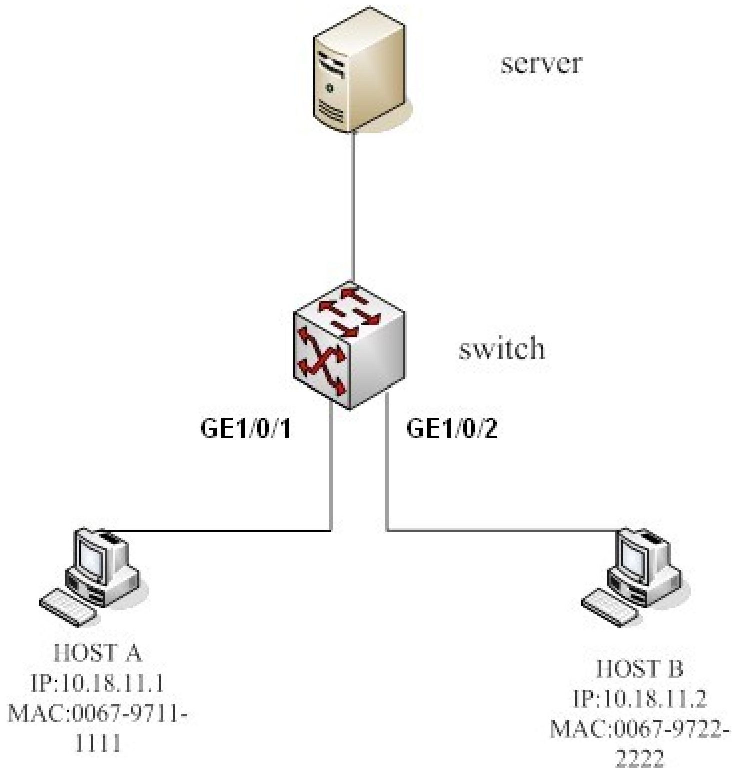


Figure 6-4. IP Source Guard networking diagram.

Configuration Ideas

Use the following ideas to configure the IP SOURCE GUARD function (assuming the user's IP is statically configured):

1. Both interface 1 and interface 2 must enable the IP SOURCE GUARD function.
2. Configure static binding entries.

Data Preparation

To complete this configuration example, the following data needs to be prepared:

1. IP and MAC of hosts A and B.
2. Connect the two ports GE 1/0/1 and GE 1/0/2 of the switch.
3. Located in VLAN 1.

Configuration Steps

```
Switch# configure
Switch(config)# interface GigabitEthernet 1
Switch(config-if)# ip source verify
Switch(config-if)# exit
Switch(config)# interface GigabitEthernet 2
Switch(config-if)# ip source verify
Switch(config-if)# exit
Switch(config)# ip source binding 00:67:97:11:11:11 vlan 1 10.18.11.1 interface
GigabitEthernet 1
```

Host A is in the binding table, host B is not present, and packets sent by host B cannot be forwarded.

6.6 802.1x Configuration

6.6.1 Introduction to 802.1x

Port-based network access control technology, based on traditional Ethernet devices, uses IEEE 802.1x protocol to provide the ability to authenticate and authorize users based on Ethernet port point-to-point connections, so that Ethernet devices can achieve provide operations Requirements, especially in the construction of broadband metropolitan area networks, can play a major role.

The 802.1x protocol is an access control and authentication protocol based on Client / Server. It can restrict unauthorized users / devices from accessing LAN / MAN through the access port. Before obtaining the various services provided by the switch or LAN, 802.1x authenticates the user / device connected to the switch port. Before the authentication is passed, 802.1x only allows EAPoL (Extended Authentication Protocol based on LAN) data to pass through the switch port to which the device is connected; after the authentication is passed, normal data can pass the Ethernet port smoothly.

The basic idea of port-based network access technology is that the network system can control the Ethernet port for the end user, so that only users allowed and authorized by the network system can access various services of the network system (such as Ethernet connection, network layer routing, Internet Access and other services).

The core part of network access technology is PAE (port access entity). In the access control process, the port access entity consists of 3 parts:

✧ Authentication people-the port that authenticates the accessed user / device.

✧ Requester-the authenticated user / device.

✧ Authentication server-a device that performs the actual authentication function on users / devices requesting access to network resources based on the information of the Authentication.

Each physical port of Ethernet is divided into two logical ports, controlled and uncontrolled. Each frame received by the physical port is sent to the controlled and uncontrolled ports. Access to the controlled port is limited by the authorization status of the controlled port. The PAE of the Authentication controls the authorized / unauthorized status of the "controlled port" based on the result of the authentication process of the authentication server. The control port in an unauthorized state denies user / device access.

6.6.2 Configure 802.1x Authorization

6.6.2.1 Globally Enable or Disable 802.1x

Purpose

This section describes how to enable or disable the 802.1x protocol globally.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
To enable 802.1x globally.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **dot1x** to enable 802.1x.
To disable 802.1x globally.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **no dot1x** to disable 802.1x.

6.6.2.2 Enable or Disable 802.1x on the Port

Purpose

This section describes how to enable or disable 802.1x on the port.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process	Parameter Description
To enable 802.1x on the port.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **interface GigabitEthernet** *interface-number* to enter the configuration view of an interface. 3. Execute the command **dot1x port-control force-auth** to enable 802.1x on the port.	*interface-number*: The specified GE interface number ranges from 1 – 28.
To disable 802.1x on the port.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **interface GigabitEthernet** *interface-number* to enter the configuration view of an interface. 3. Execute the command **no dot1x port-control force-auth** to disable 802.1x on the port.	

6.6.2.3 Set 802.1x Function

Purpose

This section describes how to set the 802.1x function.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process	Parameter Description
To configure the maximum number of	1. Execute the command **configure**. 2. Execute the command **interface**	*interface-number*: The specified GE interface

times that the device can repeatedly send an authentication request frame to an access user.	**GigabitEthernet** *interface-number*. 3. Execute the command **dot1x max-req** *max-req*.	number ranges om 1 – 28. *max-req*: Maximum number of EAP requests supported, value range is 1 – 10. *quiet-period*: Silent time, integer value, value range is 0 – 65535 (seconds). reauthenticate-period: Silent time, integer value 300 – 4294967294 (seconds). vlan-id: VLAN ID, integer value 1 – 4094. passive: Passive mode, do not actively send request / identity requests. Active: Active mode, will actively send authentication requests on the interface.
(Optional.) To set the silent time after authentication failure.	1. Execute the command **configure**. 2. Execute the command **interface GigabitEthernet** *interface-number*. 3. Execute the command **timeout quiet-period** *quiet-period*. 4. Execute the command **dot1x authentication quiet-period default**.	
(Optional.) To set the interval for re-initiating authentication after successful authentication.	1. Execute the command **configure**. 2. Execute the command **interface GigabitEthernet** *interface-number*. 3. Execute the command **dot1x timeout reauth-period** reauthenticate-period.	
To set whether to allow re-authentication.	1. Execute the command **configure**. 2. Execute the command **interface GigabitEthernet** *interface-number*. 3. Execute the command **dot1x reauth**.	
To configure the Guest VLAN function of the interface.	1. Execute the command to enter the interface configuration view (Ethernet, trunk) and interface group configuration view. 2. Execute the command **dot1x guest vlan**.	-
To delete the guest VLAN function of interface configuration.	1. Execute the command to enter the interface configuration view (Ethernet, trunk) and interface group configuration view. 2. Execute the command **no dot1x guest vlan**.	-
Port authentication timeout.	1. Execute the command to enter the interface configuration view (Ethernet, trunk) and interface group configuration view. 2. Execute the command **dot1x timeout supp-timeout** supp-time.	supp-time: The value range is 1 – 65535 (seconds). default: Specifies as default 30 seconds.
To set authentication server timeout.	1. Execute the command to enter the interface configuration view (Ethernet,	*server-timeout*: Specifies the timeout time of the

	trunk) and interface group configuration view. 2. Execute the command **dot1x timeout supp-timeout** *server-timeout*.	authentication server. It is an integer in the range of 1 – 65535 (seconds). The default value is 30 seconds.
To set the time to send EAP-Request to the next sending.	1. Execute the command to enter the interface configuration view (Ethernet, trunk) and interface group configuration view. 2. Execute the command **dot1x timeout tx-period** tx-time.	tx-time: The value range is 1 – 65535 (seconds); The default value is 30 seconds.

6.6.2.4 View 802.1x Configuration Information

Purpose

This section describes how to view the configuration information of 802.1x.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process	Parameter Description
To display authentication manager configuration.	1. Execute command to enter privileged user view. 2. Execute the command **show authentication**.	-
To display Auth Manager session information.	1. Execute command to enter privileged user view. 2. Execute the command **show authentication sessions**.	-
To display port authentication manager configuration.	1. Execute command to enter privileged user view. 2. Execute the command **show interfaces GigabitEthernet** *interface-number*.	*interface-number*: Refers to the port number of the GE interface, ranging from 1 – 28.

6.7 AAA Configuration

6.7.1 Introduction to AAA

AAA is short for Authentication, Authorization and Accounting. It provides a consistent framework for configuring these three security functions. The configuration of AAA is actually a management of network security. Network security here mainly refers to access control, including:

- Which users can access the web server?
- What services can users with access rights get?
- How to keep accounts of users who are using network resources?

AAA generally adopts a client / server structure. The client runs on the NAS (Network Access Server), and the server manages user information centrally. NAS is a server for users and a client for servers.

Figure 6-5 shows the basic network structure of AAA.is a logical address, users cannot limit the static modification of the IP address of their host.

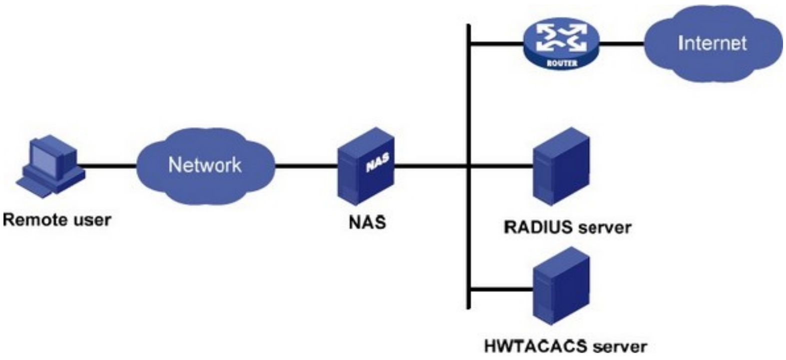


Figure 6-5. AAA basic network architecture.

Authentication Function

AAA supports the following authentication methods.

- Non-authentication: users are very trusted and their legality is not checked. Generally, this method is not used.
- Local authentication: Configure user information (including local user name, password and various attributes) on the device. The advantage of local authentication is that it is fast and can reduce operating costs; the disadvantage is that the amount of stored information is limited by the hardware conditions of the device.
- Remote authentication: Support remote authentication through RADIUS protocol or TACACS protocol. The device acts as the client and communicates with the RADIUS server or TACACS server. For the RADIUS protocol, standard or extended RADIUS protocol can be used to cooperate with iTELLIN / CAMS and other systems to complete the authentication.

Authentication Authorization

AAA supports the following authorization methods.

- Direct authorization: trust the user very much and pass the direct authorization. At this time, the user's permission is the default permission of the system.
- Local authorization: according to the relevant attributes configured for the local user account on the device.
- TACACS authorization: TACACS server authorizes users.
- Radius authorization: radius authorization is a special process. Radius authentication and authorization are done in the same process. Radius will encapsulate the authorization information in radius authentication response message when completing authentication.

6.7.2 Configure AAA Method

Purpose

This section describes how to create AAA methods.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process	Parameter Description
To add login authentication list.	1. Execute the command **configure** to enter the global configuration mode. 2. Execute the command **aaa authentication login {default|name}** {local|none|enable, | tacacs+| radius}.	**name**: Method list name string form. **default**: The default method name {local| none|enable, | tacacs+| radius}Choose 4
The configuration list is bound to ssh, console, telnet.	1. Execute the command **configure** to enter the global configuration mode. 2. Execute the command **line {ssh|console| telnet}**. 3. Execute the command **login authentication {default|name}**.	**name**: The authentication list that has been created. **default**: The default method list name.
The configuration list is bound to http or https.	1. Execute the command **configure** to enter the global configuration mode. 2. Execute the command **ip http login authentication {default|name}** for binding to http.	
To delete login authentication list.	1. Execute the command **configure** to enter the global configuration mode. 2. Execute the command **no aaa authentication login {default|name}**.	**name**: The method list name, string form. **default**: The default method list name.

6.7.3 Configure RADIUS Server

Purpose

This section describes how to configure the Radius server.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process	Parameter Description
To create a Radius server.	1. Enter the privilege configuration view. 2. Execute the command **configure** to enter the global configuration mode. 3. Execute the command **radius host** ip-address **auth-port** *auth-port* **Key** *key* **priority** *priority* **retransmit** *retransmit* **timeout** *timeout* **type{all| 802.1x|login}**.	ip4-address IPv4: Address dotted decimal form, such as (:A.B.C.D), where A – D is 0 – 255 decimal number; the following 5 parameters are not regarded as the system default. *auth-port*: 0 – 65535 *key*: RADIUS server key. *priority*: 0 – 65535 *retransmit*: 1 – 10, The default is 3.

		timeout: 1 – 30
To remove Radius server.	1. Enter the privilege configuration view. 2. Execute the command **configure** to enter the global configuration mode. 3. Execute the command **no radius host** ip-address.	ip4-address IPv4: Address dotted decimal form, such as (:A.B.C.D), where A – D is 0 – 255 decimal number.
To display default Radius server configuration.	1. Enter the privilege configuration view. 2. Execute the command **show radius default-config**.	-
To display IPV4- based Radius server configuration.	1. Enter the privilege configuration view. 2. Execute the command **show radius**.	-

6.7.4 Configure TACACS Server

Purpose

This section describes how to configure the TACACS server.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process	Parameter Description
To create and configure the name and shared secret of the Tacacs server.	1. Enter the privilege configuration view. 2. Execute the command **configure** to enter the global configuration mode. 3. Execute the command **tacacs host** ip-address **key** key.	ip4-address IPv4: Address dotted decimal form, the maximum length of the key shared key is 64.
To configure TACACS server timeout.	1. Enter the privilege configuration view. 2. Execute the command **configure** to enter the global configuration mode. 3. Execute the command **tacacs host** ip-address **timeout** *timeout*.	*timeout*: Value is 1 – 30.
To configure TACACS server priority.	1. Enter the privilege configuration view. 2. Execute the command **configure** to enter the global configuration mode. 3. Execute the command **tacacs host** ip-address **priority** *priority*.	*priority*: Server priority is 0 – 65535.
To configure TACACS server port.	1. Enter the privilege configuration view. 2. Execute the command **configure** to enter the global configuration mode.	*port*: UDP / TCP port 0 – 65535.

	3. Execute the command **tacacs host** ip-address **port** *port*.	
To remove tacacs server.	1. Enter the privilege configuration view. 2. Execute the command **configure** to enter the global configuration mode. 3. Execute the command **no tacacs host** ip-address**.**	ip-address IPv4: Address dotted decimal form.
To display tacacs server configuration information.	1. Enter the privilege configuration view. 2. Execute the command **show tacacs**.	-

6.7.5 Display AAA Configuration Information

Purpose

This section describes how to display AAA configuration information.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process	Parameter Description
To display login authentication list.	1. Enter the privilege configuration view. 2. Execute the command **show aaa authentication {enable|login} lists**.	-

6.7.6 AAA Debugging

Purpose

This section describes how to turn the debugging AAA switch on or off.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process	Parameter Description
To enable the AAA debugging switch.	1. Enter the privilege configuration view. 2. Execute the command **deunish env** to enter the debug view. 3. Execute the command **logging dbgmsg** aaa-id to enable aaa debugging.	aaa-id: Sequence number of aaa option in debug view.
To disable the AAA debugging switch.	1. Enter the privilege configuration view. 2. Execute the command **deunish env** to enter the debug view. 3. Execute the command **no logging dbgmsg** aaa-id to disable aaa debugging.	

7. Reliability Configuration

7.1 Overview

This chapter introduces the basic content, configuration process, and configuration examples of reliability management in the switch. This chapter includes the following topics:

7.2 STP Configuration

7.2.1 Introduction to STP

Cause of STP

In a Layer 2 switched network, once a loop exists, packets will continue to circulate and accumulate within the loop, generating broadcast storms, thereby occupying all available bandwidth and making the network unusable.

In this environment, the STP protocol came into being. The 802.1D standard released by IEEE in 1998 defines STP (Spanning Tree Protocol).

STP Working Process

First, the election of Root Bridge. The election is based on the bridge ID combined with the bridge priority and bridge MAC address family. The bridge with the smallest bridge ID will become the root bridge in the network. All its ports are connected to the downstream bridge, so the port role becomes the designated port. Next, the downstream bridges connected to the root bridge will each select a "thickest" branch as the path to the root bridge, and the role of the corresponding port becomes the root port. Loop this process to the edge of the network, and a tree is generated after the designated port and root port are determined. After the spanning tree stabilizes for a period of time (the default value is about 30 seconds), the designated port and root port enter the forwarding state, and other ports enter the blocking state. STP BPDUs are sent out regularly from designated ports of each bridge to maintain the status of the link. If the network topology changes, the spanning tree will be recalculated and the port status will change accordingly. This is the basic principle of spanning tree.

STP Working Process

With the deepening of applications and the development of network technology, the shortcomings of STP are also exposed in the application. The shortcomings of STP protocol are mainly manifested in the convergence speed.

When the topology changes, new configuration messages must be transmitted to the entire network after a certain delay. This delay is called Forward Delay, and the default value of the protocol is 15 seconds. Before all the bridges receive this change message, if the ports in the old topology that are being forwarded have not found that they should stop forwarding in the new topology, there may be a temporary loop. In order to solve the problem of temporary loops, STP uses a timer strategy, which is to add an intermediate state that only learns the MAC address but does not participate in forwarding from the blocking state to the forwarding state of the port. The length of time for both state switches It is Forward Delay, so as to ensure that no temporary loop will occur when the topology changes. However, this seemingly good solution actually brings about at least twice the convergence time of Forward Delay, which is unacceptable in some real-time services (such as voice and video).

7.2.2 Introduction to RSTP

Advantages of RSTP

In order to solve the shortcomings of the convergence speed of the STP protocol, in 2001 IEEE defined the rapid spanning tree protocol RSTP based on the IEEE 802.1w standard. The RSTP protocol has made three important improvements on the basis of the STP protocol to speed up the convergence speed (the fastest can be within 1 second):

- Alternate Port and Backup Port for fast switching are set for the root port and designated port. When the root port fails, the replacement port will quickly switch to the new root port and enter the forwarding state without delay; when the designated port fails, the backup port will quickly switch to the new designated port. Delayed to enter the forwarding state.
- In a point-to-point link that connects only two switching ports, the designated port only needs to perform a handshake with the downstream bridge to enter the forwarding state without delay. If three shared links connected by an Internet bridge are connected, the downstream bridge will not respond to the handshake request sent by the designated upstream port, and can only wait for twice the Forward Delay time to enter the forwarding state.

Disadvantages of RSTP

Compared with the STP protocol, the RSTP protocol does have a lot of improvements, and it is backward compatible with the STP protocol and can be mixed in a network. However, RSTP and STP belong to Single Spanning Tree (SST), which has its own many defects, mainly in three aspects:

- Because there is only one spanning tree in the entire switching network, it will cause a long convergence time when the network scale is relatively large.
- Because RSTP is a single spanning tree protocol, all VLAN share a spanning tree. In order to ensure normal communication within VLAN, each VLAN in the network must be continuously distributed along the path of the spanning tree, otherwise some VLANs will appear. Internal links are blocked and separated, which leads to the problem that the VLAN cannot communicate.
- When a link is blocked, it will not carry any traffic, and load balancing cannot be achieved, causing a great waste of bandwidth.

These defects are insurmountable by single spanning tree, so the multiple spanning tree protocol MSTP that supports VLAN appears.

7.2.3 Introduction to MSTP

Advantages of RSTP

The multiple spanning tree protocol MSTP is a new type of spanning tree protocol defined in the 802.1s standard released by IEEE in 2002. Compared with STP and RSTP, the advantages are very obvious. The characteristics of MSTP are as follows:

- MSTP introduces the concept of "domains" and divides a switching network into multiple domains. Multiple spanning trees are formed in each domain, and the spanning trees are independent of each other; among the domains, MSTP uses CIST to ensure that there is no loop in the entire network topology.

- MSTP introduces the concept of "instance (Instance)", which maps multiple VLAN to an instance to save communication overhead and resource occupancy. The calculation of the topology of each MSTP instance is independent (each instance corresponds to a separate spanning tree), and VLAN data load sharing can be achieved on these instances.
- MSTP can implement a rapid port state migration mechanism similar to RSTP.
- MSTP is compatible with STP and RSTP.

MSTP Algorithm Implementation

1. Initial state.

Each port of each device will initially generate a configuration message with itself as the root bridge. The total root and domain root are the local bridge ID, the external root path cost and internal root path cost are all 0, and the designated bridge ID is the local bridge ID, the designated port is the port, and the port receiving BPDU packets is 0.

2. The selection principle of port roles.

The selection principles of port roles are shown in Table 7-1.

Table 7-1. Port role selection principles.

Port role	Selection principle
Root port	The port priority vector of a port is better than its specified priority vector, and the root priority vector of the device is taken from the root path priority vector of the port.
Designated port	The specified priority vector of a port is better than its port priority vector.
Master port	The role of the domain boundary root port on the MSTI instance is the master port.
Alternate port	The port priority vector of a port is better than its specified priority vector, but the root priority vector of the device is not taken from the root path priority vector of the port.
Backup port	The port priority vector of the port is better than its designated priority vector, but the designated bridge ID in the port priority vector is the bridge ID of the device.

3. Priority vector calculation.

The MSTP roles of all bridges are calculated from the information carried in the packets. The most important information carried in the packets is the priority vector of the spanning tree. The calculation methods of CIST priority vector and MSTI priority vector will be introduced below.

a) CIST priority vector calculation.

The priority vector in CIST is composed of total root, external root path cost, domain root, internal root path cost, designated bridge ID, designated port ID, and port ID for receiving BPDU packets.

In order to facilitate the subsequent description, the following assumptions are made:

- Initially, the information carried in the packets sent by port PB of bridge B is as follows: the total root is RB, the external root path cost is ERCB, the domain root is RRB, the internal root path cost is IRCB, and the designated bridge ID is B , The designated port ID is PB, and the port ID for receiving BPDU packets is PB.

- The port PB of bridge B receives the information sent by the packet sent by the port PD of bridge D as follows: the total root is RD, the external root path cost is ERCD, the domain root is RRD, and the internal root path cost is IRCD The designated bridge ID is D, the designated port ID is PD, and the port ID for receiving BPDU packets is PB.
- Bridge B's port PB receives packets from bridge D's port PD and has higher priority.

Based on the above assumptions, the calculation method of each priority vector will be introduced one by one below.

(1) Message priority vector.

The message priority vector is the priority vector carried in MSTP protocol packets. According to the assumption, the message priority vector received by port PB of bridge B is: {RD: ERCD: RRD: IRCD: D: PD: PB}. If Bridge B and Bridge D are not in the same domain, the internal root path cost is meaningless to Bridge B, and it will be assigned a value of 0.

(2) Port priority vector.

In the initial situation, the port priority vector information is rooted in itself. The port priority vector of port PB is:{RB: ERCB: RRB: IRCB: B: PB: PB}.

The port priority vector is updated with the message priority vector received by the port: if the message priority vector received by the port is better than the port priority vector, the port priority vector is updated to the message priority vector; otherwise, the port priority. The level vector remains unchanged. Since the message priority vector received by port PB is better than the port priority vector, the port priority vector is updated to: {RD: ERCD: RRD: IRCD: D: PD: PB}.

(3) Root path priority vector.

The root path priority vector is calculated from the port priority vector:

- If the port priority vectors come from bridges in different domains, the external root path cost of the root path priority vector is the sum of the path cost of the port and the external root path cost of the port priority vector. As the domain root of the bridge, the internal root path cost is 0. Assuming that the path cost of the port PB of the bridge B is PCPB, the priority path of the root path of the port PB is: {RD: ERCD + PCPB: B: 0: D: PD: PB}.
- If the port priority vector comes from a bridge in the same domain, the internal path cost of the root path priority vector is the sum of the internal root path cost of the port priority vector and the port path cost. After calculation, the root path priority vector of port PB is : {RD: ERCD: RRD: IRCD + PCPB: D: PD: PB}.

(4) Bridge priority vector.

The total root ID, domain root ID, and designated bridge ID in the bridge priority vector are all local bridge IDs. The external root path cost and internal root path cost are 0, and the designated port ID and receiving port ID are all 0. The bridge priority vector of bridge B is: {B: 0: B: 0: B: 0: 0}.

(5) Root priority vector.

The root priority vector is the optimal value of the bridge priority vector and the root path priority vectors of all the specified bridge IDs and ID values of the own bridge. If the own bridge priority vector is better, the own bridge is the CIST total root. Assuming that the bridge priority vector of bridge B is optimal, the root priority vector of bridge B is: {B: 0: B: 0: B: 0: 0}.

(6) Specify priority vector.

The designated priority vector of a port is calculated from the root priority vector, and the designated bridge ID of the root priority vector is replaced with the bridge ID, and the designated port ID is replaced with its own port ID. The designated priority vector of the port PB of bridge B is: {B: 0: B: 0: B: PB: 0}.

b) MSTI priority vector calculation.

The calculation rules of each priority vector of MSTI and the calculation rules of CIST priority vector are basically the same, there are two differences:

- There is no total root and external root path cost in the MSTI priority vector, and it consists of only the domain root, internal root path cost, designated bridge ID, designated port ID, and port ID for receiving BPDU packets.
- MSTI only processes message priority vectors from the same domain.

4. Role selection process.

The calculation process of the CIST instance will be briefly described below in conjunction with the networking shown in Figure 7-1. Assume that the priority of the bridge is that Switch A is better than Switch B, Switch B is better than Switch C, and 4, 5, and 10 are link path costs, respectively. Switch A and Switch B belong to the same domain, and Switch C is a separate domain.

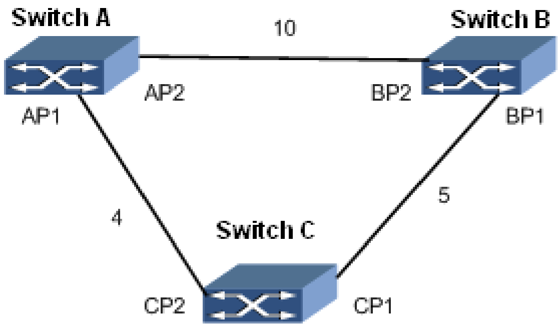


Figure 7-1. Network diagram of MSTP algorithm calculation process.

Table 7-1 shows the message priority vectors carried in the packets sent by each device in the initial situation in Figure 7-1.

Table 7-2 Initial state of each device

Device	Port	Message priority vector in the message
Switch A	AP1	{A:0:A:0:A:AP1:0}
	AP2	{A:0:A:0:A:AP2:0}
Switch B	BP1	{B:0:B:0:B:BP1:0}
	BP2	{B:0:B:0:B:BP2:0}
Switch C	CP1	{C:0:C:0:C:CP1:0}
	CP2	{C:0:C:0:C:CP2:0}

Initially, the port priority vector and the message priority vector of each port of the device are consistent.

In the initial case, the ports of each device will be calculated as designated ports and send message priority vectors with themselves as the root bridge.

a) Switch A's role selection process.

Switch A's port AP1 and port AP2 will receive packets from Switch B and Switch C respectively, Switch A will compare the port priority vectors of ports AP1 and AP2 with the received message priority vectors from other switches, Because the port priority vectors of AP1 and AP2 are superior to the message priority vectors carried in the packets, the port roles of ports AP1 and AP2 remain unchanged as the designated ports, and the device Switch A is the common root and is the domain of Switch A and Switch B Domain root. After that, the port periodically propagates the message rooted at itself.

b) Switch B's role selection process.

After receiving the packet from the port CP1 of Switch C, the port BP1 of Switch B compares the message priority vector with the port priority vector. Since the port priority vector is better than the message priority vector, the port role is not updated.

After receiving the packet from the port AP2 of Switch A, the port BP2 of Switch B processes as follows:

(1) Compare the message priority vector of the port with the port priority vector. Since the message priority vector of the port is better than the port priority vector, the port priority vector of the port is updated to the message priority vector{A: 0: A: 0: A: AP2: BP2}.

(2) Calculate the root priority vector of the port. Switch A and Switch B are in the same domain, and the root path priority vector of the port is {A: 0: A: 10: A: AP2: BP2}.

(3) Calculate the root priority vector of Switch B. Only the root path priority vector of port BP2 comes from other devices. Since the root path priority vector of port BP2 is better than the bridge priority vector of Switch B, the root priority vector of Switch B is {A: 0: A: 10: A: AP2: BP2}.

(4) Specify priority vector calculation. The specified priority vector of port BP1 is {A: 0: A: 10: B: BP1: BP2}, the port. The specified priority vector of BP2 is {A: 0: A: 10: B: BP2: BP2}.

Determination of port role: Compare the specified priority vectors of ports BP1 and BP2 with the port priority vector. Since the specified priority vector of BP1 is better than the port priority vector, the role of BP1 is the specified port, and it is sent to Switch A regularly. The specified priority vectors for the total root and domain root {A: 0: A: 10: B: BP1: BP2}; because the port priority vector of BP2 is better than the specified priority vector, and the root priority vector is taken from port BP2 Root path priority vector of BP2, the role of BP2 is the root port.

c) Switch C's role selection process.

Switch C's port CP1 receives the message priority vector {B: 0: B: 0: B: BP1: CP1} from Switch B before it is updated, and port CP2 receives the message priority vector {A: 0 from Switch A : A: 0: A: AP1: CP2}, after comparing, the message priority vectors of CP1 and CP2 are better than the port priority vector, so the port priority vectors of CP1 and CP2 are updated to {B: 0: B : 0: B: BP1: CP1} and {A: 0: A: 0: A: AP1: CP2}. Since Switch C is not in the same domain as Switch A and Switch B, the root path priority vector of port CP1 is {B: 5: C: 0: B: BP1: CP1} and the root path priority vector of port CP2 is {A: 4: C: 0: A: AP1: CP2}, the root path priority vector of CP2 is better than the root path priority vector of CP1, then the root priority vector is {A: 4: C: 0: A: AP1: CP2 }. The designated priority vectors of ports CP1 and CP2 are {A: 4: C: 0: C: CP1: CP2} and {A: 4: C: 0: C: CP2: CP2} respectively, and port CP1 is calculated as the designated port , CP2 is calculated as the root port.

After receiving the updated message priority vector {A: 0: A: 10: B: BP1: CP1} from the BP1 port CP1 of the Switch C, after comparing the message priority vector of CP1 is superior to the port priority vector, the port is updated The priority vector is{A: 0: A: 10: B: BP1: CP1}, the calculated root path priority vector of port CP1 is {A: 5: C: 0: B: BP1: CP1}. Because the priority vector of the message received by port CP2 has not changed, according to the previous calculation, the root path priority vector of port CP2 remains {A: 4: C: 0: A: AP1: CP2}, and the root path priority of CP2 The vector is better than the root path priority vector of CP1, then the root priority vector is {A: 4: C: 0: A: AP1: CP2}. The designated priority vectors for ports CP1 and CP2 are {A: 4: C: 0: C: CP1: CP2} and {A: 4: C: 0: C: CP2: CP2}, respectively. The port priority vector of CP1 is better than its specified priority vector, but the root priority vector is not taken from the root path priority vector of port CP1, so the role of CP1 is Alternate port. CP2 is still the root port.

5. Calculation result.

After the roles of devices and ports are determined, the entire tree topology is established.

Figure 7-2 shows the traffic forwarding line after the above calculation.

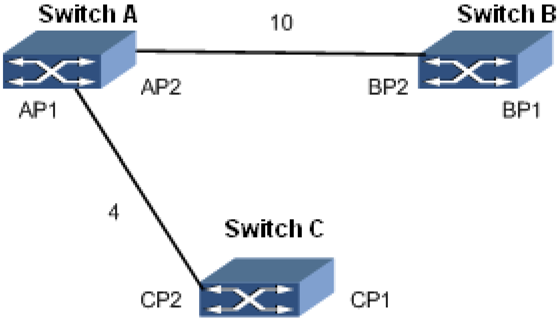


Figure 7-2. Flow forwarding circuit after calculation.

7.2.4 Spanning Tree Configuration

Background Information

As long as the following configurations are the same, the two switches belong to the same domain:

- MST domain name,
- MSTI AND VLAN mapping relationship,
- the revision level of the MST region.

Before configuring the switch to join the specified MST region, you need to complete the configuration of port physical characteristics and port VLAN characteristics.

Purpose

This section describes how to configure the switch to join the MST region.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
To configure the working mode of the switch spanning tree.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **spanning-tree mode** { **stp** | **rstp** | **mstp** } to set the working mode of the switch spanning tree.

	3. End.
To configure MST Region.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **spanning-tree mst configuration**. 3. Execute the command **revision** *range* to set the device MSTP revision level. 4. End.
To configure whether to enable port spanning tree.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **interface GigabitEthernet** *interface-number* to enter the interface configuration view. 3. Execute the command **spanning-tree** to enable or disable the port spanning tree function. 4. End.
To configure the priority of the switch in the specified MSTI.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **spanning-tree priority** *MSTI-Priority* to set the priority of the switch in the specified MSTI. 3. End.
To configure the priority of CIST instance 0.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **interface GigabitEthernet** *interface-number* to enter the interface configuration view. 3. Execute the command **spanning-tree mst 0 port-priority** *priority* to set the priority of CIST instance 0. 4. End.
To configure port priority.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **interface GigabitEthernet** *interface-number* to enter the interface configuration view. 3. Execute the command **spanning-tree port-priority** *port-priority* to set the port priority. Default priority is 128. 4. End.
To delete spanning tree instance.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **spanning-tree mst configuration** to enter the mst configuration view. 3. Execute the command **no instance** *instance-id* to delete spanning tree instances. 4. End.

Attached table:

Parameter	Explanation	Value
interface-number	GE interface.	1 – 28
range	Specify spanning tree revision level.	0 – 65535
MSTI-Priority	Priority.	It is an integer with a value range of 0 to 61440 and a step size of 4096, that is, 16 priority values can be configured, such as 0, 4096, 8192.
priority	Specify the priority of the interface.	0 – 240
port-priority	Instance priority.	The value is an integer, ranging from 0 to 240, with a step size of 16.
instance-id	Specify the spanning tree instance ID.	Integer form, value range 0-15.

7.2.5 Spanning Tree Global Parameter Configuration

Background Information

Before adjusting the MSTP parameters of the switch, you need to complete the following configuration tasks:

- Configure the physical characteristics of the port.
- Configure the VLAN that the port joins.
- Configure the switch to join the specified MST region.

Before configuring the switch to join the specified MST region, you need to complete the configuration of port physical characteristics and port VLAN characteristics.

Purpose

This section describes how to configure MSTP parameters.

In some specific network environments, it is possible to configure the MSTP parameters to achieve the best results.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
To configure spanning tree forwarding delay.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **spanning-tree forward-delay** *forward-delay* to set the spanning tree forwarding delay. 3. End.
To configure the interval between hello messages sent by the	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **spanning-tree hello-time** *hello-interval* to

protocol.	set the interval time for the protocol to send hello messages. 3. End.
To configure the maximum aging time of STP.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **spanning-tree maximum-age** *max-age* to set the maximum aging time of the switch spanning tree. 3. End.
To configure the maximum number of spanning tree hops in the MST region.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **spanning-tree max-hops** *max-hop* to set the maximum hops of the spanning tree in the MST region. 3. End.
To configure whether the interface is in edge mode.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **interface GigabitEthernet** *interface-number* to enter the interface configuration view. 3. Execute the command **spanning-tree edge** to enable interface edge mode. Execute the command **no spanning-tree edge** to disable interface edge mode. 4. End.
To configure whether the interface is point-to-point management.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **interface GigabitEthernet** *interface-number* to enter the interface configuration view. 3. Execute the command **spanning-tree link-type {point-to-point| shared}** to set the interface link type. 4. End.
To configure the priority of the current interface on the specified MSTI.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **interface GigabitEthernet** *interface-number* to enter the interface configuration view. 3. Execute the command **spanning-tree mst** *instance-id* **port-priority** *priority* to set the current interface at the specified priority. 4. End.
To configure the management path cost of the current interface on the specified MSTI (MST instance).	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **interface GigabitEthernet** *interface-number* to enter the interface configuration view. 3. Execute the command **spanning-tree mst** *instance-id* **cost** *path-cost* to set the management path cost of the current interface on the specified MSTI (MST instance).

	4. End.
To configure STP port path cost calculation method.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **spanning-tree pathcost method** { **long** | **short** } to set the calculation method of STP port path cost. 3. End.
To configure the operation of BPDU processing when STP is disabled.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **spanning-tree bpdu {filtering|flooding}** to set the operation of BPUD when STP is disabled. 3. End.
To enable or disable the BPDU filter function.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **interface GigabitEthernet** *interface-number* to enter the interface configuration view. 3. Execute the command **spanning-tree bpdu-filter** to enable BPDU filter function. Execute the command **no spanning-tree bpdu-filter** to disable the BPDU filter function. 4. End.

Attached table:

Parameter	Explanation	Value
forward-delay	Specify the spanning tree forwarding delay.	The value is an integer, the value range is 4 – 30 (seconds).
hello-interval	Specify the spanning tree hello message interval.	The value is an integer, the value range is 1 – 10 (seconds).
max-age	Specify the maximum aging time of the spanning tree.	The value is an integer, the value range is 6 – 40 (seconds).
max-hop	Specify the maximum number of spanning tree hops.	Integer form, the value range is 1 – 40 (jumps).
instance-id	Specify the spanning tree instance ID.	Integer form, the value range is 1 – 15.
priority	Specify the priority of the interface.	Integer form, the value range is 0 – 240, the step is 16.
path-cost	Specified port cost.	Integer form, the value range is 0 – 200000000.
interface-number	Specified GE interface.	Integer form, the value range is 1 – 128.

7.2.6 Maintenance and Commissioning

Purpose

When the MSTP function is not normal and you need to view, debug, or locate the problem, you can use this section to operate.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
To enable debug spanning tree function.	1. Maintain the current privileged user view. 2. Execute the command **deunish env** to enter the debug view. 3. Execute the command **logging dbgmsg** *Spanning Tree-id* to disable spanning tree debugging. 4. End.
To disable debug spanning tree function.	1. Maintain the current privileged user view. 2. Execute the command **deunish env** to enter the debug view. 3. Execute the command **no logging dbgmsg** *Spanning Tree-id* to enable spanning tree debugging. 4. End.
To display switch spanning tree configuration information.	1. Maintain the current privileged user view. 2. Execute the command **show stp** to display switch spanning tree protocol configuration information. 3. End.
To display the STP configuration information of the interface.	1. Maintain the current privileged user view. 2. Execute the command **show spanning-tree interfaces GigabitEthernet** *interface-number* to display the configuration information of the interface spanning tree protocol. 3. End.
To display the specified MSTP instance information.	1. Maintain the current privileged user view. 2. Execute the command **spanning-tree mst** *instance-id* to display MSTP instance information. 3. End.
To display the global MST configuration of the switch.	1. Maintain the current privileged user view. 2. Execute the command **show spanning-tree mst configuration** to display the global MST configuration of the switch. 3. End.
To display MSTP instance information on the interface.	1. Maintain the current privileged user view. 2. Execute the command **show spanning-tree mst** *instance-id* **interfaces GigabitEthernet** *interface-number*. 3. End.

Attached table:

Parameter	Explanation	Value
Spanning Tree-id	Specify the sequence number of the spanning tree in debug view.	The value is an integer.
interface-number	Specify the Ethernet interface number as the observation port.	Integer form, GE interface value range is 1 – 28.
instance-id	Specify the spanning tree instance ID.	Integer form, the value range is 1 – 15.

7.2.7 Configuration Example

Network Requirements

There are currently four switches that support the MSTP protocol, namely SwitchA, SwitchB, SwitchC, and SwitchD. Connect according to the following networking diagram and configure basic MSTP functions:

- SwitchA and SwitchC are in the same domain, the domain name is Domain1 and instance 1 is created.
- SwitchB and SwitchD are divided into another domain, the domain name is Domain2 and instance 1 is created.
- SwitchA is the CIST root.
- In Domain1, SwitchA is the root of the CIST domain and the root of instance 1. And configure the root protection function on the ge1 / 0/1 and ge1 / 0/2 ports of SwitchA.
- In Domain 2, SwitchB is the root of the CIST domain, and SwitchD is the root of the instance 1.
- The ge1 / 0/1 ports of SwitchC and SwitchD are configured as edge ports, and BPDU protection is applied at the same time.

Network Diagram

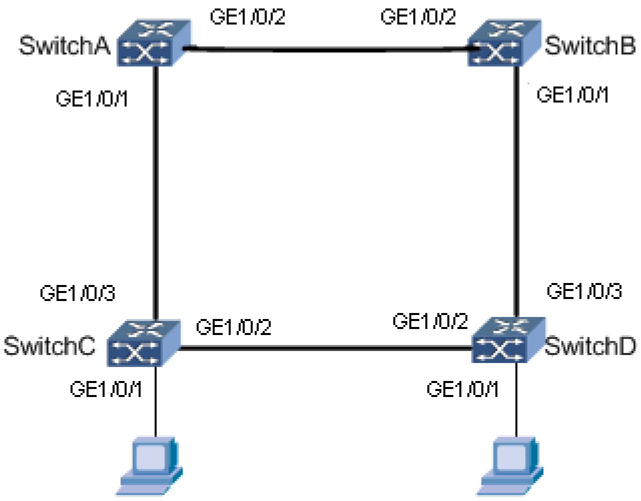


Figure 7-3. MSTP networking diagram.

Example

1. Configuration SwitchA.

#Configure SwitchA to join domain Domain1.

```
Switch(config)# spanning-tree
Switch(config)# spanning-tree mode mstp
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# name Domain1
Switch(config-mst)# revision 1
```

# Set the priority of SwitchA in instance 0 to 0 to ensure that SwitchA serves as the total root of CIST.

```
Switch(config)# spanning-tree priority 0
```

# Set the priority of SwitchA in instance 1 to 0 to ensure that SwitchA serves as the domain root of instance 1.

```
Switch(config)#spanning-tree mst 1 priority 0
```

# Create VLANs 2 to 20, and add the ports ge1 / 0/1 and ge1 / 0/2 of SwitchA to 1 to 20 respectively, enable port spanning tree function, and enable port root protection.

```
Switch(config)# vlan 2-20
Switch(config-vlan)# exit
Switch(config)# interface GigabitEthernet 1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 2-20
Switch(config-if)# spanning-tree
Switch(config-vlan)# exit
Switch(config)# interface GigabitEthernet 2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 2-20
Switch(config-if)# spanning-tree
```

2. Configuration SwitchB.

# Configure SwitchB to join domain
Domain2..

```
Switch(config)# spanning-tree
Switch(config)# spanning-tree mode mstp
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# name Domain2
Switch(config-mst)# revision 2
```

# Set the priority of SwitchB in instance 0 to 4096 to ensure that SwitchB serves as the root of CIST.

```
Switch(config)# spanning-tree priority 4096
```

# Create VLANs 2 to 20, and add the ports ge1 / 0/1 and ge1 / 0/2 of SwitchB to 1 to 20 respectively, enable port spanning tree function, and enable port root protection.

```
Switch(config)# vlan 2-20
Switch(config-vlan)# exit
Switch(config)# interface GigabitEthernet 1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 2-20
Switch(config-if)# spanning-tree
Switch(config-vlan)# exit
Switch(config)# interface GigabitEthernet 2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 2-20
Switch(config-if)# spanning-tree
```

3. Configuratio SwitchC.

# Configure SwitchC to join domain Domain1.

```
Switch(config)# spanning-tree
Switch(config)# spanning-tree mode mstp
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# name Domain1
Switch(config-mst)# revision 1
```

# Start the BPDU protection function.

```
Switch(config)#spanning-tree bpdu-guard
```

# Create VLANs 2 to 20, add ports ge1 / 0/2 and ge1 / 0/3 of SwitchC to 1 to 20 respectively, enable port spanning tree, and configure port ge1 / 0/1 as an edge port.

```
Switch(config)# vlan 2-20
Switch(config-vlan)# exit
Switch(config)# interface GigabitEthernet 2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 2-20
Switch(config-if)# spanning-tree
Switch(config-vlan)# exit
Switch(config)# interface GigabitEthernet 3
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 2-20
Switch(config-if)# spanning-tree
Switch(config-vlan)# exit
Switch(config)# interface GigabitEthernet 1
Switch(config-if)# switchport mode hybrid
Switch(config-if)# switchport hybrid pvid 20
Switch(config-if)# switchport hybrid allowed vlan add 20 untagged
```

4. Configuration SwitchD.

# Configure SwitchD to join domain
Domain2.

```
Switch(config)# spanning-tree
Switch(config)# spanning-tree mode mstp
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# name Domain2
Switch(config-mst)# revision 2
```

# Set the priority of SwitchD in instance 1 to 0 to ensure that SwitchD serves as the domain root of instance 1.

```
Switch(config)#spanning-tree mst 1 priority 0
```

# Start the BPDU protection function.

```
Switch(config)#spanning-tree bpdu-guard
```

# Create VLANs 2 to 20, add ports ge1 / 0/2 and ge1 / 0/3 of SwitchD to 1 to 20 respectively, enable port spanning tree, and configure port ge1 / 0/1 as an edge port.

```
Switch(config)# vlan 2-20
Switch(config-vlan)# exit
Switch(config)# interface GigabitEthernet 2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 2-20
Switch(config-if)# spanning-tree
Switch(config-vlan)# exit
Switch(config)# interface GigabitEthernet 3
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 2-20
Switch(config-if)# spanning-tree
Switch(config-vlan)# exit
Switch(config)# interface GigabitEthernet 1
Switch(config-if)# switchport mode hybrid
Switch(config-if)# switchport hybrid pvid 20
Switch(config-if)# switchport hybrid allowed vlan add 20 untagged
```

8. PoE Configuration

8.1 Overview

PoE is called Power Over Ethernet, which refers to power supply through 10BASE-T, 100BASE-TX, and 1000BASE-T Ethernet networks, and its reliable power supply distance is up to 100 meters. In this way, it can effectively solve the centralized power supply of terminals such as IP phones, wireless APs, portable device chargers, card readers, cameras, and data collection. For these terminals, it is no longer necessary to consider the wiring of their indoor power system, and they can achieve power supply to the device while accessing the network. In terms of versatility, the current PoE power supply also has a unified standard. As long as it follows the published 802.3af or 802.3at standard, the problem of adaptability between devices of different manufacturers can be solved.

This chapter mainly introduces the PoE related configuration of the switch, including the introduction of PoE function, configuration methods and steps. This chapter includes the following topics:

8.2 PoE Function Configuration

8.2.1 Turn PoE Power on or off

Purpose

Users can enable or disable the remote power supply function of the device port according to the needs of the network, so as to use the twisted pair of the device Ethernet port to remotely power or stop the power supply to the external PD (Powered Device) to connect In-side applications provide more possibilities.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process	Parameter Description
To enable the power supply function of the device's Ethernet interface.	1. Execute the command **configure** to enter the global view. 2. Execute the command **interface GigabitEthernet** *interface-number* to enter the configuration mode. 3. Execute the command **poe enable**. 4. End.	*interface-number*: The specified GE interface number ranges from 1 – 28.
To disable the power supply function of the device's Ethernet interface.	1. Execute the command **configure** to enter the global view. 2. Execute the command **interface GigabitEthernet** *interface-number* to enter the configuration mode.	

	3. Execute the command **no poe enable**.	

8.2.2 Configure PoE Power Supply Parameters

Background Information

At present, the switch only supports the signal line power supply mode, the timing power supply function, and the power supply alarm function.

Configure the description information of the powered device connected to the interface on the device to facilitate users to manage downstream PD devices.

A PD device conforming to the 802.af protocol standard is a standard PD device. Normally, the PSE can only detect the standard PD and supply power to it. After the PSE detects the non-standard PD function, the PSE can detect the non-standard PDE and supply power to it.

The PoE power supply port supports three priorities. Interface priority is a means to ensure that key devices can provide priority power when the power consumed by PD devices is greater than the total power that PSE can provide. When the power supply of the PSE device is insufficient, if different interfaces have the same priority, the priority is sorted according to the interface number, and the interface with the larger interface number is given priority to be guaranteed by the power supply.

Configure the threshold power of the PSE device in the global configuration mode. This configuration command is set to protect the PD from being unstable due to the power supply from the switch.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process	Parameter Description
(Optional.) To set the current maximum rated power supply of the device interface.	1. Execute the command **configure** to enter the global view. 2. Execute the command **interface GigabitEthernet** *interface-number* to enter the configuration mode. 3. Execute the command **poe max_power** *power-value* to set the current maximum rated power supply of the interface. 4. End.	*interface-number*: The specified interface number ranges from 1 – 24. *power-value*: the maximum power allocated by the specified port, in integer, ranging from 1 – 32 (watts).
(Optional.) To set the priority of the device interface power supply.	1. Execute the command **configure** to enter the global view. 2. Execute the command **interface GigabitEthernet** *interface-number* to enter the configuration mode. 3. Execute the command **poe priority** {critical|high|low } to set the priority of the interface power supply.	

8.2.3 View PoE Configuration Information

Purpose

After the user configures the PoE function and related parameters, if you need to check whether the configuration is correct, you can use the operations described in this section to view related information.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
To display this exchange Machine Poe Information.	1. Maintain the current privileged user view without executing any commands. 2. Execute the command **show poe powersupply**. 3. End.
To display the poe status information of the interface.	1. Maintain the current privileged user view without executing any commands. 2. Execute the command **show poe interface status**. 3. End.

8.2.4 Debugging PoE Information

Purpose

When the PoE function is abnormal and you need to view, debug, or locate the problem, you can use this section to operate.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
To enable debug PoE.	1. Maintain the current privileged user view without executing any commands. 2. Execute the command **deunish env** to enter the debug view. 3. Execute the command **logging dbgmsg** *poe-id* to enable the debug PoE function. 4. End.
To disable debug PoE.	1. Maintain the current privileged user view without executing any commands. 2. Execute the command **deunish env** to enter the debug view. 3. Execute the command **no logging dbgmsg** *poe-id* to disable the debug PoE function. 4. End.

Attached table:

Parameter	Explanation	Value
poe-id	Sequence number of poe in debug view.	0 – 200.

9. Multicast Constraint Mechanism Configuration

9.1 IGMP Snooping Configuration

9.1.1 IGMP Snooping Overview

IGMP Snooping is the abbreviation of Internet Group Management Protocol Snooping. It is a mechanism of multicast constraints running on Layer 2 devices and is used to manage and control multicast groups.

IGMP snooping is to listen to IGMP packets, extract the corresponding information, form a multicast membership table, and then forward the multicast service according to the group membership to ensure that the group members receive the correct multicast service, while the rest hosts cannot receive it.

9.1.2 IGMP Snooping Function Configuration

Purpose

Use the operations in this section to ensure that the group members receive the correct multicast service, while the remaining hosts cannot receive.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
To enable or disable IGMP Snooping.	1. Execute the command **configure** to enter the configuration view. 2. Execute the command **ip igmp snooping** to enable IGMP Snooping. Execute the command **no ip igmp snooping** to disable IGMP Snooping. 3. End.
To enable or disable IGMP Snooping report-suppression function.	1. Execute the command **configure** to enter the configuration view. 2. Execute the command **ip igmp snooping report-suppression** to enable IGMP Snooping report-suppression function. Execute the command **no igmp snooping report-suppression** to disable Snooping report-suppression function. 3. End.
To change IGMP version.	1. Execute the command **configure** to enter the configuration view. 2. Execute the command **ip igmp snooping version** {2|3}. 3. End.
To enable or disable IGMP Snooping vlan	1. Execute the command **configure** to enter the configuration view. 2. Execute the command **ip igmp snooping vlan** *vlan-id* to enable IGMP Snooping vlan function. Execute the command **no ip igmp snooping**

function.	**vlan** *vlan-id* to disable IGMP Snooping vlan function. 3. End.
To change the number of query packets to be sent.	1. Execute the command **configure** to enter the configuration view. 2. Execute the command **ip igmp snooping vlan** *vlan-id* **last-member-query-count** *number*. 3. End.
To change query interval.	1. Execute the command **configure** to enter the configuration view. 2. Execute the command **ip igmp snooping vlan** *vlan-id* **last-member-query-interval** *interval-number*. 3. End.
To configure the routing learning function of the enabled port.	1. Execute the command **configure** to enter the configuration view. 2. Execute the command **ip igmp snooping vlan** *vlan-id* **router learn pim-dvmrp**. 3. End.
To configure the port as a static port.	1. Execute the command **configure** to enter the configuration view. 2. Execute the command **ip igmp snooping vlan** *vlan-id* **static-port {GigabitEthernet|LAG}** *interface-number*. 3. End.
To disable the use of this interface as an uplink routing port.	1. Execute the command **configure** to enter the configuration view. 2. Execute the command **ip igmp snooping vlan** *vlan-id* **forbidden-router-port {GigabitEthernet|LAG}** *interface-number*. 3. End.
To set the port as a static routing port.	1. Execute the command **configure** to enter the configuration view. 2. Execute the command **ip igmp snooping vlan** *vlan-id* **static-router-port {GigabitEthernet|LAG}** *interface-number*. 3. End.
To add or delete VLAN static group.	1. Execute the command **configure** to enter the configuration view. 2. Execute the command **ip igmp snooping vlan** *vlan-id* **static-group** *multicast-address* **interfaces{GigabitEthernet|LAG}** *interface-number* to delete command. 3. End.
To delete static or dynamic groups of VLAN.	1. Execute the command **configure** to enter the configuration view. 2. Execute the command **no ip igmp snooping vlan** *vlan-id* **group** *multicast-address*. 3. End.
To enter IGMP configuration view.	1. Execute the command **configure** to enter the configuration view. 2. Execute the command **ip igmp profile** *Profile-id* to enter the specified view.

	3. End.
To set multicast address range.	1. Execute the command **configure** to enter the configuration view. 2. Execute the command **ip igmp profile** *Profile-id* to enter the specified view. 3. Execute the command **profile range ip** *start-address end-address* **action** {permit|deny }. 4. End.
To bind IGMP entries on the interface.	1. Execute the command **configure** to enter the configuration view. 2. Execute the command **interface {GigabitEthernet|LAG}** *interface-number* to enter the interface configuration view. 3. Execute the command **ip igmp filter** *profile-ID*. 4. End.
To remove the IGMP entry on the interface.	1. Execute the command **configure** to enter the configuration view. 2. Execute the command **interface {GigabitEthernet|LAG}** *interface-number* to enter the interface configuration view. 3. Execute the command **no ip igmp filter**. 4. End.
To set the maximum number of groups for port learning.	1. Execute the command **configure** to enter the configuration view. 2. Execute the command **interface {GigabitEthernet|LAG}** *interface-number* to enter the interface configuration view. 3. Execute the command **ip igmp max-groups** *group-number*. 4. End.
To set the action when the number of groups reaches the limit.	1. Execute the command **configure** to enter the configuration view. 2. Execute the command **interface {GigabitEthernet|LAG}** *interface-number* to enter the interface configuration view. 3. Execute the command **ip igmp max-groups action {replace|deny}**. 4. End.

Attached table:

Parameter	Explanation	Value
{2|3}	“2” specifies IGMP version 2; “3” specifies IGMP version 3.	-
vlan-id	Specify VLAN number.	1 – 4094
number	Specify the number of packages.	1 – 7
interval-number	The specified query interval.	1 – 25
response-time	Specified response time.	5 – 20

interface-number	The specified interface number.	*interface-number*: The value is an integer. The value range of the GE interface is 1 – 28; the value range of the LAG interface is 1 – 8.
multicast-address	Specified multicast address.	224.0.0.0 – 239.255.255.255
Profile-id	Specified multicast group number.	1 – 128
start-address	The specified multicast start address.	224.0.0.0 – 239.255.255.255
end-address	The specified multicast end address.	224.0.0.0 – 239.255.255.255
group-number	The specified maximum group number.	0 – 256

9.1.3 Debugging IGMP Snooping Information

Purpose

When the IGMP Snooping function is abnormal and you need to view, debug, or locate the problem, you can use this section to operate.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
To clear IGMP group dynamic, static or all types.	1. Keep current in privileged view. 2. Execute the command **clear ip igmp snooping groups** or **clear ip igmp snooping groups dynamic**, or **clear ip igmp snooping groups static**.
To clear IGMP statistics.	1. Keep current in privileged view. 2. Execute the command **clear ip igmp snooping groups** or **clear ip igmp snooping groups dynamic**, or **clear ip igmp snooping groups static**.
To display IGMP group number information.	1. Keep current in privileged view. 2. Execute the command **show ip igmp snooping groups counters**. 3. End.
To display information about all IGMP groups.	1. Keep current in privileged view. 2. Execute the command **show ip igmp snooping groups**. 3. End.
To display IGMP routing information.	1. Keep current in privileged view. 2. Execute the command **show ip igmp snooping router**.

To display static VLAN IGMP query information.	1. Keep current in privileged view. 2. Execute the command **show ip igmp snooping querier**.
To display the global information of IGMP Snooping.	1. Keep current in privileged view. 2. Execute the command **show ip igmp snooping**. 3. End.
To display IGMP related information in VLAN.	1. Keep current in privileged view. 2. Execute the command **show ip igmp snooping vlan**. 3. End.
To display multicast group configuration information.	1. Keep current in privileged view. 2. Execute the command **show ip igmp profile**. 3. End.
To enable IGMP Snooping debugging function.	1. Keep current in privileged view. 2. Execute the command **deunish env** to enter debug mode. 3. Execute the command **logging dbgmsg** *id* to enable debugging function.
To disable IGMP Snooping debugging function.	1. Keep current in privileged view. 2. Execute the command **deunish env** to enter debug mode. 3. Execute the command **no logging dbgmsg** *id* to disable debugging function.

Attached table:

Parameter	Explanation	Value
id	Sequence number of IGMP Snooping in the debug view.	0 – 200

9.2 MLD Snooping Configuration

9.2.1 MLD Snooping Overview

MLD Snooping is the abbreviation of Multicast Listener Discovery Snooping. It is an IPv6 multicast constraint mechanism that runs on Layer 2 devices and is used to manage and control IPv6 multicast groups.

By analyzing the received MLD messages, the layer 2 device running MLD snooping establishes a mapping relationship between the port and MAC multicast address, and forwards IPv6 multicast data according to the mapping relationship.

MLD Snooping forwards information only to receivers in need through Layer 2 multicast, which can bring the following benefits:

- It reduces the broadcast message in the two-layer network and saves the network bandwidth.
- The security of IPv6 Multicast information is enhanced.
- It is convenient for each host to be charged separately.

9.2.2 MLD Snooping Function Configuration

Purpose

Set the MLD snooping related configuration through the operation in this section.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process	Parameter Description
To enable or disable MLD Snooping.	1. Execute the command **config** to enter the global configuration view. 2. Execute the command **ipv6 mld snooping** to enable MLD Snooping. Execute the command **no ipv6 mld snooping** to disable MLD Snooping. 3. End.	-
To enable or disable MLD Snooping report compression.	1. Execute the command **config** to enter the global configuration view. 2. Execute **ipv6 mld snooping report-suppression** to enable the command. Execute **no ipv6 mld snooping report-suppression** to disable the command. 3. End.	-
To configure IPV6 MLD version.	1. Execute the command **config** to enter the global configuration view. 2. Execute the command **ipv6 mld snooping version** {1|2}.	"1" means version 1; "2" means version 2.
To configure the operation to receive unknown multicast packets.	1. Execute the command **config** to enter the global configuration view. 2. Execute the command **ipv6 mld snooping unknown-multicast action {router-port| drop | flood}**. 3. End.	-
To configure MLD Snooping in VLAN.	1. Execute the command **config** to enter the global configuration view. 2. Execute **ipv6 mld snooping vlan** *vlan-id* to enable the command. Execute **no ipv6 mld snooping vlan** *vlan-id* to disable the command.	*vlan-id*: Specified vlan id number, the value range is 1 – 4094.
To configure the number of queries to be sent when receiving out-of-group reports.	1. Execute the command **config** to enter the global configuration view. 2. Execute the command **ipv6 mld snooping vlan** *vlan-id* **last-member-query-count** *number*.	*vlan-id*: Specified vlan id number, value range is 1 – 4094. *number*: The value range is 1 – 7.

To configure the interval between query packets.	1. Execute the command **config** to enter the global configuration view. 2. Execute the command **ipv6 mld snooping vlan** *vlan-id* **last-member-query-interval** *interval-number*.	*interval-number*: Specify the number of intervals, ranging from 1 – 25.
To configure VLAN response time.	1. Execute the command **config** to enter the global configuration view. 2. Execute the command **ipv6 mld snooping vlan** *vlan-id* **response-time** *time*.	*time*: Specified response time, the value range is 5 – 20.
To enable route learning function.	1. Execute the command **config** to enter the global configuration view. 2. Execute the command **ipv6 mld snooping vlan** *vlan-id* router learn pim-dvmrp.	-
To add or remove static ports.	1. Execute the command **config** to enter the global configuration view. 2. Execute **ipv6 mld snooping vlan** *vlan-id* **static-port {GigabitEthernet|LAG}** *interface-number* to enable the command. Execute **no ipv6 mld snooping vlan** *vlan-id* **static-port {GigabitEthernet|LAG}** *interface-number* to disable the command.	*interface-number*: The specified interface number, the GE interface number ranges from 1 – 28; the LAG interface number ranges from 1 – 8.
To add or remove static groups.	1. Execute the command **config** to enter the global configuration view. 2. Execute **ipv6 mld snooping vlan** *vlan-id* **static-group multicast-address interfaces {LAG| GigabitEthernet}** *interface-number* to enable the command. Execute **no ipv6 mld snooping vlan** *vlan-id* **group multicast-address** to disable the command.	*multicast-address*: Specified IPV6 multicast address.
To create IPVL Multicast Group.	1. Execute the command **config** to enter the global configuration view. 2. Execute the command **ipv6 mld profile** *Profile-id* to enter the specified view. 3. End.	*Profile-id*: Specified multicast group id, the value range is 1 – 128.
To set the multicast address range.	1. Execute the command **config** to enter the global configuration view. 2. Execute the command **ipv6 mld profile** *Profile-id* to enter the specified view. 3. Execute the command **profile range ipv6** *start-address end-address* **action {permit| deny }**. 4. End.	*start-address*: The specified IPV6 start address; the end-address specified IPV6 end address.

The corresponding action when the configuration reaches the maximum value.	1. Execute the command **config** to enter the global configuration view. 2. Execute the command **interface {LAG| GigabitEthernet}** *interface-number* to enter the interface configuration view. 3. Execute the command **ipv6 mld max-groups action {deny|replace}**.	-
To clear IPv6 multicast group.	1. Execute the command **config** to enter the global configuration view. 2. Execute the command **clear ipv6 mld snooping groups [dynamic|static]***.	-
To configure the maximum number of groups for port learning.	1. Execute the command **config** to enter the global configuration view. 2. Execute the command **interface {LAG| GigabitEthernet}** *interface-number* to enter the interface configuration view. 3. Execute the command **ipv6 mld max-groups** *max-number*.	*max-number*: The specified maximum value, the value range is 0 – 256.

Attached table:

Parameter	Explanation	Value
vlan-id	Specify VLAN number.	1 – 4094
interface-number	Specify interface number.	The value is an integer. The value range of the GE interface is 1 – 28; the value range of the LAG interface is 1 – 8.

9.2.3 Debugging IGMP Snooping Information

Purpose

When the MLD Snooping function is abnormal and you need to view, debug, or locate the problem, you can use this section to operate.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
To clear IPv6 multicast group.	1. Keep current in privileged view. 2. Execute the command **clear ipv6 mld snooping groups [dynamic|static]***.
To clear MLD Snooping statistics.	1. Keep current in privileged view. 2. Execute the command **clear ipv6 mld snooping statistics**.
To display IPv6 MLD multicast group	1. Keep current in privileged view.

configuration information.	2. Execute the command **show ipv6 mld profile**.
To display port filtering configuration.	1. Keep current in privileged view. 2. Execute the command **show ipv6 mld filter**.
To display the maximum number of learnings supported by the port.	1. Keep current in privileged view. 2. Execute the command **show ipv6 mld max-group action**.
To check the action configuration of the port learning excess.	1. Keep current in privileged view. 2. Execute the command **show ipv6 mld max-group action**.
To enable MLD Snooping debugging function.	1. Keep current in privileged view. 2. Execute the command **deunish env** to enter debug mode. 3. Execute the command **logging dbgmsg** *id* to enable debugging function.
To disable MLD Snooping debugging function.	1. Keep current in privileged view. 2. Execute the command **deunish env** to enter debug mode. 3. Execute the command **no logging dbgmsg** *id* to disable debugging function.
To display all multicast group information.	1. Keep current in privileged view. 2. Execute the command **show ipv6 mld snooping groups**.
To display MLD routing information.	1. Keep current in privileged view. 2. Execute the command **show ipv6 mld snooping router**.
To display MLD Snooping global information.	1. Keep current in privileged view. 2. Execute the command **show ipv6 mld snooping**.
To display MLD Snooping information in VLAN.	1. Keep current in privileged view. 2. Execute the command **show ipv6 mld snooping vlan**.

Attached table:

Parameter	Explanation	Value
id	Sequence number of MLD Snooping in the debug view.	0 – 200

10. LLDP Configuration

10.1 Overview

LLDP (Link Layer Discovery Protocol) is a link layer protocol defined in 802.1ab. It organizes the information of the local device into TLV (Type / Length / Value, type / length / value) and encapsulates it in LLDPDU (Link Layer Discovery Protocol Data Unit is sent to directly connected neighbors, and LLDPDU received from neighbors are also stored in the form of standard MIB (Management Information Base). Through LLDP, the device can save and manage the information of itself and directly connected neighbors for the network management system to query and judge the communication status of the link. LLDP does not configure or control network elements or traffic, it just reports the configuration of the second layer. Another content in 802.1ab is to make the network management software use the information provided by LLDP to discover some contradictions of the second layer.

10.2 LLDP Related Operation Configuration

Purpose

Use the operations in this section to ensure that the group members receive the correct multicast service, while the remaining hosts cannot receive.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process	Parameter Description
To enable or disable LLDP function.	1. Execute the command **config** to enter the global configuration view. 2. Execute the command **lldp** to enable LLDP. Execute the command **no lldp** to disable LLDP. 3. End.	-
To configure the LLDP receive and transmit function on the interface.	1. Execute the command **config** to enter the global configuration view. 2. Execute the command **interface {GigabitEthernet|LAG}** *interface-number* to enter the configuration mode. 3. Execute **lldp {rx|tx}** to enable the command. Execute **no lldp {rx|tx}** to disable the command. 4. End.	**{rx|tx}**: rx : Receive; tx: transmission.
To configure the transmission interval for	1. Execute the command **config** to enter the global configuration view.	*rate*: The value range is 5 – 32767.

sending LLDP packets.	2. Execute the command **lldp tx-interval** *rate*. 3. End.	
To configure LLDP retry delay time.	1. Execute the command **config** to enter the global configuration view. 2. Execute the command **lldp reinit-delay** *reinit-delay*. 3. End.	*reinit-delay*: The value range is 1 – 10.
To configure LLDP neighbor device aging time.	1. Execute the command **config** to enter the global configuration view. 2. Execute the command **lldp holdtime-multiplier** *multiplier-value*. 3. End.	*multiplier-value*: The value range is 2 – 10.
To configure LLDP BDPU forwarding processing method.	1. Execute the command **config** to enter the global configuration view. 2. Execute the command **lldp lldpdu { bridging|filtering|flooding}**. 3. End.	-
To enable or disable LLDP med function.	1. Execute the command **config** to enter the global configuration view. 2. Execute the command **interface {GigabitEthernet|LAG}** *interface-number* to enter the configuration mode. 3. Execute the command **lldp med** to enable lldp med function. Execute the command **no lldp med** to disable lldp med function. 4. End.	-
To set quick start repeat count value.	1. Execute the command **config** to enter the global configuration view. 2. Execute the command **lldp med fast-start-repeat-count** *number*. 3. End.	*number*: The value range is 1 – 10.
To configure LLDP network policy table.	1. Execute the command **config** to enter the global configuration view. 2. Execute the command **lldp med network-policy** *policy-id* **app** *type* **vlan** *vlan-id* **vlan-type** *{tag|untag}* **priority** *priority* **dscp** *dscp-number*. 3. End.	*policy-id*: Refers to the policy ID value (1 – 32); *vlan-id*: specified VLAN number value (1 – 4095); *priority*: Refers to the priority value (0 – 7); *dscp*: number value (0 – 63).
To enable or disable tlv-	1. Execute the command **config** to enter the global configuration view.	-

select pvid on the interface.	2. Execute the command **lldp tlv-select pvid { disable| enable }**. 3. End.	
To add or remove VLAN ID on the interface.	1. Execute the command **config** to enter the global configuration view. 2. Execute the command **interface {GigabitEthernet|LAG}** *interface-number* to enter the configuration mode. 3. Execute the command **lldp tlv-select vlan-name {add|remove}** *vlan-id*.	*interface-number*: Integer form, the value range of GE interface is 1 – 28; *vlan-id*: specified VLAN number value (1 – 4095).
To configure LLDP PDU TX delay time.	1. Execute the command **config** to enter the global configuration view. 2. Execute the command **ldp tx-delay** *delay-time*. 3. End.	*delay-time*: Refers to the delay time value range 1 – 8191.

10.3 Debug LLDP Information

Purpose

When the LLDP function is not normal and you need to view, debug, or locate the problem, you can use this section to operate.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process	Parameter Description
To display LLDP global information.	1. Keep current in privileged view. 2. Execute the command **show lldp**. 3. End.	-
To display local configuration of LLDP PDU.	1. Keep current in privileged view. 2. Execute the command **show lldp local-device**. 3. End.	-
To display LLDP MED configuration information.	1. Keep current in privileged view. 2. Execute the command **show lldp med**. 3. End.	-
To display the received neighbor LLDP PDU information.	1. Keep current in privileged view. 2. Execute the command **show lldp neighbor**. 3. End.	-
To display LLDP RX / TX statistics.	1. Keep current in privileged view. 2. Execute the command **show lldp statistics**.	-

	3. End.	
To display the reload status of LLDP TLVs ports.	1. Keep current in privileged view. 2. Execute the command **show lldp interfaces GigabitEthernet** *interface-number* **tlvs-overloading**. 3. End.	*interface-number*: Integer form, the value range of GE interface is 1 – 28.
To enable LLDP debugging.	1. Keep current in privileged view. 2. Execute the command **deunish env** to enter debug mode. 3. Execute the command **logging dbgmsg** *id* to enable debugging function.	*id*: Refers to the serial number of LLDP in the debug view, ranging from 0 to 200.
To disable LLDP debugging.	1. Keep current in privileged view. 2. Execute the command **deunish env** to enter debug mode. 3. Execute the command **no logging dbgmsg** *id* to disable debugging function.	

11. UDLD Configuration

11.1 Overview

UDLD (Unidirectional Link Detection): It is a Cisco proprietary Layer 2 protocol used to monitor the physical configuration of Ethernet links connected by optical fiber or twisted pair. When a unidirectional link appears (only one direction can be used). Transmission, for example, I can send the data to you, you can also receive, but you can not receive the data sent to me), UDLD can detect this situation, close the corresponding interface and send a warning message. Unidirectional links may cause many problems, especially spanning tree, which may cause loop back. Note: UDLD needs to be supported by devices at both ends of the link to function properly.

11.2 UDLD Related Operation Configuration

Purpose

Use the operations in this section to set the UDLD related configuration.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process	Parameter Description
To enable or disable one-way link check auto recovery.	1. Execute the command **config** to enter the global configuration view. 2. Execute the command **errdisable recovery cause udld** to enable one-way link check auto recovery. Execute the command **no errdisable recovery cause udld** to disable one-way link check auto recovery.	-
To enable or disable unidirectional link detection on the port.	1. Execute the command **config** to enter the global configuration view. 2. Execute the command **interface GigabitEthernet** *interface-number* to enter the configuration mode. 3. Execute **udld** to enable the command. Execute **no udld** to disable the command.	*interface-number*: Integer form, the value range of GE interface is 1 – 28.
To enable or disable UDLD radical mode on port.	1. Execute the command **config** to enter the global configuration view. 2. Execute the command **interface GigabitEthernet** *interface-number* to enter the configuration mode.	-

	3. Execute **udld aggressive** to enable the command. Execute **no udld aggressive** to disable the command.	
To configure the interval between sending link detection information.	1. Execute the command **config** to enter the global configuration view. 2. Execute the command **udld message time** *message-rate*.	*message-rate*: Specify the value range of visual interval time (1 – 90).
To reset UDLD disable port.	1. Keep the current privileged view. 2. Execute the command **udld reset**.	-

11.3 Debug UDLD Information

Purpose

When the UDLD function is not normal, you need to view, debug or locate the problem, you can use this section to operate.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process	Parameter Description
To display the UDLD management and operation status of the port.	1. Keep the current privileged view. 2. Execute the command **show udld**. 3. End.	-
To enable UDLD debugging function.	1. Keep the current privileged view. 2. Execute the command **deunish env** to enter the debug mode. 3. Execute the command **logging dbgmsg** *id* to enable debugging function.	*id*: Refers to the serial number of the UDLD in the debug mode, and the value range is 0 – 200.
To enable UDLD debugging function.	1. Keep the current privileged view. 2. Execute the command **deunish env** to enter the debug mode. 3. Execute the command **no logging dbgmsg** *id* to disable debugging function.	

12. Operation and Maintenance Management Configuration

12.1 Overview

This chapter introduces the switch operation and maintenance management configuration, including SNMP and RMON configuration. This chapter includes the following topics:

12.2 SNMP Configuration

12.2.1 SNMP Overview

Protocol Introduction

SNMP (Simple Network Management Protocol, Simple Network Management Protocol) is currently the most widely used network management protocol in the network, and it is also an industry standard that is widely accepted and put into use. It is used to ensure that management information is transmitted between any two points and is convenient for the network. Administrators retrieve information, modify information, find faults, complete fault diagnosis, perform capacity planning, and generate reports at any node on the network. SNMP uses a polling mechanism and provides only the most basic feature set, which is particularly suitable for use in small, fast, and low-cost environments. The realization of SNMP is based on the connection less transport layer protocol UDP, which is supported by many products.

SNMP is divided into NMS and Agent. NMS (Network Management Station) is a workstation that runs client programs. Currently commonly used network management platforms are **Sun Netanager** and **IBM NetView**; Agent is server-side software that runs on network devices. The NMS can send **GetRequest**, **GetNextRequest**, and **SetRequest** messages to the Agent. After receiving the NMS request message, the Agent performs Read or Write operation according to the message type, generates a Response message, and returns the message to the NMS. The Agent will also actively send a Trap message to the NMS when the device restarts and other abnormal conditions, and report the event to the NMS.

Supported SNMP Version and MIB

In order to uniquely identify management variables in the device in SNMP messages, SNMP uses a hierarchical naming scheme to identify management objects. The collection of management objects named with a hierarchical structure is like a tree, and the nodes of the tree represent the management objects, as shown in the following figure. Management objects can be uniquely identified by a path starting from the root.

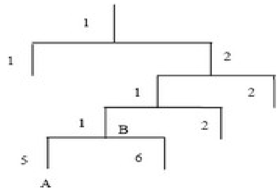


Figure 11-1. MIB tree structure.

The role of MIB (Management Information Base) is to describe the hierarchical structure of the tree. It is a collection of standard variable definitions of monitored network devices. In the above figure, the management object B can be uniquely determined by a string of numbers {1.2.1.1}, which is the Object Identifier of the management object.

The SNMP Agent in the Layer 2 switch supports SNMP V1, V2, and V3. The common MIBs supported are shown in the following table.

Table 11-1. Switches support common MIB.

MIB Attributes	MIB Content
Public MIB	MIB II based on TCP / IP network equipment
	RMON MIB
	Ethernet MIB
	IF MIB
Private MIB	DHCP MIB
	QACL MIB
	ADBM MIB
	RSTP MIB
	VLAN MIB
	Equipment management
	Interface management

12.2.2 Configure Basic SNMP Functions

Purpose

The user configures basic SNMP functions through the operations in this section.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
To configure the community name of SNMP.	1.Execute the command **configure** to enter the global configuration view. 2. Execute the command **snmp community** *name view view-name* { **ro** | **rw** } to set the SNMP community name. 3. End.
To enable or disable SNMP function.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **snmp** to enable the function. Execute the command **no snmp** to disable the function. 3. End.

To configure SNMP view.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **snmp view** *view-name* **subtree OID oid-mask** *{all*|subtreemask*}* **Viewtype** { **included** | **excluded** } to create SNMP view. 3. End.
To configure SNMP group information.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **snmp group** *group-name* **version {1|2c|3} noauth read-view** *read-view* **[write-view** *write-view*| **notify-view** *notify-view*]* to configure SNMP groups. 3. End.
To create SNMP user.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **snmp user** *user-name group-name* to create user information. 3. End.
To configure SNMP retries.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **snmp host** *server-address* **informs version {2c|3} noauth {***name***|***user-name***} udp-port** *port* **retries** *count* to set the number of SNMP retries. 3. End.
To configure SNMP port number.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **snmp host** *server-address* **traps version {1|2c|3} noauth {***name***|***user-name***} udp-port** *port* or **snmp host** *server-address* **informs version {2c|3} noauth {***name***|***user-name***} udp-port** *port* to set the port number used by SNMP protocol package.
To remove SNMP community name.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **no snmp community** *name* to delete the configured SNMP community name. 3. End.
To remove SNMP user.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **no snmp user** *user-name* to delete the configured SNMP user. 3. End.

To remove SNMP group information.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **no snmp group** *group-name* **security-mode version {1|2c|3}** to delete the configured SNMP group information.
To remove SNMP view.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **no snmp view** *view-name* **subtree all** to delete the configured SNMP view. 3. End.
To enable or disable SNMP function.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **snmp** to enable the SNMP function. Execute the command **no snmp** to disable the SNMP function. 3. End.

Attached table:

Parameter	Explanation	Value
name	Designated group name.	String form, less than 20 characters.
{ **ro** | **rw** }	Indicates the authority of the community name in the specified view, ro means read only, rw means readable and writable.	-
view-name	View name corresponding to the specified community name.	String form.
{ **included** | **excluded** }	Indicates include / exclude.	-
subtreemask	Specify mask oid string.	String form.
group-name	Specify SNMP group name.	String form.
read-view	Specify read-only view name.	String form.
write-view	Specify the read and write view name.	String form.
notify-view	Specify the name of the announcement view.	String form.
user-name	Specify username.	String form.
count	Specify the number of retries.	1 – 255
port	Specify the SNMP port number.	1 – 65535
v1|v2|v3|	Version v1, version v2, version v3.	-
server-address	Specify the IPv4 address of the host receiving trap	Dotted decimal.

	information.	

12.2.3 Configure Send Trap Function

Background Information

Trap is a message sent by the managed device to NMS without request, which is used to report important emergency events. The managed device must be configured with the trap function before it can actively send these messages.

Purpose

In this section, the user configures the device to actively send trap messages.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
To add SNMP Trap information.	1. Execute the command **configure** to enter the global configuration view. 2. (IPv4). Execute the command **snmp host** *server-address* **traps version {1|2c|3} noauth {***name***|***user-name***} udp-port** *port* or **snmp host** *server-address* **informs version {2c|3} noauth {***name***|***user-name***} udp-port** *port* to set up SNMP. 3. End.
To remove SNMP Trap Information.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **no snmp host** *server-address* **version {1|2c|3}**. 3. End.
To configure the timeout period.	1.Execute the command **configure** to enter the global configuration view. 2. (IPv4). Execute the command **snmp host** *server-address* **informs version {2c|3} noauth {***name***|***user-name***} timeout** *timeout*. 3. End.

Attached table:

Parameter	Explanation	Value
server-address	Specify the IPv4 address of the host receiving trap information.	Dotted decimal.
v1|v2|v3|	Version v1, version v2, version v3.	String form.
name	Designated group name.	String form, less than 20 characters.

{ **included** | **excluded** }	Indicates include / exclude.	-
user-name	Specify username.	String form.
port	Specify the SNMP port number.	1 – 65535
timeout	Specified timeout.	1 – 300

12.2.4 Maintenance and Commissioning

Purpose

Users can debug the SNMP protocol through this section to locate the problem.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
To display SNMP community configuration information.	1. Keep in the current privileged user view. 2. (IPv4). Execute the command **show snmp community** to display the community configuration information of SNMP. 3. End.
To display SNMP status information.	1. Keep in the current privileged user view. 2. (IPv4). Execute the command **show snmp** to display the status information of SNMP. 3. End.
To display SNMP group information.	1. Keep in the current privileged user view. 2. (IPv4). Execute the command **show snmp group** to display SNMP group information. 3. End.
To display the configuration of the SNMP notification receiver on the switch.	1. Keep in the current privileged user view. 2. (IPv4). Execute the command **show snmp host** to display the configuration of the SNMP notification receiver on the switch. 3. End.
To display SNMP user information.	1. Keep in the current privileged user view. 2. (IPv4). Execute the command **show snmp user** to display SNMP user information. 3. End.
To display SNMP view information.	1. Keep in the current privileged user view. 2. (IPv4). Execute the command **show snmp view** to display SNMP view information. 3. End.

12.2.5 Configuration Example

Network Requirements

The network management workstation (NMS) is connected to the switch via Ethernet. The network management workstation IP address is 129.102.149.23 and the switch IP address is 129.102.0.1. Perform the following configuration on the switch: set the community name and access rights, administrator ID, and switch location information, and allow the switch to send trap messages.

Network Diagram

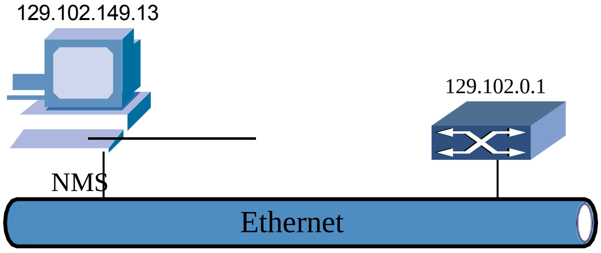


Figure 11-2. Network diagram of SNMP configuration example.

Configuration Steps

#Enter global configuration view

```
Switch#config
```

#Open snmp, and then configure community, view, etc.

```
Switch(config)# snmp
Switch(config)# snmp community public rw
Switch(config)# snmp view v3test subtree 1.3.6 oid-mask all viewtype included
Switch(config)# snmp group aa version 3 auth read-view v3test
```

#It is allowed to send Trap messages to NMS 129.102.149.23..

```
Switch(config)# snmp host 129.102.149.23 traps version 3 noauth public
```

Configure NMS

The PC where the network management is located needs to be set for login.

For Mib-Browser, the login settings are: SNMPV1, V2 use the default community name to log in, and SNMPV3 uses the user admin to log in. Users can use the network management system to complete the query and configuration of the switch. For details, please refer to the supporting manual of the network management product.

12.3 RMON Configuration

12.3.1 RMON Overview

Introduction

Remote monitoring (RMON) is a standard monitoring specification that enables network monitoring data to be exchanged between various network monitors and console systems. RMON provides network administrators with more freedom to choose consoles and network monitoring probes that meet specific network requirements.

There are currently two versions of RMON: RMON v1 and RMONv2. RMON v1 can be found in the more widely used network hardware. It defines 9 MIB groups to serve basic network monitoring; RMON v2 is an extension of RMON, focusing on the higher traffic layer above the MAC layer. Traffic and application layer traffic. RMON v2 allows network management applications to monitor packets at all network layers. This is different from RMONv1, which only allows monitoring packets at MAC and below.

RMON Implementation

RMON is implemented based on the simple network management protocol SNMP architecture and is compatible with the existing SNMP framework, including the network management workstation NMS and the agent agent running on each network device.

RMON Agent keeps track of various traffic information in the network, for example, the total number of packets on a network segment in a certain period of time, or the total number of correct packets sent to a certain host. It makes SNMP more effective and proactive in monitoring remote network devices, and provides an efficient means for monitoring the operation of sub nets. Reduce the communication traffic between the network management station and the agent Agent, so as to achieve simpler and more effective management of large networks.

RMON allows multiple monitors, and it can collect data in two ways.

- Through the dedicated RMON Probe (probe). NMS directly obtains management information from RMON Probe and controls network resources. In this way, all information of RMON MIB can be obtained.
- Embed RMON Agent directly into network devices (such as switches) to make them become network devices with RMON Probe function. NMS exchanges data information with basic SNMP commands to collect network management information. This method is limited by device resources and generally cannot obtain all the data of RMON MIB. Most of them only collect the information of four groups (alarms, events, history and statistics).

RMON1 MIB Group

RMON1 MIB group	Features	Element
Statistics	Includes statistics measured by the detector for each monitored interface of the device.	Packets dropped, packets sent, broadcast packets, CRC errors, large and small blocks, collisions, and counter packets. The range is from 64 – 128, 128 – 256, 256 – 512, 512 – 1024 and 1024 – 1518 bytes.
History	Collect and record statistical network values regularly and store them for future extraction.	Sampling cycle, number of samples and items. Provide historical data on other statistical information such as network segment traffic, error packets, broadcast packets, utilization, and collision times.
Alarm	Regularly select statistical examples from the variables of the detector. And compare with the threshold value matched before.	Alarm type, interval, upper threshold, lower threshold.
Host	Including statistics related to each host found on the network.	Host address, data packet, received bytes, transmitted bytes, broadcast transmission, etc.

HostTo pN	Prepare a table describing the hosts and sort the list according to a statistical value.	Statistics, host, start and end of cycle, rate base value, duration.
Filter	Allows the monitor to observe packets matching a filter.	Byte filter type, filter expression, etc.
Capture packet	The data packet is captured after flowing through a channel.	Capture all packets that pass through the filter or simply write down the statistics based on these packets.
Event	Control the generation and reporting of events here.	Event type, description, last time the event was sent.
Token Ring	Support Token Ring.	Not often used.

12.3.2 Configuration Statistics

Purpose

Use the operations in this section to configure RMON to collect interface traffic information.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
To clear statistics recorded on the interface.	1. Maintain the privileged view. 2. Execute the command **clear rmon interfaces GigabitEthernet** *interface-number* **statistics** to clear the statistical records on the interface. 3. End.

Attached table:

Parameter	Explanation	Value
interface-number	Specify the Ethernet interface number.	Integer form, the GE interface value range is 1 – 28.

12.3.3 Configuration History Control Table

Purpose

Using the operations in this section to configure RMON, you can periodically collect data on the specified port and save the collected information in the history table for viewing.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
To add or modify RMON history control.	1. Execute the command **configure** to enter the global configuration view.

	2. Execute the command **rmon history** *history-id* **interface GigabitEthernet** *interface-number* **[buckets** *maximum* **interval** *sampling-interval* **owner** *owner*]* to configure RMON history control. 3. End.
To remove configured RMON history control.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **no rmon history** *history-id* to delete RMON history control. 3. End.

Attached table:

Parameter	Explanation	Value
history-id	Specify RMON history control entry ID.	1 – 65535
interface-number	Specify the Ethernet interface number.	Integer form, the GE interface value range is 1 – 28.
maximum	Maximum number specified.	1 – 50.
sampling-interval	Specify sampling interval.	The value is an integer and the value range is 1 – 3600 seconds.
owner	Specify the user requesting RMON information.	String form.

12.3.4 Configure Alarm Table

Purpose

Using the operations in this section to configure RMON, you can monitor the specified alarm variable (specified by the OID of this variable) at the specified sampling interval. When the value of the monitored data exceeds the defined threshold, an alarm event will be generated.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
To configure RMON alarm entries.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **rmon alarm** *alarm-id* **interface {GigabitEthernet|LAG}** *interface-number* Counter sample { **absolute** | **delta** } **rising** rising-threshold rising-event **falling** falling-threshold falling-event startup **{rising|falling|rising-falling}** **[owner** *owner*]* to configure RMON alarm entries. 3. End.

To remove the configured RMON alarm entry.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **no rmon alarm** *alarm-id* to delete the configured RMON alarm entry. 3. End.

Attached table:

Parameter	Explanation	Value
alarm-id	Specify RMON history alarm entry ID.	1 – 65535
interface-number	Specify the Ethernet interface number.	Integer form, the GE interface value range is 1 – 28, the LAG interface value range is 1 – 8.
Counter	Specified counter type.	broadcast-pkts collisions crc-align-errors drop-events fragments jabbers multicast-pkts octets oversize-pkts pkts pkts1024to1518octets pkts128to255octets pkts256to511octets pkts512to1023octets pkts64octets pkts65to127octets undersize-pkts
sample	Specify the alarm query interval.	Integer form, the range of values is 1 – 2147483647 seconds.
rising-threshold	Specify rising threshold.	Integer form, the range of values is 0 – 2147483647 seconds.
rising-event	Specify ascending event entry number.	0 – 65535
falling-threshold	Specify falling threshold.	0 – 2147483647
falling-event	Specify the fall time entry number.	0 – 65535
owner	Define the user for RMON alarm (optional parameter).	In the form of a string, the value range is 0 – 127 characters.

{ **absolute** | **delta** }	Indicates absolute or relative value (incremental value).	-

12.3.5 Configure Event Table

Purpose

Use the operations in this section to configure RMON. When the event exceeds the alarm threshold, the device can record logs or generate alarms, or log and generate alarms at the same time.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
To configure RMON event control entries.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **rmon event** *event-id* [{ log | trap | **log trap** } name | description *description* | owner *owner*]* or **rmon event** *event-id* [**log |** description *description* | owner *owner*]* to configure RMON event control entries. 3. End.
To remove the configured RMON event control entry.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **no rmon event** *event-id* to delete the configured RMON control entry. 3. End.

Attached table:

Parameter	Explanation	Value
event-id	Specify RMON event control entry ID.	1 – 65535
{ log | trap | **log trap** }	Specify the type of event log: The log that generated the event. Trap: the alarm that generated the event. Both: both the event log and the alarm.	-
name	Designated group name.	String form, less than 20 characters
description	Descriptive information of the specified event (optional parameter).	String form.
owner	Define the user requesting RMON information (optional parameter).	String form.

12.3.6 Maintenance and Commissioning

Purpose

When RMON function is not normal and you need to view, debug or locate the problem, you can use this section to operate.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
To display configuration information of RMON alarm control entries.	1. Maintain the current privileged user view without executing any commands. 2. Execute the command **show rmon alarm**. 3. End.
To display configuration information for RMON events.	1. Maintain the current privileged user view without executing any commands. 2. Execute the command **show rmon event** {all|*event-id* }. 3. End.
To display configuration information of RMON historical control entries.	1. Maintain the current privileged user view without executing any commands. 2. Execute the command **show rmon history {** history-id |all}. 3. End.
To display statistics of RMON history control entries.	1. Maintain the current privileged user view without executing any commands. 2. Execute the command **show rmon event** {all|*event-id* }. 3. End.
To display interface RMON statistics table information.	1. Maintain the current privileged user view without executing any commands. 2. Execute the command **show rmon interfaces {GigabitEthernet|LAG}** 1 statistics. 3. End.

Attached table:

Parameter	Explanation	Value
event-id	Specify RMON event control entry ID.	1 – 65535
history-id	Specify RMON History Control Entry ID.	1 – 65535
interface-number	Specify the Ethernet interface number.	Integer form, the GE interface value range is 1 – 28, the LAG interface value range is 1 – 8.

12.3.7 Configuration Example

Network Requirements

Now monitor the subnet to which it is connected through port Ge1 / 0/2, including: real-time and historical statistics of traffic and various types of packet data; set alarm monitoring for the number of bytes of traffic on this interface, exceeding the setting; record the log when the value is exceeded; actively report the alarm information to the NMS when the alarm setting value is exceeded.

Network Diagram

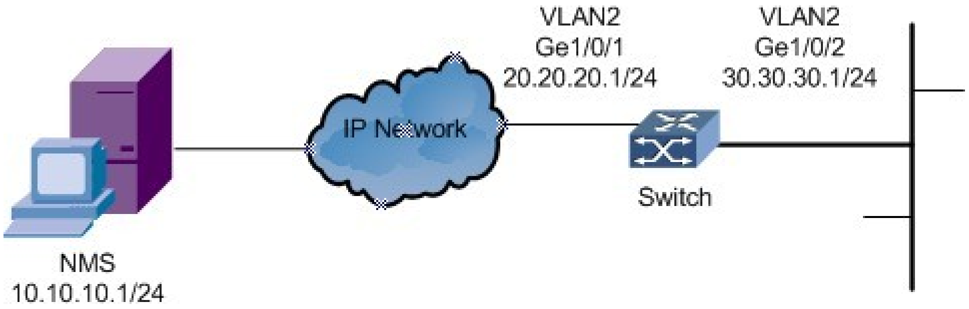


Figure 11-3. RMON configuration diagram.

Configuration Prerequisites

1. Configure the IP addresses of the interfaces Ge1 / 0/1 and Ge1 / 0/2 of the switch;

2. Configure the switch and NMS reachable;

3. Configure the SNMP of the switch.

Configuration Process

1. Configure the historical sampling of interface 2.

```
Switch# configure
Switch(config)#rmon history 1 interface GigabitEthernet 2 interval 20 owner test
```

2. Configure the rmon event.

```
Switch(config)# rmon event 2 trap public owner test
```

3. Configure the SNMP of the switch.

```
Switch(config)#rmon alarm 1 interface GigabitEthernet 2 octets 20 absolute rising 1200 1
falling 1000 1 startup rising-falling
```

4. Configure the trap host.

```
Switch(config)# snmp host 10.10.10.1 traps version 1 public
```

13. Loop Guard Configuration

13.1 Overview

This chapter introduces the switch loop guard configuration, including Loopback-detection and ERPS configuration. This chapter includes the following topics:

13.2 Loopback-Detection Configuration

13.2.1 Loopback-Detection Overview

Protocol Introduction

Loopback detection (LBDT) periodically sends detection packets through an interface to detect loops on the interface, on the downstream network or device, or between two device interfaces.

When a loop occurs on a network, broadcast, multicast, and unknown unicast packets are circulated on the network. This wastes network resources and can result in network breakdowns. Quickly detecting loops on a Layer 2 network is crucial for users to minimize the impact of loops on a network. LBDT helps users check network connections and configurations, and control the looped interface.

LBDT periodically sends detection packets on an interface to check whether the packets return to the local device (through the same interface or another interface), and determines whether a loop occurs on the interface, on the downstream network or device, or between two device interfaces. After a loop is detected, the device sends a trap to the NMS and records a log, and takes a preconfigured action on the looped interface (the interface is shut down by default) to minimize impact of the loop on the device and entire network.

Configuration Prerequisites

LBDT can only detect loops on a single node, but cannot eliminate loops in the same manner as ring network technologies including ERPS, RRPP, SEP, Smart Link, STP, RSTP, MSTP, and VBST.

13.2.2 Configure Basic Loopback-Detection Function

Purpose

The user configures basic Loopback-Detection functions through the operations in this section.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process	Parameter Description
To enable or disable the loopback feature.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **loopback-detection enable** to enable Loopback-Detection. Execute the command **no loopback-detection enable** to	-

	disable Loopback-Detection. 3. End.	
To configure loopback detection to work on the specified VLAN.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command interface interface-type port to enter the configuration view for specifying an interface. 3. Execute the command loopback-detection specified-vlan 0 – 4094 configuration specified VLAN.	interface-type: Includes 2 port types: LAG, GigabitEthernet; Port <integer>, LAG The interface value range is 1 – 8; GigabitEthernet The interface value range is 1 – 28, -vlan The interface value range 0 – 4094.
To configure controlled mode for the interface when single-link loopback.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command interface interface-type port to enter the configuration view for specifying an interface. 3. Execute the command loopback-detection control-mode (shutdown|block).	control-mode: (shutdown|block), (shutdown) shutdown for the interface, (block) blocking the forwarding of the interface.

13.2.3 Maintenance and Commissioning

Purpose

Users can debug the Loopback-Detection protocol through this section to locate the problem.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
To reset the control interface.	1. Stay in normal mode. 2. Execute the command **loopback-detection reset**. 3. End.
To display all interface configuration information for loopback detection.	1. Stay in normal mode. 2. Execute the command **loopback-detection port-info**. 3. End.
To display the enabled status of loopback detection.	1. Stay in normal mode. 2. Execute the command **loopback-detection status**. 3. End.

Other Related Notes

1. Access the web management of the switch, enter the port - Error Disabled, and set the enable state and recovery interval of loopback detection, which is 300 seconds by default.

2. Access the web management of the switch and enter status-port-error disabled to see the cause of the port exception and the time remaining for the port to recover.

13.3 ERPS Configuration

13.3.1 ERPS Overview

Protocol Introduction

ERPS (Ethernet Ring Protection Switching), the Ethernet multi-ring protection technology, is a layer-2 ring breaking protocol standard defined by ITU-T. The standard number is ITU-T G.8032/Y1344, so it is also called G.8032 . It defines RAPS (Ring Auto Protection Switching) protocol packets and protection switching mechanism.

Supported ERPS Version and Purpose

ERPS currently supports two versions, v1 and v2. v1 is the version released by the ITU-T organization in June 2008, and v2 is the version released by the ITU-T in August 2010. The v2 version is fully compatible with the v1 version, and the following functions have been extended on the basis of the v1 version:

- Multi-ring networking methods such as intersecting rings.
- Sub-rings use virtual channels or non-virtual channels to transmit RAPS packets.
- Manual switching of choke points, including forced switching and manual switching.
- The switchback mode of the ERPS ring can be configured.

In order to perform link backup and improve network reliability in an Ethernet switching network, redundant links (for example, a ring network) are usually used. However, the use of redundant links will generate loops on the network, which may cause broadcast storms and unstable MAC address tables, thereby affecting user communication quality and even causing communication interruptions.

In order to solve the loop problem, the ERPS protocol can be used. Advantages:

- Fast convergence speed, meeting carrier-class reliability.
- ERPS protocol is an ITU-T standard protocol, which can realize intercommunication with other manufacturers' equipment.
- The v2 version supports not only single-ring networking, but also multi-ring networking such as intersecting rings.

Disadvantage:

- The network topology needs to be planned in advance, and the configuration is relatively complex

13.3.2 Configure Basic ERPS Functions

Purpose

The user configures basic ERPS functions through the operations in this section.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
To enable or disable ERPS function.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **erps-ring enable** to enable ERPS.

	3. Execute the command **no erps-ring enable** to disable ERPS.
To change ERPS transmission notification method.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **ethernet tcn-propagation erps to erps** to configure the topology changing transmission notification method supported by this device as the appointed method. The ERPS ring instance detects the changing, it will send the notification packets. If configured erps method, it will send the R-APS event packets to other ERPS rings; if configured stp method, it will send the stp packets outward. 3. Execute the command **no ethernet tcn-propagation erps** to restore default configuration, ERPS ring topology changing only takes effect in this ring but does not send the notification packets.
To create an ERPS ring and enter ERPS ring configuration mode.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **erps-ring** <*ring-name*> to create an ERPS ring and enter ERPS ring configuration mode. 3. Execute the command **no erps-ring** <*ring-name*> to delete ERPS ring.
To configure the supporting version of the ERPS loop.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **erps-ring** <*ring-name*> to enter ERPS ring configuration mode. 3. Execute the command **version {v1 | v2}** to configure ERPS version. 4. Execute the command **no version** to restore default v2 version.
To configure ERPS sub ring.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **erps-ring** <*ring-name*> to enter ERPS ring configuration mode. 3. Execute the command **open-ring** to configure this ERPS ring type as a sub ring. 4. Execute the command **no open-ring** to delete an ERPS sub ring.
To configure R-APS virtual channel.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **erps-ring** <*ring-name*> to create an ERPS ring and enter ERPS ring configuration mode. 3. Execute the command **raps-virtual-channel {with | without}** to configure R-APS virtual channel, configure if there is the R-APS virtual channel in ERPS ring according to the configuration. Inputting: Success or error. If there is not R-APS virtual channel

	on the ERPS ring, the R-APS channel of all the instances of ERPS ring will be unblocked forever and it only blocks the data channel; otherwise, the R- APS channel and the data channel will be blocked at the same time; The R-APS virtual channel is not existed in ERPS ring.
To configure the port as the port 0 of the specified ERPS ring.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **erps-ring** <*ring-name*> to create an ERPS ring. 3. Execute the command **exit** to exit ERPS ring view. 4. Execute the command **interface** *interface-type port* to enter the configuration view of a specified interface. 5. Execute the command **erps-ring** <*ring-name*> **port0 [port1-none]** to configure the port 0 of the specified ERPS ring, **[port1-none]** there is only the port0 on this ERPS ring node, no port1 and it is the interconnection node. 6. Execute the command **no erps-ring** <*ring-name*> **port0** to delete the port 0 of the specified ERPS ring.
To configure the port as the port 1 of the specified ERPS ring.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **erps-ring** <*ring-name*> to create an ERPS ring. 3. Execute the command **exit** to exit ERPS ring view. 4. Execute the command **interface** *interface-type port* to enter the configuration view of a specified interface. 5. Execute the command **erps-ring** <*ring-name*> **port1** to configure the port 1 of the specified ERPS ring. 6. Execute the command **no erps-ring** <*ring-name*> **port1** to delete the port 1 of the specified ERPS ring.
To configure the ERPS ring instance.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **erps-ring** <*ring-name*> to create an ERPS ring. 3. Execute the command **erps-instance** <*instance-id*> to create the ERPS ring instance and enter into the ERPS ring instance configuration Mode. 4. Execute the command **no erps-instance** <*instance-id*> to delete an ERPS ring instance.
To configure the description string for the ERPS instance.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **erps-ring** <*ring-name*> to create an ERPS ring and enter ERPS ring configuration mode.

	3. Execute the command **erps-instance** <*instance-id*> to create the ERPS ring instance and enter into the ERPS ring instance configuration Mode. 4. Execute the command **description** <*instance-name*> to configure the description string for the ERPS instance. 5. Execute the command **no description** <*instance-name*> to delete the description string for the ERPS instance.
To configure the last byte of R-APS packets sent by ERPS ring node to carry ring-id.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **erps-ring** <*ring-name*> to create an ERPS ring and enter ERPS ring configuration mode. 3. Execute the command **erps-instance** <*instance-id*> to create the ERPS ring instance and enter into the ERPS ring instance configuration Mode. 4. Execute the command **ring-id** <*ring-id*> to configure the last byte of R-APS packets destination MAC address sent by ERPS ring node to carry ring-id. 5. Execute the command **no ring-id** <*ring-id*> to configure the last byte of R-APS packets destination MAC address sent by ERPS ring not to carry the ring-id, it means the destination MAC is 01-19-A7-00-00-01. The MAC address is 01-19-A7-00-00-01 as default.
To configure the last byte of R-APS packets sent by ERPS ring node to carry ring-id.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **erps-ring** <*ring-name*> to create an ERPS ring and enter ERPS ring configuration mode. 3. Execute the command **erps-instance** <*instance-id*> to create the ERPS ring instance and enter into the ERPS ring instance configuration Mode. 4. Execute the command **rpl {port0 | port1} {owner | neighbour}** to configure the member port of ERPS ring instance as RPL owner or RPL neighbour, the RPL node roles of different instances on the same ERPS ring cannot be configured on the same member port. 5. Execute the command **no rpl {port0 | port1}** to restore the ordinary transmission node type of the member port on the default ERPS ring.
To configure the ERPS ring instance as non-revertive.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **erps-ring** <*ring-name*> to create an ERPS ring and enter ERPS ring configuration mode. 3. Execute the command **erps-instance** <*instance-id*> to create the ERPS ring instance and enter into the ERPS ring instance

	configuration Mode. 4. Execute the command **rnon-revertive** to configure the ERPS ring instance as non-revertive. If this ERPS ring supports v1, this command is null and cannot be configured. The no command configures the ERPS ring instance as revertive. If this ERPS ring supports v1, this command is null. This command can be configured only on the RPL owner node of the sub ring. 5. Execute the command **no non-revertive** to configure the ERPS ring instance as revertive.
To configure the Guard timer.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **erps-ring** <*ring-name*> to create an ERPS ring and enter ERPS ring configuration mode. 3. Execute the command **erps-instance** <*instance-id*> to create the ERPS ring instance and enter into the ERPS ring instance configuration Mode. 4. Execute the command **guard-timer** <*guard-times*> to configure the Guard timer. The guard timer is used for the Ethernet node to avoid the error handling and the close loop according to the outdated R-APS packets. In the starting time of the timer, any R-APS packets received (the R-APS packets that the Request/State="1110" are except) will be dropped. The no command configures the guard timer as the default value. 5. Execute the command **no guard-timer** <*guard-times*> to restore guard timer default 500ms.
To configure the holdoff timer.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **erps-ring** <*ring-name*> to create an ERPS ring and enter ERPS ring configuration mode. 3. Execute the command **erps-instance** <*instance-id*> to create the ERPS ring instance and enter into the ERPS ring instance configuration Mode. 4. Execute the command **holdoff-timer** <*holdoff-times*> to configure the delay timer. 5. Execute the command **no guard-timer** <*holdoff-times*> to restore delay timer default 0s.
To configure the WTR timer.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **erps-ring** <*ring-name*> to create an ERPS ring and enter ERPS ring configuration mode. 3. Execute the command **erps-instance** <*instance-id*> to create the ERPS ring instance and enter into the ERPS ring instance configuration Mode.

	4. Execute the command **wtr-timer** <*wtr-times*> to configure the WTR timer. WTR timer is used to avoid the frequent protection switching of RPL owner node because of the periodic (intermittent) default. When RPL owner port received the default recovery packets, after some time, and then check if the default still existed on the other nodes and prevent blocking RPL owner port immediately to cause the chokepoint shocking. 5. Execute the command **no wtr-timer** <*wtr-times*> to restore WTR timer default 5min.
To configure the protection instance of ERPS ring instance.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **erps-ring** <*ring-name*> to create an ERPS ring and enter ERPS ring configuration mode. 3. Execute the command **erps-instance** <*instance-id*> to create the ERPS ring instance and enter into the ERPS ring instance configuration Mode. 4. Execute the command **protected-instance** <*instance-list*> to configure the protection instance of ERPS ring instance. ERPS ring instance can protect all the MSTP instances. The same instance cannot be quoted by multiple ERPS ring instances under the same topology. Under the same ERPS ring instance, run this command more than once to protect instance, the result will be accumulated. The no command deletes the protection instance of ERPS ring instance. 5. Execute the command **no protected-instance** <*instance-list*> to delete the protection instance of ERPS ring instance.
To configure the control vlan of ERPS ring instance.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **erps-ring** <*ring-name*> to create an ERPS ring and enter ERPS ring configuration mode. 3. Execute the command **erps-instance** <*instance-id*> to create the ERPS ring instance and enter into the ERPS ring instance configuration Mode. 4. Execute the command **control-vlan** <*vlan-id*> to configure the control vlan of R-APS packets of R-APS channel. In the ERPS ring instance, this vlan is only used to transmit ERPS protocol packets but not to forward the user business packets. It improves the ERPS protocol security. User makes sure the configuration uniqueness. This vlan is as the vlan tag when sending R-APS packets. The protection VLAN configuration of all the nodes in the instance must be identical. 5. Execute the command **no control-vlan** <*vlan-id*> to delete the control vlan of ERPS ring instance.

To run the forced switch on the port of ERPS ring node.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **erps-ring** <*ring-name*> to create an ERPS ring and enter ERPS ring configuration mode. 3. Execute the command **erps-instance** <*instance-id*> to create the ERPS ring instance and enter into the ERPS ring instance configuration Mode. 4. Execute the command **forced-switch {port0 | port1}** to run the forced switch on the port of ERPS ring node. Two or more forced switch are allowed existing at the same time in one ERPS ring instance. But only one forced switch command can be existed on one ring node. User should avoid using multiple forced switch in ERPS ring instance to cause the ERPS ring instance splitting. If the forced switch is on the current highest priority, block the data channel and R-APS channel of this ERPS ring instance on the appointed member port (port0 or port1), and unblock the other member port of this ring node; if this instance configuration is not integral, it is on the status of inactive, there will be the message of "The request is rejected because the ERP instance in inactive state!" otherwise, enter into the next step.
To run the manual switch on the port of ERPS ring node.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **erps-ring** <*ring-name*> to create an ERPS ring and enter ERPS ring configuration mode. 3. Execute the command **erps-instance** <*instance-id*> to create the ERPS ring instance and enter into the ERPS ring instance configuration Mode. 4. Execute the command **manual-switch {port0 | port1}** to run the manual switch on the port of ERPS ring node. Only one manual switch is allowed existing in one ERPS ring instance, and the premise is that there is no SF fault or FS command in ERPS ring instance. If this instance configuration is not integral, it is on the status of inactive, there will be the message of "The request is rejected because the ERP instance in inactive state!" otherwise, enter into the next step.

Attached table:

Parameter	Explanation	Value
erps	Topology changing sends the R-APS event packets to notify the connection ring of this device.	-
< ring-name >	The ERPS ring name created.	The maximum character number is 64 and it is made up with letters, numbers and the

		underlines. The first and last character cannot be the underline.
<instance-id>	Id of ERPS ring.	The range is 1 to 48.
<instance-name>	ERPS instance name.	The maximum string is 64, and it is made up with letters, numbers and underlines; the first and last characters cannot be underlines. The no command deletes the ERPS instance name.
<ring-id>	ERPS ring id.	The range is 1 to 64.
<guard-times>	Guard timer.	The interval is 10ms and the range is 10ms to 2s.
<holdoff-times>	Holdoff timer.	The interval is 1s and the range is 0 to 10s.
<wtr-times>	WTR timer.	The interval is 1min and the range is from 1 to 10min.
<instance-list>	The MSTP instance list protected by ERPS ring instance.	Init, such as i, j-k. The number of the instances in the list is not limited.

13.3.3 Maintenance and Commissioning

Purpose

Users can debug the ERPS protocol through this section to locate the problem.

Process

According to different purposes, perform the corresponding process, see the table below for details.

Purpose	Process
To run the clear command to the member port of ERPS ring node.	1. Execute the command **configure** to enter the global configuration view. 2. Execute the command **erps-ring** *<ring-name>* to create an ERPS ring and enter ERPS ring configuration mode. 3. Execute the command **erps-instance** *<instance-id>* to create the ERPS ring instance and enter into the ERPS ring instance configuration Mode. 4. Execute the command **clear command**. Run the clear command to the member port of ERPS ring node, it can clear the management command of the local activity: forced switch command and manual switch command; it can be also used to trigger the link switch under the revertive mode before WTR or WTB is time out; and trigger the link to switch from the standby link RPL back to the intrinsic link under the non-revertive mode after the fault recovery. If the forced or manual switch command

	has existed on the node of this ring instance, clear the switch command and keep the block status of the data channel and R-APS channel of the blocked member ports. And send the P-APS (NR) packets on the two member ports stably and steadily until received R-APS (NR, RB) packets and known the RPL is blocked. Or the higher level request happens on the ring (such as SF);If the local forced or manual switch has existed on the node of this ring instance, clear the command and then receive the R-APS (NR) packets whose node ID is larger than the local node ID.Unblock all the ring ports without SF fault and stop sending the R-APS (NR) packets on the two member ports. 5. End.
To read the ERPS ring information.	1. Keep in the current privileged user view. 2. Execute the command **show erps ring {**<*ring-name*>**| brief}**. 3. End.
To display the ERPS ring instance information.	1. Keep in the current privileged user view. 2. Execute the command **show erps instance {ring** <*ring-name*> **[instance** <*instance-id*> **]}**. 3. End.
To display the status information of ERPS ring instance.	1. Keep in the current privileged user view. 2. Execute the command **show erps status {ring** <*ring-name*> **[instance** <*instance-id*> **]}**. 3. End.
To display the statistic information of ERPS ring instance.	1. Keep in the current privileged user view. 2. Execute the command **show erps statistics {ring** <*ring-name*> **[instance** <*instance-id*> **]}**. 3. End.
To clear the statistic information of ERPS.	1. Keep in the current privileged user view. 2. Execute the command **clear erps statistics {ring** <*ring-name*> **[instance** <*instance-id*> **]}**. 3. End.