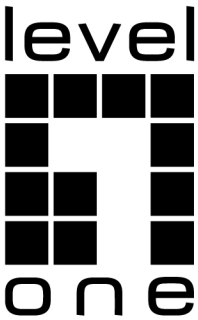
CLI Reference Guide

GEP-1061 (Version 2), GEP-2861 (Version 1)



Directory

Chapter 1 CLI Command-line Introduction

This chapter describes the CLI command line interface in detail, mainly including the following contents:

- Access the CLI of the switch
- CLI pattern introduction
- Introduction to command language
- Command fast
- Historical command

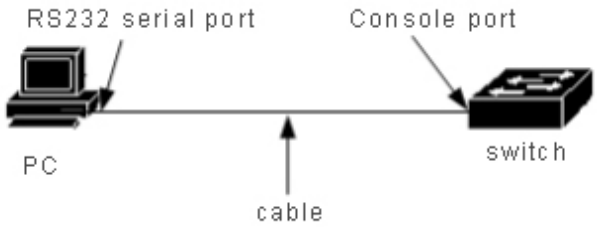
1.1 Access the CLI of the Switch

The CLI command-line interface of the switch provides an interface for user management of the switch.Users can access the CLI command line interface of the switch through the Console and Telnet terminals, respectively described below.

1.1.1 Users Access the CLI Through the Console Port

The operation steps are as follows:

Step 1: connect the PC serial port to the Console port of the switch through the configuration cable, as shown below:



:

Step 2: start the terminal emulator on the PC (such as the Windows superterminal, etc.) and configure the communication parameters of the terminal emulator.The communication parameters of the terminal are configured as follows:

Baud rate: 38400

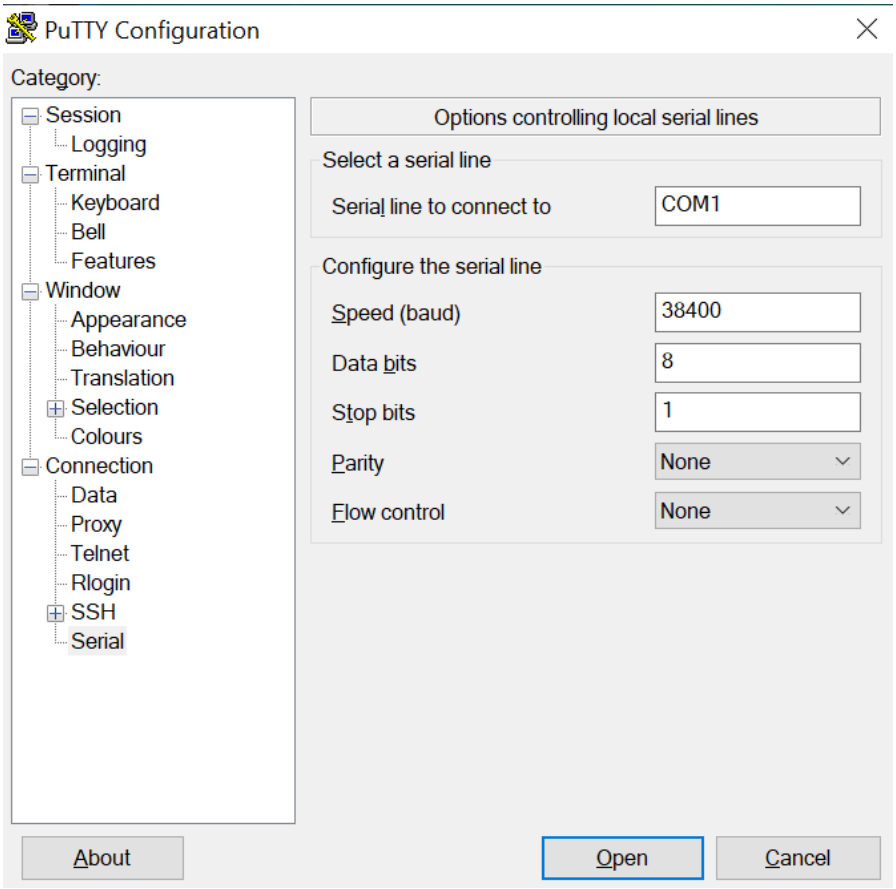
Data bit: 8

Parity: none

Stop bit: 1

Data flow control: none

The communication parameter configuration of the super terminal is as follows:



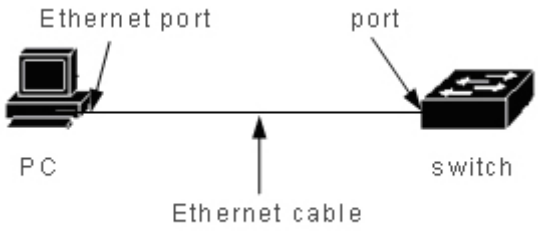
Step 3: start the Switch. When the Switch is started, the CLI prompt (Switch> by default) will be displayed on the terminal. Users can enter commands at this prompt, so that they can access the CLI of the Switch.

1.1.2 Users Access the CLI Through TELNET

The user can access the switch through the port of the switch.

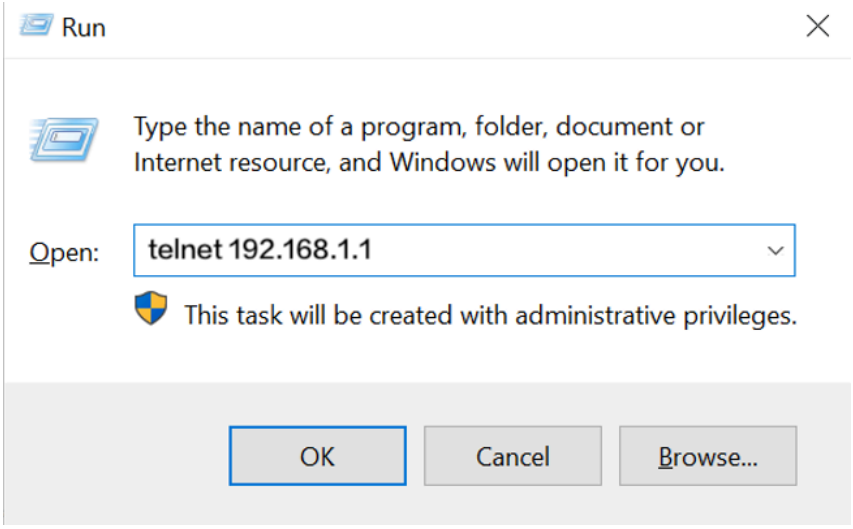
The default IP address of the port of the switch is 192.168.1.1. The operation steps to access the switch through the port are as follows:

Step 1: connect the Ethernet port of the PC to the port of the switch through the Ethernet cable.The diagram below:



Step 2: set the IP address of your PC's Ethernet port, which must be in segment 192.168.1.0/24 (for example, IP address 192.168.1.100).Ping 192.168.1.1 was used to determine the connectivity between PC and switch.

Step 3: if the PC is connected to the switch, Telnet 192.168.1.1 enters the Telnet terminal interface.The diagram below:



Step 4: enter the CLI after entering the user name and password in the Telnet interface, and the CLI prompt (default is Switch>) appears. The default user name and password of the system are admin.

There are two points to note:

- The IP address of the switch port is established on the VLAN three-layer interface. Before accessing the switch, the IP address of a VLAN interface must be set. The default IP address of VLAN1 is 192.168.1.1, which can be used directly.The IP address of the VLAN interface can be configured through the Console port.
- The user accesses the switch via a port and can connect directly to the PC and port via an Ethernet cable, or through a network, as long as there is intercommunication between the PC and a VLAN of the switch.

1.2 CLI Pattern Introduction

1.2.1 Roles of CLI Mode

The role of CLI model is mainly as follows:

- Facilitate user classification to prevent unauthorized users from using CLI illegally.

Users can be divided into two levels, that is, two categories: ordinary users and privileged users.

The average user can only view some of the running state of the switch and can only use display commands.
In addition to being able to view the running state of the switch, privileged users can also maintain and configure the switch and change its behavior.

- Convenient for users to configure the switch

Switches have many configurations, and if you put them all in one mode, it's very inconvenient for users to use them.For this reason, multiple patterns are established on the CLI, and similar commands are put into one pattern for the convenience of users' understanding and use.For example, put vlan-related commands in VLAN configuration mode and interface-related commands in interface configuration mode.

1.2.2 CLI Mode Identification

CLI prompt is the identification of CLI mode. When users use CLI, they can know the current CLI mode by looking at the CLI prompt.
The CLI prompt consists of two parts, one identifying the host and the other identifying the schema.
The host part of the CLI prompt USES the system's hostname, which is configurable and defaults to Switch, so the CLI prompt starts with Switch by default, and the CLI descriptor mentioned later generally USES the default hostname.
The pattern part of the CLI prompt is not configurable, and each pattern has its own pattern string, some of which is fixed and some of which is mutable.For example, the mode string of VLAN configuration mode is fixed, and the mode string of interface configuration mode is variable.
Such as:
CLI prompt Switch# identifies privileged mode, Switch identifies host, and # identifies mode.
The CLI prompt Switch(config-ge1/1)# identifies the interface configuration mode, and the configured port is ge1/1. Switch identifies the host, and (config-ge1/1)# identifies the interface configuration mode.
The CLI prompt Switch(config-vlan2)# identifies the interface configuration pattern, and the configured vlan2 interface, Switch identifies the host, and (config-vlan2)# identifies the pattern.

1.2.3 CLI Pattern Classification

The CLI pattern is divided into four categories: general pattern, privileged pattern, global configuration pattern and configuration subpattern, while the configuration subpattern is composed of many CLI patterns.

Ordinary users can only access ordinary mode, privileged users can access all CLI modes.

Console and Telnet terminals enter normal mode first, and enter privileged mode after entering the enable command in normal mode and successfully verifying the password.On Telnet terminals, ordinary users can only stay in ordinary mode, not in privileged mode.Enter configure terminal in privileged mode, and CLI mode enters global configuration mode.Enter the relevant commands in global configuration mode to enter each configuration submode.

The following table lists the main CLI modes of switches:

Pattern	Description	Prompt	Command to enter mode	Exit mode command
Normal mode	Provides a display command to view the status information of the switch.	Switch>	The mode in which the terminal first enters.	There is no command to exit the mode on the Console terminal. Use the exit or quit command on the Telnet terminal to exit the Telnet terminal.
Privileged mode	In addition to displaying commands to view the status of the switch, it also provides commands such as debugging, version upgrading and configuration maintenance.	Switch#	Enter the enable command in normal mode.	Use the disable command to revert to normal mode. Use exit or quit commands on Console terminals to retreat to normal mode, and exit or quit commands on Telnet terminals to exit Telnet terminals.
Global configuration mode	Generic commands that cannot be implemented in the configuration subpattern, such as configuring static routing commands, are provided.	Switch(config)#	Type configure terminal in privileged mode.	Use the exit, quit, or end commands to exit into privileged mode.
Interface	Commands to	Port:	Enter the	Use the exit or quit

configuration mode	configure ports and VLAN interfaces are provided.	Switch(config-ge1/1)# VLAN Interface: Switch(config-vlan1)#	interface <if-name> command in global configuration mode.	commands to exit into global configuration mode and the end command to exit into privileged mode.
VLAN configuration mode	The command to configure the VLAN is provided.For example, commands to create and delete vlans.	Switch(config-vlan)#	Enter the vlan database command in global configuration mode.	Use the exit or quit commands to exit into global configuration mode and the end command to exit into privileged mode.
MSTP configuration mode	The command to configure MSTP is provided.For example, commands to create and delete MSTP instances.	Switch(config-mst)#	Enter the spanning-tree MST configuration command in global configuration mode.	Use the exit or quit commands to exit into global configuration mode and the end command to exit into privileged mode.
Terminal configuration mode	Commands are provided to configure the Console and Telnet terminals, such as a command to configure timeout for the terminal.	Switch(config-line)#	Enter the line vty command in global configuration mode.	Use the exit or quit commands to exit into global configuration mode and the end command to exit into privileged mode.

1.3 Command Syntax Introduction

1.3.1 Command Composition

The CLI command consists of a keyword and a parameter. The first word must be a keyword, followed by a word that can be either a keyword or a parameter.A command must have a keyword but may have no arguments.For example, the command write has only one keyword and no arguments.The command show version has two keywords and no arguments;The command vlan <vlan-id> has a keyword and a parameter;The

command instance <instance-id> vlan <vlan-id> has two keywords and two parameters and the keywords and parameters appear alternately.

1.3.2 Parameter Types

CLI commands have two types of arguments: required and optional.Mandatory arguments must be entered when entering a command, and optional arguments may or may not be entered.If the command vlan <vlan-id> parameter is a required parameter, this parameter must be input when entering the command;The argument in the command show interface [if-name] is optional and may or may not be entered when the command is entered.

1.3.3 Command Syntax Rules

The following rules must be met when describing commands in text:

1） keywords are directly expressed by words.

Command show version.

2）parameters must be enclosed by < >.

Command vlan <vlan-id>

3）If it is an optional argument, the argument must be enclosed in [ ] .

Command show vlan [<vlan-id>]

In this case, the < > of the parameter can be omitted and changed to:

Command show vlan [vlan-id]

The parameter vlan-id can be entered or not.

If it is a required parameter, the parameter cannot have [ ] .

4）if there are multiple keywords or parameters must choose one, use {} to enclose multiple keywords or parameters, multiple keywords or parameters with | separated, before and after | need a space.

Such as multiple keywords must be selected command:

Spanning -tree MST link-type {point-to-point | Shared}

You must choose between point-to-point and Shared.

Required commands with multiple parameters:

No arp {<ip-address> | <ip-prefix>}

Keywords and parameters mixed with mandatory commands:
Show spanning-tree MST {none|instance <0-15>}ng

5）if you can choose one of multiple keywords or parameters, enclose multiple keywords or parameters with [], and separate multiple keywords or parameters with |, with a space before and after |.
The commands are as follows:
debug ip tcp [recv | send]
The keywords recv and send can be either selected or not selected.
show ip route [<ip-address> | <ip-prefix>]
show interface [<if-name> | switchport]

6）If you have a keyword or argument or a set of keywords or arguments that you can select repeatedly, add the symbol "*" after the keyword or argument.
For example, the ping command:
Ping <ip-address> [-n <count> >0-l <size> >1-r <count> >1-r <count> >3-j <count> <ip-address>* >4-k <count> <ip-address>* >5-w <timeout>]*
-j <count> <ip-address>* -- multiple IP addresses can be entered repeatedly
-k <count> <ip-address>* -- -- multiple IP addresses can be entered repeatedly
The entire option can also be retyped.

6）Arguments are represented by one or more word descriptors, and if there are multiple words, each word is separated by the symbol "-", each of which is lowercase.
Correct parameter representation: <vlan-id>, <if-name>, <router-id>, <count>, etc.
Incorrect parameter representation: <1-255>, <A.B.C.D>, <WORD>, <IFNAME>, etc.

1.3.4 Command Abbreviation

When the user enters the command on the CLI interface, the keyword of the command can be abbreviated. CLI supports the prefix matching function of the command. As long as the input word matches the keyword prefix only, CLI parses the input word into a matching keyword. This makes it convenient for users to use CLI, and users can type in very few characters to complete a command, for example, the show version command can type only sh ver.

1.3.5 Grammar Help

Syntax help is set up in the CLI command-line interface to support help at each level of commands and parameters, described as follows:

1)input directly in a CLI mode? Key, the first keyword and its description of all commands in this mode are listed on the terminal. For example, Switch (config) #?.

2) enter the previous part of a command, then enter a space before entering it? Key, all keywords or parameters at the next level and their descriptions are listed on the terminal. For example, Switch#show?.

3) enter an incomplete keyword and enter it directly? Key, all keywords and their descriptions that match this input prefix are listed on the terminal. For example, Switch#show ver?.

4) enter the previous part of a command, then enter the space and then enter the Tabkey, all the keywords at the next level will be listed on the terminal, and if the next level is a parameter, it will not be listed.

5) enter an incomplete keyword and enter the TAB key directly. If only one keyword matches the input prefix, it is directly supplemented. If multiple keywords match the input prefix, all the matching keywords are listed on the terminal.

1.3.6 Command Line Error Message

If the command entered by the user fails the syntax check, the error message is displayed on the terminal, and the common error messages are as follows.

Error Message	Error Cause
Invalid input or Unrecognized command	No matching key found. The parameter input is incorrect. Too many keywords or parameters entered.
Incomplete command	The command input is incomplete, and the keywords or parameters are not entered.
Ambiguous command	Keyword input is incomplete, there are multiple keywords and input prefix match.

1.4 Command Line Shortcut

1.4.1 Line Edit Shortcut Key

The CLI command line interface supports line editing shortcut functions, and line editing shortcuts facilitate the input and editing of CLI commands. When you enter or edit a command, the user can use the line to edit the input of the command. The following table lists all the line editing shortcuts and the features that are implemented:

Shortcut Key	Function
Ctrl+p or↑ key	Last order
Ctrl+n or↓key	Next command
Ctrl+u	Delete the entire line
Ctrl+a	The cursor returns to the beginning of the line
Ctrl+f or→key	The cursor moves one grid to the right
Ctrl+b or←key	The cursor moves one frame to the left
Ctrl+d	Deletes the character the cursor is in
Ctrl+h	Deletes the first character of the cursor
Ctrl+k	Deletes all characters at and after the cursor
Ctrl+w	Deletes all characters before the cursor
Ctrl+e	The cursor moves to the end of the line
Ctrl+c	Interrupt, do not execute the command line.If the CLI is in global configuration mode or sub-configuration mode, the CLI falls back to privileged mode.If the CLI is in normal or privileged mode, the CLI mode remains unchanged, but the CLI starts a new line.
Ctrl+z	Same function as Ctrl+c.
Tab	This key is used after the input of incomplete keywords. If there is a keyword that matches the prefix of the input, the keyword is supplemented.If more than one keyword matches the prefix of the input, list all matched keywords.If there is no keyword match, the key is invalid.

Note: some Console terminals ↑, ↓, →, ← keys are not available.

1.4.2 Display Command Shortcuts

For the commands that begin with the show keyword, some display commands can not be displayed in one screen because they display a lot of contents, and the terminal provides

the function of split screen display. After a screen is displayed, the terminal waits for user input to determine the subsequent processing. The following table lists the display command shortcuts and their functions.

Shortcuts	Function
Space	Show the next screen
Enter	Show the next line
Ctrl+c	Interrupt command execution, exit CLI mode.
Other Key	Same function as Ctrl+c.

1.5 Command History

The CLI command line interface supports the history of the command, and can remember the 20 historical commands that the user recently used to save the most recently typed command by the user. You can use the show history to display the commands that have been entered, and you can also use the Ctrl + p, Ctrl + n, or the cursor to select the history command. The history command function allows the user to enter commands.

Chapter 2 System Management Configuration

Before learning the functional configuration of the switch, users need to master some basic configurations of the system management and maintenance of the switch. This chapter describes the basic configuration of these system management and maintenance, including the following:

- System safety configuration
- System maintenance and debugging
- System monitoring
- Profile management
- Software version upgrade

2.1 System Security Configuration

In order to prevent illegal user intrusion of the switch, the system provides several measures for system management security, mainly including:

- multi-user management control
- TACACS + Authentication Authorization
- Anonymous user password control
- Enable password control
- TELNET service control
- SNMP service control
- HTTP service control

2.1.1 Multi-user Management Control

The multi-user management not only ensures the security of the switch system, but also provides the capability of multiple users to manage and maintain the switch at the same time. The multi-user management ensures the system safety by giving each user a user name, password, and authority, and the user first needs to verify the user name and password when accessing the switch, and only if the user name and the password are correct and consistent, the user can verify the pass. The user is able to access the switch after authentication, but the user's permissions define the scope of the user's access to the switch.

The multi-user management divides the user's rights into two levels: normal users and privileged users. Normal users can only stay in the normal mode of the CLI command line interface, and can only use the display command to query the information of the switch. The privileged user can access all the modes of the CLI command line interface, and all commands provided by the CLI can be used to query both the information of the switch and to maintain and manage the switch.

The multi-user management function is not only applied to the Telnet terminal but also the Console terminal. You need to verify the user name and password when using the Console terminal to access the switch before you can access the CLI. You also need to verify the user name and password when the switch is accessed through the Telnet terminal, and only the user name and password can access the CLI only after the user name and password are verified.

The commands related to multi-user management are as follows:

The command	Description	CLI Model
username <user-name> password <key> {normal | privilege}	Add a user and modify the password and permissions of that user if the specified user already exists. The first parameter is the user name, the	global configuration mode

	second parameter is the password, the optional item represents the permission, normal represents the normal user, and privatege represents the privileged user.	
no username [user-name]	Delete one or all users. If you do not enter a parameter, it means deleting all users, and if you enter a parameter, you delete a user with a specified user name.	global configuration mode
show running-config	View the current configuration of the system, you can view the configuration of multi-user management.	Privilege mode

2.1.2 TACACS+ Certificate

The TACACS + authentication authorization provides for tighter user rights management, not only to verify the user's legitimacy, but also to authorize the command. After the TACACS + authentication is started, the user first needs to verify the username and password through the TACACS + server when accessing the switch, and only if the user name and password are correct and consistent. The user is able to access the switch after authentication.

TACACS+ also divides user permissions into two levels: ordinary users and privileged users. Ordinary users can only stay in the normal mode of the CLI command line interface, and privileged users can access all modes of the CLI command line interface. On the basis of the permission level, the command execution permission is also set, and the user enters a command (except enable, end and exit), all of which must be verified on the TACACS+ server, and the verification failure will not be executed.

The TACACS + authentication authorization feature is applied only to Telnet and SSH terminals and does not control the Console terminal. The username and password need to be verified when the switch is accessed through a Telnet or SSH terminal, and only the privileged user can pass through when the user name and password are verified to pass through. TACACS + authentication is also applied to WEB login, but only password privilege is verified, and no command authorization is made.

By default, the switch does not open the TACACS + function. In this case, the multi-user management function is used for Telnet, SSH, or WEB login. After the TACACS + function is opened, the multi-user management function can continue to be configured, but not actually used.

The commands related to TACACS authentication authorization are as follows:

The command	Description	CLI Model
tacacsplus enable	Turn on TACACS+TACACS+功能	global configuration mode
tacacsplus disable	Turn off TACACS+	global configuration mode
tacacsplus host A.B.C.D	Configure the primary server address, using Cisco's ACS is recommended	global configuration mode
tacacsplus key WORD	Configure the Shared key, which is used to encrypt the transmitted data and must be consistent with the configuration on the server	global configuration mode
tacacsplus auth-type (PAP|CHAP)	Select authentication methods, including PAP and CHAP.The PAP is the default, the password is enclosed in the field, and the CHAP encapsulates the MD5 checksum of the password.	global configuration mode
show tacacsplus	View TACACS+ configuration information	global configuration mode

no tacacsplus host	Clear the primary server address	global configuration mode
no tacacsplus key	Clear Shared key	global configuration mode

2.1.3 Enable Password Control

Enable password is used to control the switch from normal mode to privileged mode. The user can only view the switch information before enable password verification, and after enable password verification, the user can configure and maintain the switch.

The enable password is not attached to the user. Any user who logs in to a Console terminal or Telnet terminal must verify the enable password to enter privileged mode.

Enter enable command in normal mode, the terminal will prompt the user to enter password, at this time the user can enter enable password, if the password verification is successful, the terminal into privileged mode, otherwise, stay in normal mode, for ordinary users regardless of whether the password verification is successful can not enter privileged mode.

The enable password defaults to null, in which case the terminal enters privileged mode without prompting for a password after entering the enable command in normal mode.

Enable password related commands are shown in the following table:

The command	Description	CLI Model
enable password <key>	Set the enable password for the system.	global configuration mode
no enable password	Clear the enable password of the system and the enable password is empty.	global configuration mode
show running-config	View the current configuration of the system and see the configuration of the enable password.。	Privileged mode
enable	Interactive command, verify the enable password of the system, after the verification is successful, the terminal enters the privilege mode.	Normal mode

Note: For the security of the system, the administrator needs to set the enable password for the system.

2.1.4 TELNET Service Control

In some cases, the administrator does not need to remotely manage the switch, but only needs to manage the switch through the Console terminal locally. In order to improve the security of the system and prevent illegal users from logging into the Telnet terminal remotely, the administrator can turn off the Telnet service. Telnet service is turned on by default.

The relevant commands for Telnet service control are as follows:

The command	Description	CLI Model
security-manage telnet enalbe	Open the Telnet service.	global configuration mode
security-manage telnet disable	Close the Telnet service.	global configuration mode
security-manage telnet number <1-100>	The number parameter ranges from 1 to 100, with a default of 5 .	global configuration mode
security-manage telnet access-group <1-99>	Specifies a ACL group, turns on the source IP address control, and does not control the source IP address if the specified ACL group does not exist or is not a standard ACL group.	global configuration mode
no security-manage telnet access-group	Turn off the source IP address control.	global configuration mode
show security-manage	You can view the configuration of the service control.	privileged mode

2.1.5 SNMP Service Control

The SNMP service control can turn on / off the SNMP service and control the IP address of the access switch through the ACL.

The relevant commands for SNMP service control are as follows:

The command	Description	CLI Model
security-manage snmp enalbe	Open SNMP service.	global configuration mode
security-manage snmp disable	Turn off SNMP service.	global configuration mode
Security-manage snmp access-group <1-99>	Specifies a ACL group, turns on the source IP address control, and does not control the source IP address if the specified ACL group does not exist or is not a standard ACL group.。	global configuration mode
no security-manage snmp access-group	Turn off source IP address control.	global configuration mode
show security-manage	You can view the configuration of the service control.	privileged mode

2.1.6 HTTP Service Control

The HTTP service control can turn on / off the HTTP service and control the IP address of the access switch through the ACL.

The relevant commands for HTTP service control are as follows:

The command	Description	CLI Model
security-manage http enalbe	Open HTTP service.	global configuration mode
security-manage http disable	Turn off HTTP service.	global configuration mode
security-manage http access-group <1-99>	Specifies a ACL group, turns on the source IP address control, and does not control the source IP address if the specified ACL group does not exist or is not a standard ACL group.	global configuration mode
no security-manage http access-group	Turn off the source IP address control.	global configuration mode
show security-manage	You can view the configuration of the service control.	privileged mode

2.1.7 SSH Service Control

A service device. When the data transfer between the server and you is tampered with by the middleman, there will be serious problems. By using SSH, you can encrypt all the transmitted data, so that the "man-in-the-middle" attack is impossible and can also prevent DNS spoofing and IP spoofing. An additional benefit of using SSH, is that the transmitted data is compressed, so it can speed up the transmission. SSH has many functions, it can replace Telnet, it can provide FTP,PoP, and even provide a secure "channel" for PPP.

2.2 System Maintenance and Debugging

The basic system maintenance and debugging functions mainly include the following:

- Configure the host name of the system
- Configure the system clock
- Configure terminal timeout properties
- The system reset
- View system information
- Network connectivity debugging
- Detect network line distance
- Traceroute debugging
- Telnet client

2.2.1 Configure the Host Name of the System

The host name of the system is used to identify the switch, which facilitates the user to distinguish between different switches, while the host name of the system is part of the CLI prompt for the terminal. The host name for the system is the Switch.
The relevant commands for the host name of the system are as follows:

The command	Description	CLI Model
hostname <name>	Sets the hostname of the system.	global configuration mode
no hostname	Clear the hostname of the system, that is, the hostname back to the default value Switch.	global configuration mode
show running-config	View the current configuration of the system and see the configuration of the hostname of the system.	privileged mode

2.2.2 Configure the Clock of the System

The switch provides the function of real-time clock, through the command can set the current clock, can also view the current clock. The clock of the system is supplied by the internal power supply, which ensures the continuous operation of the real-time clock when the system is out of power, and does not need to reset the clock after the system starts.

The switch has set the clock when it leaves the factory, and the user does not need to set it any more. If the user finds that the time is not right, the user can reset the clock.
The commands related to the system clock are as follows:

The command	Description	CLI Model
set date-time <year> <month> <day> <hour> <minute> <second>	To set the current clock of the system, you need to enter the year, month, day, hour, minute and second parameters.	privileged mode
show date-time	Displays the current clock of the system.	Normal mode,privileged mode

2.2.3 Configure Terminal Timeout Property

For the security of the terminal, when the terminal does not have key input, the terminal will do exit processing for more than a certain period of time. Console terminal and Telnet terminal exit processing is different. For Console terminal, when terminal timeout, CLI mode retreats to normal mode, for Telnet terminal, when terminal timeout, Telnet connection is interrupted and Telnet terminal exits.

The terminal timeout is 10 minutes by default, and the user can also set the terminal to never timeout.
The commands related to the terminal timeout are as follows:

The command	Description	CLI Model
exec-timeout <minutes> [seconds]	Set the terminal time out time, and if the parameter is 0, the terminal will never time out.	Terminal configuration mode
no exec-timeout	Set the terminal timeout to the default, i.e.,10 minutes.	Terminal configuration mode
show running-config	View the system's current configuration and you can view the configuration of the terminal timeout.	privileged mode

2.2.4 System Reset

The system provides a reset method:

- Reset switch

The relevant commands for the system reset are shown in the following table:

The command	Description	CLI Model
Reboot	Reset switch	privileged mode

2.2.5 Viewing System Information

The system provides rich display commands to view the system's operating status and system information, which lists only a few common system maintenance display commands, as shown in the following table:

The command	Description	CLI Model
show version	Displays the version number of the system and the time when the file is compiled and connected.	Normal mode,privileged mode
show snmp system information	Displays the basic information of the system, including how long it runs after the system is started.	Normal mode,privileged mode
show history	Displays a list of commands that are most recently entered on the CLI command line.	Normal mode,privileged mode

2.2.6 Network Connectivity Debugging

In order to debug connectivity between the switch and another device in the network, the ping command needs to be implemented on the switch, ping the IP address of the other party on the switch, and if the switch receives the ping response from the other party, the

two ends are connected, otherwise the two ends cannot communicate.

The switch not only implements the ping command, but also supports a wide range of options on the ping command, and the user makes more accurate and complex debugging by using these options.

The ping command is as follows:

The command	Description	CLI Model
ping <ip-address> [-n <count> | -l <size> | -r <count> | -s <count> | -j <count> <ip-address>* | -k <count> <ip-address>* | -w <timeout>]*	You can also take one or more options without any options when in use. If you do not have any options, the most simple ping command. The command, when executed, type Ctrl + c to interrupt the execution of the command.	privileged mode

2.2.7 Detect Network Line Distance

The command	Description	CLI Model
show cable-diag interface IFNAME	Detect the distance of the network line of the electric port.	privileged mode

2.2.8 Traceroute Debugging

In order to debug which intermediate devices the switch and another device in the network are communicating through, the traceroute command needs to be implemented on the switch. When the traceroute command is used on the switch, specify the IP address of the other party, and the middle path will be displayed during the command execution.

The switch not only implements the trace-route command, but also supports a wide range of options on the trace-route command, which allows users to perform more accurate and complex debugging by using these options.

The trace-route command is as follows:

The command	Description	CLI Model
trace-route <ip-address> [-h <maximum-hops> | -j <count> <ip-address>* | -w <timeout>]*	You can use it without any options, or you can bring one or more options. If you don't have any options, it's the simplest trace-route command. When the command is executed, you can type Ctrl c to interrupt the execution of the command.	privileged mode

2.2.9 Telnet Client

The series of switches provide a Telnet client feature that allows users to remotely access other devices through the Telnet client.

The command	Description	CLI Model
telnet <ip-address>	Parameter is the IP address of the target device.	privileged mode

2.2.10 UDLD Configuration

UDLD (UniDirectional Link Detection unidirectional link detection): is a layer 2 protocol used to monitor the physical configuration of etheric links connected by optical fiber or twisted pair. When a unidirectional link can only be transmitted in one direction, such as I can send you the data, you can also receive it, but I can not receive the data you send me, UDLD can detect this condition, close the corresponding interface and send a warning message. One-way links can cause many problems, especially the spanning tree, which may cause loops. Note: UDLD requires devices at both ends of the link All support in order to function properly.

UDLD supports two working modes: normal (normal) mode (default) and radical (aggressive) mode.

Normal (normal) mode: in this mode, UDLD can detect one-way links and mark the port for undetermined state to generate Syslog, In other words, normal mode will shut down a port only if it can explicitly determine that the associated link is faulty for an extended per iod of time.

The command	Description	CLI Model
udld enable	Global enable UDLD function	global configuration mode
udld message time <time>	UDLD message sending interval	global configuration mode
udld port	Port enable UDLD	Interface configuration mode
udld aggressive	Enable port radical mode, default normal mode	Interface configuration mode
show udld <ifname>	Viewing Port UDLD Information	privileged mode

2.3 Profile Management

Configurations are divided into current configuration and initial configuration. The current configuration refers to the configuration of the system running time, which exists in the memory of the system, and the initial configuration is the configuration used when the system starts, and it exists in the FLASH of the system, that is, the configuration file. When the user executes the relevant command, the current configuration of the system is modified, and the current configuration is written to the initial configuration only after the save command is executed for the next boot of the system. When the user does not make any configuration after the system starts, the current configuration information of the system is the same as the initial configuration information.

The current configuration and the initial configuration are in the same format, both of which are command-line text format, which is very intuitive and easy for users to read. The format of the configuration file has the following characteristics:

- The configuration file is a text file.
- All saved is a command.
- Only non-default configurations are saved, and the default configuration is not saved.
- Commands are organized in CLI mode, and commands in the same CLI mode are organized together to form a segment between segments with the words "!" Separate from each other. For commands in global configuration mode, organize commands with the same function or similar functions into a segment to "!" Separate from each other.
- For commands in configuration submode, there is a space before the command, while for commands in global configuration mode, there is no need for spaces before the

command.

2.3.1 View Configuration Information

Viewing configuration information includes viewing the current configuration and initial configuration of the system. The initial configuration is actually the configuration file in FLASH. When the configuration file does not exist in FLASH, the system starts with the default configuration. If you look at the initial configuration of the system, the system will prompt that the configuration file does not exist.

The commands to view configuration information are as follows:

The command	Description	CLI Model
show running-config	View the current configuration of the system.	privileged mode
show startup-config	View the current configuration of the system.	privileged mode

2.3.2 Save Configuration

When the user has modified the current configuration of the system, the configuration needs to be saved to the configuration file, so that the configuration still exists after the next startup, otherwise, the configuration information is lost after the restart. The save configuration is to save the current configuration to the initial configuration.

The command to save the configuration is as follows:

The command	Description	CLI Model
write	Save the current configuration.	privileged mode

Note: users need to use this command to save the configuration after configuring the switch, otherwise the configuration will be lost after the system restarts.

2.3.3 Delete Profile

When the user wants the initial configuration of the system to return to the default configuration, the configuration file can be deleted, and the current configuration has no effect on the current configuration. If you want the current configuration of the system to return to the default configuration, you need to restart the switch. Users must be careful

when deleting configuration files, otherwise the configuration will be lost.

The command to delete the configuration file is as follows:

The command	Description	CLI Model
delete startup-config	Delete the configuration file for the system.	privileged mode

2.3.4 Download From the Configuration File

For the security of the configuration file, the user can use the command to upload the configuration file to the PC for backup. When the configuration of the system is abnormal lost or modified, the original configuration file can be downloaded from the PC to the switch. After downloading the configuration file, it has no effect on the current configuration of the system, and the configuration can take effect after the switch must be restarted. WEB can also be used to upload and download configuration files, the specific operation can refer to the WEB operation manual.

The commands downloaded on the configuration file are as follows:

The command	Description	CLI Model
upload configure <ip-address> <file-name>	When the configuration file is uploaded to the PC, the first parameter is the IP address of the PC, and the second parameter is the file name of the configuration file stored on the PC.	privileged mode
download configure <ip-address> <file-name>	When the configuration file is uploaded to the PC, the first parameter is the IP address of the PC, and the second parameter is the file name of the configuration file stored on the PC.	privileged mode

```
Switch#upload config 192.168.1.2 beifen.cfg
Do you wish to continue? [Y/N]: Y
Configure file is uploading......
% Transmission overtime, Destination host unreachable or TFTP service is not up
to.
```

Check whether the TFTP service is turned on? 192.168.1.2 can you Ping

Download and use TFTP protocol on configuration file, run TFTP client software on switch and TFTP server software on PC. The steps for downloading on the configuration file are as follows:

Step 1: build a network environment.

Step 2: start TFTP server software on PC and set up the directory where the configuration file is stored.

Step 3: Save the configuration on the switch.

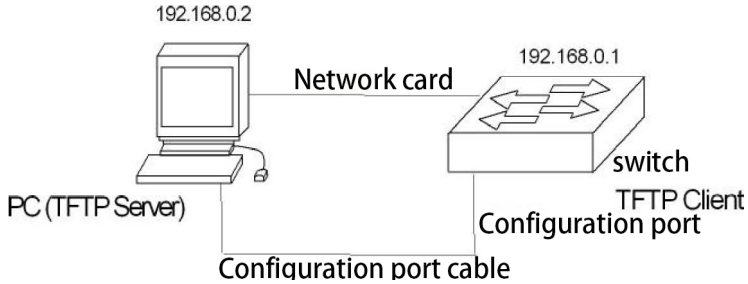
Step 4: Execute the profile upload command on the switch to back up the profile to the PC.

Step 5: When the switch needs the profile on the PC, execute the profile download command on the switch to download the profile on the PC to the switch.

Step 6: To make the configuration take effect, you must restart the switch.

Example: a switch that has been configured with VLAN and interface address needs to be downloaded on the configuration file.

Step 1: build the network environment shown below.

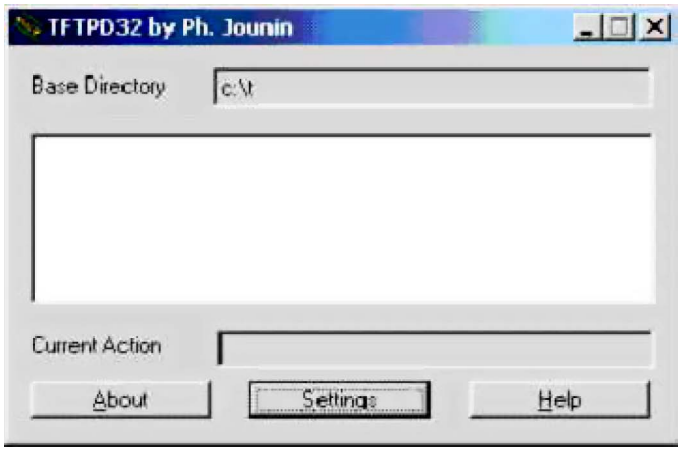


The configuration port of the switch is connected to a configuration terminal through the cable and connected to a PC through the network cable. Install TFTP Server, on PC to configure the Ethernet port IP address of PC, assuming that the IP address of PC is 192.

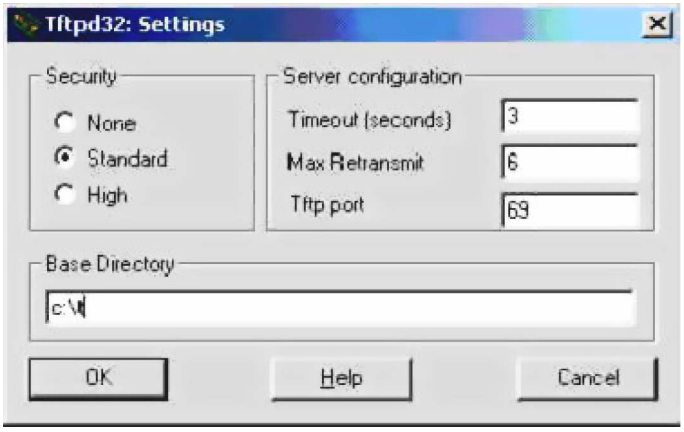
168.0.2. Then, configure the IP address of the switch, assuming that the IP address of the switch is 192 168. 0. 1. Ensure the connectivity between PC and switch.

Step 2: start the TFTP Server, configuration TFTP Server parameter.

Run the TFTP Server, window interface as shown below:



Then, set the directory for the backup configuration file. Specifically, click the[Settings] button to set the interface, as shown in the following figure:



Enter the file path in Base Directory. Click the [OK] button to confirm.

Step 3: execute the write command on the switch to save the current configuration to the configuration file.

Step 4: back up the file to PC and execute the command Switch#upload configuration 192.168.1.2 beifen.cfg.

Step 5: download the backup file to the switch if necessary and execute the command

Switch#download configuration 192.168.1.2 beifen.cfg.

Step 6: The configuration file you want to download can take effect. You must restart the switch and execute the command Switch # reset.

2.4 Software Version Upgrade

The switch supports online upgrades to the software version. The upgrade is done through the tool TFTP.

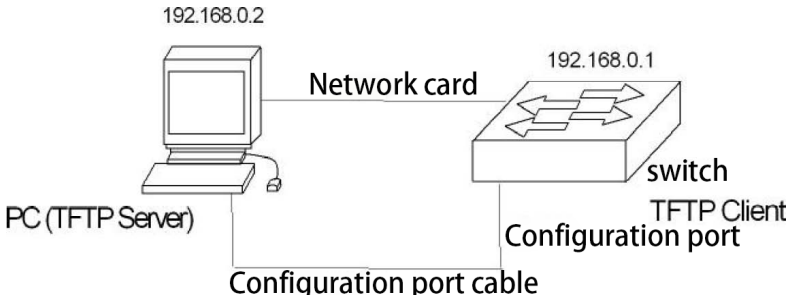
2.4.1 Softwate Version Upgrade Command

Upgrade the switch image file in global configuration mode with the following commands:
download image <ip-address> <file-name>
Where < ip-address > is the IP address of the PC running the TFTP server and < file-name > is the image file name saved on the TFTP server.
The switch cannot be powered off during the upgrade, otherwise the switch image file may be corrupted and the switch will not start. After the download, you need to restart the switch to run the newly downloaded image file program. The whole upgrade process will take a few minutes. Please wait patiently.
You can also upgrade the software version through WEB, the specific operation can refer to the WEB operation manual.

2.4.2 Software Upgrade Process

The steps to upgrade the image file are as follows:

Step 1: build an upgrade environment. As shown below.

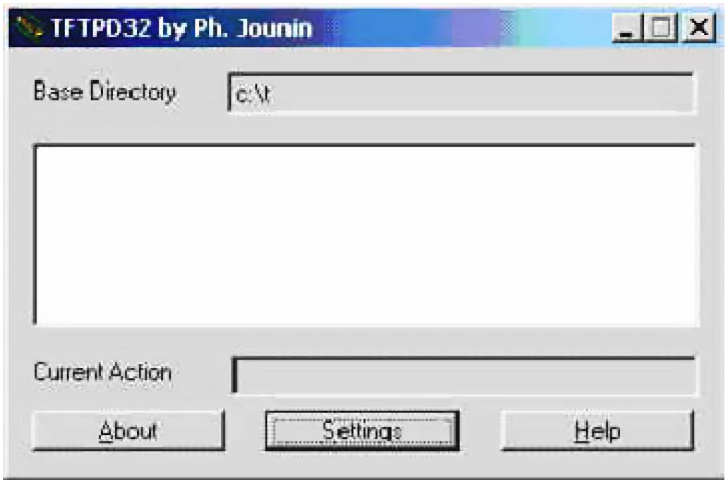


The construction process is as follows:

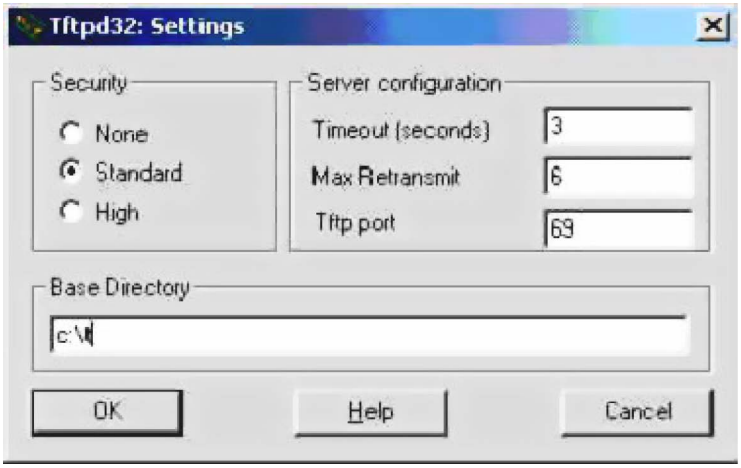
- Connect the Console port of the switch to a configuration terminal (PC). Through the cable
- Install TFTP Server. on PC
- When a new image file is copied to a path of the PC, it is assumed here that the path is c: t;
- Configure the Ethernet port IP address of the PC, where the IP address of the PC is assumed to be 192.168.0.2.
- Configure the IP address of the switch, assuming the switch has an IP address of 192.168.0.1.

Step 2: Run TFTP Server, and configure the TFTP server.

First: run the TFTP Server. TFTPD32 window interface as shown below:



Then: Set the TFTP Server file directory. After the TFTP server is started, reset the TFTP Server file directory and copy the image file to be loaded into this directory. Specifically, click the[Settings] button to display the setting interface of the TFT PD32, as shown in the following figure.



Enter the file path in Base Directory. Click the [OK] button to confirm.

Step 3: Upgrade the file.

First: Connect the port of the switch to the PC running the TFTP Server program through the Ethernet line. Use the ping command to detect if the host is in communication with the switch.

Then enter the command at the HyperTerminal Switch # prompt:

Switch # download image 192.168. 0.2 switch.img, enter, and wait for the upgrade file to complete.

Software is updating. Please wait and down't powerdown!

……

Updating is completed. Do you wish to reset?[Y/N]

After file transfer, you will be prompted if you need to restart the switch; in general, we recommend that you select'Y'to restart the switch, because the system upgrade can only take effect after restart; if your configuration file does not save, you can first select'N 'and do not restart; after completing other operations such as storage, restart the switch.

Switch#

Note:

During switch upgrade, power cannot be cut off .

Step 4: restart the switch.

Switch# reset

Chapter 3 Port Configuration

This chapter describes the configuration of the port, mainly including the following:

- General configuration of ports
- Configure MIRROR
- Configuring the STORM-CONTROL
- Configuring the STORM-CONSTRAIN
- Configure FLOW-CONTROL
- Configure port bandwidth
- Configure TRUNK
- Configure oversized frames

3.1 Port General Configuration

The administrator can close the port by configuring the port of the switch to control the access of the user under the port, if the user under the port is not allowed to access the network. This section describes the general configuration of ports, including:

- Opening and closing of ports
- Rate configuration of ports
- Displays information about the port.

3.1.1 Port Rate Configuration

The default rate configuration for all ports is adaptive (autonegotiate).

The following command configures the rate of ports in interface configuration mode:

speed {autonegotiate |full-1000 |full-100 |full-10 |half-100 |half-10 }

autotiate

Full-100

Full-10

Half-100

Half-10

For example, the rate of port 1/1 is configured to be full-duplex 100M:
Switch(config-ge1/1)# speed full-100

3.1.2 Display Port Information

The following command displays information for one or more ports in normal or privileged mode:
show interface [if-name]
for example, information that shows port 1/1:
Switch# show interface ge1/1
for example, displays information for all ports:
Switch# show interface

3.2 Configure MIRROR

Port mirroring is a very useful feature for listening for the traffic of packets received and sent by one or more ports. it can use mirrored ports to monitor packets received and sent by one or more ports. The switch supports port mirroring, which listens for incoming and outgoing data from other ports. A mirror port can listen to multiple ports at the same time. This section focuses on the configuration of MIRROR, including the following:

- Configure the listening port and the monitored port of the MIRROR
- Display MIRROR configuration

3.2.1 Configure the Monitor Port and Monitored Port of MIRROR

When the administrator configure the listening port, you need to enter this interface configuration mode to set the monitored port, such as setting the port ge1/1 listening port ge1/2, you need to enter the port ge1/1, type the command: Switch (config-ge1/1) # mirror interface ge1/2 direction both, the port ge1/1 is set to the listening port, and the ge1/2 is

set to the monitored port.

The command to set the monitored port is as follows:

Switch(config-ge1/1)#mirror interface <if-name> direction {both | receive | transmit}

At this point, the port ge1/1 is set to the listening port, < if-name > is set to the monitored port, and the following {both / receive / transmit} indicates the direction of listening: receive indicates listening for received packets; transmit listens for packets sent; and both listens for all packets sent and received. For example:

Switch(config-ge1/1)#mirror interface ge1/2 direction both

Represents the packets sent and received by the setting port ge1/1 listening port ge1/2.

If you are setting up multiple listening ports, you need to execute multiple commands.

The administrator can cancel the monitored port in the interface configuration mode, and the command is as follows:
Switch(config-ge1/1)#no mirror interface <if-name> direction { receive | transmit}

At this point < if-name > is a port that is no longer being monitored. {receive / transmit} indicates the direction in which it is not monitored: receive indicates that it does not listen for received packets; transmit indicates that it does not listen for sent packets. For example:
Switch(config-ge1/1)# no mirror interface ge1/2 receive
Indicates that the set port ge1/1 no longer listens for packets received by the port ge1/2.

The listening port will also be cleared when all monitored ports are cancelled.

3.2.2 Display MIRROR Configuration

Administrators can view the MIRROR configuration that has been set up with the following command in normal mode or privileged mode:
Switch# show mirror

The following points need to be noted:

- A port cannot be set to both a listening port and a monitored port.
- There can only be one listening port, but there can be more than one listening port.

3.3 Configure STORM-CONTROL

In real life, a NIC card sends a very high rate of unicast, multicast, and broadcast packets to cause a network to fail, All ports of the switch support the suppression of broadcast packets, multicast packets, and DLF packets.
This section describes the configuration of the STORE-CONTROL, mainly including the following:

- Default configuration
- broadcast suppression configuration
- multicast suppression configuration
- DLF suppression configuration
- Display the STORE-CONTROL configuration

3.3.1 Default Configuration

The switch supports the setting of the broadcast, multicast, and dlf switches for each port, and the three settings have a separate rate limit. The default port's broadcast packet, the multicast packet, and the DLF packet rate limit are all closed. The purpose of this function is to form a broadcast storm on the network.

3.3.2 Display MIRROR Configuration

The following command configures the broadcast suppression for this port in the interface configuration mode:
storm-control broadcast

The following command cancels the configuration of the broadcast suppression for this

port in the interface configuration mode:
no storm-control broadcast

3.3.3 Multicast Supperssion Configuration

The following command configures multicast suppression for this port in interface configuration mode:
storm-control multicast

The following command cancels the configuration of multicast suppression for this port in interface configuration mode:
no storm-control multicast

3.3.4 DLF Suppression Configuration

The following command configures the DLF suppression for this port in the interface configuration mode:
storm-control dlf

The following command cancels the configuration of the DLF suppression for this port in the interface configuration mode:
no storm-control dlf

3.3.5 Suppression Rate Configuration

The following command configures the rate of suppression for this port in the interface configuration mode:
storm-control ratelimit { broadcast | dlf | multicast } <1- 1048575 >

3.3.6 Show STORM-CONTROL Configuration

The following command displays the STORM-CONTROL configuration in normal or privileged mode:
show storm-control

3.4 Configure STORM-CONSTRAIN

Port flow threshold control function is used to control message storms on Ethernet. The port with this function will detect the unicast message traffic, the multicast message traffic and the broadcast message traffic at the arrival port regularly. If a certain type of message traffic exceeds the predetermined upper limit threshold, the user can configure to block the port or close the port, and whether to send Trap and Log information.

When a certain type of message traffic exceeds the preset upper limit threshold of this kind of message, the system provides two processing methods:
(1) block mode: if the traffic of a certain kind of message on the port is greater than the upper limit threshold, the port will pause the forwarding of this kind of message (other types of messages will be forwarded as usual), the port is in a blocking state, but the port still counts this kind of message.
(2) shutdown mode: if the traffic of a certain kind of message on the port is greater than the upper limit threshold, the port will be shut down and the system will stop forwarding all messages. You can restore the port state by executing the undo shutdown command, or by canceling the port traffic threshold configuration.

Note: for a certain type of message traffic, it can be suppressed by this function or the storm suppression function of Ethernet port, but the two functions can not be configured at the same time, otherwise the suppression effect is uncertain. For example, the unicast message flow threshold control function and unicast storm suppression function of the port can not be configured at the same time.

The CLI configuration command is as follows:

The command	Description	CLI Model
storm-constrain (broadcast|multicast|unicast) min-rate <1-1488100> max-rate <1-1488100>	Storm control of broadcast, multicast, or unknown unicast messages under the interface	Interface configuration mode
no storm-constrain (broadcast|multicast|unicast|all)	Cancel Storm Control	Interface configuration mode
storm-constrain action (block|shutdown)	The action of storm control is configured. By default, the message is not	Interface configuration mode

	subjected to storm control	
no storm-constrain action	Turn on the switch to log or report alerts during storm control	Interface configuration mode
storm-constrain enable (log|trap)	Switch on the log or report the alarm when the storm control is turned off	Interface configuration mode
no storm-constrain enable (log|trap|all)	Switch on the log or report the alarm when the storm control is turned off	Interface configuration mode
storm-constrain interval <6-180>	Configure the detection interval for storm control, which is 5 seconds by default.	Interface configuration mode
no storm-constrain interval	Restore the detection interval of storm control to the default value	Interface configuration mode
no storm-constrain	Delete the storm control function of the interface	Interface configuration mode
show storm-constrain	View storm control information for all interfaces	Interface configuration mode
show storm-constrain interface IFNAME	View storm control information for the interface	Interface configuration mode

Configuration description:

(1) View the storm control information description table for the interface.

Roject	Description
interface	Interface name
type	Message Type (1) Broadcast - broadcast message;(2) Multicast - multicast message;(3) unicast - unicast message.
rate	Min- low threshold; max- high threshold

action	Action of storm control, including (1) block-blocking message; (2) shutdown-close interface
punish-status	The message status of the current interface includes (1) block-when the rate is greater than max-rate and the storm control action is the blocking message, the status is the blocking message; (2) Normal-normal forwarding; (3) shutdown-when the rate is greater than max-rate and the storm control action is the shutdown interface, the state is the close interface
trap	Alarm switch status, on/off
log	Log switch status, on/off
interval	The time for the last storm to control the penalty
ast-punish-time	The time interval for the storm control, in seconds, the default value is 5 seconds

(2) The storm control action is configured by executing the storm-constraint action command, and the high and low threshold of the storm control is configured by executing the storm-constrin command, and the storm message can be controlled to prevent flooding. In the storm control detection time interval, when the average rate of receiving a broadcast, a multicast or a unicast message on an interface is greater than a specified high threshold, the storm control will block the interface or close the interface processing according to the configured action. When the storm control action is a blocking message, if the traffic is below the minimum threshold, the interface is restored to The normal forwarding state; when the storm control action is to close the interface, the interface cannot be automatically restored, and the no shutdown command is required to be manually executed to recover, and the shutdown action configuration can be restored by removing the port storm.

(3) Port traffic exceeds the upper limit threshold or outputs log / trap information from the lower limit threshold.

3.5 Configure FLOW-CONTROL

FLOW-CONTROL is used to prevent data packet loss in case of port blocking. In the half-duplex mode, the flow control is realized by a Backpressure technique, so that the

information source reduces the transmission rate. In full-duplex mode, traffic control follows the IEEE802.3 standard, and the blocking port sends a "Pause" packet to the information source to suspend transmission.

This section describes the configuration of FLOW-CONTROL, mainly including the following:

- Default configuration
- Set port send side flow control
- Set up port receiving side flow control
- Turn off port flow control
- Display flow control information

3.5.1 Default Configuration

The switch supports sending and receiving flow control for each port. The default port does not turn on the flow control feature.

3.5.2 Set Port Receiving and Sending Side Flow Control

The following command configure port reception and send side flow control open in interface configuration mode:

flowcontrol

3.5.3 Close Port Control

The following command turns off port send and receive side flow control in interface configuration mode:

no flowcontrol

3.5.4 Display Flow Control Information

The following command displays flow control information for all ports in normal or privileged mode:

show flowcontrol

The following command displays the flow control information for a port in normal or privileged mode:
show flowcontrol interface <if-name>
Where < if-name > is the port name where you want to query flow control information.

3.6 Configure Port Bandwidth

Port bandwidth controls the rate at which the port is sent and received.

This section provides a detailed description of the configuration of the port bandwidth, including the following:

- Default configuration
- Set port sending or receiving bandwidth control
- Unport sending or receiving bandwidth control
- Displays the bandwidth control for the port configuration.

3.6.1 Default Configuration

The switch supports setting the send and receive bandwidth for each port. The default port does not have bandwidth control.

3.6.2 Set Port Send or Receive Bandwidth Control

The following command sets port send or receive bandwidth control in interface configuration mode:
portrate {egress | ingress} <rate>
egress represents bandwidth control over the transmitted packet.
Ingress represents bandwidth control over received packets.
<rate>represents the value of the bandwidth to be set, ranging from 1 ≤ 1024000 in kbits.

3.6.3 Cancel Port Send or Receive Bandwidth Control

The following command cancels the port's bandwidth control in interface configuration mode:no portrate {egress | ingress}
Egress means to cancel the bandwidth control of sending packets.
Ingress means to cancel the bandwidth control for receiving packets.

3.6.4 Displays the Bandwidth Control for the Port Configuration

The following command looks at the bandwidth control of the port configuration in either a normal mode or a privileged mode:
show portrate interface <if-name>
where < if-name > is the port name where you want to query bandwidth control information.

```
Switch#show portrate ?
  IFNAME   Interface to display
  <cr>
Switch#show portrate   ge1/1
Port      Egress Rate kbits     Ingress Rate kbits
-----     ----------------      ----------------
ge1/1                off                   off
```

3.7 Configure TRUNK

TRUNK aggregates multiple ports into one logical port, which can be used to increase bandwidth, provide redundant backup connections, and can also be used to load balance. when trunk group is used as output logical port, the switch will select a port from the port group to send the packet according to the aggregation policy set by the user. The configuration of port and aggregation policy of trunk group is done by software, but the forwarding of

data stream is done by hardware.

All ports in the TRUNK group must be configured at the same speed and in full duplex mode. Switches can support up to 8 groups of TRUNK, up to 8 TRUNK members per group. It is important to note that each port can only belong to one TRUNK group.

LACP protocol is a kind of protocol based on IEEE802.3ad standard. LACP protocol aggregates control protocol data unit through LACPDU (Link Aggregation Control Protocol Data Unit, link) and interacts with opposite end information.

The interface in the aggregation group enables the LACP protocol, which notifies the opposite end of its system LACP protocol priority by sending LACPDU, the LACP protocol priority of the system MAC, port, the port number, and the operation Key. After receiving the LACPDU, the information is compared with the information received by other interfaces in order to select the interface that can be in the Selected state, so that the two sides can reach an agreement that the interface is in the Selected state.

Operation Key is a combination of configurations automatically generated by aggregation control according to some configurations of member ports during link aggregation, including port rate, duplex mode, up/down status, link type (that is, Trunk,Hybrid,Access type) of the default VLAN ID, port allowed to pass through the port, and so on. In the aggregation group, the member port in the Selected state has the same operation Key.
This section describes the configuration of TRUNK in detail, including the following:

- LACP protocol configuration.
- The configuration of the trunk group.
- TRUNK member port configuration
- TRUNK load balancing Policy configuration
- Display of TRUNK

3.7.1 LACP Protocol Configuration

The command	Description	CLI Model
lacp system-priority <1-65535>	Set the lacp system priority	Global configuration mode
no lacp system-priority	Restore System Priority Default 32768	Global configuration mode
lacp max-active-link-number <1-8>	set up lacp to activate the upper limit of the aggregate	Global configuration

	port	mode
no lacp max-active-link-number	The recovery lacp activates the default upper limit 8 of the aggregate port.	Global configuration mode
lacp port-priority <1-65535>	Set lacp port priority.	Interface configuration mode
no lacp port-priority	restore port priority default 32768	Interface configuration mode
lacp timeout (short|long)	Set lacp port timeout, missing governor timeout	Interface configuration mode
show lacp system-id	Show the lacp system case	privileged mode
show lacp counter <1-8>	Shows the tab aggregation port statistics.	privileged mode
show lacp counter	Displays statistics for all lacp aggregation ports	privileged mode
clear lacp <1-8> counters	Clear the statistic all lacp polymerization ports	privileged mode
clear lacp counters	Clear statistics for all lacp polymerization ports	privileged mode

The commands related to dynamic link aggregation need to be configured, and the connected end-to-end switch should also be configured accordingly, as shown below.

```
Switch(config)#trunk 1 dynamic
Switch(config)#int trunk1
Switch(config-trunk1)#trunk int ge1/2
Switch(config-trunk1)#end
Switch#show lacp summary
  Aggregator trunk1 3001
  Admin Key: 0001 - Oper Key 0004
    Link: ge1/1 (2001) sync: 1
```

3.7.2 TRUNK Group Configuration

The following command creates a manual trunk group in global configuration mode:

Trunk <trunk-id> Create a trunk group, the <trunk-id> value range is 1-8, the trunk-id> value range is 1-8, the TRUNK group ID number to be created can be configured with a maximum of 8 groups of TRUNK; the interface name of the TRUNK group after the creation is a trunk + id number, such as the trunk + id number of the TRUNK

group with group ID number 1. You can enter the interface configuration mode with the "interface trunk+id号" command in the configuration mode, and then perform the operation on the trunk group, such as using the command interface tru Nk1 enters the interface mode of TRUNK 1 to configure TRUNK 1.

The following command creates a static LACP TRUNK group in global configuration mode:
trunk <1-8> dynamic

The following command removes a TRUNK group in global configuration mode:
no trunk <trunk-id>
When you delete a TRUNK group, you must ensure that the TRUNK group does not have a member port.

3.7.3 TRUNK Group Member Port Configuration

The following command adds a new TRUNK group member port in interface configuration mode:

trunk interface IFNAME (passive|)

< if-name > is the port name that needs to be added to the TRUNK group and must be a layer 2 interface. Each group of TRUNK can add up to eight layer 2 interfaces. If the TRUNK group is a static LACP TRUNK group, the add interface defaults to the active state or can be configured to the passive state.
The following command removes all member ports of the TRUNK group in interface configuration mode:
no trunk interface
The following command removes the specified TRUNK group member port in interface configuration mode:

no trunk interface <if-name>
It can use this command multiple times to delete multiple member ports of the TRUNK group.

3.7.4 TRUNK Load Balancing Policy Configuration

The following command sets the load balancing policy for the trunk in the interface configuration mode:
trunk load-balance {dst-mac | dst-ip | src-dst-mac | src-dst-ip | src-mac | src-ip}
Dst-mac -------- balanced strategy based on objective MAC
Dst-ip ---------- balanced strategy based on destination IP
Src-dst-mac -- balanced strategy based on source MAC and destination MAC
Src-dst-ip ---- -balanced strategy based on source IP and destination IP
Src-mac -------- balanced strategy based on source MAC
Src-ip ---------- balanced strategy based on source IP

The following command sets the default TRUNK load balancing policy in interface configuration mode:

The default port load balancing policy for notr < load-balance is src-dst-mac (based on source MAC and destination MAC).

3.7.5 TRUNK Display

The following command views all TRUNK group configurations in normal or privileged mode:
show trunk

The following command views the specified TRUNK group configuration in normal or privileged mode:
show trunk <trunk-id>
Where < trunk-id > is the ID number of the TRUNK group to query.

3.8 Super Frame

3.8.1 Super Frame Introduction

In order to realize that ports can receive very large frames, ports can be set to support a specific very large frame length.

3.8.2 Super Frame Configuration

The port configuration is configured to support the jumbo frame length, and in config mode, enter the port configuration mode, such as interface ge1/1, to execute the following command:
Switch(config-ge1/1)# jumbo frame 2000

Maximum frame length supported by the display port
Switch(config)# jumbo frame 2000
Switch(config)#end
Switch#show jumbo frame
jumbo frame (bytes) 2000

3.9 Configure Redundant Port

In some special cases, such as the need to focus on ensuring the stability of some servers linked to the network, the redundant port of the switch can provide two ports to be linked to the server, and ensure that in a port-linked network where the server has only one LINK UP, the system immediately enables the other port when LINK DOWN occurs on one port.

When a port is in LINK UP in a redundant port group, we call it Active state; on the contrary, if a port is in LINK DOWN in redundant port group, we call it Disable state.

This section focuses on the configuration of redundant ports, including the following:

- Configuration of redundant ports
- Display of redundant ports

3.9.1 Configuration of Redundant Port

The switch can be configured with 8 sets of redundant ports; one set of redundant ports can only be configured with 2 ports; one port can only be configured in one redundant port group.

A redundant port group can be configured with primary-port and secondary-port. When a redundant port group is configured:

1, when the two ports are in the LINK UP state at the same time, the primary-port is set to the Acitve state and the secondary-port will be set to the Disable state;

2, if only one port is in the LINK UP state, the current LINK UP port is set to the Active state, and the other port is in the Disable state;

3, otherwise both ports are in Disable state.

If a LINK DOWN event occurs on a port out of the Active state, another port will be attempted to be set to the Active state.

Another configuration parameter is force-switch, which is when secondary-port is in the Disable state of Active,primary-port, and if the LINK UP event occurs in primary-port, it is decided whether to switch back to primary-port to Active,secondary-port to Disable. If force-switch is configured to be enable, then the switch is forced, otherwise it will be guaranteed Leave the port status of the original redundant port group.

The command	Description	CLI Model
redundant-port <1-8> primary-port IFNAME secondary-port IFNAME [force-switch]	Configure a set of redundant ports, < 1 ≤ 8 > is the group number Primary-port IFNAME is the name of the main port interface,	Global configuration mode

	Secondary-port IFNAME is the name of the standby port interface, Whether force-switch enables forced switching switches.	
redundant-port <1-8> force-switch	Enable mandatory switching switches for redundant ports.	Global configuration mode
no redundant-port <1-8>	Delete redundant port groups.	Global configuration mode
no redundant-port <1-8> force-switch	Turn off the forced switch on the redundant port.	Global configuration mode

3.9.2 Redundant Port Display

Display a command for a redundant port

The command	Description	CLI Model
show redundant-port	Display the configuration of all redundant port groups in the system	privileged mode

3.10 Configure LLDP

At present, there are more and more kinds of network equipment and their configuration is complicated. In order to make the equipment of different manufacturers discover and exchange their system and configuration information in the network, a standard information exchange platform is needed.

LLDP (Link Layer Discovery Protocol, link layer discovery protocol) is generated in this context. It provides a standard link layer discovery method, which can organize the main capabilities of the local device, management address, device identification, interface identification and other information into different TLV (Type/Length/Value, type / length / value), and encapsulate the LLDPDU (Link Layer Discovery Protocol Data Unit, link layer discovery protocol. The data unit is published to the neighbor directly connected to itself, and the neighbor receives this information and saves it in the form of standard MIB (Management Information Base, management information base for the network management system to query and judge the communication status of the link.
This section focuses on the configuration of LLDP, including the following:

- Configuration of LLDP
- Display of LLDP

3.10.1 LLDP Configuration

There are four modes of LLDP port operation:

TxRx: sends and receives LLDP messages.

Tx: only sends and does not receive LLDP messages.

Rx: only receives and does not send LLDP messages.

Disable: neither sends nor receives LLDP messages.

When the LLDP operating mode of the port changes, the port will initialize the protocol state machine. In ord to avoid that frequent change of the port operation mode, the port is continuously perform the initialization operation, the port initialization delay time can be configure, and the initialization operation is performed for a period of time when the port operation mode is changed.

The command	Description	CLI Model
lldp global enable	LLDP global enable command	Global configuration mode
lldp hold-multiplier <num>	Multiple LldpTTL	Global configuration mode
lldp timer [<reinit-delay><time>][< tx-delay><time>][< tx-interval ><time>]	Configure LLDP various timers	Global configuration mode
lldp enable	Enable interface LLDP	Interface configuration mode
lldp admin-status{ disable| rx|tx|rxtx}	Configure LLDP port working mode	Interface configuration mode
lldp check-change-interval	Configure the refresh interface	Interface

<time>	information interval	configuration mode
lldp management-address <A.B.C.D>	Configuration interface LLDP management address	Interface configuration mode
lldp tlv-enable{ dot1-tlv| dot3-tlv|med-tlv }	Configuration interface LLDP expansion capability set switch	Interface configuration mode

3.10.2 LLDP Display

LLDP Commands

The command	Description	CLI Model
show lldp configuration [ifname]	display lldp configuration information	privileged mode
show lldp local-information [ifname]	Show lldp local information	privileged mode
show lldp neighbor-information [ifname]	display lldp neighbor information	privileged mode
show lldp statistics [ifname]	Display lldp message statistics	privileged mode
show lldp status [ifname]	Displays the lldp status information	privileged mode

Chapter 4 Port -Based MAC Security

This chapter introduces the port-based MAC security configuration, including the following:

- Introduction
- MAC binding configuration
- MAC filtering configuration
- Port learning restriction configuration

4.1 Introduction

Port-based MAC security can provide three functions: MAC binding, MAC filtering and port learning control to improve the security performance of switch layer 2 forwarding.

MAC binding can bind MAC and port together, restricting a specified MAC address to access the network only on a specified port; at the same time, this port can only allow these bound MAC addresses to access the network; a port can bind multiple MAC addresses at the same time. Mac binding can be applied to a specified port at the same time as 802.1x. This feature is very useful for devices that do not have 802.1x functionality or are not convenient to use 802.1x, such as printers, file servers, and so on.

MAC filtering prevents some specified MAC addresses from accessing the network, mainly to prevent illegal devices from accessing the network. When a MAC address is configured as MAC filtering, the MAC address cannot access the network at any port of the switch, nor can it receive packets whose destination MAC is these specified MAC addresses. As with MAC bindings, one port can configure multiple MAC filtered MAC addresses at the same time. In an application, if some virus software attacks this network through forged MAC addresses, in addition to ACL, you can also use MAC Filtering to access and control attacks on these forged packets.

Port learning control can control the number of MAC addresses that a port can learn dynamically. If a port specifies the number of MAC addresses it can learn dynamically, when the number of MAC addresses learned by the port is equal to the number of port configurations, the new MAC address will no longer be learned and packets for these new MAC addresses will be discarded.

It should be noted that the MAC address referred to herein is actually the MAC + VID, and the description later in this chapter will not be described again. In addition, that MAC bind function and 802.1x can be configure at one port at the same time; the MAC filter and port learn limit can be configured at one port at the same time; the MAC binding function, 802.1x and MAC filtering, and the port learning limit can not be configured to the same port at the same time.

4.2 MAC Binding Configuration

The MAC binding configuration supports manual binding of MAC addresses and automatic binding of MAC addresses. Manual binding of MAC addresses is when the user enters the MAC address one by one through the command to bind to the port. Automatic binding MAC address is to read out the existing entries of the port in the layer 2 hardware forwarding table and bind the MAC address directly. The command to read the layer 2 hardware table is Show bridge fdb.

Configuration command

The command	Description	CLI Model
switchport-security mac-bind HHHH.HHHH.HHHH vlan <1-4094>	Manually bind a MAC address to an interface.	Interface configuration mode
switchport-security mac-bind auto-conversion number <1-16383>	The specified number of MAC addresses of an interface is automatically converted to a MAC binding configuration.	Interface configuration mode
switchport-security mac-bind auto-conversion vlan <1-4094>	The MAC address of the specified VLAN for an interface is automatically converted to a MAC binding configuration.	Interface configuration mode
show port-security mac-bind [IFNAME]	Display MAC binding configuration	privileged mode

Note:

The reason for the invalid or failed MAC address binding may be as follows:

This port has been configured for 802.1x;

The port has configured the MAC filter or configured the port learning limit;

The MAC address has been bound to other ports or MAC filtering is configured;

The switch's L2 table is full.

4.3 MAC Filter Configuration

The MAC filtering configuration supports the manual binding of the MAC address and the automatic binding of the MAC address. The manual configuration of MAC filtering is the binding of the user to the port that needs to be filtered by the command one by one. The automatic configuration MAC filtering is to read out the existing entries in the two-layer hardware forwarding table and directly perform the MAC filtering configuration. The command to read the two-layer hardware table is Show bridge fdb.

Configuration command

The command	Description	CLI Model
switch port-security mac-filter HHHH.HHHH.HHHH vlan <1-4094>	Manually configure MAC filtering for an interface	Interface configuration mode
switch port-security mac-	Automatically converts the	Interface

filter auto-conversion number <1-16383>	specified number of MAC addresses for an interface to the MAC filtering configuration	configuration mode
switch port-security mac-filter HHHH.HHHH.HHHH vlan <1-4094>	Automatically converts the MAC address of the specified VLAN of an interface to the MAC filtering configuration	Interface configuration mode
show port-security mac-filter [IFNAME]	Display MAC binding configuration	privileged mode

Note:

The reason for the invalid or failed MAC address binding may be as follows:

This port has been configured for 802.1x;

The MAC address has been bound to other ports or MAC filtering is configured;

The switch's L2 table is full.

4.4 Port Learning Limit Configuration

The switch can configure the maximum number of dynamic learning addresses per port. If a port is configured with the number of dynamic learning MAC addresses, the port can only learn the corresponding number of MAC addresses, and when the number of MAC addresses exceeds this number, it cannot be learned and forwarded on this port.

Without configuring learning restrictions, a port can learn up to 16383 MAC addresses.

Configuration command

The command	Description	CLI Model
switchport port-security learn-limit <0-16383>	Configure the number of MAC addresses that an interface can learn.	Interface configuration mode
no switchport port-security learn-limit	Delete the number of MAC addresses that an interface can learn.	Interface configuration mode
show port-security learn-lmit [IFNAME]	Display port learning configuration	privileged mode

Configuration Example

configuration port ge1/5 can only learn 7 MAC addressesSwitch#configure terminal

```
Switch(config)interface ge1/5
Switch(config-ge1/5)switchport port-security learn-limit 7
```

Note:

The reason for invalid or failed port learning may be as follows:

The port has been configured with a MAC binding or 802.1x protocol enabled.

Chapter 5 Port IP and MAC Bind

This chapter introduces the configuration of port IP and MAC binding, including the following:

- Introduction
- IP and MAC binding configuration
- Configuration Example
- Configuration troubleshooting

5.1 Introduction

Configuring IP and MAC binding on layer 2 switch ports is a static defense against ARP attacks. ARP attackers attack users by sending ARP messages with false MAC addresses, resulting in the local ARP cache table being overwritten by the attacker's MAC address, resulting in normal data flow to the attacker. Static binding of user IP address and MAC address in switch port configuration command can effectively filter ARP attack messages.

In addition to the function of preventing ARP spoofing, IP MAC binding function can also guarantee the one-to-one mapping relationship between IP and MAC, that is to say, a IP can only correspond to one MAC, one MAC can only correspond to one IP,. If the access device modifies this mapping relationship, it will not be able to communicate in this network. 802.1x anti-ARP spoofing function and DHCP SNOOPING protocol are the dynamic implementation of this function.

IP MAC binding, ACL,802.1x anti-ARP spoofing and DHCP SNOOPING all use the same system resource CFP, to pay attention to whether the resources of CFP are exhausted when configuring. At the time of design, we have worked out the compatibility relationship between them. The following table is as follows:

	IP MAC Binding	ACL	802.1x	DHCP SNOOPING
IP MAC Binding	compatible	incompatible	compatible	compatible
ACL	incompatible	compatible	incompatible	incompatible
802.1x	compatible	incompatible	compatible	incompatible
DHCP SNOOPING	compatible	incompatible	incompatible	compatible

The CFP is a limited hardware resource, and only 16 IP MAC binding entries can be configured on average to each port, so a static IP MAC binding feature can be used if only a few ports or a few IP and MAC addresses need to be controlled in one access host. Avoiding CFP feature exhaustion results in failure of data forwarding.

In addition, using 802.1x or the DHCP SNOOPING protocol, the DHCP SNOOPING protocol is to be used if a static IP address configuration is used and an 802.1x protocol access network is to be used with 801.x anti-ARP spoofing, depending on the current situation.

5.2 IP and MAC Binding Configuration

IP and MAC bind in interface mode configuration

Configure Port IP and MAC Binding

Switch#configure terminal

Switch(config)#interface ge1/1

Switch(config-ge1/1)#ip mac-bind A.B.C.D MAC

Delete port IP binding to MAC

Switch#configure terminal

Switch(config)#interface ge1/1

Switch(config-ge1/1)#no ip mac-bind A.B.C.D MAC

Display Configuration

Show binding entries for all ports

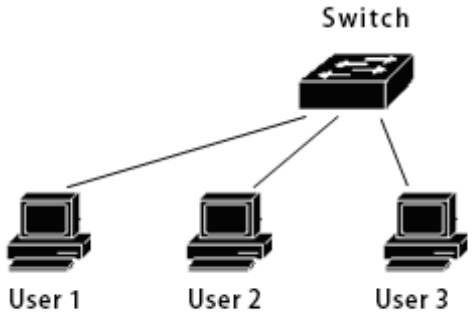
show ip mac-bind

Display a binding entry for an interface

Show ip mac-bind IFNAME

5.3 Configuration Example

In the network, the user 1, the user 2, the user 3, the IP and the MAC of the user in the port are bound, and the ARP attack can be protected.




```
Switch#configure terminal
Switch(config)#interface ge1/1
Switch(config-ge1/1)#ip mac-bind 192.168.1.100 0011.5b34.42ad
Switch(config-ge1/1)#interface ge1/2
Switch(config-ge1/2)#ip mac-bind 192.168.1.101 0011.6452.135d
Switch(config-ge1/2)#interface ge1/3
Switch(config-ge1/3)#ip mac-bind 192.168.1.102 0011.804d.a246
Switch(config-ge1/3)#end
Switch#show ip mac-bind
[ge1/1] sum: 1
        MAC                 IP
        0011.5b34.42ad      192.168.1.100
[ge1/2] sum: 1
        MAC                 IP
        0011.6452.135d      192.168.1.101
[ge1/3] sum: 1
        MAC                 IP
```

```
        0011.804d.a246          192.168.1.102
Switch#show ip mac-bind ge1/1
[ge1/1] sum: 1
        MAC                     IP
        0011.5b34.42ad          192.168.1.100
Switch#show running-config
!
spanning-tree mst configuration
!
Interface vlan1
 ip address 192.168.1.1/24
!
interface ge1/1
 ip mac-bind 192.168.1.100 0011.5b34.42ad
!
interface ge1/2
 ip mac-bind 192.168.1.101 0011.6452.135d
!
interface ge1/3
 ip mac-bind 192.168.1.102 0011.804d.a246
!
line vty
!
end
```

5.4 Configuration Troubleshooting

If the IP MAC binding configuration fails, it may be caused by the following reasons:

1. The system CFP resources are exhausted.

2. The current interface is configured with ACL filtering.

3, the configured interface is a three-tier interface or a TRUNK interface.

Chapter 6 VLAN Configuration

VLAN is an important concept in switches, which is widely used in practical applications. VLAN is the basis of internal division of multiple networks. VLAN is the abbreviation of virtual local area network, it is a network that logically organizes multiple devices together, regardless of the physical location of the device. Each VLAN is a logical network, which has all the functions and attributes of the traditional physical network. Each VLAN is a broadcast domain, the broadcast packet can only be forwarded in one VLAN, and the data communication between the VLAN,VLAN must be forwarded through three layers.

This chapter mainly includes the following:

- VLAN introduction
- VLAN configuration
- VLAN configuration example
- Based on MAC, IP subnet, protocol VLAN.
- VOICE VLAN
- VLAN mapping
- QINQ

6.1 VLAN Introduction

This section provides a detailed introduction to the VLANs, including the following:

- The benefits of VLAN
- VLAN ID
- VLAN port member type
- the default VLAN for the port
- Port's VLAN mode
- VLAN Trunking
- the forwarding of the data stream within the VLAN
- the subnet of the VLAN

6.1.1 VLAN Benefits

VLAN greatly expands the scale of physical network. The traditional physical network can only have a very small scale, which can hold up to thousands of devices, while the physical network divided by VLAN can hold tens of thousands or even hundreds of thousands of devices. VLAN has the same functions and attributes as the traditional physical network.

Using VLAN has the following benefits:

- VLAN can effectively control the traffic in the network.

In traditional networks, whether necessary or not, all broadcast packets are transmitted to all devices, adding to the load on the network and devices. VLAN can organize devices into a logical network as needed, a VLAN is a broadcast domain, broadcast packets are only transmitted within the VLAN, will not cross the VLAN. Traffic in the network can be effectively controlled by dividing VLAN.

- VLAN can improve the security of the network.

If the device in VLAN can only communicate with the device of the same VLAN, if it wants to communicate with another VLAN, it must be forwarded through three layers. If the three-layer forwarding between VLAN is not established, the VLAN can not communicate at all, so it can play the role of isolation and ensure the data security in each VLAN. For example, if the R & D department of a company does not want to share the data with the marketing department, the R & D department can set up a VLAN, marketing department to establish a VLAN, and two VLAN without establishing a three-tier communication channel.

- VLAN makes it easy to move devices.

If the devices in the traditional network move from one location to another and belong to different networks, the

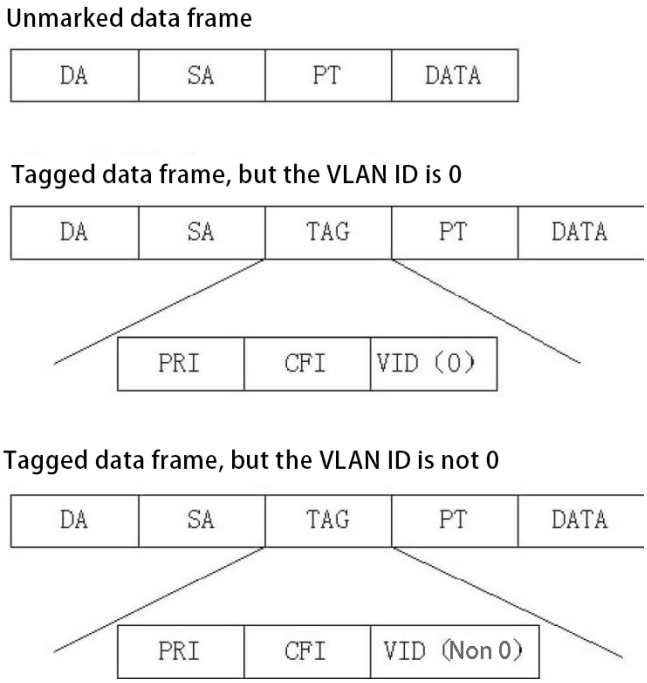
network configuration of mobile devices needs to be modified, which is very inconvenient for users. VLAN is a logical network, which can divide devices that are not in the same physical location on the same network. When the device moves, it can also make the device belong to this VLAN, so that the moving device does not need to modify any configuration.

6.1.2 VLAN ID

Each VLAN has an identification number called VLAN ID,VLAN ID from 0 to 4095, where 0 and 4095 are not used, and only 1 to 4094 are actually valid. VLAN ID uniquely identifies a VLAN.

The switch supports 4094 VLAN, and when creating VLAN, select an VLAN ID, range from 2 to 4094. 5. The switch creates VLAN1, by default and VLAN1 cannot be deleted.

There are three kinds of data frames transmitted in a VLAN in a network: unmarked data frames, data frames marked with VID 0, and data frames with VID non-0 tags. The following figure shows three different data frame formats.



All data frames inside the switch are marked. If an untagged data frame is input to the switch, the switch adds a tag to the data frame and selects a VLAN ID value into the VID of the tag. If a data frame with a VID of 0 is input to the switch, the switch selects a VLAN ID value into the VID of the tag. If a data frame with a VID non-0 tag is input to the switch, the frame does not change.

6.1.3 VLAN Port Member Type

The switch supports port-based VLANs and 802.1Q-based VLANs. One VLAN includes two port member types: an untagged member and a tagged member. A VLAN can include both the untagged port member and the tagged port member.

A VLAN can have no port membership or one or more port members. When a port belongs to a VLAN, it can be a taggered member of a VLAN or a taggered member.

A port can belong to a tagged or untagged member of one or more VLANs, which is also called a VLAN trunk port if a port belongs to a tagged member of two or more VLANs. A port can also belong to an untagged member of one or more VLANs and a tagged member belonging to another or more VLANs.

6.1.4 Defaults VLAN for the port

The port has and only one default VLAN, default VLAN is used to determine the owned VLAN. of an unmarked or tagged packet with a VID of 0 entered from that port The default VLAN is also called port VID or PVID. By default, the default VLAN for the port is 1. 1.

6.1.5 VLAN Mode for the Port

There are three VLAN modes in port: ACCESS mode, TRUNK mode and HYBRID mode. The user must first specify the VLAN mode of the port when configuring the VLAN of the port.

The port in ACCESS mode is an access port that is directly user-oriented. The port can only belong to one untagged member of VLAN, and the default VLAN is the VLAN. specified by the user. When a port belongs to only one untagged member of VLAN, you can specify that the port's VLAN mode is ACCESS mode.

The port in TRUNK mode is a relay port connected directly to the switch. The port can belong to one or more tagged members of VLAN, but not to any untagged member of VLAN. The default VLAN of this port is 1, and the default VLAN. can be modified by command.

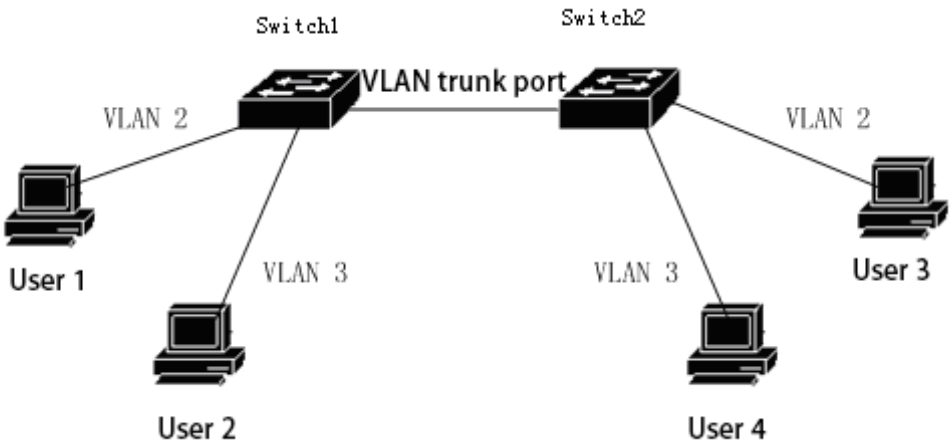
The port in HYBRID mode is a relay port connected directly to the switch, which can belong to one or more VLAN tagged members and / or one or more VLAN untagged members. The default VLAN for this port can be changed.

In practical application, users can choose the VLAN mode of the port according to the specific situation.

6.1.6 VLAN Relay

If a port belongs to two or more tagged members of VLAN, this port is also called VLAN relay port. Two switches can be connected by VLAN relay port, so that two or more common VLAN can be divided between the two switches.

The following figure is an example of a VLAN relay. The two switches are connected by VLAN relay ports and are the relay ports of VLAN 2 and VLAN 3. Each switch is divided into two VLAN, is VLAN 2 and VLAN 3, and each VLAN has one user. In this way, user 1 can communicate with user 3, user 2 can communicate with user 4, and user 1 and user 3 cannot communicate with user 2 and user 4.



6.1.7 Forwarding of Data Streams Within the VLAN

When the switch receives a packet from one port, layer 2 forwarding is performed according to the following steps:

- Determines the VLAN to which the packet belongs.
- Determine whether the packet is a broadcast packet, a multicast packet or a unicast packet.
- Determine the output port (which can be zero, one or more output ports) according to different packets, and discard the packet if there is no output port.
- Determines whether the package sent is tagged based on the type of member of the output port in the VLAN.
- Send it from the output port.

1) how to determine the VLAN: to which the packet belongs
If the received packet is tagged and the VID field in the tag is not 0, the VLAN to which the packet belongs is the VID value in the tag.

If the received packet is unmarked or tagged but the VID value in the tag is 0, the VLAN to which the packet belongs is the default VLAN. for the port

2) how to determine the type of packet:
If the destination MAC address of the received packet is FF:FF, the packet is a broadcast packet.
If the received packet is not a broadcast packet and the 40 bit of its destination MAC address is 1, the packet is a multicast packet.
If it is neither a broadcast packet nor a multicast packet, that packet is a unicast packet.

3) How to determine the output port of a packet:
If the input packet is a broadcast packet, all member ports of the VLAN to which the packet belongs are the output port of the packet.
if the input data packet is a multicast data packet, first, searching the two-layer hardware multicast forwarding table according to the destination multicast MAC address and the VLAN to which the multicast packet belongs, and if the matched multicast entry is found, Then the output port in the multicast entry and the common port (and operation) in the member port in the owning VLAN are the output ports of the data packet, and if there is no common port, the data packet is discarded. if the matched multicast entry is not found in the two-layer hardware multicast forwarding table, the output port is determined according to the forwarding mode of the two-layer hardware multicast forwarding table, All the member ports of the VLAN are the output ports of the data packet. If the forwarding mode is registered, the output port is not output, and the packet is discarded.
If the input packet is a unicast packet, first look up the layer 2 hardware forwarding table according to the destination MAC address and the VLAN to which it belongs. If a matching entry is found, the output port in the entry and the common port (and operation) in the member port of the VLAN are the output ports of the packet, and if there is no common port, the packet is discarded. If no matching entry is found in the layer 2 hardware forwarding table, the packet is processed as a broadcast packet, and all member ports of the VLAN to which it belongs are the output ports of the packet.

4) send packets:
After determining the output port of the input packet, the packet should be sent out of all the output ports.
If an output port is an untagged member of the VLAN to which the packet belongs, the packet is sent from the output port without marking.
If an output port is a tagged member of the VLAN to which the packet belongs, the packet is marked when it is sent from the output port, and the VID value in the tag is the value of the VLAN to which the packet belongs.

6.2 VLAN Configuration

This section provides a detailed introduction to the configuration of VLAN, including the following:

- Create and delete VLAN
- Configure the VLAN mode of the port
- VLAN configuration of ACCESS Mode

- VLAN configuration of TRUNK Mode
- VLAN configuration of HYBRID Mode
- VLAN subnet configuration
- View information about VLAN

6.2.1 Create and Delete VLAN

Before creating and deleting VLAN, users need to use the vlan database command to enter VLAN configuration mode in global configuration mode, where VLAN. is created and deleted

The system has created VLAN 1 by default, and VLAN 1 cannot be deleted by the user. The commands for creating and deleting VLAN are as follows:

The command	Description	CLI Model
vlan <vlan-id>	Create a VLAN. If the VLAN already exists, no processing is done, otherwise this VLAN. is created Parameters range from 2 to 4094.	VLAN configuration mode
no vlan <vlan-id>	Create a VLAN. If the VLAN already exists, no processing is done, otherwise this VLAN. is created Parameters range from 2 to 4094.	VLAN configuration mode

6.2.2 Configure the VLAN Mode of the Port

You need to specify the VLAN mode for the port before configuring the port's VLAN mode, which is ACCESS mode by default.The VLAN mode commands for the specified ports are shown in the following table:

The command	Description	CLI Model
switchport mode access	The VLAN mode of the specified port is ACCESS mode. After executing this command, the port is a untagged member of the VLAN1, and the default	Interface configuration mode

	VLAN for the port is 1.	
switchport mode trunk	The VLAN mode of the specified port is TRUNK mode. after this command is executed, the port is a tagged member of vlan 1 and the default vlan of the port is 1.	Interface configuration mode
no switchport trunk	The VLAN mode of the port is no longer TRUNK mode, back to the default, that is, ACCESS mode.	Interface configuration mode
switchport mode hybrid	The VLAN mode of the specified port is HYBRID mode. After executing this command, the port is a untagged member of the VLAN1, and the default VLAN for the port is 1.	Interface configuration mode
no switchport hybrid	The VLAN mode of the port is no longer HYBRID mode, back to the default, that is, ACCESS mode.	Interface configuration mode

6.2.3 ACCESS Mode VLAN Configuration

The port's VLAN mode needs to be specified before the port is configured as a VLAN. In this VLAN mode, the port is the untagged member of the VLAN1, and the default VLAN for the port is 1. The VLAN configuration command for the ACCESS mode is as follows:

The command	Description	CLI Model
switchport access vlan <vlan-id>	The configuration port is the untagged member of the specified VLAN, and the default VLAN of the port is the specified VLAN. The parameters range from 2 to 4094.	Interface configuration mode
no switchport access vlan	The VLAN configuration of the port returns to the	Interface configuration

	default, that is, the port is a untagged member of the VLAN1 and the default VLAN for the port is 1.	mode

6.2.4 TRUNK Mode VLAN Configuration

Before the port is configured with VLAN, the VLAN mode of the port needs to be specified as TRUNK mode. In this VLAN mode, the port defaults to the tagged member of the VLAN1, and the default VLAN of the port is the VLAN configuration command in 1.TRUNK mode, as follows:

The command	Description	CLI Model
switchport trunk native vlan <vlan-id>	Configure the port's default VLAN, or pvid. parameters range from 2 to 4094.	Interface configuration mode
switchport trunk allowed vlan all	The configuration port is the tagged member of all VLANs, which are also the tagged members of these VLANs for later newly created VLANs.	Interface configuration mode
switchport trunk allowed vlan none	With the exception of VLAN1, the port is no longer an tagged member of all other VLAN.	Interface configuration mode
switchport trunk allowed vlan add <vlan-list>	Configure the port to become a tagged member of one or more VLAN specified. The parameter < vlan-list > can be one VLAN, one VLAN range or more VLAN. For example, the parameters can be "1", "2 ≤ 4" or "1, 3, 5".	Interface configuration mode
switchport trunk allowed vlan remove <vlan-list>	Removes ports from one or more specified VLAN and is no longer a tagged member of these VLAN. The parameter < vlan-list > can be one VLAN, one VLAN	Interface configuration mode

	range or more VLAN. For example, the parameters can be "1", "2 ≤ 4" or "1, 3, 5".	

6.2.5 HYBRID Mode VLAN Configuration

Before the port is configured with VLAN, the VLAN mode of the port needs to be specified as HYBRID mode. In this VLAN mode, the port defaults to the untagged member of the VLAN1, and the default VLAN of the port is the VLAN configuration command in 1.HYBRID mode, as follows:

The command	Description	CLI Model
switchport hybrid native vlan <vlan-id>	The configuration port is the untagged member of the specified VLAN and the default VLAN for the port is the specified VLAN. The range of parameters is from 2 to 4094.	Interface configuration mode
no switchport hybrid vlan	Clear the port from the default VLAN, is no longer the tagged or untagged member of the default VLAN, and the default VLAN of the port returns to 1 .	Interface configuration mode
switchport hybrid allowed vlan all	The tagged port is a tagged member of all vlans (except VLAN1) and is also a tagged member of these vlans for newly created vlans.	Interface configuration mode
switchport hybrid allowed vlan none	With the exception of VLAN1, the port is no longer tagged or untagged member of all other vlans. The port's default VLAN is back to 1.	Interface configuration mode
switchport hybrid allowed	Configure the port to	Interface

vlan add <vlan-list> egress-tagged enable	become a untagged member of one or more VLAN specified. The parameter < vlan-list > can be one VLAN, one VLAN range or more VLAN. For example, the parameters can be "1", "2 ≤ 4" or "1, 3, 5".	configuration mode
switchport hybrid allowed vlan add <vlan-list> egress-tagged disable	Configure the port to become a untagged member of one or more VLAN specified. The parameter < vlan-list > can be one VLAN, one VLAN range or more VLAN. For example, the parameters can be "1", "2 ≤ 4" or "1, 3, 5".	Interface configuration mode
switchport hybrid allowed vlan remove <vlan-list>	Removes ports from one or more specified VLAN and is no longer a tagged or untagged member of these VLAN. If the default VLAN of the port belongs to the specified VLAN, the default VLAN returns to 1 .	Interface configuration mode

6.2.6 View VLAN Information

The commands to view VLAN information are as follows:

The command	Description	CLI Model
show vlan [vlan-id]	If you do not enter parameters, all VLAN information is displayed, and if you enter parameters, a specified VLAN information is displayed. Parameters range from 1 to 4094.	Normal mode Privilege mode

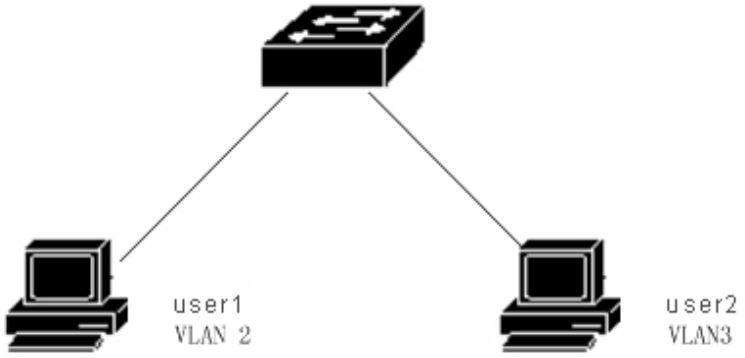
show interface switchport	Displays VLAN related information for all ports of the system, such as VLAN mode, default VLAN, etc.	Normal mode Privilege mode
show running-config	View the current configuration of the system and you can see the configuration of VLAN.	Privilege mode

6.3 VLAN Configuration Example

6.3.1 VLAN Base on PORT

1) Configuration

There are two users, user 1 and user 2, who need to be in different vlans due to their different network functions and environments.User 1 belongs to VLAN 2 and connects to port ge1/1 of the switch. User 2 belongs to VLAN 3 and connects to port ge1/2 of the switch.



The switches are configured as follows:

Create VLAN

Switch#config t

Switch(config)#vlan database

Switch(config-vlan)#vlan 2

Switch(config-vlan)#vlan 3

Assign ports to VLAN

Switch#config t

Switch(config)#interface ge1/1

Switch(config-ge1/1)#switchport mode access

Switch(config-ge1/1)#switchport access vlan 2

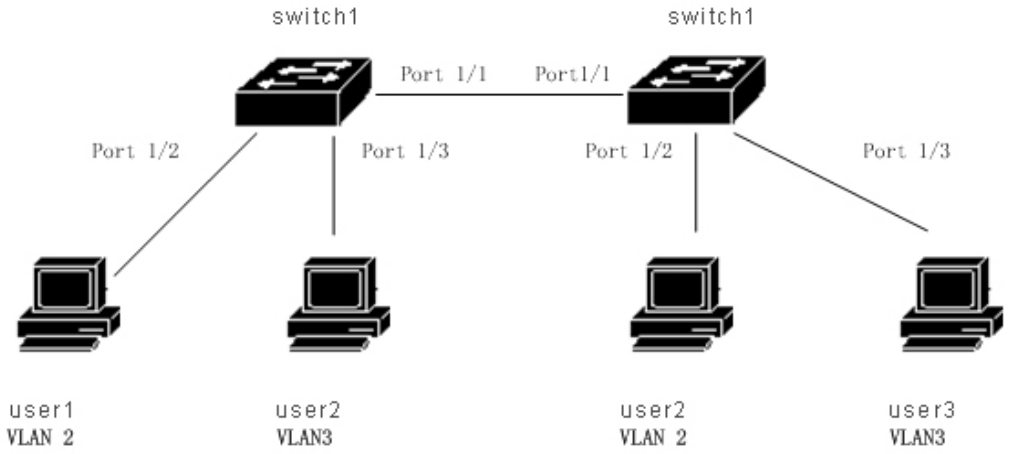
Switch(config-ge1/1)#exit
Switch(config)#interface ge1/2
Switch(config-ge1/2)#switchport mode access
Switch(config-ge1/2)#switchport access vlan 3

2) Erratum

If, after configuration, it is found that the PC machine between different VLAN can not communicate, it is a normal phenomenon, because the communication between different VLAN must go through three layers of routing and forwarding. If the PC machine in the same VLAN cannot communicate, the following verification must be made:
show vlan
View all VLAN member ports.
show vlan <vlan-id>
To see if the port connected to a particular PC is within the specified VLAN

6.3.2 VLAN Base on 802.1Q

1) Configuration



There are two switches that connect to two users:

User	Belonging to VLAN	Connection Port	Switches	Cascade Port
User 1	2	1/2	Switch 1	1/1
User 2	3	1/3	Switch 1	1/1
User 3	2	1/2	Switch 2	1/1
User 4	3	1/3	Switch 2	1/1

Need to be configured on both switches.

Switch 1 configuration:

```
Switch#config t
Switch(config)#vlan database
Switch(config-vlan)#vlan 2
Switch(config-vlan)#vlan 3
Switch#config t
Switch(config)#interface ge1/1
Switch(config-ge1/1)#switchport mode trunk
Switch(config-ge1/1)#switchport trunk allowed vlan add 2
Switch(config-ge1/1)#switchport trunk allowed vlan add 3
Switch(config)#interface ge1/2
Switch(config-ge1/2)#switchport mode access
Switch(config-ge1/2)#switchport access vlan 2
Switch(config-ge1/2)#exit
Switch(config)#interface ge1/3
Switch(config-ge1/3)#switchport mode access
Switch(config-ge1/3)#switchport access vlan 3
```

Switch 2 configuration:

```
Switch#config t
Switch(config)#vlan database
Switch(config-vlan)#vlan 2
Switch(config-vlan)#vlan 3
Switch#config t
Switch(config)#interface ge1/1
Switch(config-ge1/1)#switchport mode trunk
Switch(config-ge1/1)#switchport trunk allowed vlan add 2
Switch(config-ge1/1)#switchport trunk allowed vlan add 3
Switch(config)#interface ge1/2
Switch(config-ge1/2)#switchport mode access
Switch(config-ge1/2)#switchport access vlan 2
Switch(config-ge1/2)#exit
Switch(config)#interface ge1/3
Switch(config-ge1/3)#switchport mode access
Switch(config-ge1/3)#switchport access vlan 3
```

2) Erratum

The vlan, across the switch can communicate with the PC in the same vlan, if not. You need to see the following:

- Whether the port connected to the pc machine belongs to the corresponding VLAN, and applies ACCESS mode to join the vlan.

- Cascade port 1 ≤ 1 is added to each vlan, and port 1 ≤ 1 is in TRUNK mode.

6.4 MAC, IP Subnet, Protocol VLAN

The VLAN based on MAC is divided according to the MAC address of the source of the message. After the device receives the message of untagged (or tag is 0) from the port, it will determine the VLAN, to which the message belongs according to the source MAC address of the message, and then automatically divide the message into the specified VLAN for transmission.

The VLAN based on IP subnet is divided according to the IP address and subnet mask of the message source. When the device receives the untagged message from the port, the VLAN, to which the message belongs is determined according to the source address of the message, and then the message is automatically divided into the specified VLAN for transmission. This feature is mainly used to transmit the message sent by the specified network segment or IP address in the specified VLAN.

The protocol-based VLAN allocates different VLAN ID. to the message according to the protocol type to which the message received by the port belongs. The protocols that can be used to divide VLAN are IP,IPV6,IPX and so on.

Before configuring the VLAN based on MAC, IP subnet, protocol, the corresponding VLAN must be created.

The command	Description	CLI Model
mac-vlan mac WORD vlan <1-4094>	create a source MAC address-based VLAN	Interface configuration mode
no mac-vlan mac WORD	Delete all VLAN based on the source MAC address	Interface configuration mode
no mac-vlan	Delete a source MAC address-based VLAN	Interface configuration mode
show mac-vlan	Create a VLAN based on the source IP subnet	Privilege mode
ip-subnet-vlan ip A.B.C.D A.B.C.D vlan <1-4094>	Displays all VLAN based on the source MAC address	Interface configuration mode
no ip-subnet-vlan ip A.B.C.D A.B.C.D	Delete all VLAN based on the source IP subnet	Interface configuration mode
no ip-subnet-vlan	Delete a VLAN based on the source IP subnet	Interface configuration

		mode
show ip-subnet-vlan	Displays all the source IP subnets-based VLAN	Privilege mode
protocol-vlan ether-type (ip|ipv6|ipx|…|<0-65535>) vlan <1-4094>	create a protocol-based VLAN	Interface configuration mode
no protocol-vlan ether-type (ip|ipv6|ipx|…|<0-65535>)	Delete a protocol-based VLAN.	Interface configuration mode
no protocol-vlan	Delete all protocol-based VLAN	Interface configuration mode
show protocol-vlan	Show all protocol-based VLAN	Privilege mode
show vlan-partition interface IFNAME	the status of a VLAN that enables a MAC, IP subnet, and protocol to be enabled on the display interface	Privilege mode

6.5 Voice VLAN

Voice VLAN is a VLAN. that is specially divided for the voice data stream of the user. By dividing the Voice VLAN and adding the port connected to the voice device to the Voice VLAN, the QoS (Quality of Service, quality of service (QoS) parameters can be configured for the voice data, so as to improve the priority of the voice data message and ensure the call quality.

The device can determine whether the data stream is a voice data stream according to the source MAC address OUI field in the data message entering the port. The message whose source MAC address conforms to the OUI address of the voice device set by the system is considered to be a voice data stream and is divided into Voice VLAN for transmission.

Users can set the OUI address in advance, or they can use the default OUI address as the criterion, as follows

Number	OUI Address	Manufacturer
1	0001-e300-0000	Siemens phone
2	0003-6b00-0000	Cisco phone
3	0004-0d00-0000	Avaya phone
4	00d0-1e00-0000	Pingtel phone
5	0060-b900-0000	Philips/NEC phone
6	00e0-7500-0000	Polycom phone
7	00e0-bb00-0000	3com phone

Add the IP phone access port to the Voice VLAN by hand. Then the OUI address is matched by identifying the

source MAC, of the message. After the matching is successful, the system will send ACL rules and configure the priority of the message.

Voice VLAN security mode and normal mode, security mode: only OUI matching language streams are allowed to be transmitted in Voice VLAN, while OUI mismatched data streams are not allowed to be transmitted in Voice VLAN; normal mode: all data streams can be transmitted in Voice VLAN.

Before you can configure Voice VLAN, you must create the corresponding VLAN.

The command	Description	CLI Model
voice-vlan security (enable|disable)	Voice VLAN security mode enable	Global configuration mode
voice-vlan oui WORD mask WORD	Configure user OUI	Global configuration mode
voice-vlan oui WORD mask WORD description WORD	Configure user OUI, and name	Global configuration mode
no voice-vlan oui WORD mask WORD	Delete user OUI configuration through OUI address and mask	Global configuration mode
no voice-vlan oui description WORD	Remove user OUI configuration by naming	Global configuration mode
no voice-vlan oui	Delete all user OUI configurations	Global configuration mode
no voice-vlan default-oui WORD mask WORD	Remove the dealt OUI configuration from the mask through the OUI address	Global configuration mode
no voice-vlan default-oui description WORD	Delete the defualt OUI configuration by naming	Global configuration mode
no voice-vlan default-oui	Delete all defualt OUI configurations	Global configuration mode
voice-vlan default-oui resume	Restore all defualt OUI configurations	Global configuration mode
show voice-vlan oui	Display all defualt and user OUI configurations	Privilege mode
voice vlan <1-4094>	Interface enable Voice	Interface

(enable|disable)	VLAN	configuration mode
voice vlan qos map-queue <0-7> remark-dscp <0-63>	Interface configuration qos priority, default queue is 6, DSCP is 46	Interface configuration mode
no voice vlan qos	Restore interface qos priority default configuration	Interface configuration mode
no voice vlan	Delete interface configuration Voice VLAN	Interface configuration mode
show voice-vlan state	Show the configuration of Voice VLAN for all interfaces	Privilege mode

6.6 VLAN Mapping

VLAN mapping (that is, the VLAN Mapping) function can modify the VLAN Tag, carried by the message to provide the following mapping relationship: 1:1 VLAN mapping: modify the VLAN ID in the message carrying VLAN Tag to another VLAN ID.

Before configuring the VLAN mapping, you must create the corresponding VLAN.

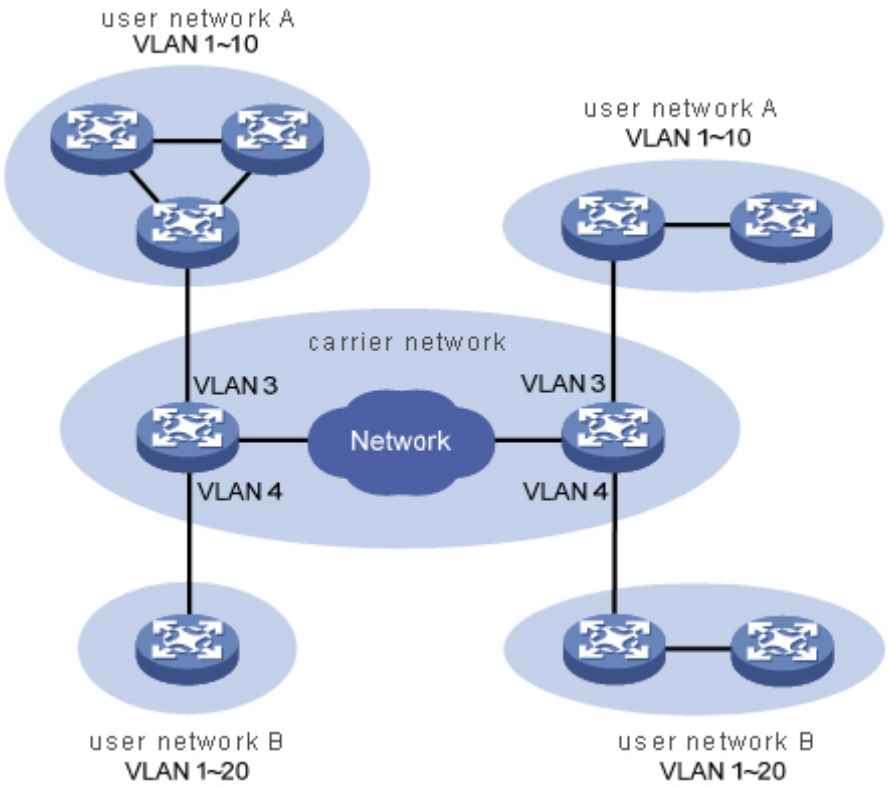
The command	Description	CLI Model
vlan-mapping vlan <1-4094> map-vlan <1-4094>	Configure a VLAN mapping relationship for a port	Interface configuration mode
no vlan-mapping vlan <1-4094>	Delete a VLAN mapping relationship for a port	Interface configuration mode
no vlan-mapping	Delete all VLAN mapping relationships for a port	Interface configuration mode
show vlan-mapping	Show all configured VLAN mapping	Privilege mode

6.7 QinQ

The port QinQ characteristic provided by the device is a simple and flexible two-layer VPN technology, which encapsulates the outer VLAN Tag, for the private network message of the user on the edge device of the operator

network so that the message carries two layers of VLAN Tag through the backbone network of the operator (public network). In the public network, the device only transmits the message according to the outer VLAN Tag, and learns the source MAC address table item of the message into the MAC address table of the VLAN where the outer Tag is located, while the user's private network VLAN Tag will be transmitted as the data part of the message during the transmission process.

The QinQ feature allows operators to use one VLAN to serve users with multiple VLAN. As shown in the following figure, the private network VLAN of user network A is VLAN 1 ≤ 10, and the private network VLAN of user network B is VLAN 1 ≤ 20. The VLAN assigned by the operator to subscriber network A is VLAN 3, and the VLAN assigned to subscriber network B is VLAN 4. When the message with VLAN Tag of subscriber network A enters the operator network, the message is wrapped on a layer of VLAN Tag; with VLAN ID of 3 when the user network B When a message with VLAN Tag enters the operator network, the message is wrapped on a layer of VLAN Tag. with VLAN ID of 4. In this way, the messages of different user networks are completely separated in the public network transmission, even if the VLAN range of the two user networks overlaps, there will be no confusion in the public network transmission.



The QinQ feature enables the network to provide up to 4094X4094 VLANs to meet the requirements of the metropolitan area network for the number of VLANs. It mainly solves the following problems:

(1) The problem of public network VLAN ID resource is relieved.
(2) The user can plan its own private network VLAN ID and will not result in conflict with the public network VLAN ID.
(3) to provide a simple two-tier VPN solution for small metropolitan area network or enterprise network.
QinQ can be divided into two types: basic QinQ and flexible QinQ..

The main contents are as follows:

(1) the basic QinQ: basic QinQ is implemented based on port mode. When the basic QinQ function of the port is turned on, when the port receives the message, the device will type the VLAN Tag. of the default VLAN for the message If you receive a message with VLAN Tag, the message becomes a double Tag message; if you receive a message without VLAN Tag, the message becomes a message with port default VLAN Tag.

(2) flexible QinQ: flexible QinQ is a more flexible implementation of QinQ, which is based on the combination of port and VLAN. In addition to realizing all the basic QinQ functions, the messages received by the same port can also do different actions according to different VLAN, adding different outer VLAN Tag. for messages with different inner VLAN ID.

The command	Description	CLI Model
qinq tpid WORD	Configure the tpid value that is carried in the port VLAN Tag and the default is 0x8100	Interface configuration mode
no qinq tpid	Recovery port default tpid	Interface configuration mode
qinq uplink	Configure port to uplink port	Interface configuration mode
no qinq uplink	Cancel the uplink configuration of the port	Interface configuration mode
qinq customer	Configure the port as the customer port	Interface configuration mode
no qinq customer	Cancel the customer configuration of the port	Interface configuration mode
qinq outer-vid <1-4094> inner-vid VLAN_ID	Configure a VLAN conversion for the interface.	Interface configuration mode
no qinq inner-vid VLAN_ID	Delete a VLAN conversion for an interface	Interface configuration mode
no qinq outer-vid <1-4094>	Delete a VLAN conversion for an interface	Interface configuration mode
show qinq	Displays the qinq situation for all configurations	Privilege mode

Chapter 7 QoS Configuration

This chapter describes QoS and its configuration, including the following:

- QoS Introduction
- QoS configuration
- QoS configuration example

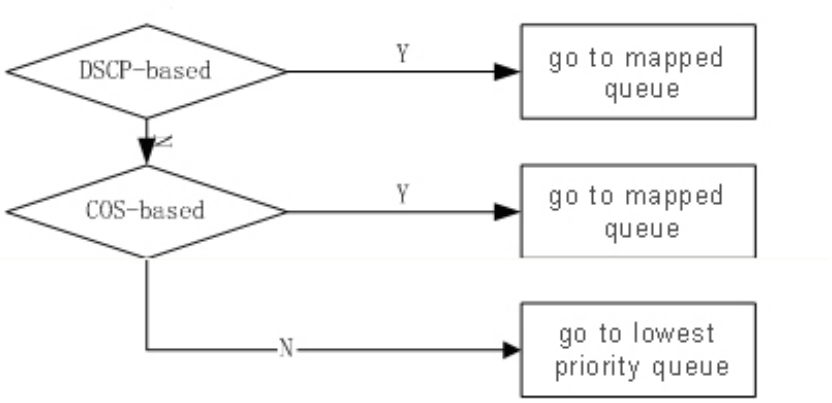
7.1 QoS Introduction

With the switch's QoS capabilities, you can give priority to the important data streams forwarded through the switch, making the bandwidth of your network more reasonable and network performance predictable.

In the switch, a queue at the output end of the data packet is determined at the input end according to the priority information of the data packet.

The switch implements the QoS based on the (802.1p), the QoS based on DSCP (DiffServ), and the MAC-based QoS. The DSCP-based QoS can be configured on one physical port; the physical port defaults to a COS-based QoS.

The following figure is the packet forwarding process for QoS enabled:



The switch supports 0 to 7 priority queues, with the highest priority of the queue 7 and the lowest priority of the queue 0. The scheduling mode of the priority queue has three SPs, WRR, WFQ. The SP is the strict priority scheduling, that is, the data packet of the queue 7 is always preferentially forwarded, and the data packet of the queue 6 is started until the packet of the queue 7 is finished. The packet of the queue 5 is forwarded before the packet of the queue 6 is forwarded, and finally the data packet of the queue 0 is forwarded. WRR refers to the right priority polling, when the switch forwards the data packet, the switch polls and forwards the data packet from the high priority queue to the low priority queue according to the configuration of the weight, First, the data packet of the priority number of the high priority is transmitted, and the priority number data packet is forwarded to the lowest priority queue until the lowest priority queue is forwarded, and the data packet is forwarded from the high priority to push the class. Similar to the WQ and WRR queue scheduling algorithms, byte-count and weight are supported on the weight algorithm, and SP packets are also supported and can be replaced with each other. the difference is as follows: WRR supports the maximum time delay, and can ensure that the maximum time of the message in the configured queue from the incoming queue to the exit queue does not exceed the set maximum time delay; and the WFQ supports the bandwidth guarantee, and can ensure that the port flow is congested The minimum queue bandwidth obtained.

In order to facilitate user configuration, we introduced the concept of the QosProfile. The QoProfile is an attribute of the mapping relationship configured for 802.1p and priority queues that cannot be configured by the user. Their mapping relationship is as follows:

Qos Profile	802.1p (CoS) value	Priority Query
Qp0	0	0

Qp1	1	1
Qp2	2	2
Qp3	3	3
Qp4	4	4
Qp5	5	5
Qp6	6	6
Qp7	7	7

7.1.1 COS based on QoS

Port QoS. based on COS is enabled by default The switch obtains the priority value of the VLAN TAG in the packet entering the port and determines the output queue of the packet according to the mapping relationship between the user configuration cos value and the queue. If the packet does not have VLAN TAG or the VID of VLAN TAG is 0, the switch populates the packet according to the default VID of the port configured by the user and the default priority of the port, and then determines the output queue of the packet according to the default priority.

7.1.2 DSCP based on QoS

If a port has a DSCP-based QoS enabled, the switch gets the DSCP value in the IP packet entering the port and determines the output queue for the packet based on the user's configured DSCP value and the mapping relationship of the queue.

Cosdscp type is an extension based on dscp type cos type, which is essentially one of dscp type or cos type. If the cosdscp type is now, the IP message system will automatically match the dscp priority, and the non-ip message system will be based on cos priority. Schedules according to the priority type(dscp/cos).

7.1.3 Policy based on QOS

QoS policies include classes, policy actions. A class is used to identify a flow, and a user can define a series of rules by a command to classify a packet; a policy action is used to define a QoS action made by a message of a matching rule. if a port is enabled with the policy-based QoS, the switching opportunity classifies the data packets entering the port, and the switching opportunity processes the data packet of the port according to the corresponding policy action for the data packet meeting the classification requirement, and the data packet which does not meet the classification requirement is not processed, And then the output queue of the data packet is determined according to the priority mapping relation.

7.2 QoS Introduction

7.2.1 Deafault Configuration for QoS

CI	Price	Whether to configure
Number of Queues	8	No
Scheduling mode	WRR	Yes
Whether SP scheduling is enabled	disable	Yes
Whether WFQ scheduling is enabled	disable	Yes
Queue weight	qp0[1],qp1[2],qp2[4],qp3[8],qp4[16] qp5[32],qp6[64],qp7[127]	Yes
Mapping relationship between COS and qosprofile	COS0[qp0] COS1[qp1] COS2[qp2] COS3[qp3] COS4[qp4] COS5[qp5] COS6[qp6] COS7[qp7]	No
Mapping relationship between DSCP and qosprofile	DSCP0~DSCP7[qp0] DSCP8~DSCP15[qp1] DSCP16~DSCP23[qp2] DSCP24~DSCP31[qp3] DSCP32~DSCP39qp4] DSCP40~DSCP47[qp5] DSCP48~DSCP55[qp6] DSCP56~DSCP64[qp7]	Yes
Properties of Qosprofile	qp0 cos[0] queue 0 qp1 cos[1] queue 1 qp2 cos[2] queue 2 qp3 cos[3] queue3 qp5 cos[4] queue 4 qp5 cos[5] queue 5 qp6 cos[6] queue 6 qp7 cos[7] queue 7	No

Whether the DSCP-based qos is enabled for the interface	disable	No
Whether the COS-based qos is enabled for the interface	enable	No
Interface user priority (COS value)	0	Yes

7.2.2 Configuration Scheduling

The default schedule for the switch is the WRR. The SP, WFQ scheduling mode can be configured by command.

The command	Description	CLI Model
qos sched { sp | wrr | wfq}	Configure QoS scheduling	Interface configuration mode

7.2.3 Configure Queue Weight

The command	Description	CLI Model
qos qosprofile (qp0| qp1| qp2| qp3| qp4| qp5| qp6| qp7) weight <1-127>	Configure the weight of each priority queue	Interface configuration mode
no qos qosprofile (qp0| qp1| qp2| qp3| qp4| qp5| qp6| qp7) weight	The weight of the recovery queue is configured by default	Interface configuration mode

The queue weight refers to the number of packets forwarded by the priority queue at a time the poll is forwarded, so it is important to note that the weight of the low priority queue does not exceed the weight of the high priority queue when configuring the queue weight.

7.2.4 Configure the Mapping Relationship Between DSCP and QosProfile

The command	Description	CLI Model
qos dsc-map-qp <0-63> qosprofile {qp0|qp1|qp2|qp3|qp4|qp5|qp6|qp7}	Configure the mapping relationship between DSCP and qosprofile.	Global configuration mode
no qos dscp-map-qp <0-63>	Restore the mapping relationship between DSCP	Global configuration

	and qosprofile to the default configuration.	mode

7.2.5 Configure Port QoS

Configuration steps of QoS policy: define classes, define policy actions, and apply policies.

Define classes and define a set of flow classification rules:

There are a total of 802.1p priorities, DSCP,ACL three flow classification rules, a class can only use one set of flow classification rules, a set of flow classification rules can be used by multiple class. The default configuration does not match any rules.

The command	Description	CLI Model
qos class <1-256> name WORD	Name the specified class	Global configuration mode
qos class <1-256> match cos <0-7> (<0-7>…)	Define matching 802.1p priority rules to configure 8 rules at the same time	Global configuration mode
qos class <1-256> match dscp <0-63> (<0-63>…)	Define matching DSCP rules, you can configure 8 rules at the same time	Global configuration mode
qos class <1-256> match acl <1-99>|<100-199>…	Define matching ACL rules, only one set of rules can be configured at a time	Global configuration mode
no qos class <1-256>	Restore the default configuration	Global configuration mode
show qos class (<1-256>|)	Displays information about configured classes	Privilege mode

Define a policy to define a set of QoS actions for a matching rule:
There are a total of mapping message output queues, heavy-mark DSCP, statistics, copy to CPU, mirroring, and speed-limiting six QoS actions, where the copy to the CPU and the image cannot be configured at the same time. A policy can be connected to multiple classes, and one class can be connected by a number of policies. A policy can use a set of QoS actions for a class. Policy does not connect to any class and does not use any QoS actions when configured by default.

The command	Description	CLI Model
qos policy <1-256> name	Name the specified policy	Global

WORD		configuration mode
qos policy <1-256> class <1-256> remark dscp <0-63>	Match the classification rule, the DSCP value of the remarking message	Global configuration mode
no qos policy <1-256> class <1-256> remark	Remove the action of the re - marking message.	Global configuration mode
qos policy <1-256> class <1-256> meter <1-1000000> <1-65535>	Matching classification rules, limiting the bandwidth and burst traffic of the message,	Global configuration mode
no qos policy <1-256> class <1-256> meter	Actions to remove restricted message bandwidth and burst traffic	Global configuration mode
qos policy <1-256> class <1-256> statistic-packets	Match the classification rule and count the number of messages	Global configuration mode
no qos policy <1-256> class <1-256> statistic-packets	The act of removing the number of statistical messages	Global configuration mode
qos policy <1-256> class <1-256> mirror-to cpu	Match the classification rule, the message is mirrored to the CPU	Global configuration mode
qos policy <1-256> class <1-256> mirror-to monitor-interface	Match the classification rule, the message is mirrored to the mirror port (effective when the mirror port is configured)	Global configuration mode
no qos policy <1-256> class <1-256> mirror	Remove actions to mirror messages	Global configuration mode
no qos policy <1-256> (class <1-256>|)	Policy delete corresponding matching rules and actions	Global configuration mode
qos policy <1-256> class <1-256> map-queue <0-7>	Match the classification rules and assign messages to the corresponding output	Global configuration mode

	queue.	
no qos policy <1-256> class <1-256> map-queue	Match classification rules and assign messages to default output queue 0	Global configuration mode
clear interface IFNAME qos policy statistic-packets	Clear statistics for interface qos policies	Global configuration mode
show qos policy (<1-256>|)	Displays information about configured policies	Privilege mode
show qos	Displays information about the configured qos	Privilege mode

Applying a policy to apply the corresponding policy to the interface;

Only the flow in the inlet direction acts, one interface can have only one policy, and one policy can be used by multiple interfaces.

One port can only enable one selection to enable one QoS. QoS function can only be configured on physical port, not in TRUNK group or three-layer interface.

The command	Description	CLI Model
qos {dscp-based| cos-based| dscpcos-based| apply-policy <1-256>}	Enable the QoS function of the port.	Interface configuration mode
no qos	Restore the default port-based.	Interface configuration mode
show qos	Display configuration information for all qos	Privilege mode
show qos interface IFNAME	Displays information about the qos configured by the interface	Privilege mode
show qos interface	Displays information for all interfaces configured for qos.	Privilege mode

7.2.6 Configure Port User Priority（COS Value）

The command	Description	CLI Model
qos user-priority <0-7>	Configure the user priority of the port (COS value)	Interface configuration

		mode
no qos user-priority	The user priority (COS value) of the recovery port is the default configuration.	Interface configuration mode

7.3 Basic QoS Configuration Example

Configure the ge1/3 user priority (COS value) to 3, and the COS-based QoS feature starts by default:

```
Switch#configure terminal
Switch#(config)#interface ge1/3
Switch#(config-ge1/3)#qos user-priority 3
Switch#(config-ge1/3)#end
```

Configure the interface ge1/3 to start the DSCP-based QoS function, and the DSCP value 3 maps to priority queue 2:

```
Switch#configure terminal
Switch#(config)#qos dscp-map-qp 3 qosprofile qp2
Switch#(config)#interface ge1/3
Switch#(config-ge1/3)#qos dscp-based
Switch#(config-ge1/3)#end
```

7.4 Policy QoS Configuration Example

Configure the ACL to capture the data streams of the source MAC1, MAC2, and MAC3, respectively
(you can modify the acl rules according to your requirements, and here is just a simple example)

```
access-list 700 permit host 0000.0000.1111 vid any ip any any
access-list 701 permit host 0000.0000.2222 vid any ip any any
access-list 702 permit host 0000.0000.3333 vid any ip any any
```

Configure the QOS class to match the data flow of the source MAC1,MAC2,MAC3 separately
(you can modify the matching rule cos or dscp, according to your requirements. Here is just a simple example)

```
qos class 10 match acl 700
qos class 11 match acl 701
qos class 12 match acl 702
```

Configure QOS policy and re-mark 802.1p priority of data stream with MAC1, MAC2 and MAC3 respectively.
(you can modify the strategy according to your needs, and here is just a simple example)

```
qos policy 10 class 10 remark cos 7
```

qos policy 10 class 11 remark cos 5
qos policy 10 class 12 remark cos 3

Issue QOS policy to port
interface ge1/23
qos apply-policy 10

View configuration information and test results are captured at the G1/24 port
Switch#show qos interface ge1/23

Chapter 8 MSTP Configuration

This chapter describes the MSTP and its configuration, mainly including the following:

- MSTP Introduction
- MSTP Configuration
- MSTP Configuration Example

8.1 MSTP Introduction

The switch supports the IEEE802.1d,IEEE802.1w,IEEE802.1s standard STP protocol.

8.1.1 Overview

MSTP uses RSTP to converge quickly, so that multiple VLAN are aggregated into one spanning tree instance, each of which has a spanning tree topology independent of other spanning tree instances. This architecture provides multiple forwarding paths for data streams, can load balance, and reduces the number of spanning tree instances that are required to support a large number of VLAN.

8.1.2 Multi-spanning Tree Domain

For examples involved in multi-spanning tree (MST) computation, the same MST configuration information for the switch must be configured consistently. A set of connected switches with the same MST configuration constitutes the MST domain.

The MST configuration determines the domain to which each switch belongs. The configuration includes domain names, revision numbers, and MST instances and VLAN assignment maps; this information generates a unique summary (Digest). In the MST configuration The summary in the same domain is the same and must be the same, and this information can be viewed through the show spanning-tree mst config command.

A domain can have one or more members with the same MST configuration; each member must have the ability to handle RSTP BPDU. There is no limit on the number of MST domains in a network, but each domain supports up to 16 instances. You can only assign one VLAN to one instance of the build tree at a time.

8.1.3 IST, CIST and CST

The built-in tree (IST), runs within the MST domain.

In each MST domain, MSTP maintains multiple generated instances. Instance 0 is a special instance of a domain called IST. All other MST instances are the numbers 1 to 15.

This IST is just a spanning tree instance that receives and sends BPDU; all other spanning tree instance information is compressed in MSTI BPDU. Because MSTI BPDU carries information about all instances, the number of BPDU that needs to be processed by a switch that supports multiple tree instances means simplification.

All MST instances in the same domain share the same protocol timer, but each MST instance has its own topology parameters, such as a root switch ID, root path cost, and so on. By default, all VLAN is assigned to IST.

The common and internal spanning tree (CIST), is a collection of all IST, and (connecting the MST domain and a single spanning tree) in each MST domain.
The spanning tree calculated in one domain appears to be a sub-tree of the CST that contains all the switch domains. CIST is formed by the result of the spanning-tree calculation run between the switches that support the 802.1W and 802.1D protocols. The CIST in the MST domain is the same as the CST in the field.
The Common Spanning Tree (CST), which runs the spanning tree in the MST domain.

8.1.4 Intra-domain Operation

IST connects to all MSTP switches in a domain. When the IST converges, the root of the IST becomes the IST master, which is the switch with the lowest bridge ID in the domain and the path overhead to the CST root. If there is only one domain in the network, IST master is also the CST root. If the CST root is outside the domain, one of the MSTP switches of the (boundary) at the boundary of the domain is selected as IST master.
When a MSTP switch initializes, it sends BPDU asking it to set its own path cost to 0 as CST root and IST master, to CST root and IST master. The switch also initializes all MST instances and requires them to be their root. If the MST root information received by the switch takes precedence over the information stored on the current port (low bridge ID, low path cost, etc.), it abandons its requirement to become IST master.
In initialization, a domain may have many subdomains, each with its own IST master. When the switch receives a higher priority IST message, it leaves its old subdomain to join a new subdomain that may contain a true IST master. Therefore, all subdomains shrink, with the exception of subdomains that contain real IST master.
In order to operate correctly, all switches in the MST domain must recognize the same IST master. So, switches in any two domains synchronize the role of the port of one of their MST instances, just if they converge to a public IST master.

8.1.5 Interdomain Operation

If there are multiple domains or early STP switches in the network, MSTP establishes and maintains MSTs that contain MST domains in all networks and all early STP switches. MST instances join IST at the domain boundary (boundary) to become CST.
IST connects to switches in all MSTP domains and looks like a subtree of CST (encircling all switching domains). The root of the subtree becomes a IST master.MST domain that looks like a virtual switch adjacent to the STP switch and MST domain.
Only the CST instance sends and receives BPDUs, and MST instances increase their spanning-tree information to BPDUs to influence the neighbor switch and compute the last spanning-tree topology. Because this, spanning tree parameters related to BPDU transmission (such as hello time, forward time, max-age, and max-hops) are configured only in the CST instance but not all of the MST instances. parameters related to spanning tree topology (for example, switch priority, port VLAN cost Port VLAN priority can be configured in a CST instance and an MST instance.

The MSTP switch uses the RSTP BPDU of version 3 or the BPDU of 802.1D and the switch for 802.1D. The MSTP switch communicates with the MSTP BPDU and the MSTP switch.

8.1.6 Hop Count

IST and MST instances do not use message-age and maximum-age information in the IST and MST instances that configure the generative tree topology. Instead, the path to the root is spent and the hop-count mechanism equivalent to IP TTL is used.

You can configure the maximum hop number of that domain and apply it to that domain IST and all MST instances. The hop calculation implementation is the same as the message-age result (decided after a reconfiguration is raised). The instance root switch always sends a BPDU (or-M-record) with a cost of 0 and a hop-count of the maximum. When a switch receives BPDU, it subtracts the remaining hops by 1 and propagates the remaining hops in the BPDU it produces. When the count reaches 0, the switch discards the BPDU and age the port information.

In a domain, the Message-age and maximum-age information in the RSTP BPDU section remain the same, and the same value is propagated on the specified port of the domain of the boundary (boundary).

8.1.7 Boundary Port

A boundary port is a spanning tree domain that connects the MST domain to a single running RSTP, or a single, 801.1D spanning tree domain, or other differently configured MST domains. A border port is also connected to a LAN, either a single spanning tree switch or a switch with a different MST domain configuration.

The MST port role is not important at the border port, and their states are forced to be the same as the IST port state (the MST port on the boundary is for when the IST port is for forwarding). An IST port at the boundary can have any role other than the backup port.

At a shared boundary, the MST port waits for forward-delay time to expire in the blocking state before transitioning to the lehold state. The MST port is waiting for another forward-delay time to expire before transitioning to forwarding.

If the border port is a point-to-point connection and is a IST root port, the IST port is switched to the forwarding state by transitioning to the forwarding state MST port.

If a border port is switch to a forwarding state in an instance, it is for in all instances and a topology change is triggered. If a border port with a IST root or a specified port role receives a topology change notification, the MSTP switch triggers a topology change on the active one of the IST instances and all MST instances on that port.

8.1.8 MSTP and 802.1d STP Interoperability

A switch running MSTP supports a built-in protocol migration mechanism that enables him to use with 802.1D. If the switch receives an 802.1D-configured BPDU from one port, it sends an 802.1D BPDU at that port. MSTP

switches can be detected when a domain's border port receives a MSTP BPDU or RSTP BPDU for a different domain of an 802.1D BPDU.

However, if the switch no longer receives the 802.1D BPDU, it will not automatically revert to the MSTP mode because it cannot determine if the other's switch has been removed from the connection, unless the other's switch is the specified switch. Also, when a switch connected to this switch has been added to this domain, the switch may continue to assign a border port role to one port. Restart the protocol's migration process (forced and neighbor switch negotiation).

If all the switches connected to each other are RSTP switches, they can handle MSTP BPDU and RSTP BPDU. Therefore, the MSTP switch is on the boundary port or sends a version 0 configuration and TCN BPDU or version 3 MSTP BPDU. A boundary port connected to the LAN, whose specified switch is either a separate spanning tree switch or a switch with a different MST configuration.

8.1.9 Port Role

MSTP adopts the fast convergence algorithm of RSTP. The following is a brief introduction to the MSTP port role and the fast convergence in conjunction with RSTP.

RSTP provides fast convergence to specify port roles and determine active topologies. Based on IEEE802.1D STP, high priority switches are selected as root switches. When RSTP specifies a port role to a port:

Root port-provides optimal path cost when the switch forwards packets to the root switch.

Designated port-connect to the specified switch. When forwarding packets from LAN to the root switch produces the lowest path cost. The port through which the specified switch is connected to the LAN is called the specified port.

Alternate port- provides a replacement path from the current root port to the root switch.

Backup port- acts as a backup of the path from the specified port to the spanning tree leaf. A Backup port exists only when two ports are connected to a point-to-point loop together or when a switch has two or more connections to a shared LAN segment.

Disable port- has no port role in the build tree operation.

Master port — On the shortest path to the domain root or to the total root, it is the port that connects the domain to the total root.

The root port or the specified port role is included in the active topology. The alternate port or backup port role is not included in the active topology.

Throughout a stable topology and fixed port role, RSTP ensures that each root port and specified port is immediately migrated to the forwarding state when all replacement ports and backup ports are always in the discarding state. Port status controls forwarding and learning processing.

Fast Convergence

RSTP provides quick recovery in the following cases: switch failure, port failure, or LAN failure, which provides quick recovery for edge ports, new root ports, and connection to a point-to-point connection:

Edge ports-if you configure a port as an edge port, the edge port is immediately migrated to the forwarding state. You can open it for the boundary port only when the port is connected to a separate terminal or make sure that

there is no need to calculate the build tree on the device.

Root ports-if RSTP selects a new root port. It blocks an old root port and immediately migrate the new root port to the forwarding state.

Point-to-point links — If you connect a port to another port through a point-to-point connection and the local port becomes a designated port, it negotiates a fast migration with the other port through a proposal-agreement handshake to determine a fast convergence loop (loop-free) topology.

Topology Change

This section describes the differences between RSTP and 802.1D in dealing with spanning-tree topology changes.

Detection-unlike any migration between blocking and forwarding states in 802.1D, topology changes occur only from blocking to forwarding states (only topology changes are considered in order to increase connectivity). State changes at one edge of the port (edge port) do not cause topology changes. When a RSTP switch detects a topology change, it floods it to learn information to all non-edge ports (nonedge ports) except The port outside of the received TC information.

Notification-Unlike 802.1D, with TCN BPDUs, RSTP does not use it. However, for interoperability with 802.1D, the RSTP switch processes and generates a TCP BPDU.

Acknowledge — When an RSTP switch receives a TCN message from an 802.1D switch at a designated port, it responds to a TCN with an 802.1D BPDU and sets the TCA flag bit. However, if the TC-while timer (same as the topology-change timer of 802.1D) is active, the TC-while timer is heavy (reset) when the root port is connected to the 802.1D switch and a configuration BPDU with the TCA is received)。This behavior is only required to support the 802.1D switch. RSTP BPDU never has TCA flag bits.

Propagation-when a RSTP switch receives an TC message from another switch through a specified port or root port, it propagates to all non-edge ports, specified ports and root ports (except for receiving ports). All such ports on the switch start TC-while timer and flood the information they learn.

Protocol migration-in order to be backward compatible with the 802.1D switch, RSTP selectively sends the 802.1D configuration BPDU and TCN BPDU. based on each port

When an initialization has been initiated, the migrate-delay timer starts (specifies that the minimum value is sent when the RSTP BPDU is sent. When the timer is active, the switch processes all BPDU received from the port and ignores the protocol type.

After the migration-delay timer of the port has been aborted, if the switch receives an 802.1D BPDU, it assumes that it is connected to an 802.1D switch and starts using the 802.1D protocol BPDU. However, if the RSTP switch is using 802.1D BPDU, on one port and receives a RSTP BPDU, port after timer aborts, it restarts timer and starts using RSTP BPDU.

8.1.10 Introduction to 802.1D Spanning Tree

Spanning Tree Protocol is based on the following:

1) A unique group address (01-80-C2-00-00-00) identifies all switches on a particular LAN. This group of addresses can be identified by all switches;

2) Each switch has a unique identifier;

3) The port of each switch has a unique Port Identifier. Managing the configuration of the spanning tree also requires: a relative priority for each switch; a relative priority for each port of each switch; and a path cost for each port.

The switch with the highest priority is called the root switch. Each switch port has a root path cost, and the root path cost is the sum of the path spent by the switch to the individual segments of the root switch. The root path in one switch takes the lowest value as the root port, and if multiple ports have the same root path cost, the port with the highest priority is the root port.
In each LAN, there is a switch called the specified (designated) switch, which belongs to the switch with the least cost of the root path in the LAN. The port that connects the LAN to the specified switch is the specified port (designated port). Of the LAN If more than two ports in the specified switch are connected to the LAN, the port with the highest priority is selected as the specified port.
The elements that must be determined to form a build tree:

1) Determine the root switch.

A, at first all switches thought they were root switches;

B. The switch sends BPDU to the LAN broadcast connected to it, and its root_id is the same as the value of bridge_id;

C, when the switch receives a configuration BPDU from another switch, if it is found that the value of the root_id field in the received configuration BPDU is greater than the value of the root_id parameter in the switch, the frame is discarded, otherwise the root_id, root path of the switch is updated with the value of parameters such as root_path_cost, and the switch will continue to broadcast the configuration BPDU. at a new value

2) Determine the root port.
The port that takes the root path in one switch is the lowest port called the root port.
If multiple ports have the same minimum root path cost, the port with the highest priority is the root port. If two or more ports have the same minimum root path cost and highest priority, the port with the minimum port number is the default root port.

3) Identify the designated switch of the LAN

A, at first, all switches thought they were designated switches for LAN.

B, when a switch receives an BPDU, from another switch with a lower root path cost (in the same LAN), the switch no longer claims to be a designated switch. If two or more switches in a LAN have the same root path cost, the switch with the highest priority is selected as the specified switch.

C, if the specified switch receives a configuration BPDU, sent by other switches on the LAN at some point because of a competition for the specified switch, the designated switch sends a responsive configuration BPDU, to reconfirm the specified switch.

Decide to specify the port.

The port connected to the LAN in the specified switch of the LAN is the specified port. If the specified switch has two or more ports connected to the LAN, the port with the lowest identification is the specified port.
With the exception of the root port and the specified port, all ports will be set to blocking. In this way, after determining the root switch, the root port of the switch, and the specified switch and port of each LAN, the topology of a spanning tree is also determined.

8.2 MSTP Configuration

8.2.1 Default Configuration

command parameter	default value
spanning-tree mst enable(firing mstp)	close
Spanning-tree mst priority(switch cist priority)	32768
spanning-tree mst hello-time(switch cist hello-time)	2 second
spanning-tree mst forward-time(switch cist forward-time)	15 second
spanning-tree mst max-age(switch cist max-age)	20 second
spanning-tree mst max-hops(switch cist max-hops)	20 second
instance 1 priority (Instance priority)	32768
spanning-tree mst instance 1 priority(Port instance priority)	128
spanning-tree mst instance 1 path-cost(Port instance path-cost)	20000000
spanning-tree mst priority （Port cist priority）	128

spanning-tree mst path-cost（Port cist path-cost）	20000000

8.2.2 General Configuration

Start MSTP

The system is off by default to configure MSTP at startup.

The configuration process for starting MSTP is:Switch#configure terminal

Switch(config)#spanning-tree mst enable

The command to close MSTP is:

Switch#configure terminal

Switch(config)#no spanning-tree mst

Configure max-age

Configuring max-age is the configuration of all instances, and max-age is the number of seconds the switch waits to receive the build tree configuration information before trigger a reconfiguration.

The default configuration is 20 seconds and the configuration range is 6 to 40 seconds.

Configuration process:

Switch#configure terminal

Switch(config)#spanning-tree mst max-age <seconds>

Configure max-hops

Max-hops is the number of hops specified in a domain before the BPDU is dropped.

The default value is 20 and the configuration range is 1 to 40.

Configuration process:

Switch#configure terminal

Switch(config)#spanning-tree mst max-hops <hop-count>

Configure forward-time

Configuring forward-time is for all instances. Forward-time is the number of seconds the port waits from discarding to learning and learning to forwarding.

The default configuration is 15 seconds and the configuration range is 4 to 30 seconds. Forward-time must meet the following criteria:2 * (forward-time-1)> = max-age, according to the generation number protocol forward-time.

Configuration process:

Switch#configure terminal

Switch(config)#spanning-tree mst forward-time <seconds>

Configure hello-time

Configuring helltime is the configuration for all instances. helltime is the interval between the root switch to generate configuration information.

The default configuration time is 2 seconds and the configuration range is 1 to 10 seconds. According to the generated number protocol hello-time must meet the following conditions: 2 * (hello-time 1) = < max-age.

Configuration process:

Switch#configure terminal

Switch(config)# spanning-tree mst hello-time <seconds>

Configure the priority (priority) for CIST bridge

The default configuration is 32768, the configuration range is < 0 ≤ 61440 >; the value of CIST priority can only be a multiple of 4096.

Configuration process:

Switch#configure terminal

Switch(config)#spanning-tree mst priority <priority>

Configuration and CISCO compatibility

The switch uses the 802.1s-based MSTP protocol, the length of each MSTI message is 16 bytes, and the length of the BPDUs per MSTI message for CISCO switches is 26 bytes. For interoperability with CISCO switches, configure the switch to start and CISCO-compatible switches.

In the case of a startup and CISCO-compatible configuration, the same domain is considered to be the same as long as the domain name and revision number are the same when it is determined whether to be the same domain.

The default system does not start this feature.

Open and CISCO compatible:

Switch#configure terminal

Switch(config)#spanning-tree mst cisco-interoperability enable

Turn off compatibility with CISCO:

Switch#configure terminal

Switch(config)#spanning-tree mst cisco-interoperability disable

Reset protocol check task

In order to be compatible with the 802.1 DSTP protocol, the system can automatically reconnoitre the protocol running by the other system. Depending on the protocol the other side runs to determine the protocol this port runs.

In some cases, the protocol is to be reset. For example, after a system has negotiated a port to run the STP protocol, the device running the STP protocol for a period of time has been replaced with one host. At this point, I need to configure this port as the fast port, but the port has run the stp protocol, and the task of the protocol negotiation has stopped; the task to reset this protocol negotiation is required to re-negotiate the protocol between it and the host.

Reset the protocol reconnaissance mission of the entire equipment:

Switch#clear spanning-tree detected protocols

Reset the protocol reconnaissance mission for a port:Switch#clear spanning-tree detected protocols interface <if-name>

8.2.3 Domain Configuration

Two or more devices in the same domain, they must have the same VLAN instance mapping, the same modified version number and the same domain name.

A domain has one or more members with the same MST configuration, each of which can handle RSTP BPDUS capabilities. There is no limit to the number of members in a network, but each domain can support up to 16 instances.

The configuration of the instance is described in the instance configuration, which only describes the domain name configuration and the revised version number configuration.

Configure domain names:

Switch#configure terminal

Switch(config)#spanning-tree mst configuration

Switch(config-mst)#region <region-name>

Configuration revision number:

Switch#configure terminal

Switch(config)#spanning-tree mst configuration

Switch(config-mst)# revision <revision-num>

8.2.4 Instance Configuration

The system supports 16 instances, and the range of the instance ID number is 0-15. A VLAN can only be assigned to one spanning tree instance at a time.

There is only one instance 0 by default, and all VLAN belongs to this instance.

The process of configuring an instance:

Switch#configure terminal

Switch(config)#spanning-tree mst configuration

Switch(config-mst)#instance <instance-id> vlan <vlan-id>

Configure the priority (priority) for MSTI bridge

The default configuration is 32768, the configuration range is < 0 ≤ 61440 >; the value of MSTI priority can only be a multiple of 4096.

Configuration process:

Switch#configure terminal

Switch(config)#spanning-tree mst configuration

Switch(config-mst)#instance <instance-id> priority <priority>

8.2.5 Port Configuration

The port configuration information related to MSTP is described below. Only the simple configuration sections, port fast and root guard are described here separately later.

The process of configuring a port to join to an instance:
Switch#configure terminal
Switch(config)#interface <if-name>
Switch(config)#spanning-tree mst instance <instance-id>

Configure the priority (priority) of the CIST port

The default configuration is 128, the configuration range is < 0 ≤ 240 >, and the priority of the CIST port can only be a multiple of 16.

Configuration process:
Switch#configure terminal
Switch(config)#interface <if-name>
Switch(config)#spanning-tree mst priority <priority>

Configure the priority of the MSTI port

The default configuration 128, the configuration range is <0-240>, and the value of the MSTI port's priority can only be a multiple of 16.

Configuration process:
Switch#configure terminal
Switch(config)#interface <if-name>
Switch(config)#spanning-tree mst instance <instance-id> priority <priority>

Path-cost to configure the CIST port
The default configuration is 20000000, and the configuration range is 1 ≤ 200000000. The following is a table of bandwidth and path cancellation maps:

Bandwidth (bps)	Path flower elimination
100,000(100K)	200000000
1,000,000(1M)	20000000
10,000,000(10M)	2000000
100,000,000(100M)	200000

1,000,000,000(1G)	20000
10,000,000,000(10G)	2000
100,000,000,000(100G)	200
1,000,000,000,000(1T)	20
>1000000000000	2

Configuration procedure

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config)#spanning-tree mst path <path-cost>

Configure the path cost of the MSTI port (path-cost)

The default configuration is 20000000, and the configuration range is 1 ≤ 200000000. Bandwidth and path costs are the same as the table above.

Configuration procedure

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config)#spanning-tree mst instance <instance-id> path-cost <path-cost>

Configure the version number of the sending protocol package.

The default configuration sends the MSTP protocol package, the configuration range is 0 ≤ 3, the mapping relationship is 0% stp2 / rstp, 3 / mstp.

Configuration procedure

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config)# spanning-tree mst force-version <version-id>

Configure connection type

If one port is connected to another port in a point-to-point manner, and the local port becomes a designated port (designated port,), RSTP negotiates a fast migration of the port to which it is connected into a root port through the proposal-agreement (proposal-protocol) process to determine an acyclic topology.

The following is a brief introduction to the negotiation process of proposal-agreement.

When the switch receives a proposal message on one of its ports and that port is selected as the new root port, RSTP forces all other ports to synchronize the new root port information.

If all other ports are synchronized with better (superior) root information received from the root port, the switch is synchronized.

When RSTP forces it to synchronize new root information, it migrate to the blocking state if a specified port is in the forwarding state and is not configured as an edge port. Typically, when RSTP forces a port to synchronize a new root message and the port does not meet the above conditions, the port state is set to blocking.

When ensuring that all ports are synchronized, the switch sends an acknowledgement message to the specified port corresponding to the root port. When the switch is connected to a point-to-point connection in their port role, RSTP immediately migrates the port state of forwarding.

If it is a shared connection, the state of the port is determined by the calculation process of 802.1D.

The default port connection type is a point-to-point connection.

The connection type of the configuration port is a point-to-point connection:

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config)#spanning-tree mst link-type point-to-point

The connection type of the configuration port is a shared connection:

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config-ge1/2)#spanning-tree mst link-type shared

8.2.6 PORTFAST Related Configuration

1) Port Fast

Port Fast immediately transfers a access or trunk port from the blocking state to the forwarding state, bypassing the listening and learning states. You can use Port Fast to connect to a separate workstation and server, allowing these devices to connect to the network immediately without waiting for spanning tree to converge.

Configure a port to fast port:

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config)#spanning-tree mst portfast

2) BPDU Filtering

BPDU filtering can be opened globally or on a per-port basis, but their characteristics are different.

In the global layer, you can use the spanning-tree mst portfast bpdu-filter command to start the BPDU filtering function on the port in the portfast bpdu-filter default state.

At the port layer, you can use spanning-tree mst portfast bpdu-filter enable to open BPDU filter. on any port

This feature prevents the port fast port from receiving or sending BPDUs.

Configure BPDU Filtering

In global configuration mode:Switch#configure terminal

Switch(config)# spanning-tree mst portfast bpdu-filter

In interface configuration mode:

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config)#spanning-tree mst portfast bpdu-filter enable

3) BPDU Guard

BPDU protection features can be opened globally on the switch or on a per-port basis, but their characteristics are different.

In the global layer, you can use spanning-tree mst portfast bpdu-guard to turn on the BPDU guard function of the port in the portfast bpdu-gurad default state.

At the port layer, you can open BPDU guard. on any port

When a port configured with BPDU gurad receives BPDU, spanning tree shutdown this port. In a valid configuration, the port of Port Fast-enabled does not receive BPDU. Receiving a BPDU on a Port Fast-enabled port represents an invalid configuration, such as an unauthorized device's connection, BPDU guard entering a error-disabled state.

Error-disabled is when a BPDU is received from a port that starts a BPDU guard, an error-disable timer is started if the system is configured with an error-disable mechanism. Error-disable restarts the port after the system's system configuration has timed out.

In global configuration mode:

Switch#configure terminal

Switch(config)# spanning-tree mst portfast bpdu-guard

In interface configuration mode:

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config)#spanning-tree mst portfast bpdu-guard enable

error-disable Configuration

Start the error-disable mechanism

Switch#configure terminal

Switch(config)#spanning-tree mst errdisable-timeout enable

Configure error-disable timeout

Switch#configure terminal

Switch(config)#spanning-tree mst errdisable-timeout interval <seconds>

8.2.7 Root Guard Related Configuration

A two-layer network of one SP can contain many switches that are not part of their own. In such a topology, the spanning tree can reconfigure itself and select a customer switch as the root switch. You can avoid this by configuring root guard at the port of the SP switch that is connected to the switch on the customer's network. If the spanning-tree calculation results in the port being selected as root port on the client network, the root guard

configures the port as the root-in state to prevent the client switch from becoming the root. Change the machine or exist to the root of the path.

If a switch outside the SP network becomes the root switch, the port is blocked (root-inconsistent stat) and the spanning tree selects a new root switch. The customer's switch does not become the root switch and there is no path to the root.

If the switch operates in MST mode to force the port to become the specified port. If a boundary port because root guard is blocked in the IST instance, this port is block in all MST instances. A boundary port is a port connected to a LAN that specifies that the switch is either an 802.1D switch or a switch with a different MST domain configuration.

The VLAN.VLAN to which the Root guard is applied to all ports on one port can be aggregated and mapped to a MST instance.

Configuration procedure

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config)#spanning-tree mst guard root

8.3 MSTP Configuration Example

(1)Configuration

The three switches are connected into a ring, and the spanning tree protocol for each switch needs to be turned on to avoid the occurrence of loops. Perform the configuration on each switch separately.

Configuration of switch 1:

Switch>en

Switch#configure terminal

Switch(config)#spanning mst enable

Configuration of switch 2:

Switch>en

Switch#configure terminal

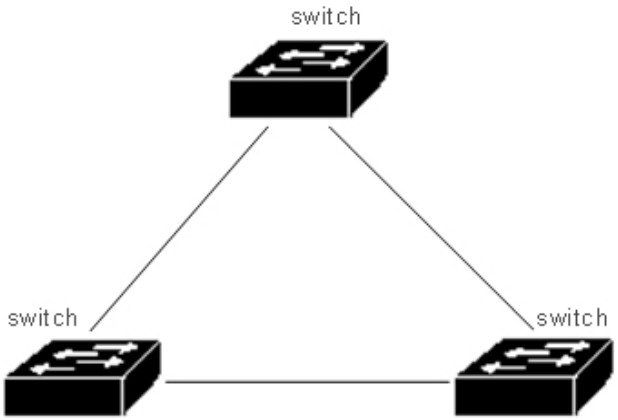
Switch(config)#spanning mst enable

Configuration of switch 3:

Switch>en

Switch#configure terminal

Switch(config)#spanning mst enable



(2)Troubleshooting:

See which switch is selected as the root bridge:

The value of CISTRoot observed by show spanning-tree mst, is the smallest of the three exchanges, that is, the root election result is correct.

Switch#show spanning-tree mst

View the port status of the switch in the build tree:

Execute the instruction show spanning-tree mst interface ge1/1 to observe the State value of PORT ge1/1 in instance 0Switch#show spanning-tree mst interface ge1/1

Chapter 9 EAPS Configuration

This chapter describes EAPS and its configuration, including the following:

- EAPS introduction
- EAPS basic concept
- Introduction to EAPS agreement
- EAPS configuration
- Restriction
- Configuration Example

9.1 EAPS Introduction

EAPS is the abbreviation of Ethernet Automatic Protecting Switching. Eaps uses standard Ethernet and VLAN technology to provide loop topology and loop recovery mechanism. In the event of a failure in the ring, EAPS has the ability to restore data communication within 1 second. EAPS operation is not limited by the number of nodes, and the recovery time of the ring is not limited by the number of nodes. EAPS does not rely on other devices, that is to say, there can be devices in the EAPS ring that do not support EAPS protocol.

9.2 EAPS Basic Concept

The following describes some of the basic concepts involved in the EAPS:

1, Eaps Domain, is in a network, a EAPS Domain is running in a separate ring. It is a series of node devices that make up a separate loop, and a EAPS Domain contains one Master Node and one or more Transit Node.

2. Master Node, a switch running EAPS or an EAPS node device, one EAPS Domain with and only one Master Node.

Transit Node, is a switch running EAPS, or EAPS node device, in an EAPS Domain with the exception of Master Node.

4, Primary Port, a port in a EAPS Domain that connects to a EAPS node device. A node device has and only one Primary Port is connected to this ring in a EAPS Domain.

5, Secondary Port, a port in a EAPS Domain that connects to a EAPS node device. A node device has and only one Secondary Port is connected to this ring in a EAPS Domain.

6, Control VLAN, controls that VLAN, has and has only one Control VLAN. in one EAPS Domain that is responsible for EAPS Domain protocol packet transmission

7, protected VLAN, is protected that VLAN, must have one Protected VLAN, or more than one Protected VLAN. in a VLAN, that transmits business data in EAPS Domain

9.3 EAPS Protocol Introduction

A EAPS Domain runs on a EAPS ring. A EAPS Domain contains one Master Node and one or more Transit Node; each EAPS node contains the same Control VLAN and multiple Protected VLAN; each EAPS node contains one Primary Port and one Secondary Port, in a EAPS Domain. Both ports belong to this ring Control VLAN. And all Protected VLAN.. Connect all the nodes in the EAPS Domain through the Primary Port and Secondary Port of each EAPS node device to form a EAPS ring.

Under normal circumstances, when all Primary Port and Secondary Port in EAPS Domain are LINK UP, the Secondary Port (that blocks Master Node sets the port state of Secondary Port to Blocking), to eliminate the loop of business data in EAPS Domain. When the EAPS Domain fails, open the Secondary port of the Master Node (set Secondar.) The status of the y Port is Forwarding, allowing it to forward traffic data and restore the normal forwarding of the traffic data.

There is no difference between Primary Port and Secondary Port treated by Transit Node.

Here are two types of fault checking and loop recovery for EAPS:

9.3.1 Link-Down Alarm

When Transit Node discovers that LINK DOWN appears on its own Primary Port or Secondary Port port, it immediately sends a LINK-DOWN protocol packet from Control VLAN to Master Node. through the port of another LINK UP
When Master Node receives this LINK-DOWN protocol package:
Master Node immediately enters the Failed state from the Complete state, opens the state of the Secondary Port (set Secondary Port to refresh its own layer 3 forwarding table for Forwarding), sends a RING-DOWN-FLUSH-FDB notification to EAPS Domain other Transit to refresh its own forwarding table, and relearns the second and third layer forwarding table.
When Master Node discovers the local Primary Port has LINK DOWN, its operation and the operation of receiving the LINK-DOWN protocol package are the same.
When Master Node finds that the local Secondary Port has LINK DOWN, Master Node immediately enters the Failed state from Complete state, refreshes its own layer 2 and 3 forwarding tables, sends RING-DOWN-FLUSH-FDB protocol packets, notifies EAPS Domain other Transit to refresh their own forwarding tables, and relearns the second and third layer forwarding tables.

9.3.2 Loop Check

Master Node regularly sends HEALTH protocol packets from Primary Port. If the ring is a complete, Master Node that can receive the HEALTH protocol package in its own Secondary Port, Master Node restarts its Fail-period timer, Master Node with a status of Complete.
If fail-period does not receive its own HEALTH protocol package before the expiration date, Master Node will leave the Complete state and enter the Failed state, open the Secondary Port state to refresh its own layer 3 forwarding table for Forwarding), send RING-DsOWN-FLUSH-FDB notification to EAPS Domain other Transit to refresh its own forwarding table, and re-learn the second and third layer forwarding table.

9.3.3 Ring Recovery

Master Node sends HEALTH packets from its Primary Port regardless of whether the ring is Complete or Failed or otherwise. When the Master Node is in the Failed state, once the HEALTH protocol package is received from its Secondary Port, the ring returns to the Complete state. At this point, the Master Node sets the state of the Secondary Port to the blocking state and refreshes its own layer 2 and 3 forwarding. Table, and send a RING-UP-FLUSH-FDB package to notify other devices to refresh their layer 2 and 3 forwarding tables and relearn layer 2 and 3 forwarding tables.

The secondary port of Master Node may still be in the ForwardState when the port of the Transimt Node is returned from LINK DOWN back to LINK UP and Master Node discovery loop recovery, which in this case results in a temporary loop. Therefore, when the Trans Node is in the LINK UP state at one port and the port of the other LINK DOWN becomes LINK UP, the Transimt Node will enter a "Front Forwar" Ding status "(PRE-FORWARDING), in which the port of the LINK UP will also be in the Pre-forwarding state, unable to forward the business data, interrupting the possible data loop. When Master Node recovers and sends RING-UP-FLUSH-FDB, Transit Node receives the protocol packet and switches the node state to the LINK-UP state, sets the port of the Pre-forwarding state to the Forwarding state, and resumes the service. Normal forwarding of data.
If Transit Node does not receive the RING-UP-FLUSH-FDB protocol package, it is set to the Forwarding state by

the port of the Pre-forwarding state after double the fail-time time.

9.3.4 Extreme Compatible EAPS

Extreme products were the first manufacturers to support EAPS, and the EAPS protocol supported by switches is in accordance with RFC3619 standards, while there are some differences between EAPS protocol packets for Extreme devices and RFC3619 protocol package definitions. The EAPS protocol supported by the switch is fully compatible with Extreme devices, and the compatible switch is turned on by default.

9.3.5 Multiple EAPS Domain

Switches can support multiple EAPS Domain, and a total of 16.

9.4 EAPS Configuration

The basic configuration of the EAPS protocol consists of several basic elements:ControlVLAN, Node Mode, PrimaryPort, SecondaryPort, ProtectedVLAN, HelloTime, and FailTime. HelloTime and FailTime have default configurations, HelloTime is 1 second, FailTimer is 3 seconds.

9.5 Reatriction

1, Primary Port must belong to a EAPS Domain Control VLAN and all Protected VLAN TRUNK schema members.

2, Eaps protocol can not run at the same time as MSTP protocol, if MSTP is started or MSTP instance is configured, EAPS protocol can not be started.

3, a VLAN that starts the VLLP protocol cannot be configured as a EAPS Control VLAN or Protected VLAN.

4, the Control VLAN of Eaps can only contain Primary Port and Secondary Port, and can only be the TRUNK schema of VLAN.

5, if a VLAN is configured as the Control VLAN, of the Domain of EAPS and the Domain has been started, the VLAN cannot be deleted, and its port members cannot be modified or deleted. Control VLAN cannot configure a three-tier interface.

6, Primary Port and Secondary Port in protected VLAN can only be TRUNK mode. Other member ports are not restricted.

7, a port can only be configured as a EAPS Domain Primary Port or Secondary Port.

8, the same VLAN can only belong to one EAPS Domain Control VLAN or Protected VLAN.

9, the control VLAN for all nodes in a EAPS Domain must be the same.

9.6 EAP Command Brief Introduction

To create a EAPS Domain, first make sure that the VLAN and port configurations meet the above conditions.

There are some sequential requirements for configuring EAPS. First, create a EAPS Domain, to configure other parameters according to the previous requirements before starting EAPS Domain; otherwise, the startup will not be successful. If you want to change the hello time to a value greater than the current fail time, change the fail time to a larger number first; otherwise, the configuration will not be successful. There are no specific requirements for other configuration sequences.

Control-vlan,mode,primary-port, secondary-port cannot be modified when a EAPS Domain has been started; protected-vlan, fail-timer, hello-time, extreme-interoperability can be modified.

Primary-port and secondary-port support LACP ports (that is, TRUNK groups).

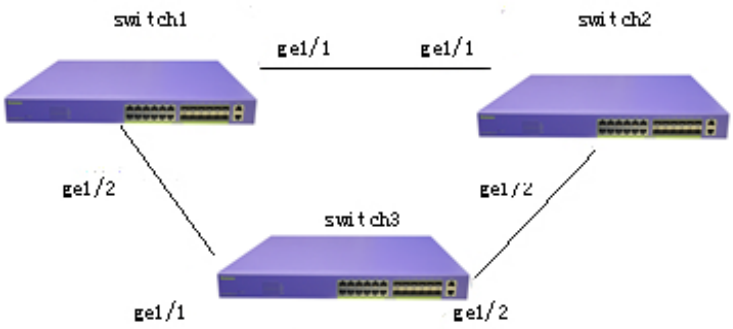
9.6.1 EAPS Configuration Command

The command	Description	CLI Model
eaps create <ring-id>	Create a EAPS Domain	Global configuration mode
eaps control-vlan <ring-id> <vlan-id>	Configure a control VLAN. for EAPS Domain	Global configuration mode
eaps protected-vlan <ring-id> <vlan-id>	Add a protected VLAN. for EAPS Domain	Global configuration mode
eaps mode <ring-id> <master|transit>	Configure a running node mode for EAPS Domain.。	Global configuration mode
eaps primary-port <ring-id> <ifname>	Configure a Primary Port for EAPS Domain.	Global configuration mode
eaps secondary-port <ring-id> <ifname>	Configure a Secondary Port for EAPS Domain.	Global configuration mode
eaps data-span <ring-id>	Configure EAPS ring data cross-loop forwarding	Global configuration mode
eaps fail-time <ring-id> <secs>	Time to configure a fail-period timer for an EAPS Domain. The default is 3 seconds. The unit is in seconds.	Global configuration mode
eaps hello-time <ring-id> <secs>	Configure the timing of a EAPS Domain to send HEALTH packets. The default is 1 second. The unit is seconds. Hello-timer must be less than fail-time.	Global configuration mode
eaps extreme-interoperability <ring-id> <enable|disable>	Startup or shutdown is compatible with the Extreme device, and the default is startup compatibility.	Global configuration mode
eaps enable <ring-id>	Start an EAPS Domain	Global configuration mode
eaps disable <ring-id>	Close an EAPS Domain	Global configuration mode

show eaps	Displays information about the EAPS Domain that has been started in the system.	Normal mode/ privileged mode
Show eaps <ring-id>	Display the details of a EAPSDomain	Normal mode/ privileged mode

9.7 Single Loop Configuration Example

There are three switches, switch1,switch2,switch3, that protect VLAN 1 from forming loops when forwarding traffic through the EAPS protocol, and ensure that backup links are enabled when a link between switch1,switch2,switch3 is disconnected. According to the above requirements, switch1 can be configured as master mode; switch2 and switch3 can be configured as transit mode. Add a protocol packet transmission control VLAN VLAN 2.



Configuration of switch1:

The master, control VLAN that switch1 is configured as EAPS Domain ring 1 is VLAN 2, the protected VLAN is VLAN 1, and the primary port is ge1/1,secondary-port is the default value for other ge1/2, configurations.

Switch#configure terminal

add VLAN 2 and 3Switch(config)#vlan database
Switch(config-vlan)#vlan 2-3
Switch(config-vlan)#exit

configure ge1/1 as trunk members of VLAN 1 and VLAN 2.
Switch(config)#interface ge1/1
Switch(config-ge1/1)#switchport mode trunk
Switch(config-ge1/1)#switchport trunk native vlan 3
Switch(config-ge1/1)#switchport trunk allowed vlan add 1,2

configure ge1/2 as trunk members of VLAN 1 and VLAN 2.
Switch(config-ge1/1)#interface ge1/2
Switch(config-ge1/2)#switchport mode trunk
Switch(config-ge1/2)#switchport trunk native vlan 3

```
Switch(config-ge1/2)#switchport trunk allowed vlan add 1,2

Switch(config-ge1/2)#exit
Switch(config)#exit
Switch#show vlan
 VLAN   Name         State        Member ports ([u]-Untagged, [t]-Tagged)
 ----   --------   ---------   ------------------------------------------------
 1      vlan1      active      [t]ge1/1 [t]ge1/2 [u]ge1/3 [u]ge1/4 [u]ge1/5
                                 [u]ge1/6 [u]ge1/7 [u]ge1/8 [u]ge1/9 [u]ge1/10
                                 [u]ge1/11 [u]ge1/12
 2      vlan2      active      [t]ge1/1 [t]ge1/2
 3      vlan3      active      [u]ge1/1 [u]ge1/2

Switch#configure terminal

# create a EAPS Domain ring 1

Switch(config)#eaps create 1

# configure VLAN 2 to control VLAN

Switch(config)#eaps control-vlan 1 2

# Configure VLAN 1 as a protected VLAN

Switch(config)#eaps protected-vlan 1 1

# Configure the switch1 as the master node

Switch(config)#eaps mode 1 master

# configure ge1/1 as primary-port

Switch(config)#eaps primary-port 1 ge1/1

# configure ge1/2 as secondary-port

Switch(config)#eaps secondary-port 1 ge1/2

# start EAPS Domain ring 1
```

Switch(config)#eaps enable 1

Configuration of Switch2

Switch2 is configured as a transit for EAPS Domainring1, the control VLAN is VLAN2, the protected VLAN is VLAN1, the primary-port is ge1/1, the secondary-port is ge1/2, and the other configurations use default values.

Switch#configure terminal

add VLAN 2 and 3

Switch(config)#vlan database

Switch(config-vlan)#vlan 2-3

Switch(config-vlan)#exit

configure ge1/1 as trunk members of VLAN 1 and VLAN 2.

Switch(config)#interface ge1/1

Switch(config-ge1/1)#switchport mode trunk

Switch(config-ge1/1)#switchport trunk native vlan 3

Switch(config-ge1/1)#switchport trunk allowed vlan add 1,2

configure ge1/2 as trunk members of VLAN 1 and VLAN 2.

Switch(config-ge1/1)#interface ge1/2

Switch(config-ge1/2)#switchport mode trunk

Switch(config-ge1/2)#switchport trunk native vlan 3

Switch(config-ge1/2)#switchport trunk allowed vlan add 1,2

Switch(config-ge1/2)#exit

Switch(config)#exit

Switch#show vlan

VLAN	Name	State	Member ports ([u]-Untagged, [t]-Tagged)
1	vlan1	active	[t]ge1/1 [t]ge1/2 [u]ge1/3 [u]ge1/4 [u]ge1/5 [u]ge1/6 [u]ge1/7 [u]ge1/8 [u]ge1/9 [u]ge1/10
2	vlan2	active	[t]ge1/1 [t]ge1/2
3	vlan3	active	[u]ge1/1 [u]ge1/2

Switch#configure terminal

create a EAPS Domain ring 1

Switch(config)#eaps create 1

configure VLAN 2 to control VLAN

Switch(config)#eaps control-vlan 1 2

Configure VLAN 1 as a protected VLAN

Switch(config)#eaps protected-vlan 1 1

configure switch as a transit node

Switch(config)#eaps mode 1 transit

configure ge1/1 as primary-port

Switch(config)#eaps primary-port 1 ge1/1

configure ge1/2 as secondary-port

Switch(config)#eaps secondary-port 1 ge1/2

start EAPS Domain ring 1

Switch(config)#eaps enable 1

Configuration of Switch3

The transit, control VLAN that Switch3 is configured as EAPS Domain ring 1 is VLAN 2, the protected VLAN is VLAN 1, and the primary port is ge1/1,secondary-port is the default value for other ge1/2, configurations.

Switch#configure terminal

add VLAN 2 and 3

Switch(config)#vlan database

```
Switch(config-vlan)#vlan 2-3

Switch(config-vlan)#exit

# configure ge1/1 as trunk members of VLAN 1 and VLAN 2.

Switch(config)#interface ge1/1

Switch(config-ge1/1)#switchport mode trunk

Switch(config-ge1/1)#switchport trunk native vlan 3

Switch(config-ge1/1)#switchport trunk allowed vlan add 1,2

# configure ge1/2 as trunk members of VLAN 1 and VLAN 2.
Switch(config-ge1/1)#interface ge1/2
Switch(config-ge1/2)#switchport mode trunk
Switch(config-ge1/2)#switchport trunk native vlan 3
Switch(config-ge1/2)#switchport trunk allowed vlan add 1,2

Switch(config-ge1/2)#exit
Switch(config)#exit
Switch#show vlan
 VLAN   Name         State        Member ports ([u]-Untagged, [t]-Tagged)
 ----   --------   ---------   ------------------------------------------------
 1      vlan1      active      [t]ge1/1 [t]ge1/2 [u]ge1/3 [u]ge1/4 [u]ge1/5
                                [u]ge1/6 [u]ge1/7 [u]ge1/8 [u]ge1/9 [u]ge1/10
                                [u]ge1/11 [u]ge1/12
 2      vlan2      active      [t]ge1/1 [t]ge1/2
 3      vlan3      active      [u]ge1/1 [u]ge1/2


Switch#configure terminal

# create a EAPS Domain ring 1

Switch(config)#eaps create 1

# configure VLAN 2 to control VLAN

Switch(config)#eaps control-vlan 1 2
```

Configure VLAN 1 as a protected VLAN

Switch(config)#eaps protected-vlan 1 1

configure switch3 as a transit node
Switch(config)#eaps mode 1 transit

configure ge1/1 as primary-port

Switch(config)#eaps primary-port 1 ge1/1

configure ge1/2 as secondary-port

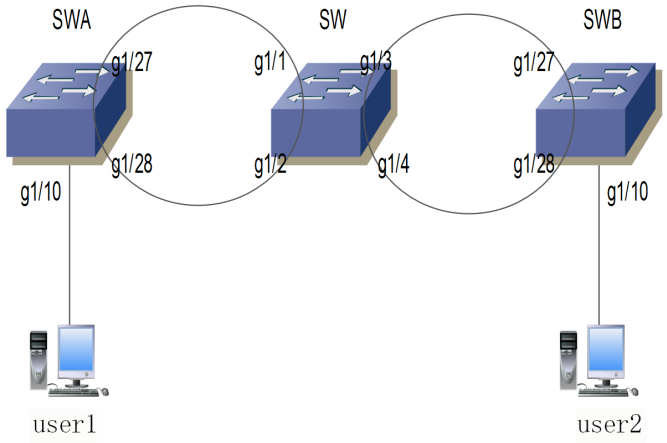
Switch(config)#eaps secondary-port 1 ge1/2

start EAPS Domain ring 1

Switch(config)#eaps enable 1

9.8 Example of Cross-loop Data Forwarding Configuration

There are three switches SWA,SW,SWB, to realize vlan1 vlan2 interworking through EAPS protocol cross-loop. The topology is as follows:



The SWA ring 1 controls the vlan111, protection vlan1,2, configuration as follows:
vlan database
vlan 2
vlan 111

interface ge1/10

```
 switchport access vlan 2
interface ge1/27
 switchport mode trunk
 switchport trunk allowed vlan add 2
 switchport trunk allowed vlan add 111
interface ge1/28
 switchport mode trunk
 switchport trunk allowed vlan add 2
 switchport trunk allowed vlan add 111

eaps create 1
eaps mode 1 Transit
eaps primary-port 1 ge1/27
eaps secondary-port 1 ge1/28
eaps control-vlan 1 111
eaps protected-vlan 1 1
eaps protected-vlan 1 2
eaps enable 1
```

SW Ring 1 docked with SWA to control vlan111, to protect vlan1,2. Ring 2 docks with SWB to control vlan222, to protect vlan3333 (virtual vlan, interfaces need to be added at the same time). If you want to implement ring 1 and ring 2 data cross-loop forwarding, you need to configure the command eaps data-span. The configuration is as follows:

```
vlan database
 vlan 2
 vlan 111
 vlan 222
 vlan 3333

interface ge1/1
 switchport mode trunk
 switchport trunk allowed vlan add 2
 switchport trunk allowed vlan add 111
interface ge1/2
 switchport mode trunk
 switchport trunk allowed vlan add 2
 switchport trunk allowed vlan add 111
interface ge1/3
 switchport mode trunk
 switchport trunk allowed vlan add 2
```

```
 switchport trunk allowed vlan add 222
 switchport trunk allowed vlan add 3333          ###Add virtual vlan 3333
interface ge1/4
 switchport mode trunk
 switchport trunk allowed vlan add 2
 switchport trunk allowed vlan add 222
 switchport trunk allowed vlan add 3333          ###Add virtual vlan 3333

eaps create 1
eaps mode 1 Master
eaps primary-port 1 ge1/1
eaps secondary-port 1 ge1/2
eaps control-vlan 1 111
eaps protected-vlan 1 1
eaps protected-vlan 1 2
eaps data-span 1
eaps enable 1

eaps create 2
eaps mode 2 Transit
eaps primary-port 2 ge1/3
eaps secondary-port 2 ge1/4
eaps control-vlan 2 222
eaps protected-vlan 2 3333                      ###here is the virtual protection vlan
eaps data-span 2
eaps enable 2
```

SWB ring 2 is in butt joint with SW ring 2 to control vlan222 to protect vlan1,2. The configuration is as follows:

```
vlan database
 vlan 2
 vlan 222

interface ge1/10
 switchport access vlan 2

interface ge1/27
 switchport mode trunk
 switchport trunk allowed vlan add 2
 switchport trunk allowed vlan add 222

interface ge1/28
```

```
 switchport mode trunk
 switchport trunk allowed vlan add 2
 switchport trunk allowed vlan add 222

eaps create 2
eaps mode 2 Master
eaps primary-port 2 ge1/27
eaps secondary-port 2 ge1/28
eaps control-vlan 2 222
eaps protected-vlan 2 1
eaps protected-vlan 2 2
eaps enable 2
```

After this configuration, the interworking between user 1 and user 2 is realized, and the vlan1 data is also interoperable. The eaps node pattern can be modified according to the requirements.

Chapter 10 ERPS Configuration

10.1 ERPS Overview

ERPS (Ethernet Ring Protection Switching, Ethernet protection switching protocol) is a kind of ring network protection protocol developed by ITU, also known as G. 8032. It is a link layer protocol specially used in Ethernet ring network. When the Ethernet network is complete, it can prevent the broadcast storm caused by the data loop, and when a link on the Ethernet is disconnected, it can quickly recover the communication between the nodes of the ring network. ERPS protocol provides a fast Ethernet protection mechanism, which can quickly restore the network transmission in the event of a failure of the ring network, thus ensuring that Barrier switches are highly available and reliable under the condition of ring network topology.

10.2 ERPS Technology Introduction

10.2.1 ERPS Ring

ERPS rings are based on the principle of minimizing rings, each ring must be the smallest ring, divided into main ring and subring: the main ring is a closed ring; the subring is a non-closed ring or a closed ring; all need to be configured by command.

Each ERPS ring (whether the main ring or the subring) has five states: (1) Idle state: each physical link in the ring network is connected; (2) Protection state: the state of one or more physical links in the ring network when one or more physical links are disconnected; (3) Manual switch state: manually change the state of the ring; (4) Forced switch state: force to change the state of the ring; (5) Pending state: pending intermediate state.

10.2.2 ERPS Node

The layer 2 switching device with ERPS ring is called node. Each node can not add more than two ports to the same ERPS ring, one port is RPL port, the other port is normal ring port.
Globally, the roles of nodes are divided into the following two categories: (1) intersecting nodes: in intersecting ERPS rings, nodes belonging to multiple rings are called intersecting nodes; (2) non-intersecting nodes: in intersecting ERPS rings, nodes that belong to only one ERPS ring are called non-intersecting nodes.
There are three types of node modes specified in ERPS protocol: RPL owner node, RPL neighbour node and ordinary ring node. (1) RPL owner node: a ERPS ring has only one RPL owner node, which is determined by user configuration to prevent loops in ERPS ring by blocking RPL port. When RPL owner node receives fault message to learn that other nodes or links on ERPS ring fail, RPL port will automatically release RPL port, this port will restore the reception and transmission of traffic. Ensure that traffic will not be interrupted; (2) RPL neighbour node: a node directly connected to the RPL port of a RPL owner node. Under normal circumstances, the RPL port of the, RPL owner node and the RPL port of the RPL neighbour node will be blocked to prevent loop generation. When the ERPS ring fails, both the RPL port of the, RPL owner node and the RPL port of the RPL neighbour node are released; (3) normal ring nodes: in the ERPS ring, except the RPL owner node and RPL neighbo The nodes other than the ur node are ordinary ring nodes. The RPL port of the ordinary ring node is no different from the ordinary ring port. The ring port of the ordinary ring node is responsible for monitoring the link state of the ERPS protocol directly connected to itself, and notifying other nodes of the change message of the link state in time.

10.2.3 Links and Channels

(1) RPL (Ring Protection Link, environmental protection link): each ERPS ring has and has only one RPL, the RPL port of the RPL owner node. When the etheric ring is in the Idle state, the RPL link is in a blocking state and does not forward the data message in order to avoid the formation of a loop.

(2) the sub-ring link: among the intersecting rings, the sub-ring is assigned to the sub-ring and the sub-ring is formed by the link of the sub-ring;

(2) RAPS (Ring Auto Protection Switch) virtual channel: In the intersection ring, the intersecting nodes are used for transmitting the sub-ring protocol message, but the path that does not belong to the sub-ring is called the RAPS virtual channel of the sub-ring.

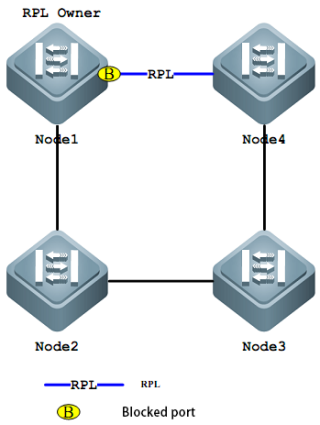
(3)

10.2.4 ERPS VLAN

There are two types of VLANs in the ERPS: (1) RAPS VLAN: used to pass the ERPS protocol message, the ports that access the ERPS ring on the device belong to the RAPS VLAN, and only the ports that are connected to the ERP ring can join this VLAN. The RAPS VLANs for different rings must be different. The configuration IP address is not allowed on the interface of the RAPS VLAN; (2) Data VLAN: opposite to the RAPS VLAN, the data VLAN is used to transfer the data message, and the data VLAN can contain both the ERP ring port and the non-ERP ring port.

10.3 ERPS Working Principle

10.3.1 Normal Condition

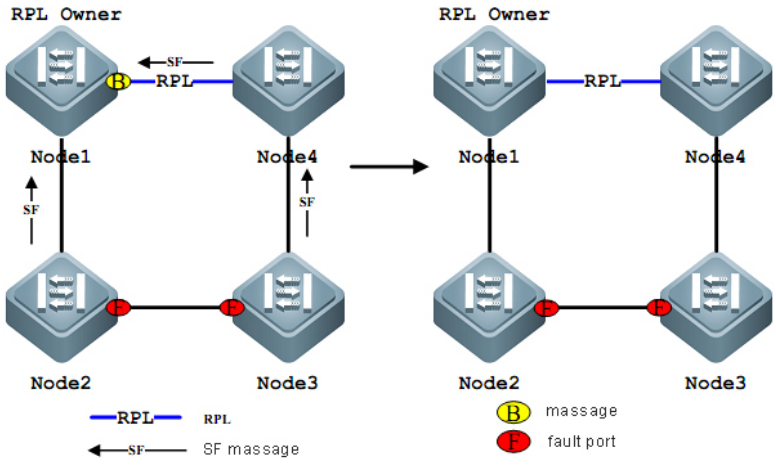


The main results are as follows: (1) all nodes are connected in a ring way in physical topology;

(2) the loop protection protocol ensures that it will not form a loop by blocking the RPL link. As shown in the figure above, the link between Node1 and Node4 is RPL link.

(3) Fault detection is carried out for each link between adjacent nodes.

10.3.2 Link Failure

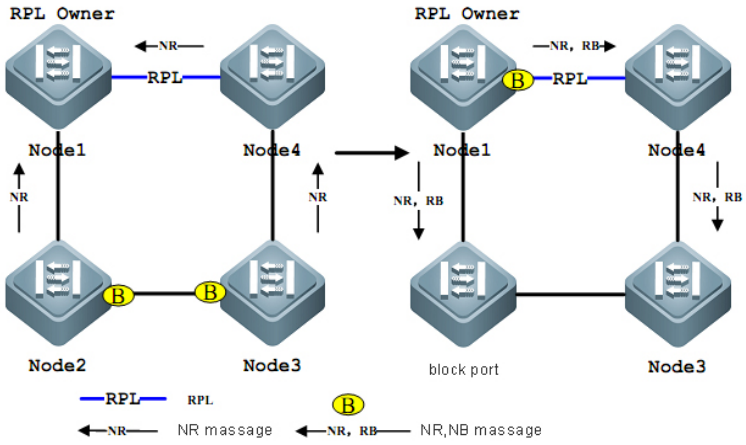


The main results are as follows:

(1) the nodes adjacent to the fault link block the fault link, and use RAPS (SF) message to report the fault to other nodes in the ring. As shown in the figure above, assuming the link failure between Node2,Node3, Node2 and Node3 will block the fault link after waiting for the holdoff timer to timeout, and send RAPS (SF) messages to each node on the ring network respectively.

(2) RAPS (SF) message triggers RPL owner node to open RPL port. Raps (SF) message also triggers all nodes to update their MAC table items, and then the node enters a protected state.

10.3.3 Link Recovery



The main results are as follows:

(1) when the fault recovers, the nodes adjacent to the fault continue to maintain the blocking state and send a RAPS (NR) message indicating that there is no local fault;

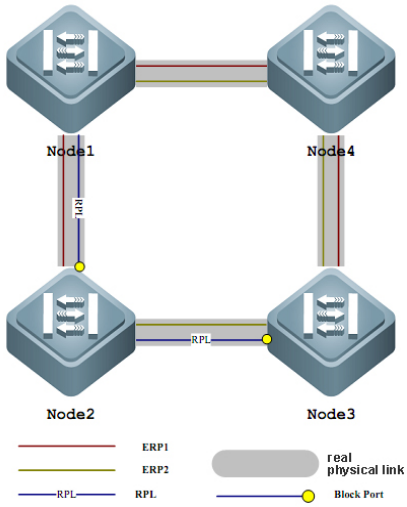
(2) after the guard timer is exhausted, after the, RPL Owner node receives the first RAPS (NR) message, it starts the WTR timer;

(3) when the WTR timer is exhausted, the RPL Owner node blocks the RPL and sends a RAPS (NR, RB) message;

(4) after receiving the message by other nodes, updating the respective MAC table items, sending the node of the RAPS (NR) message to stop sending the message periodically, and opening the originally blocked port. The ring network again returns to its original normal state.

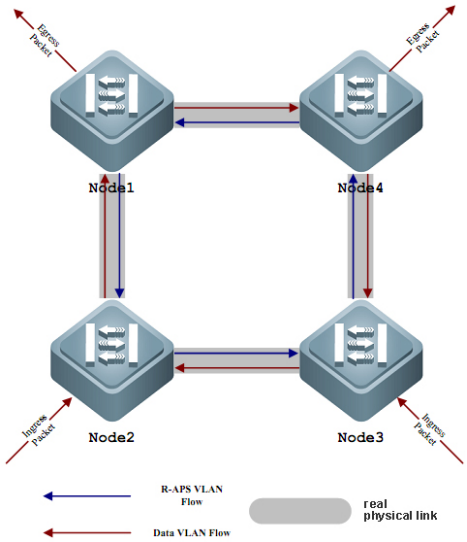
10.4 ERPS Technical Characteristics

10.4.1 ERPS Load Balancing



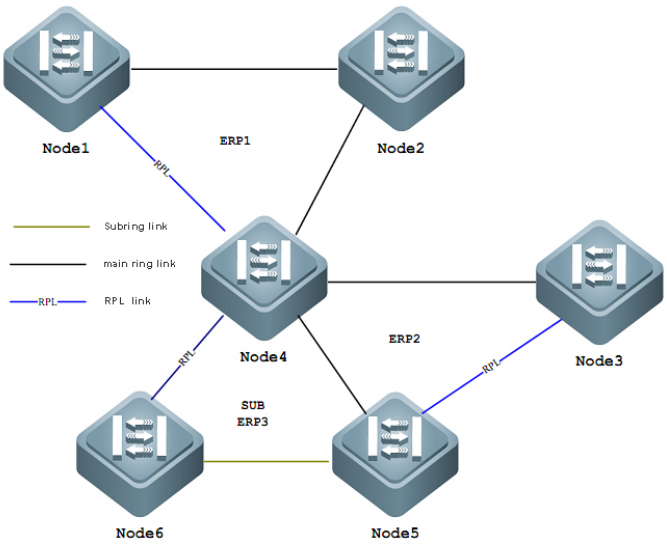
By configuring multiple instances and multiple ERPS rings on the same physical ring network, different ERPS rings send the traffic of different VLAN (called protected VLAN) to realize the different topology of different VLAN data traffic in the ring network, so as to achieve the purpose of load sharing. As shown in the figure above, a physical ring network corresponds to two instances and two ERPS rings. The VLAN protected by the two ERPS rings is different. Node2 is the RPL owner node of ERP1 and Node3 is the RPL owner node of ERP2. With configuration, different VLAN can be implemented separately Blocking different links to achieve single-loop load sharing.

10.4.2 Good Sefety



There are two types of VLAN, in ERPS, one is RAPS VLAN, the other is that data VLAN.RAPS VLAN is only used to transmit ERPS protocol messages, while ERPS only processes protocol messages from RAPS VLAN, and does not process any protocol attack messages from data VLAN to improve the security of ERPS.

10.4.3 Support Polycyclic Intersection Tangent



As shown in the figure above, ERPS supports the addition of multiple rings in the same node (Node4) in the form of tangent or intersection, which greatly increases the flexibility of networking.

10.5 ERPS Protocol Command

The command	Description	CLI Model
erps <1-8>	Create an instance of ERPS	Global configuration mode
no erps <1-8>	Delete a ERPS instance	Global configuration mode
node-role (interconnection | none-interconnection)	The role of the configuration node in the ERPS ring, the interconnect node, or the non-interconnect node	ERPS mode
ring <1-32>	Create a ERPS ring	ERPS mode
no ring <1-32>	Delete a ERPS ring	ERPS mode
ring <1-32> ring-mode (major-ring | sub-ring)	Configure ERPS ring mode, main ring or subring	ERPS mode

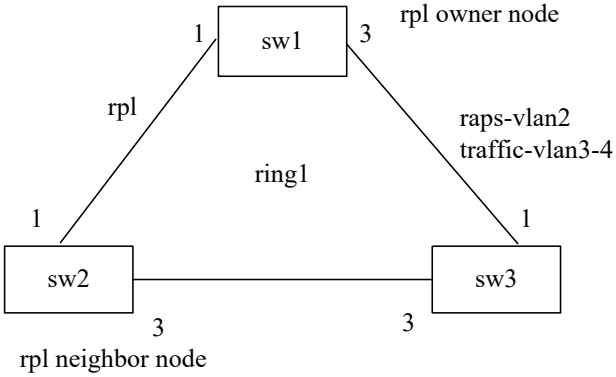
ring <1-32> node-mode (rpl-owner-node | rpl-neighbor-node | ring-node)	Configure ERPS Ring Node Mode, RPL owner Node, RPL neighbor Node or normal Ring Node	ERPS mode
ring <1-32> raps-vlan <2-4094>	Configure ERPS Ring Protocol VLAN	ERPS mode
no ring <1-32> raps-vlan	Delete ERPS Ring Protocol VLAN	ERPS mode
ring <1-32> traffic-vlan <1-4094>	Configure ERPS Ring data VLAN	ERPS mode
no ring <1-32> traffic-vlan <1-4094>	Delete ERPS ring data VLAN	ERPS mode
ring <1-32> (rpl-port|rl-port) IFNAME	Configure ERPS ring port, RPL port or normal ring port	ERPS mode
no ring <1-32> (rpl-port|rl-port)	Delete the ERPS ring port	ERPS mode
ring <1-32> revertive-behaviour (revertive|non-revertive)	Configure ERPS ring recovery behavior, recoverable or unrecoverable	ERPS mode
ring <1-32> hold-off-time <0-10000>	Configure ERPS ring hold-off time	ERPS mode
no ring <1-32> hold-off-time	Restore the default time of ERPS ring hold-off	ERPS mode
ring <1-32> guard-time <10-2000>	Configure ERPS ring guard time	ERPS mode
no ring <1-32> guard-time	Restore the default time of ERPS ring guard	ERPS mode
ring <1-32> wtr-time <1-12>	Configure ERPS ring wtr time	ERPS mode
no ring <1-32> wtr-time	Restore the ERPS loop wtr default time.	ERPS mode
ring <1-32> wtb-time <1-10>	Configure ERPS loop wtb time.	ERPS mode
no ring <1-32> wtb-time	Restore the ERPS loop wtb default time	ERPS mode
ring <1-32> raps-send-time <1-10>	Configuring the ERPS loop protocol message sending time	ERPS mode

no ring <1-32> raps-send-time	Restore the default sending time of ERPS Ring Protocol message	ERPS mode
ring <1-32> (enable|disable)	Turn the ERPS ring on or off	ERPS mode
ring <1-32> forced-switch IFNAME	Forced switching of ERPS ring ports	ERPS mode
ring <1-32> clear forced-switch	Clear forced switching of ERPS rings	ERPS mode
ring <1-32> manual-switch IFNAME	Manually switch the ERPS ring port.	ERPS mode
ring <1-32> clear manual-switch	Clear the manual switch of the ERPS ring	ERPS mode
ring <1-32> clear recovery	Manual recovery when clearing the unrecoverable behavior of the ERPS ring or manual recovery before the expiration of the WTR/WTB	ERPS mode
show erps	Displays a brief description of all ERPS instances and rings of the device	Privilege mode
show erps <1-8>	Displays the details of a single ERPS instance and ring of the device	Privilege mode

10.6 ERPS Typical Application

10.6.1 Single-loop Example

As shown in the following figure, the sw1,sw2 and sw3 nodes constitute a erps single ring ring1, node 1, 3 ports as the erps ring port, the ring protocol vlan is 2, the data vlan is 3, 4, the SW1 node is the rpl owner node, the sw2 node is the rpl neighbor node, and the link between sw1 and sw2 is the rpl link.



(1) configure sw1:

Switch>enable
Switch#configure terminal
Create erps Protocol and data vlan
Switch(config)#vlan database
Switch(config-vlan)#vlan 2-4
Switch(config-vlan)#exit
Configure Ring Port vlan Mode to join erps Protocol and data vlan for trunk,
Switch(config)# interface xe1/1
Switch(config-xe1/1)# switchport mode trunk
Switch(config-xe1/1)# switchport trunk allowed vlan add 2
Switch(config-xe1/1)# switchport trunk allowed vlan add 3
Switch(config-xe1/1)# switchport trunk allowed vlan add 4
Switch(config-xe1/1)# switchport trunk allowed vlan remove 1
Switch(config-xe1/1)#exit
Switch(config)# interface xe1/3
Switch(config-xe1/3)# switchport mode trunk
Switch(config-xe1/3)# switchport trunk allowed vlan add 2
Switch(config-xe1/3)# switchport trunk allowed vlan add 3
Switch(config-xe1/3)# switchport trunk allowed vlan add 4
Switch(config-xe1/3)# switchport trunk allowed vlan remove 1
Switch(config-xe1/3)#exit
Configure erps instance 1, erps single loop 1.
Switch(config)#erps 1
Switch(config-erps-1)#ring 1
Switch(config-erps-1)# ring 1 ring-mode major-ring
Switch(config-erps-1)# ring 1 node-mode rpl-owner-node
Switch(config-erps-1)# ring 1 raps-vlan 2
Switch(config-erps-1)# ring 1 traffic-vlan 3
Switch(config-erps-1)# ring 1 traffic-vlan 4

```
Switch(config-erps-1)# ring 1 rpl-port xe1/1
Switch(config-erps-1)# ring 1 rl-port xe1/3
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)#exit
```

(2) Configuration sw2:

```
Switch>enable
Switch#configure terminal
Create erps Protocol and data vlan
Switch(config)#vlan database
Switch(config-vlan)#vlan 2-4
Switch(config-vlan)#exit
Configure Ring Port vlan Mode to join erps Protocol and data vlan for trunk,
Switch(config)# interface xe1/1
Switch(config-xe1/1)# switchport mode trunk
Switch(config-xe1/1)# switchport trunk allowed vlan add 2
Switch(config-xe1/1)# switchport trunk allowed vlan add 3
Switch(config-xe1/1)# switchport trunk allowed vlan add 4
Switch(config-xe1/1)# switchport trunk allowed vlan remove 1
Switch(config-xe1/1)#exit
Switch(config)# interface xe1/3
Switch(config-xe1/3)# switchport mode trunk
Switch(config-xe1/3)# switchport trunk allowed vlan add 2
Switch(config-xe1/3)# switchport trunk allowed vlan add 3
Switch(config-xe1/3)# switchport trunk allowed vlan add 4
Switch(config-xe1/3)# switchport trunk allowed vlan remove 1
Switch(config-xe1/3)#exit
Configure erps instance 1, erps single loop 1.
Switch(config)#erps 1
Switch(config-erps-1)#ring 1
Switch(config-erps-1)# ring 1 ring-mode major-ring
Switch(config-erps-1)# ring 1 node-mode rpl-neighbor-node
Switch(config-erps-1)# ring 1 raps-vlan 2
Switch(config-erps-1)# ring 1 traffic-vlan 3
Switch(config-erps-1)# ring 1 traffic-vlan 4
Switch(config-erps-1)# ring 1 rpl-port xe1/1
Switch(config-erps-1)# ring 1 rl-port xe1/3
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)#exit
```

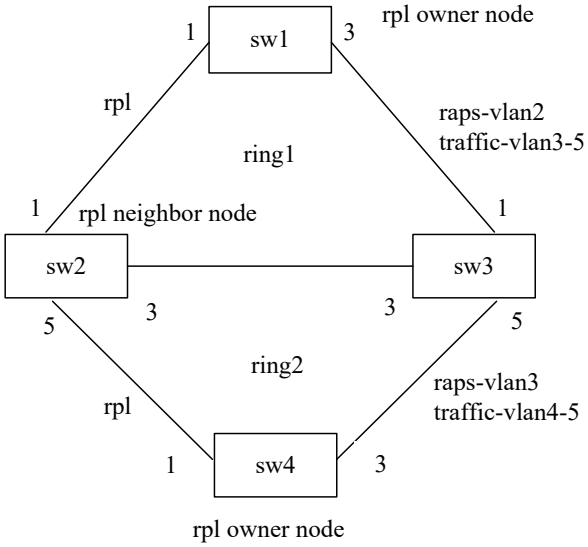
(3) Configuration sw3:

```
Switch>enable
Switch#configure terminal
Create erps Protocol and data vlan
Switch(config)#vlan database
Switch(config-vlan)#vlan 2-4
Switch(config-vlan)#exit
Configure Ring Port vlan Mode to join erps Protocol and data vlan for trunk,
Switch(config)# interface xe1/1
Switch(config-xe1/1)# switchport mode trunk
Switch(config-xe1/1)# switchport trunk allowed vlan add 2
Switch(config-xe1/1)# switchport trunk allowed vlan add 3
Switch(config-xe1/1)# switchport trunk allowed vlan add 4
Switch(config-xe1/1)# switchport trunk allowed vlan remove 1
Switch(config-xe1/1)#exit
Switch(config)# interface xe1/3
Switch(config-xe1/3)# switchport mode trunk
Switch(config-xe1/3)# switchport trunk allowed vlan add 2
Switch(config-xe1/3)# switchport trunk allowed vlan add 3
Switch(config-xe1/3)# switchport trunk allowed vlan add 4
Switch(config-xe1/3)# switchport trunk allowed vlan remove 1
Switch(config-xe1/3)#exit
Configure erps instance 1, erps single loop 1.
Switch(config)#erps 1
Switch(config-erps-1)#ring 1
Switch(config-erps-1)# ring 1 ring-mode major-ring
Switch(config-erps-1)# ring 1 node-mode ring-node
Switch(config-erps-1)# ring 1 raps-vlan 2
Switch(config-erps-1)# ring 1 traffic-vlan 3
Switch(config-erps-1)# ring 1 traffic-vlan 4
Switch(config-erps-1)# ring 1 rpl-port xe1/1
Switch(config-erps-1)# ring 1 rl-port xe1/3
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)#exit
```

10.6.2 Multi-ring Example

As shown in the figure below, the sw1, sw2 and sw3 nodes form the 1,3 ports of an erps main ring ring1, sw1, sw2 and sw3 node as the main ring ring1 ring port. The protocol vlan of the main ring ring 1 is 2, the data vlan is 3, 4, 5, sw1 node is the main ring ring1rpowner node, the sw2 node is the main ring ring1rplnesighbor node, the link between sw1 and sw2 is the main ring ring1rpl link.

Sw2, sw3, and sw4 nodes form a 1,3 port of a 5-port and a sw4 node of an erps sub-ring ring2, sw2, sw3 node as a subring ring2 ring port, the protocol vlan of the sub-ring ring2 is 3, the data vlan is 4,5, and the sw4 node is a sub-ring ring2 rpl owner node, and the link between sw2 and sw4 is a sub-ring ring2 rpl link.



(1) configure sw1:

Switch>enable

Switch#configure terminal

Create erps Protocol and data vlan

Switch(config)#vlan database

Switch(config-vlan)#vlan 2-5

Switch(config-vlan)#exit

Configure Ring Port vlan Mode to join erps Protocol and data vlan for trunk,

Switch(config)# interface xe1/1

Switch(config-xe1/1)# switchport mode trunk

Switch(config-xe1/1)# switchport trunk allowed vlan add 2

Switch(config-xe1/1)# switchport trunk allowed vlan add 3

Switch(config-xe1/1)# switchport trunk allowed vlan add 4

Switch(config-xe1/1)# switchport trunk allowed vlan add 5

Switch(config-xe1/1)# switchport trunk allowed vlan remove 1

Switch(config-xe1/1)#exit

Switch(config)# interface xe1/3

Switch(config-xe1/3)# switchport mode trunk

Switch(config-xe1/3)# switchport trunk allowed vlan add 2

Switch(config-xe1/3)# switchport trunk allowed vlan add 3

Switch(config-xe1/3)# switchport trunk allowed vlan add 4

Switch(config-xe1/3)# switchport trunk allowed vlan add 5

Switch(config-xe1/3)# switchport trunk allowed vlan remove 1

```
Switch(config-xe1/3)#exit
Configure erps instance 1, erps main ring 1
Switch(config)#erps 1
Switch(config-erps-1)#ring 1
Switch(config-erps-1)# ring 1 ring-mode major-ring
Switch(config-erps-1)# ring 1 node-mode rpl-owner-node
Switch(config-erps-1)# ring 1 raps-vlan 2
Switch(config-erps-1)# ring 1 traffic-vlan 3
Switch(config-erps-1)# ring 1 traffic-vlan 4
Switch(config-erps-1)# ring 1 traffic-vlan 5
Switch(config-erps-1)# ring 1 rpl-port xe1/1
Switch(config-erps-1)# ring 1 rl-port xe1/3
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)#exit
```

(2) Configuration sw2:

```
Switch>enable
Switch#configure terminal
Create erps Protocol and data vlan
Switch(config)#vlan database
Switch(config-vlan)#vlan 2-5
Switch(config-vlan)#exit
Configure Ring Port vlan Mode to join erps Protocol and data vlan for trunk,
Switch(config)# interface xe1/1
Switch(config-xe1/1)# switchport mode trunk
Switch(config-xe1/1)# switchport trunk allowed vlan add 2
Switch(config-xe1/1)# switchport trunk allowed vlan add 3
Switch(config-xe1/1)# switchport trunk allowed vlan add 4
Switch(config-xe1/1)# switchport trunk allowed vlan add 5
Switch(config-xe1/1)# switchport trunk allowed vlan remove 1
Switch(config-xe1/1)#exit
Switch(config)# interface xe1/3
Switch(config-xe1/3)# switchport mode trunk
Switch(config-xe1/3)# switchport trunk allowed vlan add 2
Switch(config-xe1/3)# switchport trunk allowed vlan add 3
Switch(config-xe1/3)# switchport trunk allowed vlan add 4
Switch(config-xe1/3)# switchport trunk allowed vlan add 5
Switch(config-xe1/3)# switchport trunk allowed vlan remove 1
Switch(config-xe1/3)#exit
Switch(config)# interface xe1/5
Switch(config-xe1/5)# switchport mode trunk
```

Switch(config-xe1/5)# switchport trunk allowed vlan add 3
Switch(config-xe1/5)# switchport trunk allowed vlan add 4
Switch(config-xe1/5)# switchport trunk allowed vlan add 5
Switch(config-xe1/5)# switchport trunk allowed vlan remove 1
Switch(config-xe1/5)#exit
Configure erps instance 1, erps main ring 1, subring 2
Switch(config)#erps 1
Switch(config-erps-1)# node-role interconnection
Switch(config-erps-1)#ring 1
Switch(config-erps-1)# ring 1 ring-mode major-ring
Switch(config-erps-1)# ring 1 node-mode rpl-neighbor-node
Switch(config-erps-1)# ring 1 raps-vlan 2
Switch(config-erps-1)# ring 1 traffic-vlan 3
Switch(config-erps-1)# ring 1 traffic-vlan 4
Switch(config-erps-1)# ring 1 traffic-vlan 5
Switch(config-erps-1)# ring 1 rpl-port xe1/1
Switch(config-erps-1)# ring 1 rl-port xe1/3
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)#ring 2
Switch(config-erps-1)# ring 2 ring-mode sub-ring
Switch(config-erps-1)# ring 2 node-mode ring-node
Switch(config-erps-1)# ring 2 raps-vlan 3
Switch(config-erps-1)# ring 2 traffic-vlan 4
Switch(config-erps-1)# ring 2 traffic-vlan 5
Switch(config-erps-1)# ring 2 rpl-port xe1/5
Switch(config-erps-1)# ring 2 enable
Switch(config-erps-1)#exit

(3) Configuration sw3:
Switch>enable
Switch#configure terminal
Create erps Protocol and data vlan
Switch(config)#vlan database
Switch(config-vlan)#vlan 2-5
Switch(config-vlan)#exit
Configure Ring Port vlan Mode to join erps Protocol and data vlan for trunk,
Switch(config)# interface xe1/1
Switch(config-xe1/1)# switchport mode trunk
Switch(config-xe1/1)# switchport trunk allowed vlan add 2
Switch(config-xe1/1)# switchport trunk allowed vlan add 3
Switch(config-xe1/1)# switchport trunk allowed vlan add 4

```
Switch(config-xe1/1)# switchport trunk allowed vlan add 5
Switch(config-xe1/1)# switchport trunk allowed vlan remove 1
Switch(config-xe1/1)#exit
Switch(config)# interface xe1/3
Switch(config-xe1/3)# switchport mode trunk
Switch(config-xe1/3)# switchport trunk allowed vlan add 2
Switch(config-xe1/3)# switchport trunk allowed vlan add 3
Switch(config-xe1/3)# switchport trunk allowed vlan add 4
Switch(config-xe1/3)# switchport trunk allowed vlan add 5
Switch(config-xe1/3)# switchport trunk allowed vlan remove 1
Switch(config-xe1/3)#exit
Switch(config)# interface xe1/5
Switch(config-xe1/5)# switchport mode trunk
Switch(config-xe1/5)# switchport trunk allowed vlan add 3
Switch(config-xe1/5)# switchport trunk allowed vlan add 4
Switch(config-xe1/5)# switchport trunk allowed vlan add 5
Switch(config-xe1/5)# switchport trunk allowed vlan remove 1
Switch(config-xe1/5)#exit
Configure erps instance 1, erps main ring 1, subring 2
Switch(config)#erps 1
Switch(config-erps-1)# node-role interconnection
Switch(config-erps-1)#ring 1
Switch(config-erps-1)# ring 1 ring-mode major-ring
Switch(config-erps-1)# ring 1 node-mode ring-node
Switch(config-erps-1)# ring 1 raps-vlan 2
Switch(config-erps-1)# ring 1 traffic-vlan 3
Switch(config-erps-1)# ring 1 traffic-vlan 4
Switch(config-erps-1)# ring 1 traffic-vlan 5
Switch(config-erps-1)# ring 1 rpl-port xe1/1
Switch(config-erps-1)# ring 1 rl-port xe1/3
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)#ring 2
Switch(config-erps-1)# ring 2 ring-mode sub-ring
Switch(config-erps-1)# ring 2 node-mode ring-node
Switch(config-erps-1)# ring 2 raps-vlan 3
Switch(config-erps-1)# ring 2 traffic-vlan 4
Switch(config-erps-1)# ring 2 traffic-vlan 5
Switch(config-erps-1)# ring 2 rpl-port xe1/5
Switch(config-erps-1)# ring 2 enable
Switch(config-erps-1)#exit
```

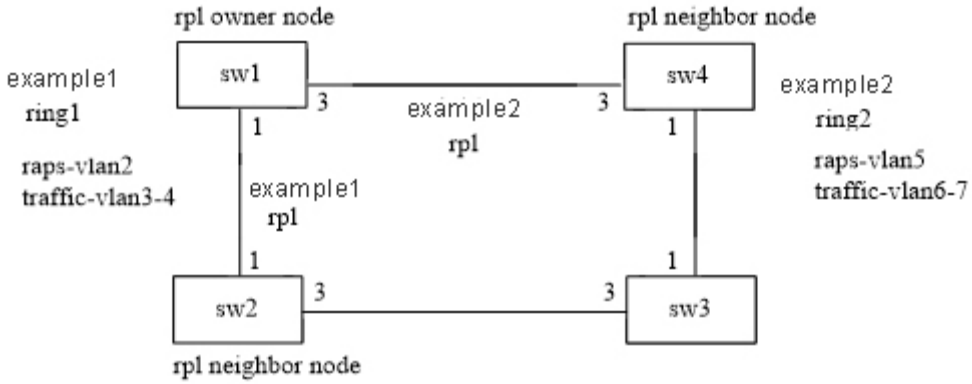
(4) configure sw4:

```
Switch>enable
Switch#configure termina
Create erps Protocol and data vlan
Switch(config)#vlan database
Switch(config-vlan)#vlan 3-5
Switch(config-vlan)#exit
Configure Ring Port vlan Mode to join erps Protocol and data vlan for trunk,
Switch(config)# interface xe1/1
Switch(config-xe1/1)# switchport mode trunk
Switch(config-xe1/1)# switchport trunk allowed vlan add 3
Switch(config-xe1/1)# switchport trunk allowed vlan add 4
Switch(config-xe1/1)# switchport trunk allowed vlan add 5
Switch(config-xe1/1)# switchport trunk allowed vlan remove 1
Switch(config-xe1/1)#exit
Switch(config)# interface xe1/3
Switch(config-xe1/3)# switchport mode trunk
Switch(config-xe1/3)# switchport trunk allowed vlan add 3
Switch(config-xe1/3)# switchport trunk allowed vlan add 4
Switch(config-xe1/3)# switchport trunk allowed vlan add 5
Switch(config-xe1/3)# switchport trunk allowed vlan remove 1
Switch(config-xe1/3)#exit
Configure the erps instance 1, erps subring 2
Switch(config)#erps 1
Switch(config-erps-1)#ring 2
Switch(config-erps-1)# ring 2 ring-mode sub-ring
Switch(config-erps-1)# ring 2 node-mode rpl-owner-node
Switch(config-erps-1)# ring 2 raps-vlan 3
Switch(config-erps-1)# ring 2 traffic-vlan 4
Switch(config-erps-1)# ring 2 traffic-vlan 5
Switch(config-erps-1)# ring 2 rpl-port xe1/1
Switch(config-erps-1)# ring 2 rl-port xe1/3
Switch(config-erps-1)# ring 2 enable
Switch(config-erps-1)#exit
```

10.6.3 Example of Multi-instance Load Balancing

As shown in the following figure, the sw1,sw2,sw3 and sw4 nodes constitute a erps instance 1 single ring ring1, node 1, 3 ports as erps ring ports, the ring protocol vlan is 2, the data vlan is 3, 4, the SW1 node is the rpl owner node, the sw2 node is the rpl neighbor node, and the link between sw1 and sw2 is the rpl link.

sw1, sw2, sw3, and sw4 nodes form an erps instance 2 single-loop ring 2. the 1,3 ports of each node are used as erps ring ports, the protocol vlan of the loop is 5, the data vlan is 6,7, the sw1 node is rplowner node, the sw4 node is rplneighbor node, and the link between sw1 and sw4 is rpl link.



(I) configuration example 1:

Configure sw1:

Switch>enable

Switch#configure terminal

Create erps Protocol and data vlan

Switch(config)#vlan database

Switch(config-vlan)#vlan 2-4

Switch(config-vlan)#exit

Configure Ring Port vlan Mode to join erps Protocol and data vlan for trunk,

Switch(config)# interface xe1/1

Switch(config-xe1/1)# switchport mode trunk

Switch(config-xe1/1)# switchport trunk allowed vlan add 2

Switch(config-xe1/1)# switchport trunk allowed vlan add 3

Switch(config-xe1/1)# switchport trunk allowed vlan add 4

Switch(config-xe1/1)# switchport trunk allowed vlan remove 1

Switch(config-xe1/1)#exit

Switch(config)# interface xe1/3

Switch(config-xe1/3)# switchport mode trunk

Switch(config-xe1/3)# switchport trunk allowed vlan add 2

Switch(config-xe1/3)# switchport trunk allowed vlan add 3

Switch(config-xe1/3)# switchport trunk allowed vlan add 4

Switch(config-xe1/3)# switchport trunk allowed vlan remove 1

Switch(config-xe1/3)#exit

Configure erps instance 1, erps single loop 1.

Switch(config)#erps 1

Switch(config-erps-1)#ring 1

```
Switch(config-erps-1)# ring 1 ring-mode major-ring
Switch(config-erps-1)# ring 1 node-mode rpl-owner-node
Switch(config-erps-1)# ring 1 raps-vlan 2
Switch(config-erps-1)# ring 1 traffic-vlan 3
Switch(config-erps-1)# ring 1 traffic-vlan 4
Switch(config-erps-1)# ring 1 rpl-port xe1/1
Switch(config-erps-1)# ring 1 rl-port xe1/3
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)#exit
```

Configure sw2:

```
Switch>enable
Switch#configure terminal
```

Create erps Protocol and data vlan

```
Switch(config)#vlan database
Switch(config-vlan)#vlan 2-4
Switch(config-vlan)#exit
```

Configure Ring Port vlan Mode to join erps Protocol and data vlan for trunk,

```
Switch(config)# interface xe1/1
Switch(config-xe1/1)# switchport mode trunk
Switch(config-xe1/1)# switchport trunk allowed vlan add 2
Switch(config-xe1/1)# switchport trunk allowed vlan add 3
Switch(config-xe1/1)# switchport trunk allowed vlan add 4
Switch(config-xe1/1)# switchport trunk allowed vlan remove 1
Switch(config-xe1/1)#exi
Switch(config)# interface xe1/3
Switch(config-xe1/3)# switchport mode trunk
Switch(config-xe1/3)# switchport trunk allowed vlan add 2
Switch(config-xe1/3)# switchport trunk allowed vlan add 3
Switch(config-xe1/3)# switchport trunk allowed vlan add 4
Switch(config-xe1/3)# switchport trunk allowed vlan remove 1
Switch(config-xe1/3)#exit
```

Configure erps instance 1, erps single loop 1.

```
Switch(config)#erps 1
Switch(config-erps-1)#ring 1
Switch(config-erps-1)# ring 1 ring-mode major-ring
Switch(config-erps-1)# ring 1 node-mode rpl-neighbor-node
Switch(config-erps-1)# ring 1 raps-vlan 2
Switch(config-erps-1)# ring 1 traffic-vlan 3
Switch(config-erps-1)# ring 1 traffic-vlan 4
Switch(config-erps-1)# ring 1 rpl-port xe1/1
```

```
Switch(config-erps-1)# ring 1 rl-port xe1/3
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)#exit
```

Configure sw3:

```
Switch>enable
Switch#configure terminal
Create erps Protocol and data vlan
Switch(config)#vlan database
Switch(config-vlan)#vlan 2-4
Switch(config-vlan)#exit
Configure Ring Port vlan Mode to join erps Protocol and data vlan for trunk,
Switch(config)# interface xe1/1
Switch(config-xe1/1)# switchport mode trunk
Switch(config-xe1/1)# switchport trunk allowed vlan add 2
Switch(config-xe1/1)# switchport trunk allowed vlan add 3
Switch(config-xe1/1)# switchport trunk allowed vlan add 4
Switch(config-xe1/1)# switchport trunk allowed vlan remove 1
Switch(config-xe1/1)#exit
Switch(config)# interface xe1/3
Switch(config-xe1/3)# switchport mode trunk
Switch(config-xe1/3)# switchport trunk allowed vlan add 2
Switch(config-xe1/3)# switchport trunk allowed vlan add 3
Switch(config-xe1/3)# switchport trunk allowed vlan add 4
Switch(config-xe1/3)# switchport trunk allowed vlan remove 1
Switch(config-xe1/3)#exit
Configure erps instance 1, erps single loop 1.
Switch(config)#erps 1
Switch(config-erps-1)#ring 1
Switch(config-erps-1)# ring 1 ring-mode major-ring
Switch(config-erps-1)# ring 1 node-mode ring-node
Switch(config-erps-1)# ring 1 raps-vlan 2
Switch(config-erps-1)# ring 1 traffic-vlan 3
Switch(config-erps-1)# ring 1 traffic-vlan 4
Switch(config-erps-1)# ring 1 rpl-port xe1/1
Switch(config-erps-1)# ring 1 rl-port xe1/3
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)#exit
```

configuring sw4:

```
Switch>enable
```

Switch#configure terminal
Create erps Protocol and data vlan
Switch(config)#vlan database
Switch(config-vlan)#vlan 2-4
Switch(config-vlan)#exit
Configure Ring Port vlan Mode to join erps Protocol and data vlan for trunk,
Switch(config)# interface xe1/1
Switch(config-xe1/1)# switchport mode trunk
Switch(config-xe1/1)# switchport trunk allowed vlan add 2
Switch(config-xe1/1)# switchport trunk allowed vlan add 3
Switch(config-xe1/1)# switchport trunk allowed vlan add 4
Switch(config-xe1/1)# switchport trunk allowed vlan remove 1
Switch(config-xe1/1)#exit
Switch(config)# interface xe1/3
Switch(config-xe1/3)# switchport mode trunk
Switch(config-xe1/3)# switchport trunk allowed vlan add 2
Switch(config-xe1/3)# switchport trunk allowed vlan add 3
Switch(config-xe1/3)# switchport trunk allowed vlan add 4
Switch(config-xe1/3)# switchport trunk allowed vlan remove 1
Switch(config-xe1/3)#exit
Configure erps instance 1, erps single loop 1.
Switch(config)#erps 1
Switch(config-erps-1)#ring 1
Switch(config-erps-1)# ring 1 ring-mode major-ring
Switch(config-erps-1)# ring 1 node-mode ring-node
Switch(config-erps-1)# ring 1 raps-vlan 2
Switch(config-erps-1)# ring 1 traffic-vlan 3
Switch(config-erps-1)# ring 1 traffic-vlan 4
Switch(config-erps-1)# ring 1 rpl-port xe1/1
Switch(config-erps-1)# ring 1 rl-port xe1/3
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)#exit

(2)configuration example 2:
Configure sw1:
Switch>enable
Switch#configure terminal
Create erps Protocol and data vlan
Switch(config)#vlan database
Switch(config-vlan)#vlan 5-7
Switch(config-vlan)#exit

Configure Ring Port vlan Mode to join erps Protocol and data vlan for trunk,
Switch(config)# interface xe1/1
Switch(config-xe1/1)# switchport mode trunk
Switch(config-xe1/1)# switchport trunk allowed vlan add 5
Switch(config-xe1/1)# switchport trunk allowed vlan add 6
Switch(config-xe1/1)# switchport trunk allowed vlan add 7
Switch(config-xe1/1)# switchport trunk allowed vlan remove 1
Switch(config-xe1/1)#exit
Switch(config)# interface xe1/3
Switch(config-xe1/3)# switchport mode trunk
Switch(config-xe1/3)# switchport trunk allowed vlan add 5
Switch(config-xe1/3)# switchport trunk allowed vlan add 6
Switch(config-xe1/3)# switchport trunk allowed vlan add 7
Switch(config-xe1/3)# switchport trunk allowed vlan remove 1
Switch(config-xe1/3)#exit
Configure erps instance 2, erps single loop 2
Switch(config)#erps 2
Switch(config-erps-2)#ring 2
Switch(config-erps-2)# ring 2 ring-mode major-ring
Switch(config-erps-2)# ring 2 node-mode rpl-owner-node
Switch(config-erps-2)# ring 2 raps-vlan 5
Switch(config-erps-2)# ring 2 traffic-vlan 6
Switch(config-erps-2)# ring 2 traffic-vlan 7
Switch(config-erps-2)# ring 2 rpl-port xe1/3
Switch(config-erps-2)# ring 2 rl-port xe1/1
Switch(config-erps-2)# ring 2 enable
Switch(config-erps-2)#exit

Configure sw2:
Switch>enable
Switch#configure terminal
Create erps Protocol and data vlan
Switch(config)#vlan database
Switch(config-vlan)#vlan 5-7
Switch(config-vlan)#exit
Configure Ring Port vlan Mode to join erps Protocol and data vlan for trunk,
Switch(config)# interface xe1/1
Switch(config-xe1/1)# switchport mode trunk
Switch(config-xe1/1)# switchport trunk allowed vlan add 5
Switch(config-xe1/1)# switchport trunk allowed vlan add 6
Switch(config-xe1/1)# switchport trunk allowed vlan add 7

```
Switch(config-xe1/1)# switchport trunk allowed vlan remove 1
Switch(config-xe1/1)#exit
Switch(config)# interface xe1/3
Switch(config-xe1/3)# switchport mode trunk
Switch(config-xe1/3)# switchport trunk allowed vlan add 5
Switch(config-xe1/3)# switchport trunk allowed vlan add 6
Switch(config-xe1/3)# switchport trunk allowed vlan add 7
Switch(config-xe1/3)# switchport trunk allowed vlan remove 1
Switch(config-xe1/3)#exit
Configure erps instance 2, erps single loop 2
Switch(config)#erps 2
Switch(config-erps-2)#ring 2
Switch(config-erps-2)# ring 2 ring-mode major-ring
Switch(config-erps-2)# ring 2 node-mode ring-node
Switch(config-erps-2)# ring 2 raps-vlan 5
Switch(config-erps-2)# ring 2 traffic-vlan 6
Switch(config-erps-2)# ring 2 traffic-vlan 7
Switch(config-erps-2)# ring 2 rpl-port xe1/1
Switch(config-erps-2)# ring 2 rl-port xe1/3
Switch(config-erps-2)# ring 2 enable
Switch(config-erps-2)#exit

Configure sw3:
Switch>enable
Switch#configure terminal
Create erps Protocol and data vlan
Switch(config)#vlan database
Switch(config-vlan)#vlan 5-7
Switch(config-vlan)#exit
Configure Ring Port vlan Mode to join erps Protocol and data vlan for trunk,
Switch(config)# interface xe1/1
Switch(config-xe1/1)# switchport mode trunk
Switch(config-xe1/1)# switchport trunk allowed vlan add 5
Switch(config-xe1/1)# switchport trunk allowed vlan add 6
Switch(config-xe1/1)# switchport trunk allowed vlan add 7
Switch(config-xe1/1)# switchport trunk allowed vlan remove 1
Switch(config-xe1/1)#exit
Switch(config)# interface xe1/3
Switch(config-xe1/3)# switchport mode trunk
Switch(config-xe1/3)# switchport trunk allowed vlan add 5
Switch(config-xe1/3)# switchport trunk allowed vlan add 6
```

Switch(config-xe1/3)# switchport trunk allowed vlan add 7
Switch(config-xe1/3)# switchport trunk allowed vlan remove 1
Switch(config-xe1/3)#exit
Configure erps instance 2, erps single loop 2
Switch(config)#erps 2
Switch(config-erps-2)#ring 2
Switch(config-erps-2)# ring 2 ring-mode major-ring
Switch(config-erps-2)# ring 2 node-mode ring-node
Switch(config-erps-2)# ring 2 raps-vlan 5
Switch(config-erps-2)# ring 2 traffic-vlan 6
Switch(config-erps-2)# ring 2 traffic-vlan 7
Switch(config-erps-2)# ring 2 rpl-port xe1/1
Switch(config-erps-2)# ring 2 rl-port xe1/3
Switch(config-erps-2)# ring 2 enable
Switch(config-erps-2)#exit

configuring sw4:
Switch>enable
Switch#configure terminal
Create erps Protocol and data vlan
Switch(config)#vlan database
Switch(config-vlan)#vlan 5-7
Switch(config-vlan)#exit
Configure Ring Port vlan Mode to join erps Protocol and data vlan for trunk,
Switch(config)# interface xe1/1
Switch(config-xe1/1)# switchport mode trunk
Switch(config-xe1/1)# switchport trunk allowed vlan add 5-7
Switch(config-xe1/1)# switchport trunk allowed vlan remove 1
Switch(config-xe1/1)#exit
Switch(config)# interface xe1/3
Switch(config-xe1/3)# switchport mode trunk
Switch(config-xe1/3)# switchport trunk allowed vlan add 5-7
Switch(config-xe1/3)# switchport trunk allowed vlan remove 1
Switch(config-xe1/3)#exit
Configure erps instance 2, erps single loop 2
Switch(config)#erps 2
Switch(config-erps-2)#ring 2
Switch(config-erps-2)# ring 2 ring-mode major-ring
Switch(config-erps-2)# ring 2 node-mode rpl-neighbor-node
Switch(config-erps-2)# ring 2 raps-vlan 5
Switch(config-erps-2)# ring 2 traffic-vlan 6

```
Switch(config-erps-2)# ring 2 traffic-vlan 7
Switch(config-erps-2)# ring 2 rpl-port xe1/3
Switch(config-erps-2)# ring 2 rl-port xe1/1
Switch(config-erps-2)# ring 2 enable
Switch(config-erps-2)#exit
```

Chapter 11 AAA Configuration

This chapter describes how to configure the switch's 802.1x and RADIUS to prevent unauthorized users from accessing the network. For the use of the 802.1x client and authentication billing system, please refer to their respective operating manuals. This chapter mainly includes the following contents:

- 802.1x Introduction
- RADIUS Introduction
- Configuring 802.1x
- Configuring RADIUS

AAA is the abbreviation of Authentication, Authorization, and Accounting. It provides a consistent framework for configuring three security functions: authentication, authorization, and billing. AAA configuration is actually a management of network security, which mainly refers to access control. Which users can access the network? What services are available to users with access rights? How to account for the users who are using the network resources?

Verify that the user has access

Which services are available to authorized users

Record the user's use of network resources.

The company has launched a complete AAA solution with 802.1x clients, various certified switches and an authentication billing system. An 802.1x client is installed on a PC connected to the Internet. When users need to access the network, they need to use the 802.1x client for authentication. Only authenticated users can use the network. This is a switch that supports authentication. It receives the client's authentication request and transmits the username and password to the authentication and accounting system. The switch itself does not perform the actual authentication. The authentication and accounting system receives the authentication request sent by the switch to perform actual authentication, and performs charging processing on the user who has successfully authenticated.

Use the 802.1x protocol to communicate between the 802.1x client and the switch, and the RADIUS protocol to communicate between the switch and the authentication billing system.

11.1 802.1x Introduction

The 802.1x protocol is a port-based access control and authentication protocol. The port referred to here is a logical port, which can be a physical port, a MAC address, or a Vlan ID. The switch implements a MAC address-based and port-based 802.1x protocol.

802.1x is a Layer 2 protocol. The authenticated switch and the user's PC must be in the same subnet. The protocol packet cannot span the network segment. 802.1x authentication uses a model of the client server, and there must be one server to authenticate all users.

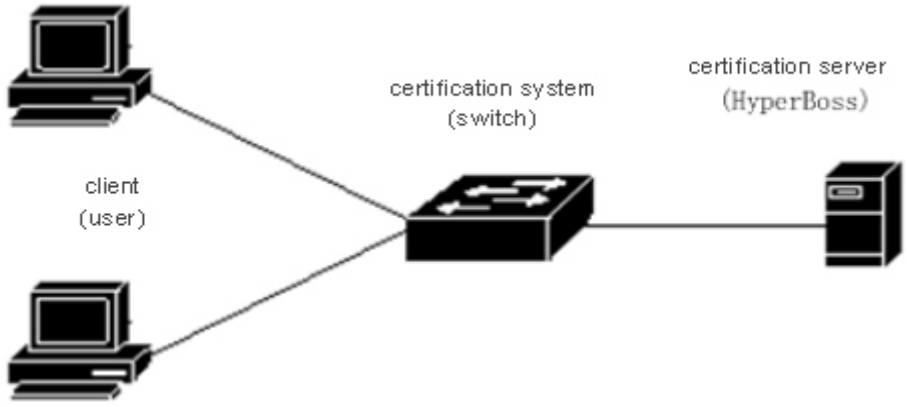
In MAC mode, only the authentication stream can pass through the port of the switch before the user passes the authentication, and only the data stream can pass through the port of the switch after the authentication is successful, that is to say, the user must pass the authentication to access the network. In port mode, Guest Vlan is enabled, and by default is off. When the Guest Vlan is closed, the data passes in the same way as the MAC mode, but after authentication, the port is opened instead of the MAC address being registered. When the Guest Vlan is opened, the data can pass through the Guest Vlan before the authentication of the user, and then through the Auth Vlan after the authentication is successful. This method can be used to restrict the user's access to the specified limited range before the authentication, and access to the public network after the authentication.

This section mainly includes:

- 802.1x device composition
- Introduction of the protocol package
- Protocol flow interaction
- 802.1x port status

11.1.1 802.1x device composition

802.1x device consists of three parts: a Supplicant System, an Authenticator System, and an Authentication Server System. As shown below.



802.1 x devices

The client refers to the device requesting access to the network, generally the user terminal system, such as the user's PC. On the user terminal system, an 802.1x client software must be installed, which implements the client part of the 802.1x protocol. The client initiates an 802.1x authentication request and requests the authentication server to verify its username and password. If the authentication is successful, the user can access the network.

An authentication system refers to an authenticated device, such as a switch. The authentication system controls whether the user can access the network through the status of the user's logical port (the MAC address). If the logical port status of the user is unauthorized, the user cannot access the network. If the logical port status of the user is authorized, Then the user can access the network.

The authentication system is a relay between the client and the authentication server. The authentication system requests the identity information of the user, and forwards the identity information of the user to the authentication server, and forwards the authentication result sent by the authentication server to the client. The authentication system is implemented in the server part of the 802.1x protocol near the user end. The client part of the RADIUS protocol is implemented near the authentication server. The RADIUS protocol client of the authentication system sends the EAP information to the RADIUS server. It is sent to the authentication server, and the EAP information is decapsulated from the RAIDUS protocol packet sent from the authentication server and transmitted to the 802.1x client through the 802.1x server part.

An authentication server refers to a device that actually authenticates a user. The authentication server receives the identity information of the user sent by the authentication system and performs authentication. If the authentication succeeds, the authentication server authorizes the authentication system and allows the user to access the network. If the authentication fails, the authentication server tells the authentication system that the authentication fails, and the user cannot access the network. . The authentication server and the authentication system communicate through the EAP extended RADIUS protocol. The company provides an authentication and billing system to authenticate and bill users.

11.1.2 Introduction of the protocol package

The authentication data stream transmitted by the 802.1x protocol on the network is the EAPOL (EAP Over LAN) frame format. All user identity information (including the username and password) is encapsulated in the EAP (Extended Authentication Protocol), and the EAP is encapsulated in the EAPOL frame.The username exists in EAP in plain text, while the password exists in EAP in MD5 encrypted form. The username exists in EAP in plain text, while the password exists in EAP in MD5 encrypted form.

The EAPOL frame format is shown below. PAE Ethernet Type is the Ethernet protocol model of EAPOL with a value of 0x888E.

Protocol Version is the EAPOL version number and has a value of 1.

Packet Type refers to the EAPOL frame type.

Packet Body Length is the length of the EAPOL frame content. Packet Body refers to the content of the EAPOL frame.

	Octet Number
PAE Ethernet Type	1-2
Protocol Version	3
Packet Type	4
Packet Body Length	5-6
Packet Body	7-N

EAPOL frame format

The switch uses three EAPOL protocol frames：

EAPOL-Start：The value of the Packet Type is 1, and the authentication initiates the frame, when the user needs to be authenticated, the EAPOL-Start is first initiated, and the client is sent to the switch.

EAPOL-Logoff：The value of the Packet Type is 2, send this frame to notify the switch when the user does not need to use the network.

EAPOL-Packet：The value of the Packet Type is 0, authentication information frame, used to carry authentication information.

The EAP package format is shown below.Code refers to the type of EAP package, including Request, Response, Success, and Failure. Identifier refers to an identifier used to match Response and Request. Length refers to the length of the EAP packet, including the header. Data refers to EAP packet data.

The EAP package includes:

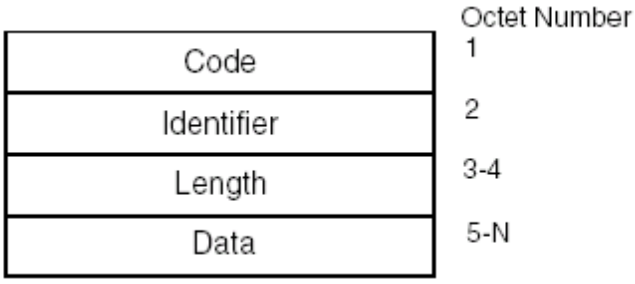
EAP-Request：Code value is 1, the EAP request packet is sent from the switch to the client to request the username and/or password.

EAP-Response：Code value is 2, the EAP response packet is sent from the client to the switch, and the username

and/or password are sent to the switch.

EAP-Success：Code value is 3, the EAP packet is sent to the client from the switch to tell the client that the authentication is successful.

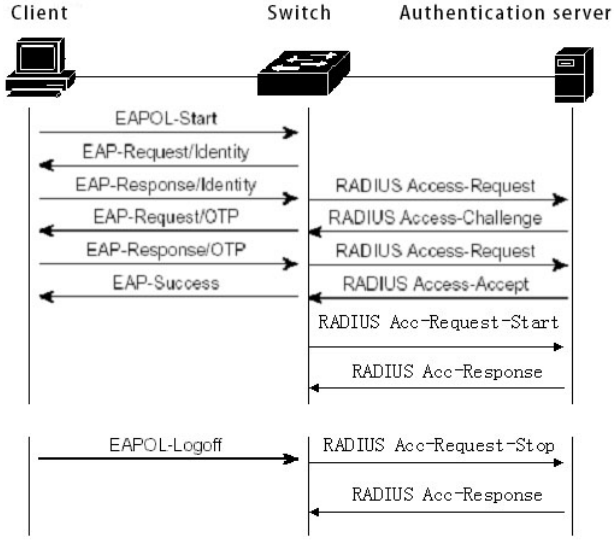
EAP-Failure：Code value is 4, and the EAP failure packet is sent from the switch to the client, which tells the client that the authentication fails.



EAP package format

11.1.3 Protocol flow interaction

When the switch is enabled with 802.1x and the port status is Auto, all access users on the port must pass the authentication before accessing the network. The protocol interaction is shown below.



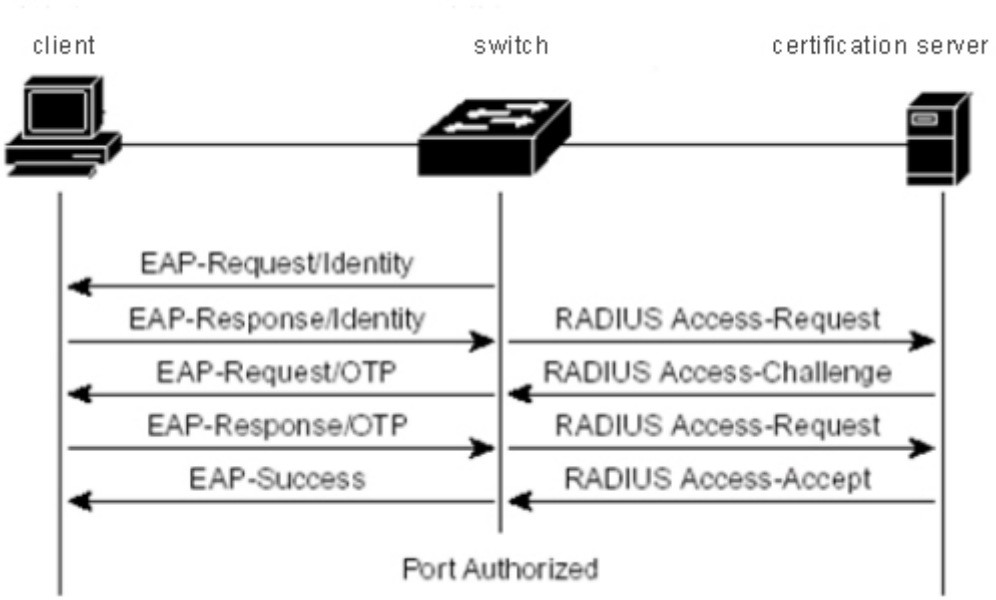
Client initiates the authenticated protocol interaction

When the user needs to access the network, the client first sends the EAPOL-Start to the switch request authentication, the switch sends the EAP-Request to the user's user name after receiving the authentication request, the client returns the EAP-Response, and the switch extracts the EAP information out of the package to be sent to the authentication server in the RADIUS packet, The authentication server requests the user's password, the switch sends an EAP-Request to the client to request the user's password, the client returns the EAP-Response, and the switch encapsulates the EAP information in the RADIUS packet. Send to the authentication server, the authentication server according to the user name and password to authenticate the user. If the authentication is successful, the authentication server notifies the switch, the switch sends EAP-Success to the client and the user's logical port is authorized. When the client receives EAP-Success, it

indicates that the authentication is successful and the user can access the network.

If the user no longer needs to use the network, the client sends eapol-logoff to the switch, which changes the user's logical port state to an unauthorized state, at which time the user cannot access the network.

The switch provides a mechanism to prevent the client from going offline abnormally. When the authentication time arrives, the switch initiates the re-authentication. If the authentication is successful, the user can continue to use the network, and if the authentication fails, the user will not be able to use the network. The protocol interaction is shown below.



Protocol interaction for re-authentication

11.1.4 802.1x Port State

Port state refers to the physical port state of the switch. Authorized authorized status: N/A status, Auto status, force-authorized status and force-unauthorized status.

When the switch does not turn on 802.1x, all ports are in N/A state. When the switch port is set to an Auto state, the Force-authorized state, or the Force-unauthorize state, the 802.1x of the switch must be enabled first.

When the switch's port is in the N/A state, all users under the port can access the network without authentication. When the switch receives 802.1x protocol packets from this port, the protocol packets are discarded.

When the port of the switch is in Force-authorized state, all users under the port can access the network without authentication. When the switch receives the EAPOL-Start packet from the port, the switch sends back the EAP-Success packet, and when the switch receives other 802.1x protocol packets from the port, discard these protocol packets.

With the Force-unauthorized status of the switch, all users on the unauthorized port cannot access the

network, and the authorization request is not allowed. When the switch receives 802.1x protocol packets from this port, these protocol packets are discarded.

Distinguish authentication mode when the port of the switch is in Auto mode. In the port mode, if the Guest Vlan is not configured, the user must pass authentication to access the network. If the Guest Vlan is configured, users can access the Auth Vlan with authentication and Guest Vlan without authentication. All users under the port must be authenticated before they can access the network. The 802.1x protocol interaction is shown in the figure. If the user needs to authenticate, the port is usually set to Auto.

When the switch port is set to the Auto state, the anti-ARP spoofing function is enabled at the same time; the anti-ARP spoofing function can control the data packet of the information provided by the client and the sender IP of the ARP packet only when the source MAC address and the source IP of the IP packet are both authenticated. Packets with the sender MAC that meets the information provided by the client at the time of authentication can be forwarded by this port, otherwise they will be discarded. To configure this function, the client must be a statically configured IP address. If the IP address is dynamically obtained through the DHCP protocol, the DHCP SNOOPING protocol can be enabled to implement this function. For more details, refer to the IP MAC binding configuration.

11.2 RADIUS Introduction

When the user authenticates, the RADIUS protocol supporting EAP extension is used between the switch and the authentication server. Radius protocol adopts the client / server model, the switch needs to implement the RADIUS client, and the authentication server needs to implement the RADIUS server.

To ensure the security of the interaction between the switch and the authentication server and prevent the interaction between the illegal switch or the illegal authentication server, the switch and the authentication server should authenticate each other. The switch and the authentication server need the same key. When the switch or authentication server sends the RADIUS protocol packet, all the protocol packets should use the HMAC algorithm to generate the message digest according to the key. When the switch and the authentication server receive the RADIUS protocol packet, the message digest of all the protocol packets should be verified with the key. If the authentication passes, it is considered to be a legitimate RADIUS protocol package. Otherwise, It is an illegal RADIUS protocol package and should be discarded.

This section mainly includes the following:

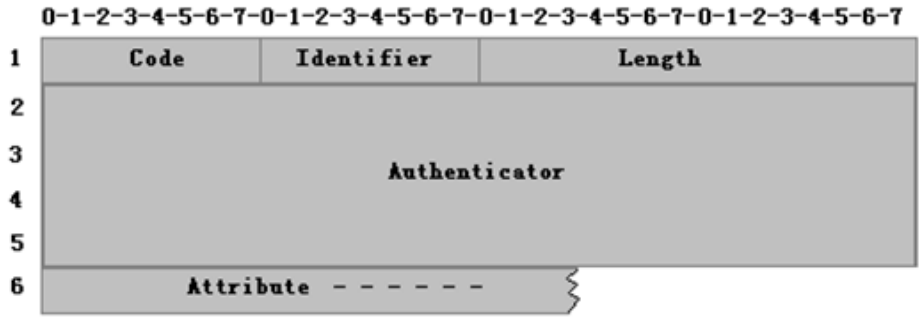
- Introduction of protocol package
- Protocol flow interaction
- User validation methods

11.2.1 Introduction of protocol package

RADIUS is a protocol built on top of UDP. RADIUS can encapsulate authentication information and accounting information. The early RADIUS authentication port was 1645. Currently, port 1812 is used. The earlier RADIUS accounting port is 1646. Currently, port 1813 is used.

RADIUS is carried on UDP, so RADIUS must have a timeout retransmission mechanism. In order to improve the reliability of communication between the authentication system and the RADIUS server, two RADIUS server schemes are generally adopted, that is, an alternate server mechanism is adopted.

RADIUS message format is shown below. Code refers to the RADIUS protocol message type. Identifier indicator identifier, used to match the request and reply. Length refers to the length of the entire message (including the header). Authenticator is a 16-byte string, a random number for the request packet, and a message digest generated by MD5 for the response package. Attribute refers to the attributes in the RADIUS protocol package.



RADIUS message format

The switch uses the following RADIUS protocol packages:

Access-request: Code value is 1, authentication request package sent to the authentication server from the authentication system, on which the user name and password are packaged

Access-accept: Code value is 2, response package sent to the authentication system from the authentication server indicates the success of the user authentication.

Access-Reject: Code value is 3, response package sent to the authentication system from the authentication server indicates that the user authentication failed.

Access-Challenge：Code value is 11, reply package sent to the authentication system from the authentication server indicates that the authentication server needs further information from the user, such as password and so on.

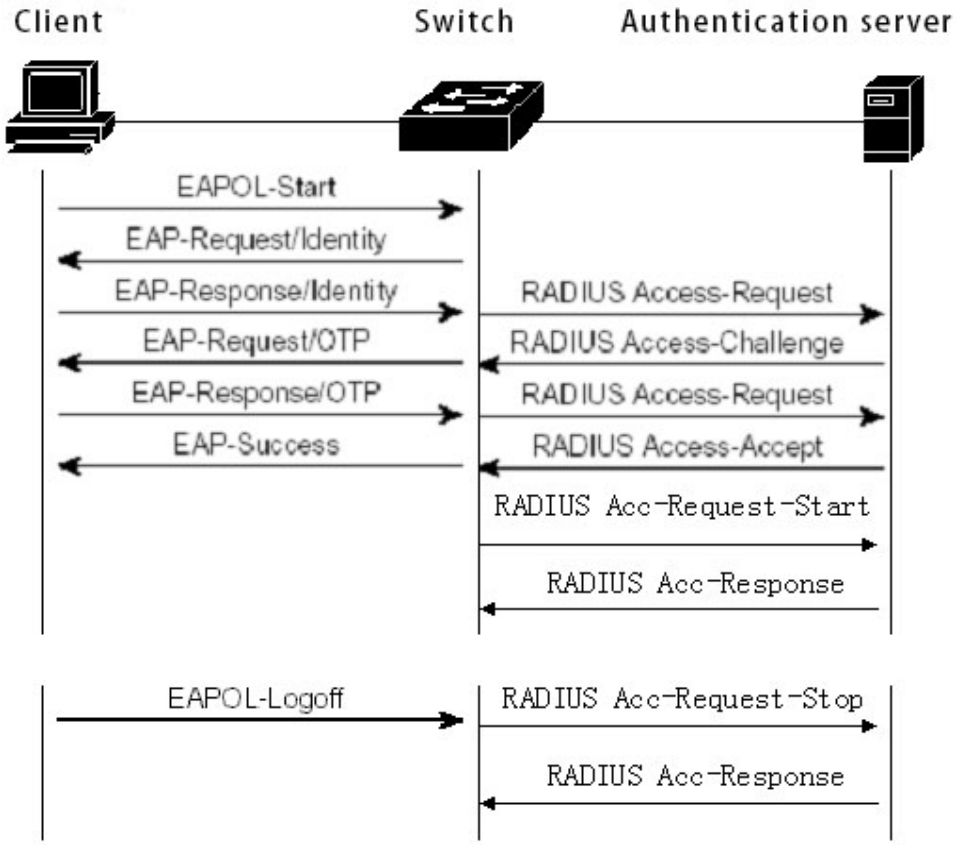
Accounting-Request：Code value is 4, billing request package sent to the authentication server from the authentication system, including the start and end billing packets, on which the billing information is packaged.

Accounting-Response: Code value is 5, charging reply packet sent from the authentication server to the authentication system indicates that the charging information has been received.

11.2.2 Protocol flow interaction

When the user initiates the authentication, the authentication system and the authentication server interact through RADIUS protocol. The protocol flow interaction of the authentication system without RADIUS billing packets is shown below. In general, after successful user authentication or when the user goes offline, the

authentication system needs to send RADIUS billing packets to the authentication server, and the protocol flow interaction is shown in the figure.



When the user performs authentication, the switch encapsulates the username in the Access-Request packet and sends it to the authentication server. The server answers the password of the Access-Challenge requesting user, the switch requests the password of the client user, and the client encapsulates the password in the EAP. After the EAP is obtained, the packet is encapsulated in the Access-Request and sent to the authentication server. The authentication server authenticates the user. If the authentication succeeds, the Access-Accept is sent back to the switch. After receiving the packet, the switch notifies the client that the authentication succeeds and sends Accounting- The Request informs the authentication server to start accounting, and the authentication server sends back the Accounting-Response.

When the user does not want to use the network, notify the switch user to go offline, the switch sends Accounting-Request to notify the authentication server to end the billing, the billing information is packaged in this package, and the authentication server sends back the Accounting-Response.

11.2.3 User authentication method

There are three user authentication methods for RADIUS, as follows:

- The user passes the user name and his password to the switch in clear text. The switch passes the user name and password to the RADIUS server through the RADIUS protocol packet, and the RADIUS server looks up the database. If the same username and password exist, the authentication is passed, otherwise the authentication is not passed.

- When a user requests Internet access, the switch generates a 16-byte random code for the user. The user generates a response to the random code, password and other domain encryption, and sends the user name and response to the switch. The switch passes the username, response, and the original 16-byte random code to the RADIUS server. RADIU looks up the database on the switch side according to the user name, and obtains the same password as that used by the client side for encryption. Then, it encrypts the password according to the random code of 16 bytes transmitted, and compares the result with the transmitted response. If the password is the same, the authentication has passed; if not, the authentication has failed.
- EAP(Extensible Authentication Protocol). With this method of authentication, the switch is not really involved in authentication, and only serves as a forwarding between the user and the RADIUS server. when the user requests the internet, the switch requests the user's user name and forwards the user name to the RADIUS server, the RADIUS server generates a 16-byte random code to the user and stores the random code, the user generates a response to the random code, the password and other domain encryption, Pass the user name and response to The switch forwards the switch to the RADIUS server.
- RADIU looks up the database on the switch side according to the user name, and obtains the same password as that used by the client for encryption. Then it encrypts the password according to the 16-byte random code stored, and compares the result with the transmitted response. If the password is the same, the authentication has passed; if not, the authentication has failed.

  The company's authentication and billing solution uses the EAP user authentication method.

11.3 Configuring 802.1x

This section describes the configuration of 802.1x in detail, including:

- 802.1x default configuration
- Start and close 802.1x
- Configure 802.1x port status
- Configure the re-authentication mechanism
- Configure the maximum number of port access hosts
- Configure interval and number of retransmissions
- Configuration port -- a transmission port
- Configure 802.1x client version number
- Configure whether the client version number is checked
- Configuration authentication mode
- Configure whether to check the timing packet of the client
- Displays the 802.1x information

11.3.1 802.1x default configuration

The switch 802.1x configuration default is as follows:

- 802.1x is off.
- The status of all ports is N/ A.
- The re-authentication mechanism is closed and the re-authentication interval is 3600 seconds
- The maximum number of access hosts for all ports is 100.
- The timeout interval for resending EAP-Request is 30 seconds.
- Timeout resending of EAP - Request are 3 times.
- The time that the user authentication failed to wait is 60 seconds.
- The server timeout retransmission interval is 10 seconds.

The switch provides a command in global CONFIG mode to return all configurations to the default state, as follows:

Switch(config)#dot1x default

11.3.2 Start and close 802.1x

The first step in configuring 802.1x is to start 802.1x. In global CONFIG mode, enter the following command to start 802.1x: Switch(config)#dot1x

When 802.1x is turned off, all port states return to N ≤ A state. In global CONFIG mode, enter the following command to turn off 802.1x: Switch(config)#no dot1x

11.3.3 Configure 802.1x port status

Start 802.1x before setting 802.1x port status. If all users under the port must be authenticated to access the network, the port must be set to Auto state.

The following command sets port ge1/1 to Auto in interface configuration mode and enables anti-ARP spoofing:

Switch(config-ge1/1)dot1x control auto

If the anti-ARP spoofing configuration fails, it may be caused by the following reasons:

1、System CFP resources are exhausted

2、The current interface is configured with the ACL filtering function.

3、The current interface enables DHCP SNOOPING

4、The configured interface is a Layer 3 interface or a trunk interface.

The following command sets the port ge1/1 to the Force-authorized state in interface configuration mode:

Switch(config-ge1/1)dot1x control force-authorized

The following command sets the port ge1/1 to the Force-unauthorized state in interface configuration mode:

Switch(config-ge1/1)dot1x control force-unauthorized

The following command sets the port ge1/1 to the N/A state in interface configuration mode:

Switch(config-ge1/1)no dot1x control

Note: If a port has been bound to a MAC address, then this port cannot be set to Auto, Force-authorized, or Force-unauthorized state.

11.3.4 Configure 802.1x port authentication mode

Be sure to start 802.1x before setting the 802.1x port authentication mode. If only one user to be authenticated is connected to the port, the port must be set to portbase if the authentication is enabled. If it is to be MAC address-based, set it to macbase. The default state is macbase.

The following command sets the port ge1/1 to portbase state in interface configuration mode:

Switch(config-ge1/1)dot1x method portbase

The following command sets the port ge1/1 to macbase state in interface configuration mode:

Switch(config-ge1/1)dot1x method macbase

11.3.5 Configure 802.1x port guest vlan

Be sure to start 802.1x before setting up 802.1x port guest vlan and configure the port to be Auto and portbase. If you want the user authentication under the port to be able to access the configuration vlan, after passing the guest vlan, authentication, the port must be configured with guest vlan.

Note that guest vlan only supports access mode and does not support trunk. Once the guest vlan is configured on the port, its mode cannot be modified. The guest vlan cannot be configured in non-access mode. When configuring guest vlan, you must ensure that the vlan has been created.

The following command sets the guest vlan of the port to 2 in interface configuration mode:

Switch(config-ge1/1)dot1x guest-vlan 2

11.3.6 Configure the re-authentication mechanism

In order to prevent the switch and the authentication server from being aware of the abnormal disconnection of the client, the switch provides a re-authentication mechanism, and the switch initiates the authentication every time between the re-authentication intervals.

The following command starts the reauthentication mechanism in global CONFIG mode:

Switch(config)#dot1x reauthenticate

The following command turns off the reauthentication mechanism in global CONFIG mode:

Switch(config)#no dot1x reauthenticate

The following command sets the interval for re-authentication in global CONFIG mode:

Switch(config)#dot1x timeout re-authperiod <interval>

Note:Do not set the interval for recertification too short, otherwise the network bandwidth and CPU resources of the switch are too high.

11.3.7 Configure the maximum number of port access hosts

Each port of the switch can control the maximum number of hosts accessed, which can restrict users from illegally accessing the network using multiple hosts. The maximum number of port access hosts is 100, and the maximum can be set to 100. If the maximum number of access hosts is set to 0, the port denies any user access.

The following command sets the maximum number of port ge1/1 access hosts in interface configuration mode:

Switch(config-ge1/1)dot1x support-host <number>

11.3.8 Configure interval and number of retransmissions

The 802.1x protocol standard specifies the protocol interaction and the number of intervals and the number of retransmissions of the protocol state machine. The switch uses the standard interval and the number of retransmissions, and it is recommended that the user do not change the intervals and the number of retransmissions when in use.

Tx-period indicates the interval at which the switch resends the EAP-Request protocol packet; max-req indicates the number of times the switch resends the EAP-Request; quiet-period indicates the interval for the re-authentication when the user authentication fails; server-timeout indicates The interval at which the switch resends the RADIUS packet to the authentication server. The supp-timeout indicates the interval at which the switch resends the eap request packet to the client.

The following command configures these intervals and the number of retransmissions in the global CONFIG mode:

Switch(config)#dot1x timeout tx-period <interval>

Switch(config)#dot1x max-req <number>

Switch(config)#dot1x timeout quiet-period <interval>

Switch(config)#dot1x timeout server-timeout <interval>

Switch(config)#dot1x timeout supp-timeout <interval>

11.3.9 Configuration port is a transmission port

When the switch does not enable 802.1x authentication, and other switches in the subnet have 802.1x authentication enabled, you can configure the port connecting the client and the authentication switch as the transmission port, and forward the eapol between the client and the 802.1x authentication switch. Certification package. Thereby implementing 802.1x authentication of other switches to the client.

The following command sets the port ge1/1 to the transport port in interface configuration mode:
Switch(config-ge1/1)dot1x transmit-port

The following command sets the port ge1/1 to non- transport port in interface configuration mode:
Switch(config-ge1/1)no dot1x transmit-port

11.3.10 Configure 802.1x client version number

Configure the version number of the 802.1x client, only clients whose version is not less than the configured version number can be authenticated, otherwise the authentication fails. The default client version number of the switch is 2.0.

The following command configures the client version number in global config mode:
Switch(config)# dot1x client-version <string>

11.3.11 Configure whether the client version number is checked

If the configuration checks the version number of the 802.1x client, if configured to check, the switch first checks the client version number when authenticating. The default is configured to check.

The following command is configured to open a check on the client version number in global CONFIG mode:
Switch(config)# dot1x check-version open

11.3.12 Configuration authentication mode

The authentication mode of 802.1x packet is configured by the switch, and the authentication mode initiated by the client is divided into general authentication and extended authentication. The switch can be configured to authenticate in which way first. If the authentication mode initiated by the client is not consistent with the authentication mode configured by the switch, the client will switch to another authentication method to initiate the authentication after a certain number of authentication failures.

The following commands configure the authentication of the switch in global CONFIG mode to extend the authentication mode:
Switch(config)# dot1x extended

11.3.13 Configure whether to check the client's timing package

The configuration switch checks whether the client's timing packet is checked, and after the authentication is successful, the switching opportunity requires the client to send an 802.1x packet at a scheduled time, but not all clients will send an 802.1x packet at a timing after the authentication is passed, so that the switch is configured to check if the client's timing packet is checked by the command.

The following command is configured for the switch to check the timing package for the client in global CONFIG mode

Switch(config)# dot1x check-client

11.3.14 Display 802.1x information

The following command displays the information for 802.1x in normal mode/ privileged mode, and when the command is show dot1x, all the 802.1x configuration information is displayed, including configuration information for all ports; when the command is show dot1x interface, the information for all access users under the port is displayed:

Switch#show dot1x

Switch#show dot1x interface

11.4 Configure RADIUS

This section describes the configuration of RADIUS in detail, including the following:

- RADIUS default configuration
- Configure the IP address of the authentication server
- Configure shared key
- Start and close billing
- Configure RADIUS port and attribute information
- Configuring RADIUS roaming
- Display RADIUS information

11.4.1 RADIUS default configuration

The default configuration for switch RADIUS is as follows:

- The IP address of the primary authentication server and backup authentication server is not configured, that is, the IP address is 0.0.0.0
- The shared key is not configured, that is, the shared key string is empty.
- Billing is started by default.
- RADIUS authentication UDP port is 1812 and the charging UDP port is 1813
- The value of the RADIUS attribute NASPort is 0xc353, the value of the NSPorType is 0x0f, and the value of the NSPorServer is 0x02.

11.4.2 Configure the IP address of the authentication server

In order to communicate RADIUS between the switch and the authentication server, the IP address of the authentication server needs to be configured on the switch. In practical application, we can use one authentication server, two authentication servers, one as the main authentication server and one as the backup authentication server. If the switch is configured with the IP addresses of two authentication servers, the switch can switch to communicate with the backup authentication server after the switch interrupts communication with the primary authentication server.

The following command configures the IP address of the primary authentication server in the global CONFIG mode:

Switch(config)#radius-server host <ip-address>

The following command configures the IP address of the backup authentication server in the global CONFIG mode:

Switch(config)#radius-server option-host <ip-address>

11.4.3 Configure shared key

The switch and the authentication server are mutually authenticated, and a shared secret key is required on both the switch and the authentication server. Note that the shared key on the switch must be the same as the authentication server.

The following command configure the shared key for the switch in global CONFIG mode:
Switch(config)#radius-server key <string>

11.4.4 Start and close billing

If the switch turns off billing, the switch does not send RADIUS billing packets to the authentication server after successful authentication or when the user is offline. In general, in practical application, billing is open.

The following command starts billing in global CONFIG mode:

Switch(config)#radius-server accounting

The following command turns off billing in global CONFIG mode: Switch(config)#no radius-server accounting

11.4.5 Configuring RADIUS Ports and Attribute Information

Recommendation: Do not modify the RADIUS port and attribute information configuration.

The following command modifies the RADIUS certified UDP port in global CONFIG mode:

Switch(config)#radius-server udp-port <port-number>

The following command modifies the RADIUS property information in global CONFIG mode:

Switch(config)#radius-server attribute nas-portnum <number>

Switch(config)#radius-server attribute nas-porttype <number>

Switch(config)#radius-server attribute service-type <number>

11.4.6 Configuring RADIUS roaming

When MAC,IP or VLAN binding is made to the client, when the client is moved to another place, the bound client cannot authenticate 802.1x because of the change of MAC address, IP address or VLAN. Turning on the radius roaming feature ignores the client's MAC,IP or VLAN binding to continue 802.1x authentication.

The following commands configure RADIUS roaming in global CONFIG mode:

Switch(config)#radius-server roam

The following command turns off RADIUS roaming in global CONFIG mode:

Switch(config)#no radius-server roam

11.4.7 Display RADIUS information

The following command displays RADIUS configuration information in normal / privileged mode:

Switch#show radius-server

11.5 Configuration example

Enable the 802.1x protocol and set the port ge1/1 to the Auto state. Set the primary authentication server to 198.168.80.111 and set the shared key of the switch to abcdef.

Switch#

Switch# dot1x

Switch#config t

Switch(config)#radius-server host 198.168.80.111

Switch(config)#radius-server key abcdef

Switch(config)# interface ge1/1

Switch(config-ge1/1)# dot1x control auto

Chapter 12 GMRP configuration

This chapter mainly includes:

- Introduce GMRP
- Configure GMRP
- Display GMRP

12.1 Introduce GMRP

Currently, the GARP Multicast Registration Protocol (GMRP) is a multicast registration protocol based on GARP, which is used to maintain multicast registration information in the switch. All GMRP-capable switches can receive multicast registration information from other switches and dynamically update local multicast registration information. They can also propagate local multicast registration information to other switches. This information exchange mechanism ensures the consistency of multicast information maintained by all GMRP-enabled devices in the same switching network.

When a host wants to join a multicast group, it will issue a GMRP join message. The switch joins the GMRP join message to the multicast group and broadcasts the GMRP join message in the VLAN where the receiving port is located. The multicast source in the VLAN can know the existence of the multicast member. When a multicast source sends a multicast packet to a multicast group, the switch forwards the multicast packet to the port connected to the multicast group member. This implements Layer 2 multicast in the VLAN.

12.2 Configure GMRP

The main configurations of GMRP include:

Open GMRP

View GMRP

In the configuration task, you must first enable global GMRP and then enable port GMRP.

12.2.1 Turn on GMRP settings

Order	Description	Configuration mode
set gmrp enable | disable	Enable/disable all vlan gmrp globally	Global configuration mode
set gmrp enable vlan <vlan-id>	使能全局特定 vlan gmrp Enable global specific vlan gmrp.	Global configuration mode
set gmrp registration{fixed | forbidden | normal} <if-name>	Configure interface registration multicast mode	Global configuration mode
set gmrp timer {join | leave | nleaveall} <time-value>	Configure the time of various timers	Global configuration mode
set port gmrp enable <if-name>	Enable port GMRP function	Global configuration mode
set port gmrp disable <if-name>	Disable port GMRP function	Global configuration mode

12.2.2 View GMRP information

After the configuration is complete, you can run the show command in any view to display the running status of the GMRP after the configuration.

Order	Description	configuration mode
show gmrp configuration	View GMRP configuration information	Privilege mode

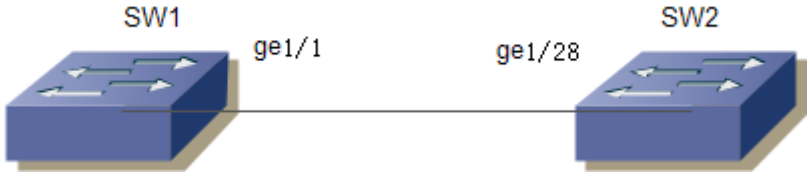
show gmrp machine	View GMRP state machine information	Privilege mode
show gmrp statistics vlanid	View gmrp statistics of a specific vlanid	Privilege mode
show gmrp timer <ifname>	View timer information of a specific port	Privilege mode

12.3 Example of typical configuration of GMRP

1. Networking requirements

To realize dynamic registration and update of multicast information between switches, GMRP needs to be started on switches

2. Network diagram



GMRP sample group diagram

3. Configuration steps

Configure SW1

Start the global GMRP

Switch(config)# set gmrp enable

Start the port GMRP on the Gigabit Ethernet port ge1/1

Switch(config)# set port gmrp enable ge1/1

Switch(config)#

Configure SW2

Start the global GMRP

Switch(config)# set gmrp enable

Start the port GMRP on the Gigabit Ethernet port ge1/28

Switch(config)# set port gmrp enable ge1/28

Switch(config)#

Chapter 13 IGMP SNOOPING configuration

In the metropolitan area network/Internet, when the same data packet is sent to multiple but not all receivers in the network by unicast, since it is necessary to copy the packet to each receiving endpoint, as the number of receivers increases, it is required. The number of packets sent will also increase linearly, which will increase the overall burden on hosts, switching routing devices and network bandwidth resources, and the efficiency will be greatly affected. With the increasing demand for multi-point video conferencing, video on demand, and group communication applications, in order to improve resource utilization, multicast mode has increasingly become a popular transmission method in multipoint communication.

The switch implements the IGMP SNOOPING function to serve multicast applications. IGMP SNOOPING listens to IGMP packets on the network to implement dynamic learning of IP multicast MAC addresses.

This chapter describes the concept and configuration of IGMP SNOOPING, including

- Introduce IGMP SNOOPING
- Configure IGMP SNOOPING
- IGMP SNOOPING configuration example

13.1 Introduce IGMP SNOOPING

Traditional network multicast packets in a subnet as broadcast processing, which is easy to make the network traffic, resulting in network congestion. When IGMP SNOOPING is implemented on the switch, IGMP SNOOPING can dynamically learn IP multicast MAC address, maintain the output port list of IP multicast MAC address, so that the multicast data stream is only sent to the output port, which can reduce the network traffic.

This section mainly includes the following:

- IGMP SNOOPING process
- Layer 2 dynamic multicast
- Join a group
- Leave a group

13.1.1 IGMP SNOOPING Process

IGMP SNOOPING is a layer 2 network protocol, which listens to the IGMP protocol packets passing through the switch, maintains a multicast group according to the receiving port, VLAN ID and multicast address of these IGMP protocol packets, and then forwards these IGMP protocol packets. Only by adding the port of the multicast group can the multicast data stream be received, which reduces the traffic of the network and saves the bandwidth of the network.

The multicast group includes a multicast group address, a member port, a VLAN ID, and an Age time.

The formation of the IGMP SNOOPING multicast group is a learning process. When a port of the switch receives an IGMP REPORT packet, IGMP SNOOPING generates a new multicast group, and the port that receives the IGMP REPORT packet is added to the multicast group. When the switch receives an IGMP QUERY packet, if the multicast group already exists in the switch, the port that receives the IGMP QUERY is also added to the multicast group. Otherwise, the IGMP QUERY packet is forwarded. IGMP SNOOPING also supports the Leave mechanism of IGMP V2. If IGMP SNOOPING is configured with fast-leave as ENABLE, the receiving port can leave the multicast group immediately when receiving the leave packet of IGMP V2; if the fast-leave leave waiting time is configured (Fast-leave-timeout), then the multicast group leaves the multicast group after waiting for this time to expire.

IGMP SNOOPING has two update mechanisms, one is the leave mechanism described above. In most cases, IGMP SNOOPING removes expired multicast groups through age time. When the multicast group joins IGMP SNOOPING, the time to join is recorded, and when the multicast group remains in the switch for more than a configured age time, the switch removes the multicast group.

When a port receives a Leave protocol package, it is immediately removed from the multicast group it belongs to, which may affect the continuity of network data flow. This port may be connected to a HUB or a network device without the IGMP SNOOPING capability that is connected to a number of receiving multicast data streams. One device sending Leave may affect other devices to receive the multicast data stream. The mechanism of fast-leave-timeout can prevent the occurrence of this situation. By configuring a leave waiting time through fast-leave-timeout, the port receives the leave package and waits for a long time for fast-leave-timeout before deleting it from the multicast group to which it belongs, which may guarantee the continuity of network multicast stream.

13.1.2 Layer 2 dynamic multicast

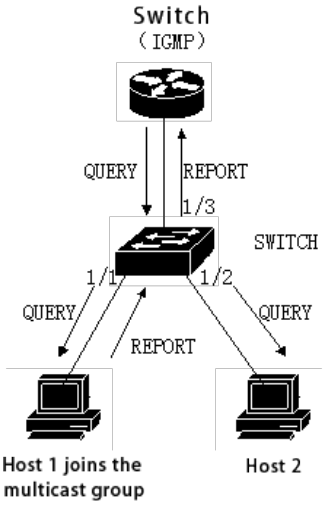
The multicast MAC address entries in the two-layer hardware multicast forwarding table can be obtained through the IGMP snooping dynamic learning. The IP multicast MAC address is learned dynamically by IGMP Snooping.

When the switch turns off IGMP SNOOPING, the layer 2 hardware multicast forwarding table is in unregistered forwarding mode, the multicast MAC address can not be learned dynamically, there is no entry in the layer 2 hardware multicast forwarding table, and all layer 2 multicast data streams are treated as broadcast.

When the network has a multicast environment, in order to effectively control the multicast traffic of the network, the switch can turn on the IGMP SNOOPING, and the layer 2 hardware multicast forwarding table is in the registration and forwarding mode. The switch can learn the multicast MAC address by listening to the IGMP protocol packets on the network, and the layer 2 multicast stream that matches the entries in the layer 2 hardware multicast forwarding table can be forwarded.

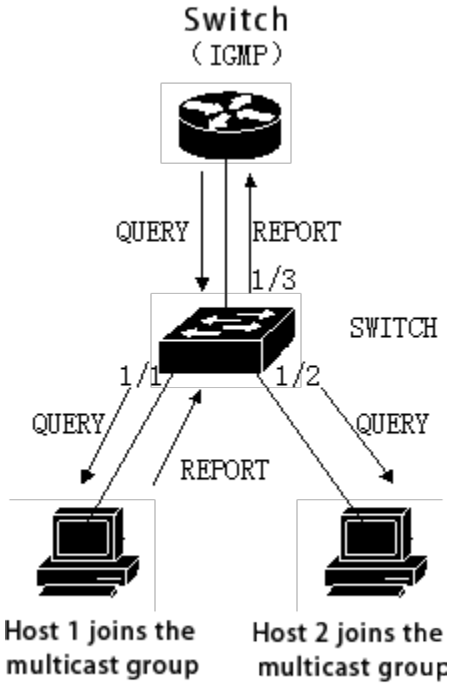
11.1.3 Join a group

When a host wants to join a multicast group, the host sends a IGMP REPORT packet in which the host specifies the multicast group to which the host is to join. When the switch receives a IGMP QUERY packet, the switch forwarded the packet to all other ports of the same VLAN, and a IGMP REPORT packet is returned when the host under the port who wants to join the multicast group receives the IGMP QUERY packet. When the switch receives a IGMP REPORT packet, a layer 2 multicast entry is established, and the port of the IGMP QUERY packet and the IGMP R are received The port of the EPORT packet is added to the layer 2 multicast entry and becomes its output port.



As shown in the figure above, all the devices are in a subnet, assuming that the VLAN of the subnet is 2. The router runs the IGMPv2 protocol and sends the IGMP QUERY package regularly. Host 1 wants to join multicast group 224.1.1.1. Upon receiving the IGMP QUERY package from port 1/3, the switch logs the port and forwards the package to ports 1/1 and 1/2. Host 1 sends back an IGMP REPORT package after receiving the IGMP QUERY package, while host 2 does not send the IGMP REPORT package because it does not want to join the multicast group. Upon receiving the IGMP REPORT package from port 1/1, the switch forwards the package from query port 1/3 and creates a tier 2 multicast entry (assuming the entry does not exist), which includes the following items:

Layer 2 multicast address	VLAN ID	Output port list
01:00:5e:01:01:01	2	1/1，1/3



As with the above condition, as in FIG.1, the host 1 has joined the multicast group 224.1. 1.1, and now the host 2 wants to join the multicast group 224.1. 1.1. When the host 2 receives the IGMP QUERY packet and returns an IGMP REPORT packet, the switch forwards the packet from the inquiry port 1/3 after receiving the IGMP REPORT from the port 1/2 and the packet port 1/2 is added to the two-layer multicast entry, and the two-layer multicast entry becomes:

Layer 2 multicast address	VLAN ID	Output port list
01:00:5e:01:01:01	2	1/1，1/2，1/3

13.1.4 Leave a group

In order to form a stable multicast environment, devices running IGMP (such as routers) will send an IGMP QUERY packet to all hosts at regular intervals. A host that has joined a multicast group or wants to join a multicast group will send an IGMP REPORT after receiving the IGMP QUERY.

If the host wants to leave a multicast group, there are two ways: active leave and passive leave. Active leave means that the host sends an IGMP LEAVE packet to the router. Passive leave means that the host does not return an IGMP REPORT after receiving the IGMP QUERY from the router.

Corresponding to the way the host leaves the multicast group, there are also two ways to separate the port from the layer 2 multicast entry on the switch: timeout departure and receiving IGMP LEAVE packet departure.

When the switch does not receive a IGMP REPORT packet of a multicast group from a port for more than a certain time, the port is cleared from the corresponding layer 2 multicast entry, and if the layer 2 multicast entry does not have a port, the layer 2 multicast entry is deleted.

。When the fast-leave of the switch is configured as ENABLE, if a port receives an IGMP LEAVE packet from a multicast group, the port is cleared from the corresponding layer 2 multicast entry, and if the layer 2 multicast entry

does not have a port, the layer 2 multicast entry is deleted.

Fast-leave is generally used to connect to a host under one port; if there is more than one host under a port, the fast-leave-timeout waiting time can be configured, which can ensure the continuity and reliability of the multicast stream in the network.

13.2 Configure IGMP SNOOPING

13.2.1 IGMP SNOOPING default configuration

IGMP SNOOPING is turned off by default, and the layer 2 hardware multicast forwarding table is in unregistered forwarding mode.

Fast-leave is closed by default

The Fast-leave-timeout time is 300 seconds.

The age time of the REPORT port of the multicast group is 400 seconds by default.

The age time of the QUERY port of the multicast group is 300 seconds by default.

13.2.2 Open and close IGMP SNOOPING

The IGMP SNOOPING protocol can be opened globally or partially open. Only IGMP SNOOPING can be turned on to enable or disable IGMP SNOOPING for a VLAN.

Open the global IGMP SNOOPING

Switch#configure terminal

Switch(config)#ip igmp snooping

Open IGMP SNOOPING for a VLAN

Switch#configure terminal

Switch(config)#ip igmp snooping vlan <vlan-id>

Turn off global IGMP SNOOPING

Switch#configure terminal

Switch(config)#no ip igmp snooping

Closes the IGMP SNOOPING of a VLAN.

Switch#configure terminal

Switch(config)#no ip igmp snooping vlan <vlan-id>

13.2.3 Configure the survival time

Configure the lifetime of the query group.

Switch#configure terminal

Switch(config)#ip igmp snooping group-membership-timeout <interval> vlan <vlan-id>

The unit of Interval is milliseconds

Configure the lifetime of the query group.

Switch#configure terminal

Switch(config)#ip igmp snooping query-membership-timeout <interval> vlan <vlan-id>

The unit of Interval is milliseconds.

13.2.4 Configure fast-leve

Start fast-leave of VLAN

Switch#configure terminal

Switch(config)#ip igmp snooping fast-leave vlan <vlan-id>

Turn off fast-leave

Switch#configure terminal

Switch(config)#no ip igmp snooping fast-leave vlan <vlan-id>

Configure fast-leave wait time

Switch#configure terminal

Switch(config)# ip igmp snooping fast-leave-timeout <interval> vlan <vlan-id>

Restore default fast-leave wait time

Switch#configure terminal

Switch(config)#no ip igmp snooping fast-leave-timeout vlan <vlan-id>

13.2.5 Configure MROUTER

Configure static query ports

Switch#configure terminal

Switch#interface ge1/6

Switch(config-ge1/6)#ip igmp snooping mrouter vlan [vlan-id]

13.2.6 Display information

Display the IGMP SNOOPING configuration information

Switch#show ip igmp snooping

Display the configuration information of a VLAN

Switch#show ip igmp snooping vlan <vlan-id>

Display aging information of the REPORT multicast group

Switch#show ip igmp snooping age-table group-membership

Display the aging information of QUERY

Switch#show ip igmp snooping age-table query-membership

Displays forwarding information of multicast group

Switch#show ip igmp snooping forwarding-table

Display MROUTER information

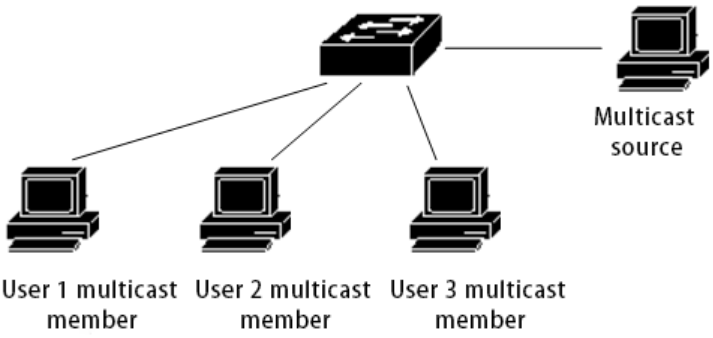
Switch#show ip igmp snooping mrouter

Displays the current configuration of the system, including the configuration of IGMP SNOOPING

Switch#show running-config

13.3 IGMP SNOOPING configuration example

Enable IGMP SNOOPING on the switch, user 1, user 2, user 3 can be added to a specific multicast group



Switch#config t

Switch(config)#vlan database

Switch(config-vlan)#vlan 200

Switch(config)#ip igmp snooping

Switch(config)#interface ge1/1

Switch(config-ge1/1)#switchport mode access

Switch(config-ge1/1)#switchport access vlan 200

Switch(config)#interface ge1/2

```
Switch(config-ge1/2)#switchport mode access
Switch(config-ge1/2)#switchport access vlan 200
Switch(config)#interface ge1/3
Switch(config-ge1/3)#switchport mode access
Switch(config-ge1/3)#switchport access vlan 200
Switch(config)#ip igmp snooping group-membership-timeout 60000 vlan 200
```

Chapter 14 MVR configuration

This chapter includes：

- Brief introduction of MVR
- Configure MVR
- MVR configuration example

14.1 MVR introduction

Multicast VLAN Registration (MVR) is applied to multicast streaming applications in service provider networks, such as TV on demand. The MVR allows subscribers on the port to subscribe to or cancel multicast streams in the multicast VLAN, allowing data flows within one multicast VLAN to be shared by other VLANs. MVR has two purposes: (1) It can effectively and securely transfer multicast streams between VLANs through simple configuration; (2) Support dynamic join and leave of multicast groups;

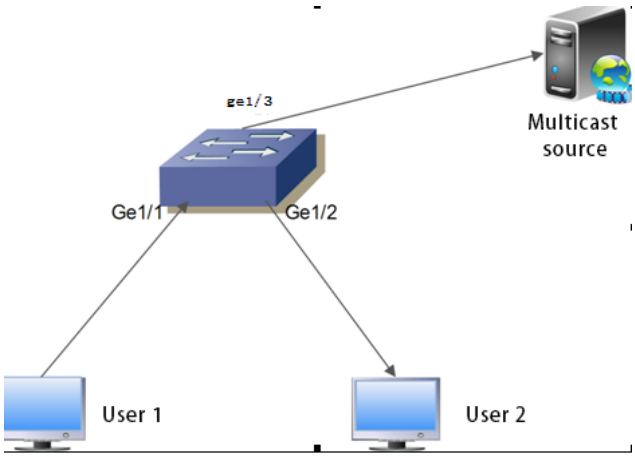
MVR operates in the same way as IGMP snooping. Two functions can be started at the same time. The MVR only processes the joining and leaving of the configured multicast group. The joining and leaving of other groups are managed by IGMP snooping. The difference between the two is that the multicast stream in IGMP snooping can only be forwarded in one VLAN, and the multicast stream of the MVR can be forwarded in different VLANs.

14.2 Configure MVR

Order	Description	CLI mode
mvr (enable|disable)	Start the global MVR	Global configuration mode
no mvr	Clear all MVR configurations	Global configuration mode
mvr group A.B.C.D	Configure IP Multicast address	Global configuration mode
no mvr group A.B.C.D	Delete IP Multicast address	Global configuration mode
mvr group A.B.C.D <1-256>	Configure the IP multicast address and configure a continuous MVR group address	Global configuration mode
mvr vlan <1-4094>	Specify the VLAN to receive multicasting data	Global configuration mode
no mvr vlan	Restore the default VLAN1 for receiving multicasting data	Global configuration mode
mvr-interface (enable|disable)	Start the port MVR	Interface configuration mode
show mvr	Display MVP configuration information	Privilege mode

14.3 MVR configuration example

The networking topology is shown in the following figure, and the user 1 and the user 2 belong to vlan10 vlan20, and the user 1 and the user 2 see the same program, the program range is 225.1. 1.1-225.1. 1.64, and the mvr vlan is 100:



Configure the vlan, start the global IGMP snooping, configure the mvr vlan, mvr program group range, and global enable mvr:

```
Switch#configure terminal
Switch(config)#ip igmp snooping
Switch(config)# mvr enable
Switch(config)#mvr vlan 100
Switch(config)#mvr group 225.1.1.1 64
Switch#
```

Configure switch user port Ge1/ 1Ge1/2, and up-port Ge1/28:

```
Switch#configure terminal
Switch(config)#interface ge1/1
Switch(config-ge1/1)#switchport mode hybrid
Switch(config-ge1/1)#switchport hybrid allowed vlan add 10 egress-tagged disable
Switch(config-ge1/1)#switchport hybrid allowed vlan add 100 egress-tagged disable
Switch(config-ge1/1)#mvr enable
Switch(config-ge1/1)#

Switch#configure terminal
Switch(config)#interface ge1/2
Switch(config-ge1/2)#switchport mode hybrid
Switch(config-ge1/2)#switchport hybrid allowed vlan add 20 egress-tagged disable
Switch(config-ge1/2)#switchport hybrid allowed vlan add 100 egress-tagged disable
Switch(config-ge1/2)#mvr enable
Switch(config-ge1/2)#

Switch#configure terminal
Switch(config)#interface ge1/28
Switch(config-ge1/28)#switchport mode trunk
Switch(config-ge1/28)#switchport trunk allowed vlan add 100
Switch(config-ge1/28)#
```

Chapter 15 DHCP SNOOPING configuration

In a dynamically accessed network environment, the host obtains an IP address and network parameters through a DHCP server. DHCP SNOOPING is a listening protocol proposed for ARP attacks. After the DHCP packet is received, the IP address assigned to the client by the DHCP server is dynamically bound to the client's MAC address, and the ARP attack packet is filtered on the switch.

The switch supports DHCP SNOOPING function and can effectively defend against ARP attacks. DHCP SNOOPING listens for DHCP messages on the network and binds port ARP information.

Four linked DHCP server physical ports can be configured to prevent unknown servers from interfering with the network to a certain extent.

When the switch is powered off, it causes the binding table to be lost and needs to be re-learned; the switch provides the download function on the binding table, and the binding table can be saved in the tftp server.

This chapter describes the concept and configuration of DHCP SNOOPING, including:

- Introduce DHCP SNOOPING
- Configure DHCP SNOOPING
- DHCP SNOOPING configuration example

15.1 Introduce DHCP SNOOPING

The ARP protocol creates a loophole in network security due to a simple trust mechanism. When an ARP attack packet carrying a fake MAC address arrives at the host, it will directly overwrite the local ARP cache table without restriction, resulting in normal data flow to the attacker. Therefore, ARP information binding is implemented on the network layer 2 switch, which can effectively filter ARP attack packets so that the attack packets cannot reach the attacked host. If there is an unexpected DHCP server entering the network, the IP address allocation will be confused. The DHCP SNOOPING protocol provides the physical port for binding the linked server. The non-specified physical port cannot forward the DHCP protocol packet issued by the DHCP server, which can reduce the chance of the unknown server entering the network.

This section mainly includes:

- DHCP SNOOPING Process
- DHCP SNOOPING binding table
- The physical port of the DHCP SNOOPING binding server
- Download from the DHCP SNOOPING binding table

15.1.1 DHCP SNOOPING Process

The DHCP SNOOPING protocol only listens for three messages of the DHCPrequest, the DHCPack, and the DHCPrelease, does not receive other types of DHCP messages, and binds the IP and MAC mapping relationships according to the messages.

The global DHCP SNOOPING switch is responsible for opening the switch to receive the DHCP message, the IP message of the UDP port of 67,68.

15.1.2 DHCP SNOOPING binding table

The address is the IP address assigned by the server, at which time the lease timer is started, the interval is the lease value provided by the DHCP server contained in the DHCPack message, the timer is restarted when the contract is renewed, and the binding table entry is deleted when the lease expires. Interface information records the interface where the client is located, that is, the interface corresponding to the binding relationship between IP address and MAC address.

When the DHCPrequest message is received, the binding table entry is created, the entry type is REQ, recording IP address, MAC address, interface information, and a 10-second delay timer is started.

When the DHCPrequest message is received, the binding table entry of type REQ already exists, the entry is updated, and the delay timer is restarted.

When an DHCPrequest message is received and a binding table entry of type ACK already exists, the interface information is recorded.

When the DHCPack message is received, if there is a binding table entry of REQ type, the IP address assigned by the server in the DHCPack message is recorded, the delay timer is turned off, and the lease timer is started.

When a DHCPack message is received, a binding table entry of the REQ type is not present, and the message is discarded.

When a DHCPack message is received, an ACK type binding table entry is already present, and if the interface has changed, the binding table entry of the original interface is deleted and the entry is updated.

If the interface is not changed, the IP address assigned by the server changes, and the binding table entry of the original interface is deleted and the entry is updated.

If the interface is not changed, the IP address is not changed, indicating that it is a renewal process and the lease timer is restarted.

The time-delay timer times out and the binding table entry of type REQ is deleted.

When the lease timer times out, the binding table entry of type ACK is deleted.

15.1.3 The physical port of the DHCP SNOOPING binding server

DHCP SNOOPING specifies the physical port of the linked server, and DHCP messages can be received only on the specified port. If there are multiple DHCP servers in the network, the OFFER provided by the unspecified port server will be filtered and the IP address cannot be assigned to the client. The specified port is beneficial to the unified allocation of IP addresses in the network, and the address pool of unknown servers is not in IP planning, and some clients can not connect to the network properly. To a certain extent, the probability of network communication anomalies caused by private access to the server is reduced.

15.1.4 Download from the DHCP SNOOPING binding table

DHCP SNOOPING records the binding relationship between IP and MAC by listening to DHCP messages and maintains its binding table. When the switch fails to restart or fails unexpectedly, the binding table will be lost, and the switch needs to relearn the binding table entry after restart. In the network topology, if the host is not directly connected, it is difficult to identify the network connection interruption and restart the DHCP discover process, and it will be difficult for the switch to learn the binding information again. To do this, save the binding table on the tftp server and download the binding table after the switch restarts, which can resolve the switching during restart The brief memory blank that appears on the machine. The switch provides the function of uploading and downloading the binding table, and the administrator can upload or download the binding table manually through the command, or configure the automatic upload command to upload the binding table regularly; when restarting, the binding table command downloads the backed up binding table file from the tftp server and writes it to the binding table of the DHCP SNOOPING protocol module.

15.2 DHCP SNOOPING configuration

15.2.1 DHCP SNOOPING default configuration

DHCP SNOOPING is closed by default

The default interval for an entry delay timer of type REQ in the DHCP SNOOPING binding table is 10 seconds.

15.2.2 Global Open and Close DHCP SNOOPING

The DHCP SNOOPING, of an interface can be turned on or off only after the DHCP SNOOPING is turned on globally. The DHCP SNOOPING of all interfaces must be turned off before the global DHCP SNOOPING can be turned off.

Open the global DHCP SNOOPING

Switch#configure terminal

Switch(config)#ip dhcp snooping [IF_LIST]

Parameter is the physical port list of the linked DHCP server to be bound, a total of four can be specified, the port list is separated by the "," number, such as: ge1/1,ge1/25,ge1/26

Turn off the global DHCP SNOOPING

Switch#configure terminal

Switch(config)#no ip dhcp snooping

15.2.3 Interface opens and closes the DHCP SNOOPING

Open the DHCP SNOOPING. of an interface

Switch#configure terminal

Switch(config)#interface ge1/1

Switch(config-ge1/1)#dhcp snooping

Close the DHCP SNOOPING. of an interface

Switch#configure terminal

Switch(config)#interface ge1/1

Switch(config-ge1/1)#no dhcp snooping

15.2.4 DHCP SNOOPING binding table upload&download

Upload the DHCP SNOOPING binding table to the TFTP server

Switch#configure terminal

Switch(config)#dhcp snooping upload A.B.C.D FILE_NAME

Parameter: the IP address of the A.B.C.D tftp server; the name of the binding table file saved by FILE_NAME on the tftp server.

Download the DHCP SNOOPING binding table from the TFTP server
Switch#configure terminal
Switch(config)#dhcp snooping download A.B.C.D FILE_NAME

Configure the timed upload DHCP SNOOPING binding table to the TFTP server.
Switch#configure terminal
Switch(config)#dhcp snooping auto-upload A.B.C.D FILE_NAME interval
Parameters: interval timing upload interval, ranging from 1 minute to one day.

Cancel the configuration of uploading the DHCP SNOOPING binding table to the TFTP server.
Switch#configure terminal
Switch(config)#no dhcp snooping auto-upload

Automatically download DHCPSNOOPING binding table from TFTP server during configuration restart.
Switch#configure terminal
Switch(config)#dhcp snooping reset-download A.B.C.D FILE_NAME

Cancel the configuration of automatically downloading the DHCP SNOOPING binding table from the TFTP server during restart.
Switch#configure terminal
Switch(config)#no dhcp snooping reset-download

15.2.5 Display information

Displays the DHCP SNOOPING configuration information
Switch#show dhcp snooping

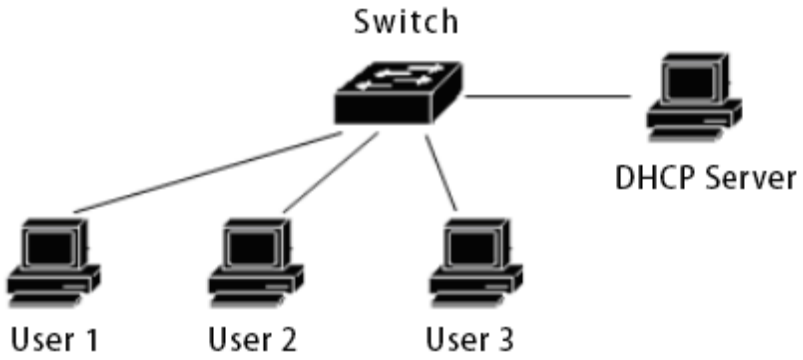
Display DHCP SNOOPING binding table information
Switch#show dhcp snooping binding-table

Displays the current configuration of the system, including DHCP SNOOPING configuration.
Switch#show running-config

15.3 DHCP SNOOPING configuration example

15.3.1 Configure

Enable DHCP SNOOPING function on layer 2 switch, user 1, user 2, user 3 dynamically obtain IP address and network parameters through DHCP server. User 1, user 2, user 3 are located in the interface to start the DHCP SNOOPING function, and the interface dynamically binds ARP information.



Switch#configure terminal
Switch(config)#ip dhcp snooping ge1/9
Switch(config)#interface ge1/1
Switch(config-ge1/1)#dhcp snooping
Switch(config-ge1/1)#interface ge1/2
Switch(config-ge1/2)#dhcp snooping
Switch(config-ge1/2)#interface ge1/3
Switch(config-ge1/3)#dhcp snooping
Switch(config-ge1/3)#end
Switch#show dhcp snooping
DHCP Snooping is enabled globally
DHCP Server interface：ge1/9
Enable interface: ge1/1 ge1/2 ge1/3
Switch#show dhcp snooping binding-table

IP	MAC	FLAG	PORT	LEASE
192.168.1.100	00:11:5b:34:42:ad	ACK	ge1/1	23:59:58
192.168.1.101	00:11:64:52:13:5d	ACK	ge1/2	23:50:01
192.168.1.102	00:11:80:4d:a2:46	ACK	ge1/3	20:34:45

Switch#show running-config
!
ip dhcp snooping ge1/9
!
spanning-tree mst configuration
!

```
interface vlan1
 Ip address 192.168.1.1/24
!
interface ge1/1
 dhcp snooping
!
interface 1/2
 dhcp snooping
!
interface 1/3
 dhcp snooping
!
line vty
!
End
Switch#
```

15.4 DHCP SNOOPING configuration troubleshooting

The DHCP snooping configuration failure may be caused by the following reasons:

1、System CFP resources are exhausted

2、The interface is configured with ACL filtering to cause DHCP SNOOPING to fail globally.

3、The interface is configured with IP and MAC bindings causing the DHCP SNOOPING to fail globally.

4、Current interface is configured with ACL filtering

5、The current interface has 802.1x anti-ARP spoofing enabled.

6、The configured interface is a Layer 3 or a trunk.

Chapter 16 MLD SNOOPING configuration

In the metropolitan area network/Internet, when the same data packet is sent to multiple but not all receivers in the network by unicast, since it is necessary to copy the packet to each receiving endpoint, as the number of receivers increases, it is required. The number of packets sent will also increase linearly, which will increase the overall burden on hosts, switching routing devices and network bandwidth resources, and the efficiency will be greatly affected. With the increasing demand for multi-point video conferencing, video on demand, and group communication applications, in order to improve resource utilization, multicast mode has increasingly become a popular transmission method in multipoint communication.

The switch implements the MLD SNOOPING function to serve multicast applications. MLD SNOOPING listens to MLD packets on the network to implement dynamic learning of IPV6 multicast MAC addresses.

This chapter describes the concept and configuration of MLD SNOOPING, including：

- MLD SNOOPING introduction
- MLD SNOOPING configuration
- MLD SNOOPING configuration example

16.1 MLD SNOOPING introduction

Traditional network multicast packets in a subnet as broadcast processing, which is easy to make the network traffic, resulting in network congestion. When MLD SNOOPING is implemented on the switch, MLD SNOOPING can dynamically learn IPV6 multicast MAC address, maintain the list of output ports of IPV6 multicast MAC address, so that the multicast data stream is only sent to the output port, which can reduce network traffic.

This section mainly includes the following:

- MLD SNOOPING process
- Layer 2 dynamic multicasting
- Join a group
- Leave a group

16.1.1 MLD SNOOPING process

he MLD SNOOPING is a two-layer network protocol, which monitors the MLD protocol packet passing through the switch, and maintains a multicast group according to the receiving port, the VLAN ID and the multicast address of the MLD protocol packets, and then forwards the MLD protocol packets. Only the ports of the multicast group are added can receive the multicast data stream; thus, the flow of the network is reduced, and the network bandwidth is saved.

The multicast group includes a multicast group address, a member port, a VLAN ID, and an Age time.

The formation of the MLD SNOOPING multicast group is a learning process. When a port of the switch receives the MLD REPORT packet, MLD SNOOPING generates a new multicast group, and the port that receives the MLD REPORT packet is added to the multicast group. When the switch receives an MLD QUERY packet, if the multicast group already exists in the switch, the port that receives the MLD QUERY is also added to the multicast group. Otherwise, the MLD QUERY packet is forwarded. MLD SNOOPING also supports the Done mechanism of MLD V2; if MLD SNOOPING is configured with fast-leave as ENABLE, its receiving port can leave the multicast group immediately when receiving the Done packet of MLD V2; if the fast-leave leaving waiting time is configured (Fast-leave-timeout), then the multicast group leaves the multicast group after waiting for this time to expire.

MLD SNOOPING has two update mechanisms. One is the Done mechanism described above. In most cases, MLD SNOOPING removes expired multicast groups through age time. When the multicast group joins the MLD SNOOPING, the time to join is recorded, and when the multicast group remains in the switch for more than a configured age time, the switch removes the multicast group.

When the port receives DONE package, the port is immediately removed from the multicast group to which it belongs, which may affect the continuity of the network data stream, as the port below may be connected to a HUB or a network device without the MLD SNOOPING function, A number of receiving multicast data stream devices are connected under this device. One device sends a DONE, which may affect other devices and may not receive the multicast data stream. the Fast-leave-timeout mechanism prevents this from occurring and is matched by the

Fast-leave-timeout Set a time to leave the waiting time, and wait for Fast-release-timeout to be deleted from the multicast group to which it belongs, which may guarantee the continuity of the multicast flow of the network.

16.1.2 Layer 2 dynamic multicast

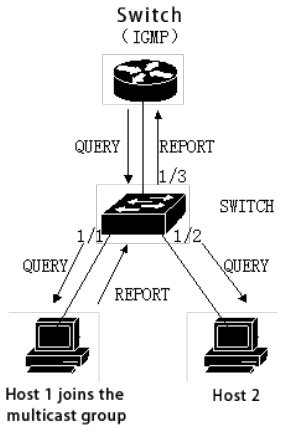
The multicast MAC address entries in the Layer 2 hardware multicast forwarding table can be learned dynamically through MLD SNOOPING. Dynamically learned by MLD SNOOPING is the IPV6 multicast MAC address.

When the switch turns off MLD SNOOPING, the layer 2 hardware multicast forwarding table is in unregistered forwarding mode, the multicast MAC address can not be learned dynamically, there is no entry in the layer 2 hardware multicast forwarding table, and all layer 2 multicast data streams are treated as broadcast.

When the network has a multicast environment, in order to effectively control the multicast traffic of the network, the switch can turn on the MLD SNOOPING, and the layer 2 hardware multicast forwarding table is in the registration and forwarding mode. The switch can learn the multicast MAC address by listening to the MLD protocol packets on the network, and the layer 2 multicast stream that matches the entries in the layer 2 hardware multicast forwarding table can be forwarded.

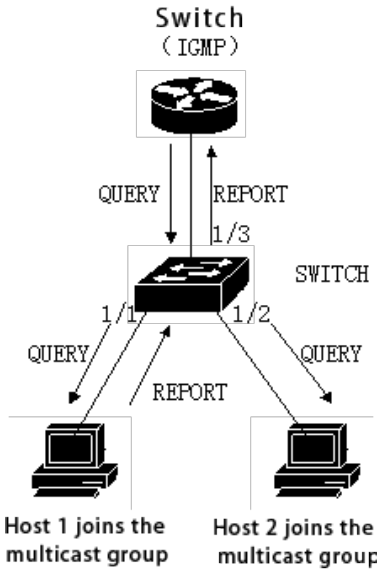
16.1.3 Join a group

When a host wants to join a multicast group, the host sends an MLD REPORT packet, in which the multicast group to which the host wants to join is specified. When the switch receives an MLD QUERY packet, the switch forwards the packet to all other ports in the same VLAN. When the host that wants to join the multicast group on the port receives the MLD QUERY packet, it will send back an MLD REPORT packet. When the switch receives an MLD REPORT packet, it will create a Layer 2 multicast entry. The port that receives the MLD QUERY packet and the MLD REPORT packet will join the Layer 2 multicast entry and become its output port.



As shown in the figure above, all devices are in one subnet, assuming that the VLAN of the subnet is 2. The router runs the MLDv2 protocol and periodically sends the MLD QUERY packet. Host 1 wants to join the multicast group ff15::1. After the switch receives the MLD QUERY packet from the 1/3 port, it records the port and forwards the packet to ports 1/1 and 1/2. After receiving the MLD QUERY packet, host 1 sends back an MLD REPORT packet. Host 2 does not want to join the multicast group and does not send the MLD REPORT packet. After receiving the MLD REPORT packet from port 1/1, the switch forwards the packet from query port 1/3 and creates a Layer 2 multicast entry (assuming the entry does not exist). The Layer 2 multicast entry includes the following items :

Layer 2 multicast address	VLAN ID	Output port list
33:33:00:00:00:01	2	1/1，1/3



As shown in figure 1, host 1 has joined the multicast group ff15::1, now that host 2 wants to join the multicast group ff15::1. When host 2 receives the MLD QUERY packet and sends back a MLD REPORT packet, when the switch receives the MLD REPORT from port 1 / 2, the switch will forward the packet from the query port 1 / 3 and the packet port 1 / 2 will be added to the layer 2 multicast entry, and the layer 2 multicast entry will become:

Layer 2 multicast address	VLAN ID	Output port list
33:33:5e:00:00:01	2	1/1，1/2，1/3

16.1.4 Leave a group

In order to form a stable multicast environment, devices running MLD (such as routers) will send an MLD QUERY packet to all hosts at regular intervals. A host that has joined a multicast group or wants to join a multicast group will send back an MLD REPORT after receiving the MLD QUERY.

There are two ways for a host to leave a multicast group: active leave and passive leave. Active leave means that the host sends an MLD LEAVE packet to the router. Passive leave means that the host does not return MLD REPORT after receiving the MLD QUERY from the router.

Corresponding to the way the host leaves the multicast group, there are two ways to leave the Layer 2 multicast entry on the switch: timeout and receiving the MLD DONE packet.

When the switch has not received the MLD REPORT package of a multicast group from one port for a certain time, the port is to be cleared from the corresponding two-layer multicast entry, and if the two-layer multicast entry does not have a port, the two-layer multicast entry is deleted.

When the fast-leave configuration of the switch is ENABLE, if a port receives a multicast group MLD LEAVE packet, the port is cleared from the corresponding Layer 2 multicast entry. If the Layer 2 multicast entry does not have a

port, then delete this Layer 2 multicast entry.

Fast-leave is generally applied to a host connected to a port. If there is more than one host under one port, you can configure the fast-leave-timeout wait time to ensure the continuity and reliability of the multicast stream in the network.

16.2 MLD SNOOPING configuration

16.2.1 MLD SNOOPING default configuration

MLD SNOOPING is turned off by default, and the layer 2 hardware multicast forwarding publication is in unregistered forwarding mode.

Fast-leave is closed by default
The fast-leave-timeout time is 300 seconds.
The age of the multicast group REPORT port is 400 seconds by default.
The age of the multicast group QUERY port is 300 seconds by default.

16.2.2 Open and close MLD SNOOPING

The MLD SNOOPING protocol can be opened globally or a partial VLAN can be opened separately; only the global open MLD SNOOPING can open or close the MLD SNOOPING of a VLAN.

Open the global MLD SNOOPING
Switch#configure terminal
Switch(config)#ipv6 mld snooping

Open the MLD SNOOPING of the VLAN
Switch#configure terminal
Switch(config)#ipv6 mld snooping vlan <vlan-id>

Close global MLD SNOOPING
Switch#configure terminal
Switch(config)#no ipv6 mld snooping

Close the MLD SNOOPING of the VLAN
Switch#configure terminal
Switch(config)#no ipv6 mld snooping vlan <vlan-id>

16.2.3 Configure survival time

Configure the lifetime of multicast group

Switch#configure terminal

Switch(config)#ipv6 mld snooping group-membership-timeout <interval> vlan <vlan-id>

The unit of Interval is milliseconds

Configure the lifetime of the query group

Switch#configure terminal

Switch(config)#ipv6 mld snooping query-membership-timeout <interval> vlan <vlan-id>

The unit of Interval is milliseconds

16.2.4 Configure fast-leave

Start a fast-release of a VLAN

Switch#configure terminal

Switch(config)#ipv6 mld snooping fast-leave vlan <vlan-id>

Turn off fast-leave

Switch#configure terminal

Switch(config)#no ipv6 mld snooping fast-leave vlan <vlan-id>

Configure fast-leave wait time

Switch#configure terminal

Switch(config)# ipv6 mld snooping fast-leave-timeout <interval> vlan <vlan-id>

Restore the default fast-release wait time

Switch#configure terminal

Switch(config)#no ipv6 mld snooping fast-leave-timeout vlan <vlan-id>

16.2.5 Configure MROUTER

Configure a static query port

Switch#configure terminal

Switch#interface ge1/6

Switch(config-ge1/6)#ipv6 mld snooping mrouter vlan [vlan-id]

16.2.6 Display information

Displays the MLD SNOOPING configuration information.

Switch#show ipv6 mld snooping

Display configuration information of a VLAN

Switch#show ipv6 mld snooping vlan <vlan-id>

Display aging information for REPORT multicast groups

Switch#show ipv6 mld snooping age-table group-membership

Display aging information of QUERY

Switch#show ipv6 mld snooping age-table query-membership

Displays forwarding information of a multicast group

Switch#show ipv6 mld snooping forwarding-table

Displays forwarding information for a multicast group

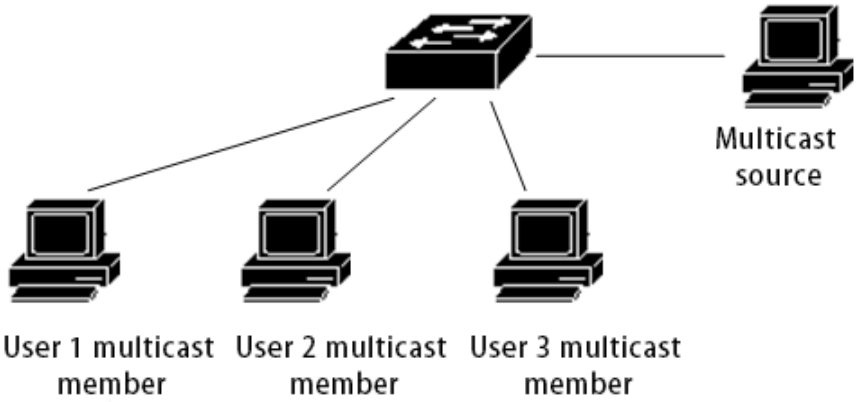
Switch#show ipv6 mld snooping mrouter

Displays the system's current configuration, including the configuration of the MLD SNOOPING

Switch#show running-config

16.3 MLD SNOOPING configuration example

Enable MLD SNOOPING on the switch, user 1, user 2, user 3 can be added to a specific multicast group



Switch#config t

Switch(config)#vlan database

Switch(config-vlan)#vlan 200

Switch(config)#ipv6 mld snooping

Switch(config)#interface ge1/1

Switch(config-ge1/1)#switchport mode access

Switch(config-ge1/1)#switchport access vlan 200

Switch(config)#interface ge1/2

Switch(config-ge1/2)#switchport mode access

Switch(config-ge1/2)#switchport access vlan 200

Switch(config)#interface ge1/3

Switch(config-ge1/3)#switchport mode access

Switch(config-ge1/3)#switchport access vlan 200

Switch(config)#ipv6 mld snooping group-membership-timeout 60000 vlan 200

Chapter 17 ACL configuration

In the actual network, network access security is a very concerned issue for administrators. Switches support ACL filtering to provide network access security. By configuring ACL rules, the switch filters the input data stream according to these rules to achieve network access security.

This chapter describes how to configure ACL, including the following：

- Introduction of the ACL Repository
- ACL filtering introduction
- ACL Repository Configuration
- ACL based on time period
- ACL filter configuration
- ACL configuration example

17.1 Introduction of the ACL Repository

The ACL (access list control) resource library is a collection of multiple groups of access rules. the acl resource library does not have the function of controlling data forwarding. it is just a collection of rules with conflicting ordering. When the ACL repository is referenced by an application, these applications control the forwarding of data according to the rules provided by the ACL resource. ACL can be applied to port access filtering, service access filtering, QoS and more.

The ACL resource base has standard IP rule group (group number 1: 99,1300), extended IP rule group (group number 100199,2000 / 2699), IP MAC group < group number 700799 >, ARP group (group number 1100 ≤ 1199). Conflict rule priority order is automatically carried out within each set of rules. When a user configures a ACL rule, the system inserts the rule into the appropriate location according to the collation.

In application, when a packet passes through a port, the switch compares the fields in each rule with all the corresponding fields in the packet; when multiple rules match exactly at the same time, the first exactly matched rule takes effect; and the matching rule determines whether the packet is forwarded or discarded. The so-called perfect match is that the value of the field in the rule is exactly the same as the value of the corresponding field in the packet. Only if a rule of ACL is exactly matched will the rule do the corresponding deny or permit operation.

In switches, rules within the same group are sorted automatically. The automatic sorting of rules is relatively complex. In the sorting process, the rules with large scope are behind and the ones with small scope are in front of each other. The size of the range is determined by the constraint of the rule; the less the constraint of the rule, the larger the range of the rule matching, and the smaller the scope of the rule matching. The constraint conditions of the rule are mainly reflected in the wildcard of the address and the number of some non-address fields. Wildcard is a bit string. IP address is a four-byte address, MAC address is six bytes. Bits is'1'to indicate that there is no need to match, and bits to'0' means to match. Non-address fields refer to protocol types, IP protocol types, protocol ports, and these fields also hide a wildcard. Their length is the byte length of the corresponding field, so the same field length is uniform, just calculate the number of fields.

Take port access filtering as an example to illustrate the necessity of regular sorting and the advantages of automatic sorting. If the user needs to reject address forwarding with a source address of 192.168.0.0 ≤ 16 and allow address forwarding with a source address of 192.168.1.0 / 24, you can configure the following two rules:

Access-list 1 permit 192.168.1.0 0.0.0.255-Rule 1

Access-list 1 deny 192.168.0.0 0.0.255.255-Rule 2

Referred to as Rules 1 and 2.

These two rules are in conflict; because the address of rule 1 is contained in the address of rule 2, and one is deny, and the other is permit; according to the filtering principle of ACL, different orders have different results. If the above requirements are to be met, the order of the above two rules must be: rule 1 at the front and rule 2 at the bottom. The switch automatically implements the above sorting function, no matter what order the user configure the above rules, the final order is that rule 1 is in front of rule 2. When a packet with a source address of 192.168.1.1 is forwarded, the first comparison is made The first rule, then compare the second rule, both rules match, the previous effective (forward);

if the source address is 192.168.1.1, only the first match, then discard (do not forward).

Without sorting, users may configure Rule 2 first, then Rule 1, and Rule 2 first.

Access-list 1 deny 192.168.1.0 0.0.255.255-Rule 2

Access-list 1 permit 192.168.2.0 0.0.0.255-Rule 1

Because the previous rule 2 contains the following rule 1, it may lead to a situation where packets that exactly match rule 1 also exactly match rule 2, which takes effect every time; and fails to meet the requirements of the application.

In the switch, '0.255.255' means that the wildcard bits,bits is' 1 'for no matching, and the bits for' 0' indicates that the match is to be matched. From this, we can see that the wildcard bits of rule 2 is' 0.255.255s, which needs to match two bytes (the wildcard bits in 16 bits); rule 1 is' 00.255x] and the need to match three bytes (24 bits); so the rule 'range' of rule 2 is larger, so it is followed. In extended IP, row The sequence needs to consider more rules fields, such as the IP protocol type, the communication port, and so on. Their sort rules are the same, that is, the more the configuration limits the more rule's' range 'is, the more the' range 'is. The ordering of the rules is implemented in the background, and the user commands can only be displayed in the order of the user's configuration.

The filtering fields supported by ACL include the source IP, destination IP,IP protocol type (such as TCP,UDP,OSPF), the source port (e.g. 161), and the destination port. Users can configure different rules for access control according to different needs.

In a switch, a set of rules may be apply by a plurality of applications; for example, a set of rules are referenced by port access filtering and service access filtering at the same time or simultaneously by port access filtering of both ports.

17.2 ACL filtering introduction

ACL filtering is carried out at the input port of the switch, and the regular matching of the data stream input to this port is carried out to filter the port. ACL filtering is processed by the line speed of the switch, which will not affect the forwarding efficiency of the data stream.

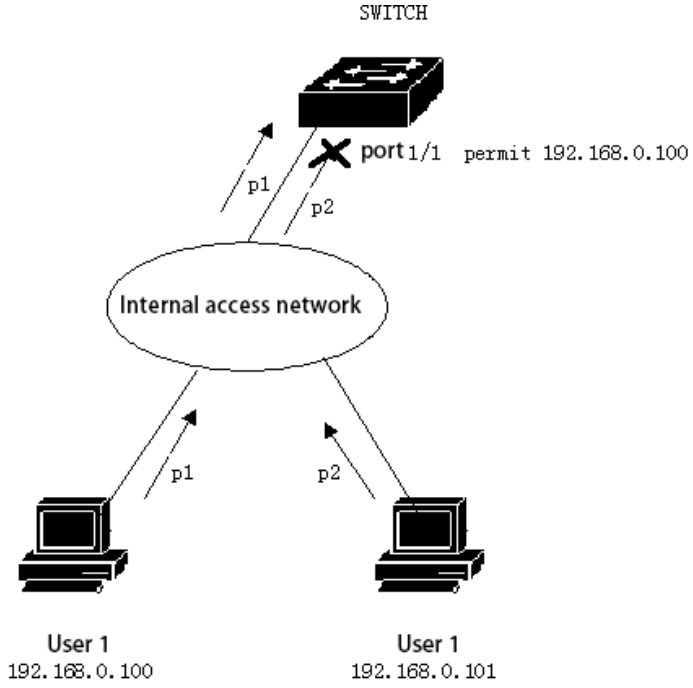
When ACL filtering is not configured on a port of the switch, all data streams entered through that port do not match rules and can be forwarded through that port. When a port of the switch is configured with ACL filtering, all input data streams through that port will match rules. If the matching rule is permit, the data stream is allowed to be forwarded, and if it is deny, the data stream is not allowed to be forwarded and discarded.

When configuring ACL filtering for a port, a port can select multiple ACL rule groups, which are imported into the port's CFP. If there are no rules in the group rules that reject or allow all IP protocol packets, a rule that denies all IP protocols is added when written to CFP. When the rules of the ACL repository change, the rules written to the CFP also change automatically.

For example, there is only one rule in a set of rules: access-list 1 permit 192.168.1.0 0.0.0.255. by default, a rule that denies all IP protocol packages is hidden, and there are actually two rules imported into the port's CFP. When the data stream is filtered, only the data stream with the source address from 192.168.1.0 to 192.168.1.255 can be forwarded through this port, and all other data streams are filtered out.

For example, there are two rules in a set of rules: access-list 1 deny 1. 0. 0. 0. 0. 0. 0. 0. 0. 255and access-list 1 permit any. There is a rule that allows all IP protocol packages, and there are no hidden rules, and there are actually two rules imported into the port's CFP. When the data stream is filtered, only the data stream with the source address from 192.168.1.0 to 192.168.1.255 is filtered out, and all other data streams can be forwarded.

The following figure is an example of ACL filtering. Switch port 1 ≤ 1 selects a ACL rule group 1, and there is only one rule in this group of rules, access-list 1 permit 192.168.0.100. Under port 1 / 1 of the switch, there are two users who want to access the network from that port. The IP address of user 1 is 192.168.0.100, and the IP address of user 2 is 192.168.0.101. Only user 1 can access the network through port 1 / 1 of the switch, and the data stream p2 sent by user 2 is discarded at port 1 / 1 of the switch.



When multiple ports do ACL filtering, you can choose the same ACL rule group and use the same filtering rules.

Whether a set of rules or multiple sets of rules are referenced by one port, they are automatically sorted, even if the sorting between the two sets of rules intersects.

When a user references a set of rules, if the set of rules changes, the port that references the rules automatically responds to the user's configuration; there is no need to reconfigure the reference to the port.

17.3 ACL Repository Configuration

The switch does not have any rules by default.

The resource base in the switch supports four kinds of ACL rules: standard IP rule, extended IP rule, IP MAC group, ARP group. Here are four types of rules to introduce the configuration of ACL.

Standard IP rules: standard IP rules control packet forwarding through source IP addresses.

Command form：access-list <groupId> {deny | permit} <source>

Parameter declaration:

Access control list group numbers, standard IP ACLs support from 1 to 99 groups or 1300 to 1999.

If the match is complete, the packet forwarding is deny/permit.

The source IP comes in three ways of input:

1) A.B. C.D wilcard can control the IP address from one network segment

2) Any is equivalent to A.B.C.D 255.255.255.255

3) Host A.B.C.D is equivalent to A.B.C.D 0.0.0.0

Wildcard: determines which bits needs to match, '0 'for matching and' 1 'for no match.

Extended IP rule: extended IP rule is an extension of standard IP rule, which can control packet forwarding through source IP, destination IP,IP protocol type and service port.

Form of command: access-list <groupId> {deny | permit} <protocol> <source> [eq <srcPort>] <destination> [destPort] <tcp-flag>

Parameter declaration:

Access control list group numbers, extended IP ACLs support from 100 to 199 groups or 2000 to 2699.

If the match is complete, the packet forwarding is deny/permit.

The protocol types above the ip layer, such as: tcp, udp, etc., can also be entered with the corresponding number 6(tcp). if you do not need to control these protocols, you can enter ip or 0.

Source IP has three input modes

1) A.B.C.D wildcard can control the IP address from a network segment;

2) Any is equivalent to A.B.C.D 255.255.255.255

3) Host A.B.C.D is equivalent to A.B.C.D 0.0.0.0

srcPort：For the case where the protocol is tcp or udp, the source port of the packet can be controlled. The input mode can be some familiar port service name, such as:ww or number, such as 80.

destination：Destination IP has three input methods:

1) A.B.C.D wildcard can control the IP address from a network segment;

2) Any is equivalent to A.B.C.D 255.255.255.255

3) Host A.B.C.D is equivalent to A.B.C.D 0.0.0.0

DestPort: The destination port of the packet can be controlled in the case of the protocol is tcp or udp, and the input method is the same as the srcPort.

Tcp-flag：For protocol is tcp. The tcp field matching of the data packet can be controlled, and the optional parameters are ack, sh, psh, rst, syn, urg.

The IP MAC rule: IP MAC group can control the MAC address of the source destination and the IP address of the source destination of the IP packet.

Form of command: access-list <groupid> {deny | permit} <src-mac> vid <vlan-id|any> ip <src-ip> <dst-ip>

Parameter declaration:

groupId：Access control list group numbers, extended IP ACLs support from 700 to 799 groups.

deny/permit：If the match is complete, the packet forwarding is deny/permit.

src-mac：Source MAC address.

MAC address has three input methods:

1) HHHH.HHHH.HHHH wildcard can control the MAC address from a segment;
2) Any equivalent to HHHH. HHHH. HHHH FFFF.FFFF.FFFF.
3) Host A.B.C.D is equivalent to HHHH.HHHH.HHHH 0000.0000.0000

Vid：The outer vid, can be a vlan-id, or any any vlan-id

src-ip： source IP address

dst-ip：Destination IP address

IP address has three input methods:

1) A.B.C.D wildcard can control the MAC address from a segment;
2) Any equivalent to A.B.C.D 255.255.255.255
3) Host A.B.C.D is equivalent to A.B.C.D 0.0.0.0

ARP rule: the ARP group can control the operation type of ARP package, sender MAC and sender IP.

Form of command: access-list <groupid> {deny | permit} arp <sender-mac> <sender-ip>

Parameter declaration:

groupId：Access control list group number, extended IP ACL support from 1100 to 1199.

deny/permit：If the match is complete, the packet forwarding is deny/permit.

sender-mac：The MAC address of the sender of the ARP packet

MAC address has three input methods:

1) HHHH.HHHH.HHHH wildcard can control the MAC address from a segment;
2) Any equivalent to HHHH. HHHH. HHHH FFFF.FFFF.FFFF.
3) Host A.B.C.D is equivalent to HHHH.HHHH.HHHH 0000.0000.0000

sender-ip：The IP address of the sender of the ARP package.

IP address has three input methods:

1) A.B.C.D wildcard can control the MAC address from a segment;
2) Any equivalent to A.B.C.D 255.255.255.255
3) Host A.B.C.D is equivalent to A.B.C.D 0.0.0.0

List of other commands:

show access-list [groupId]

Displays a list of rules configured in the current ACL. If groupId is entered, the rule list for the current group is displayed; otherwise, all rule lists are displayed.

no access-list <groupId>

Removes the specified list of rules. All rules for the Group Id group.

17.4 ACL based on time period

The time period is used to describe a special time range. Users may have the requirement that some ACL rules need to take effect at one or some specific time, while at other times they are not used for message filtering, commonly referred to as filtering by time. At this time, the user can first configure one or more time periods, and then reference the time period by the name of the time period under the corresponding rule, which only takes effect within the specified time period, thus realizing ACL filtering based on the time period.

If the time period referenced by the rule is not configured, the system gives a prompt and allows such a rule to be created successfully, but the rule cannot take effect immediately until the user has configured the referenced time period and the system time is within the specified time range. The ACL rule will not take effect.

There are two situations in which the time period is configured:

(1) Configuring a relative time period: takes the form of a time of a day to a time.

(2) Configure absolute time period:adopt x year x month x day x hour x point--x year x month x day x hour x point.

Configure time-based ACL:

Order	Description	CLI mode
time-range WORD cycle-time from <0-23> <0-59> to <0-23> <0-59>	To configure a relative time period that contains only time points.	Global configuration mode
time-range WORD cycle-time days from <0-6> to <0-6>	onfigure a period of time for a period of time only for the relative time period of the week	Global configuration mode
time-range WORD cycle-time from <0-23> <0-59> to <0-23> <0-59> days from <0-6> to <0-6>	To configure a time period for an absolute time period that contains the time of days	Global configuration mode
time-range WORD utter-time from <2000-2100> <1-12> <1-31> <0-23> <0-59> to <2000-2100> <1-12> <1-31> <0-23> <0-59>	To configure a time period for an absolute time period that contains the time of day	Global configuration mode
no time-range WORD cycle-time	Delete all relative time periods for a certain time period	Global configuration mode
no time-range WORD utter-time	Delete all absolute time periods in a certain time period	Global configuration mode
no time-range WORD	Delete a certain time period (including deleting all relative time periods and absolute time periods)	Global configuration mode
no time-range	Delete all time periods	Global configuration mode
show time-range WORD cycle-time	Displays all relative time periods for a certain time period.	Privileged mode
show time-range WORD utter-time	Displays all absolute time periods for a certain time period	Privileged mode
show time-range WORD	Display a certain time period (including all absolute time periods and absolute time periods)	Privileged mode
show time-range	Displays all time periods	Privileged mode
acl (<1-99>|<100-199>|<1300-1999>|<2000-2699>|<700-799>|<1100-1199>) time-range WORD	A certain acl rule applies to a certain period of time, which works when acl is applied to the interface.	Global configuration mode
no acl (<1-99>|<100-199>|<1300-1999>|<2000-2699>|<700-799>|<1100-1	Cancel the application of so-and-so acl rules for a certain time period or all time periods	Global configuration mode

199>) time-range (WORD|)		
show acl (<1-99>|<100-199>|<1300-1999>|<2000-2699>|<700-799>|<1100-1199>) time-range	Displays all time periods for a certain acl rule application	Privileged mode
show all acl time-range	Displays the time period for all the acl rule applications	Privileged mode

It is to be noted that:

(1) A number of relative time periods are assigned to a certain time period, and the relationship between the relative time periods is or. The system time is in an active state in any relative time period.

(2) Configuring a plurality of absolute time segments for a certain time period, the relationship between the absolute time segments is OR, and the system time is in any absolute time period, and the time period is in an active state;

(3) If the relative time period and the absolute time period are configured for a certain time period at the same time, the relative time period and the absolute time period are related to each other, and the system time is activated only in the relative time period and the absolute time period at the same time.

(4) Up to 256 time periods can be defined, up to 256 relative time periods and absolute time periods can be configured in a time period, and a acl rule can be applied to up to 256 time periods. When the acl rule associated with the time period is applied to the interface, the time period begins to play a role.

17.5 ACL filter configuration

The switch does not do ACL filtering on all ports by default.

List of commands:

access-group <groupId>

Mode: Layer 2 interface configuration mode

Parameters:

groupId：And port bound ACL group number.

Function: Configure the ACL port filtering.

Note: if the above command configuration fails or is invalid, there may be the following reasons:

There are too many rules in the ACL group or hardware resources are exhausted or consumed by other applications.

Display the ACL port filter configuration

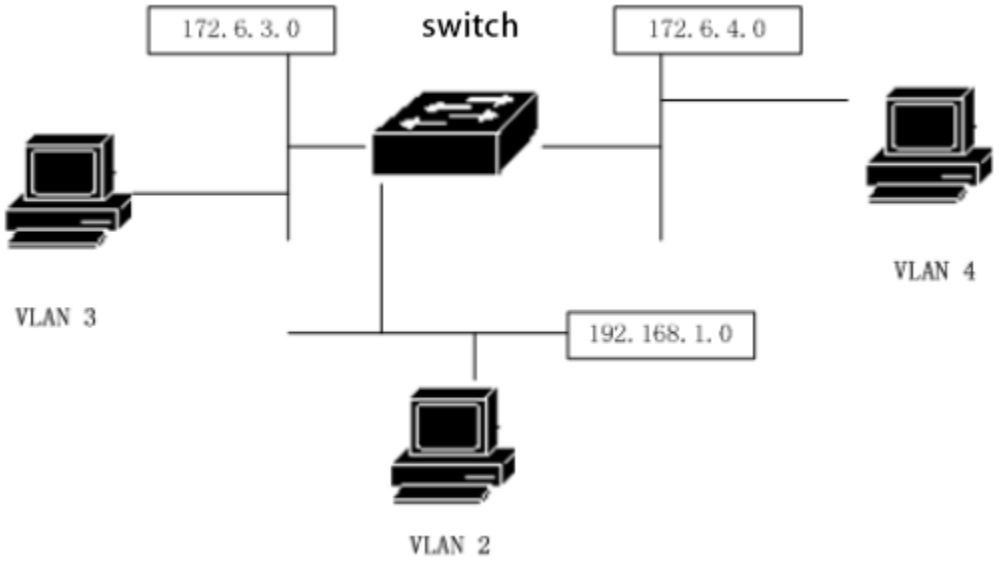
show acccess-group

Delete the current port and ACL port filtering related configuration

no acl- group <groupId>

17.6 ACL configuration example

A switch connects three subnets, designs an ACL, and blocks the source address as 192.168.1.0 network address. Allow traffic from other network addresses to pass. The 192.168.1.0 network segment is connected to the 1/1 port of the switch.



The configuration on the switch is as follows

Switch#config t

Switch(config)#vlan database

Switch(config-vlan)#vlan 2

Switch(config-vlan)#vlan 3

Switch(config)#interface ge1/1

Switch(config-ge1/1)# switchport mode access

Switch(config-ge1/1)#switchport access vlan 2

Switch(config)#interface vlan2

Switch(config-vlan2)#ip add 192.168.1.1/24

Switch(config)#interface ge1/2

Switch(config-ge1/2)#switchport mode access

Switch(config-ge1/2)#switchport access vlan 3

Switch(config)#interface vlan3

Switch(config-vlan2)#ip add 172.16.3.1/24

Switch(config)#access-list 10 deny 192.168.1.0 0.0.0.255

Switch(config)#access-list 10 permit any

Switch(config)#interface ge1/1

Switch(config-ge1/1)#access-group 10

Switch(config)#interface ge1/2

Switch(config-ge1/2)#access-group 10

Note: The time period and time period association ACL rule can be configured according to the specific requirements. The reference configuration is as follows:

Switch(config)#time-range test cycle-time from 8 30 to 17 30 days from 1 to 5

Switch(config)#acl 1 time-range test

Switch(config)#interface ge1/20

Switch(config-ge1/2)#access-group 1

17.7 ACL configuration exclusion

If the ACL configuration fails, there may be the following reasons:

1、Make sure that all IP are common before configuring the access control list, and then add the access control list. This access control list blocks the IP data flow through the switch with the source address of 1. 0. 0. 0. Pay attention to the way the subnet inverse code is written. Use the show access-list command to list the access control list for viewing, be sure to note that the source address and destination address are not written backwards. Then check the access control list. And the default access control list ends with an implicit deny any statement, and if you want everything else to pass, you need to Add a permit any statement, otherwise it won't pass.

2、The system is configured with static IP MAC binding.

3、The DHCP SNOOPING protocol is enabled for the current interface.

4、The system CFP resources are exhausted.

Chapter 18 TCP/ IP Basic Configuration

For a layer 2 switch with network management function, it is necessary to provide basic network configuration for TCP/IP protocol and realize the communication function with other devices.

This chapter mainly includes the following:

- Configure VLAN interface
- Configure ARP
- Configure a static route
- Example of IP Routing Configuration

18.1 Configure VLAN interface

In the switch, each layer 3 interface is attached to a VLAN, so the layer 3 interface is also called VLAN interface. The creation and deletion of VLAN interface is done manually. The switch can be divided into up to 4094 VLAN, but only 32 subnetworks can be established. The creation of a subnet interface can be created according to the needs of the user; the subnet interface can be manually deleted by the user, or it can be deleted with the VLAN where the subnet is located.

Each VLAN interface has a name. The name of the VLAN interface is the string "vlan" followed by the VLAN ID number, such as the name of the three-tier interface of VLAN 1 is "vlan1" and the name of the three-tier interface of VLAN 4094 is "vlan4094".

Like ports, VLAN interfaces have management and link states. At present, the switch does not provide the configuration of the management state of the VLAN interface. As long as the VLAN interface is created, the management state of the VLAN interface is always related to the port contained in the VLAN corresponding to the interface. As long as the link state of one port in the VLAN is RUNNING, the link state of the VLAN interface is RUNNING,. If all ports in the VLAN are not RUNNING, the link state of the VLAN interface is not RUNNING.

On the VLAN interface, you can configure the IP address and indicate the network prefix of the network segment that is connected to this interface (which can be converted to a network mask). The switch currently supports only one IP address on one VLAN interface. Before you configure an IP address, the user needs to create a VLAN and add the associated port to the VLAN. By default, the switch has an interface to VLAN1, and the IP address of 192.168. 0.1/24 is set on this interface, and the user can also modify the IP address of the VLAN1 interface. the interface for other VLANs other than VLAN1 is not set by default P address.

The commands to configure the IP address of the VLAN interface are as follows:

Order	Description	CLI模式 CLI mode
Ip interface vlan <2-4094>	Create a VLAN interface	Global configuration mode
No Ip interface vlan <2-4094>	Delete a VLAN interface	Global configuration mode
ip address <ip-prefix>	A.B.C.D/M。Set the IP address on the VLAN interface. Parameters include the IP address of the interface and the network prefix of the connected network segment. If the VLAN interface originally has an IP address, delete the original IP address before setting the specified IP address. The format of the parameter is A.B.C.D.	Interface configuration mode
no ip address [ip-prefix]	Delete the IP address of the VLAN interface. If a parameter is specified, the parameter must be the same as the parameter given at the time of setting, otherwise this command is invalid. The format of the parameter is A.B.C.D.	Interface configuration mode

View the commands for the VLAN interface as follows:

Order	Description	CLI mode
show interface [if-name]	View the information of VLAN interface, including IP address, MAC address, management status and link status of the interface. The parameter is the interface name of the VLAN interface. If no parameter is specified, view the information of all ports and VLAN interfaces.	Normal mode，privileged mode
show running-config	To view the current configuration of the system, you can view the configuration of the VLAN interface.	Privileged mode

Example:

The subnet 193.1.1.0 is configured on the VLAN3 interface, the subnet prefix is 24 (that is, mask 255.255.255.0), the IP address of the interface is 193.1.1.1, and the information of the VLAN3 interface is viewed. The order is as follows:

switch(config)#interface vlan3

switch(config-vlan3)#ip address 193.1.1.1/24

switch(config-vlan3)#end

switch#show interface vlan3

18.2 Configure ARP

ARP (Address Resolution Protocol) protocol is a protocol that provides mapping from IP address to corresponding MAC address. When the source sends the Ethernet data frame to the destination located in the same VLAN, the destination is determined according to the 48-bit Ethernet MAC address, and the destination determines whether the packet needs to be received according to the destination MAC address of the packet.

Assuming that the hosts A and B of the two adjacent network segments communicate through the switch, host A sends a ARP request message to the interface of the switch directly connected to host A before sending data to host B. after receiving the ARP reply, the host A sends the packet to the interface. After receiving this packet, the switch first broadcasts a ARP request message to host B, gets the ARP response message from host B, and then sends the packet to host B.

There is an ARP cache on the switch, called ARP table, which stores the mapping record from IP address to MAC address in the directly connected network. Each item in the MAC table has a survival time, the default is 20 minutes. When the switch does not receive the ARP request or reply message of the IP address during the survival period, the ARP table item corresponding to the IP address will be deleted.

This section includes the following:

- Configure static ARP
- Configure ARP Bindings
- Configure ARP aging time
- View information about ARP

18.2.1 Configure static ARP

There are two different ARP table items in the ARP table, one is static ARP, the other is dynamic ARP.. Static ARP is a ARP table item configured by the user through the command. The system does not automatically refresh and delete, and requires the user to complete it by hand. Dynamic ARP is a kind of ARP, system which is automatically created and deleted, updated and maintained in real time according to the received ARP request or response packet, but the user can delete the dynamic ARP table item manually.

The switch defaults to no static ARP entries. Note that static and dynamic ARP entries in the original subnet segment are deleted when a VLAN interface is deleted or the subnet segment IP of the interface changes.

The commands for configuring static ARP are as follows:

Order	Description	CLI mode
arp <ip-address> <mac-address> [if-name]	Configure static ARP entries. The first parameter is the IP address and the IP address must be in a subnet segment. The second parameter is the MAC address, the MAC address must be a unicast MAC address, and the MAC address is in the format of HHHH. HHHH. HHHH, such as 0010.5 cb1.7825. The third parameter is the two-layer interface name, optional, and the static arp table entry is associated with a specific two-layer interface.	Global configuration mode
no arp {<ip-address> | <ip-prefix> | all | dynamic | static }	Delete the ARP table item. It includes deleting an IP ARP table item; deleting a network segment ARP table item; deleting all ARP table items; deleting all dynamic ARP table items; deleting all static ARP table items.	Global configuration mode
arp static {<ip-prefix> | all}	Modify any or all dynamic ARP table items within a network segment to static ARP table items.	Global configuration mode
arp aging <time>	Configure arp aging time to take effect only for dynamic learning arp.	Global configuration mode

18.2.2 View information about ARP

The commands to view information about ARP are as follows:

Order	Description	CLI mode
show arp [<ip-prefix> | dynamic | static]	View the ARP table item information in the ARP table, including all ARP table items, ARP table items for a network segment, dynamic ARP table items, and static ARP table items.	General mode, privileged mode
show running-config	View the current configuration of the system, you can see the configuration of ARP.	Privileged mode

18.3 Configure a static route

A static route is defined by the user, and a route that can cause the packet to reach the destination address from the source address through the specified path. You can send packets that are unable to determine the route to the default gateway by configuring a static route as the default route.

Static routing is manually configured by administrators. It is suitable for networks with simple network structure. Administrators only need to configure static routing to make the switch work properly. Static routing does not occupy valuable network bandwidth because there will be no routing updates.

The default route is also a static route. Simply put, the default route is the route that is used if no matching route entry is found. That is, the default route is used only when there is no suitable route. In the routing table, the default route appears as a route to the network 0.0.0.0/0 (mask 0.0.0.0). If the destination of the packet is not in the routing table and there is no default route in the routing table, the packet will be discarded and an ICMP packet will be returned to indicate the destination address or network unreachable information. The default route is very useful in the network. In a typical network with hundreds of switches, running a dynamic routing protocol may consume a large amount of bandwidth resources, and using default routes can save the time occupied by routing and the bandwidth resources occupied by packet forwarding. To a certain extent, it can meet the needs of a large number of users to communicate at the same time.

Switches can configure multiple static routes to the same destination, but only one of them is activated for actual data forwarding. The switch is not configured with static routing by default.

The commands of configuring static routing are as follows:

Order	Description	CLI mode
ip route <ip-prefix> <nexthop-address>	Set up static routing. The first parameter specifies the network segment IP and network prefix length, and the second parameter specifies the next hop IP address.	Global configuration mode
ip route <ip-address> <mask-address> <nexthop-address>	The function is the same as the previous command. The first parameter specifies the IP address of the network segment, the second parameter specifies the mask of the network segment, and the third parameter specifies the next hop IP address.	Global configuration mode

no ip route <ip-prefix> [nexthop-address]	Delete a static route. The first parameter specifies the network segment IP and network prefix length, and the second parameter specifies the next hop IP address. If there is no second parameter, all routes that match the specified network segment are deleted. If there is a second parameter, the route that matches both the specified segment and the next hop is deleted.	Global configuration mode
no ip route <ip-address> <mask-address> [nexthop-address]	The function is the same as the previous command. The first parameter specifies the IP address of the network segment, the second parameter specifies the mask of the network segment, and the third parameter specifies the next hop IP address. If there is no third parameter, all routes that match the specified network segment are deleted. If there is a third parameter, the route that matches both the specified segment and the next hop is deleted.	Global configuration mode

The commands to view the route are as follows:

Order	Description	CLI mode
show ip route [<ip-address> | <ip-prefix>	View the information for the active route, and you can choose to view all routes, a route, a route to a network segment, and a static route.	General mode, privileged mode
show ip route database	View information about all routes (both active and unactivated), and you can choose to view all routes.	General mode, privileged mode
show running-config	To view the current configuration of the system, you can view the configuration of a static route.	Privileged mode

Example:

Set the destination network to 200.1.1.0, the subnet mask to 255.255.255.0, and the next hop to 10.1.1.2. The configuration commands are:

Switch(config)#ip route 200.1.1.0 255.255.255.0 10.1.1.2

Or Switch(config)#ip route 200.1.1.0/24 10.1.1.2

Delete static route with destination IP address 200.1.1.0, subnet mask 255.255.255.0, next hop 10.1.1.2. The configuration commands are:

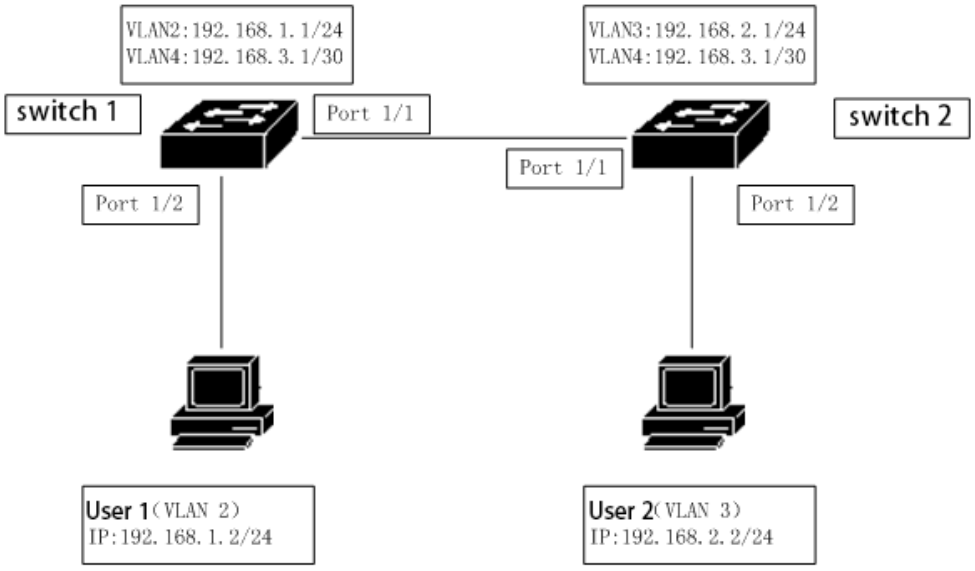
Switch(config)#no ip route 200.1.1.0/24

Or Switch(config)#no ip route 2001.1.0/24 10.1.1.2

Or Switch(config)#no ip route 200.1.1.0 255.255.255.0

Or Switch(config)#no ip route 200.1.1.0 255.255.255.0 10.1.1.2

18.4 Example of TCP/IP basic configuration



In the figure, switch 1 is a layer 2 switch and switch 2 is a layer 3 switch.

18.4.1 Layer 3 interface

Configure a three-layer interface corresponding to VLAN2 on switch 1 while assigning an IP address 192.168.1.1/24.

The configuration is as follows:

Switch#config t

Switch(config)#vlan database

Switch(config-vlan)#vlan 2

Switch(config-vlan)#exit

Switch(config)#interface ge1/2

Switch(config-ge1/2)#switch access vlan 2

Switch(config)#ip interface vlan 2

Switch(config)#interface vlan2

Switch(config-vlan2)#ip add 192.168.1.1/24

Authentication: The user 1 can ping the IP address of the three-layer interface corresponding to the VLAN2 of the switch 1.

18.4.2 Static routing

User 2 wants to access switch 1, and must pass the routing function of switch 2 to access switch 1.

The switch 1 is configured as follows:

Switch#config t
Switch(config)#ip route 192.168.2.0 255.255.255.0 192.168.3.2

The switch 2 is configured as follows:
Switch#config t
Switch(config)#ip route 192.168.1.0/24 192.168.3.1

Verification: User 2 can ping Universal Switch 1.

18.4.3 ARP

Configure the static ARP, of user 1 to allow only user 1 to access from VLAN2. Suppose the MAC address of user 1 is 00 / 00 / 00 / 00 / 01.

The switch 1 is configured as follows:
Switch#config t
Switch(config)#arp 192.168.1.2 0000.0000.0001

Authentication: The user 1 can ping the IP address of the three-layer interface corresponding to the VLAN2 of the switch 1.

Chapter 19 SNMP configuration

Switches provide SNMP for remote management of switches. This chapter describes how to configure SNMP, including:

- Introduce SNMP
- Configure SNMP
- SNMP configuration example

19.1 Introduce SNMP

SNMP is a simple network management protocol. It is the most widely used network management protocol. It has five functions: fault management, charging management, configuration management, performance management and security management. It provides the information format of communication between the network management application software and the network management agent (agent).

The SNMP network management protocol has four elements: management workstation, management agent, management information base, network management protocol. The management agent is on the switch, is the service end of the management workstation to access the switch, and the information of the management workstation to access the network management agent is organized in the form of the MIB to form the management information base.

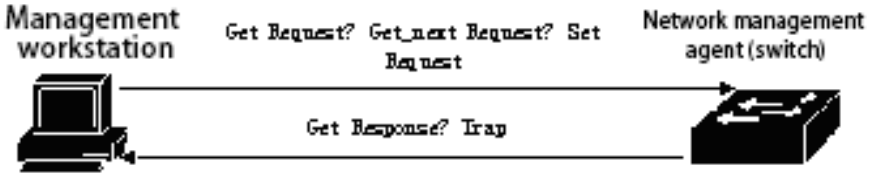
SNMP has three operations: GET operation, SET operation, and TRAP operation. The GET operation enables the management station to obtain the value of the object in the agent. The SET operation enables the management station to set the value of the object in the agent. The TRAP operation enables the agent to notify the management workstation of the event.

The TRAP message is actively distributed to the management workstation when an event occurs, including cold start, hot start, link up of the port, link down, common body name authentication failure, STP state switching, and the like.

At present, there are three versions of SNMP: SNMPV1, SNMPV2, SNMPV3, the later version is the previous upgrade, the function is enhanced, and the security is improved. The switch supports all three SNMP versions and can be parsed for three versions of the SNMP protocol package. When a TRAP message is sent, it can be sent using any of the SNMPV1, SNMPV2, and SNMPV3.

The switch supports RFC, BRIDGE and private MIB objects, and the switch can be fully managed via SNMP. Listed below are some of the MIBs supported by the switch: RFC 1213, RFC 1493, RFC 1724, RFC 1850, RFC 1907, RFC 2233, RFC 2571, RFC 2572, RFC 2573, RFC 2574, RFC 2575, RFC 2674, etc.

The figure is an example of SNMP protocol interaction between a management workstation and a management agent. The management workstation can access the switch management agent by sending the SNMP message of Get Request,GetNext Request,GetBulk Request and Set Request, obtain or set the value of the MIB object of the switch, and the switch management agent sends back the SNMP message of Get Response to the management workstation. When some events occur on the switch, the management agent of the switch actively sends SNMP TRAP cancellation Interest to the management station.



Managing the SNMP protocol interaction between the workstation and the management agent

19.2 Configure SNMP

SNMP configuration includes switch community configuration, TRAP workstation, snmp system information configuration and snmpV3 engine id,user and group configuration. The switch has a read-only common body by default, and the common body name public, switch can be configured with up to eight common bodies. The switch is not configured with TRAP workstations by default. The switch has a local engine id, switch that can modify the local engine id. by default The switch has a user nam by default E initialnone, which belongs to an unauthenticated unencrypted user name, and the switch can configure multiple different levels of user names. Switch default has a group name:initial, switch that can configure different group name according to different user names.

The commands for SNMP are as follows:

Order	Description	CLI mode
snmp community <community-name> {ro | rw}	Configure the common body name of the access network management, which is an interactive command. When configured, users can enter the required created common body name and read / write permissions at the prompt.	Global configuration mode
no snmp community <community-name>	Delete the specified SNMP common body name.	Global configuration mode
snmp trap <notify-name> host <ipaddress> version {1 | 2c | 3}	Add or modify the send target for snmp trap. This is an interactive command. Notify name is unique, and if you modify the existing name, you can modify the trap to send the target item. Host is the destination address to send trap; version is sent as snmpV1,snmpV2c or snmpV3. This command is configured by default with a target port of 162.	Global configuration mode
no snmp trap <notify-name>	Delete the specified SNMP trap.	Global configuration mode
snmp system information <contact | location | name> <information-string>	Configure system information, including contact, location and name.	Global configuration mode
no snmp system information <contact | location | name >	Delete a system configuration information.	Global configuration mode
snmp engine-id local <engine-id-octet-string>	Configure the engine ID used by SNMP version 3. The ID is a 24-bit hexadecimal number; and when the input is less than 24 bits, it is automatically filled with 0.	Global configuration mode
snmp user <user-name> <group-name> v3 [auth {md5 | sha} <auth-key>]	The snmp user command is a user name that sets the local engine ID of snmpv3. And the group name corresponding to the user name, if the user name supports authentication, you need to set the authentication protocol (md5 or sha) and the corresponding authentication password.	Global configuration mode

no snmp user <user-name> <group-name> v3	Delete a user name corresponding to the local engine ID of the snmpv3.	Global configuration mode
snmp group <group-name> v3 {auth | noauth} [notify <notify view name> | write <write view name> | read <read view name>]	The snmp group command is a view that sets a group name, the security level is (auth or noauth), the notification, the writable or readable, specified by the security model (v3).	Global configuration mode
no snmp group <group-name> v3 {auth | noauth}	Delete a group name, and the security level is the view specified by the auth or noauth), security model (v3).	Global configuration mode
show snmp community	Displays all the current utility names and the corresponding read and write access information.	Normal mode/ privileged mode
show snmp trap	Displays all the current trap names and the target IP address and version information for the corresponding trap.	Normal mode/ privileged mode
show snmp system information	Displays system information for SNMP settings.	Normal mode/ privileged mode
show snmp engine-id	Display the local engine-id. of SNMPV3	Normal mode/ privileged mode
show snmp user [specify name of user]	Displays a user name information corresponding to the local engine ID of the snmpv3. Includes the group name corresponding to the user name and the authentication and encryption information supported by the user name.	Normal mode/ privileged mode
show snmp group	Displays all group names, security levels (auth or noauth), notifications specified by security model (v3), writable or readable view information.	Normal mode/ privileged mode

19.3 SNMP Configuration Example

Configure a common body name operation permission called private to read and write.

Configure an SNMP trap named test and send the destination IP to 192.168. 0.10; the SNMP version used is 1.

The specific content of the contact of the configuration system is: E-mail: networks@abc.com.

The specific contents of the location of the configuration system are as follows: Shenzhen,China.

The name of the configuration system is: abcSwitch.

Set the user name in initialm5 that supports the m5 authentication, the group is intia, and the authentication password is abcefg.

Setting the group name initial, security level is the notification specified by the (auth), security model (v3),

and the writable or readable view names are internet,internet,internet.

The switch's configured as follows:

Switch#config t

Switch(config)#snmp community private rw

Switch(config)#snmp system information contact E-mail:networks@abc.com

Switch(config)#snmp system information location Shenzhen,China

Switch(config)#snmp system information name abcSwitch

Switch(config)# snmp user initialmd5 initial v3 auth md5 abcdefg

Switch(config)# snmp group initial v3 authpriv read internet write internet notify internet

Chapter 20 Configure RMON

This chapter mainly includes the following:

- Introduce RMON
- Configure RMON
- RMON configuration example

20.1 Introduce RMON

RMON (Remote Monitoring, remote network monitoring) is a standard monitoring specification, which is mainly used to monitor the data flow in a network segment and even in the whole network. RMON specification is one of the most widely used network management standards at present. RMON specification is extended by SNMP MIB, so it is also the most important enhancement to MIB II standard. RMON makes SNMP more effective and more active in monitoring remote devices.

RMON monitoring system consists of two parts: detector (agent or monitor) and management station. RMON agent stores network information in RMON MIB, which is directly embedded into network devices (such as routers, switches, etc.). The management station uses SNMP to obtain RMON data information.

This device supports the four most commonly used groups in RMON:

(1) Statistical group (statistics): provides statistics for each interface, most of which are counters, which record the information collected by the monitor from the interface.

(2) History group: Save the data that is sampled at a fixed time interval for the specified interface.

(3) Alarm group (alarm): samples the specified data of all interfaces at a fixed time interval and compares it with the set threshold value, which triggers the corresponding event when the condition is met.

(4) Event group (event): Set the event, and you can select the record log or send Trp.

20.2 RMON configuration

The RMON command includes the configuration of four groups, view the configuration, and view the data:

Order	Description	CLI mode
rmon statistics <1-100> (owner WORD|)	Enables statistical group configuration for the specified serial number for this port, which is an interactive command. The configuration is that the user can enter the serial number and owner at the prompt, where the owner is optional (the same below). The serial number is the number of the statistical group configuration, and the value range is 1 to 100.	Port configuration mode
no rmon statistics <1-100>	Unconfigure the statistical group for the specified serial number.	Port configuration mode
rmon history <1-100> buckets <1-100> interval <1-3600> (owner WORD|)	Specifies the history group parameter for the serial number for this port configuration, which is an interactive command. The configuration user can enter the serial number, the number of request buckets, the time interval and the owner according to the prompt. The serial number is the number of the history group configuration, the value range is 1 to 100; the number of request buckets is the maximum number of saved data, the value range is 1 to 100; the sampling time interval is in seconds, the value range is 1 to 3600.	Port configuration mode
no rmon history <1-100>	Cancel the history group configuration for the specified sequence number.	Port configuration mode
rmon alarm <1-60>	Configure the alarm group parameter for the specified serial	

WORD <1-3600> (absolute|delta) rising-threshold <1-2147483647> <1-60> falling-threshold <1-2147483647> <1-60> (owner WORD|)	number, which is an interactive command. Configuration users can enter serial numbers, monitoring objects, time intervals, comparison methods, upper limit threshold, upper event sequence number, lower limit threshold value, lower limit time sequence number and owner according to the prompt. The serial number is the number of the alarm group configuration, and the value range is 1 to 60; the OID, sampling time interval of the monitoring object is a MIB node in seconds, and the value range is 1 to 3600; absolute or delta, can be selected to represent the absolute value (the value of each sample) and the relative value (each sampling is relative to the last sample). The upper and lower threshold values range from 1 to 2147483647; events must be configured in advance, and the range of number values is 1 to 60.	Global configuration mode
no rmon alarm <1-60>	Unconfigure the alarm group for the specified serial number.	Global configuration mode
rmon event <1-60> (log|log-trap WORD|none|trap WORD) (description WORD|) (owner WORD|)	Configure the event group parameter for the specified ordinal number, which is an interactive command. Configuration users can enter serial numbers, event types, shared body names, descriptions, and owners according to prompts. The serial number is the number of the event group configuration, with values ranging from 1 to 60; the event type can select log (logging), log-trap (logging and issuing Trap), none (without any action) and trap (when Trap), is selected log-trap or trap, the common body name must also be specified (the shared body name configuration is ignored on this device).	Global configuration mode
no rmon event <1-60>	Unconfigure the event group for the specified serial number.	Global configuration mode
show rmon (statistics|history-control|alarm|event) config	View RMON configuration information, which is an interactive command. The configuration user can enter the view object at the prompt.	Global configuration mode
show rmon statistics-data interface IFNAME|	Viewing RMON statistics group data, the configuration user must enter the interface name.	Global configuration mode
show rmon history-data interface IFNAME|	Viewing RMON history group data, the configuration user must enter the interface name.	Global configuration mode

20.3 RMON configuration example

Enable statistics group configuration for port ge1/1 with serial number of 10 and owner tereco.

Enable history group data collection for port ge1/8, serial number 2, save up to 80 pieces of data, sampling interval is 1 minute, no owner.

Configure an event with a sequence number of 1, log the log, and no owner.

An event with a sequence number of 3 is configured, and Trp is sent, with the common body named public

and no owner.

The alarm group with serial number 5 is enabled to monitor the number of bytes received per port. When the number of bytes per half minute is greater than 1000, the Trap alarm is issued and the log is logged less than 10:00. There is no owner.

The switch is configured as follows:

```
Switch#configure terminal
Switch(config)#interface ge1/1
Switch(config-ge1/1)#rmon statistics 10 owner tereco
Switch(config-ge1/1)#exit
Switch(config)#interface ge1/8
Switch(config-ge1/8)#rmon history 2 buckets 80 interval 60
Switch(config-ge1/8)#exit
Switch(config)#rmon event 1 log
Switch(config)#rmon event 3 trap public
Switch(config)#rmon alarm 5 1.3.6.1.2.1.2.2.1.10 30 delta rising-threshold 1000 3 falling-threshold 10 1
```

Chapter 21 Cluster configuration

The switch provides cluster management function, which can realize a set of network devices managed by a single device. This chapter describes how to configure cluster management, including the following:

- Introduction to Cluster Management
- Configuration management equipment
- Configure member equipment
- Cluster management display and maintenance
- Examples of typical configuration of Cluster Management

21.1 Introduction to Cluster Management

21.1.1 Cluster definition

A cluster is a collection of network devices that can be managed as a single device.

Cluster management purpose: to solve the problem of centralized management of a large number of decentralized network equipment.

Cluster advantages: save public network IP address; simplify configuration management tasks. The network manager only needs to configure the public network IP address on one switch in the cluster to manage and maintain the other switches in the cluster.

The switch that configures the public network IP address and performs the management function is the command switch, the other managed switches are member switches, and the command switch and the member switch form a``cluster'' .

The cluster configurations and manages the switches within the cluster through the following three protocols.

- NDP（Neighbor Discovery Protocol）
- NTDP（Neighbor Topology Discovery Protoco）
- Cluster （Cluster Management Protocol）

The working process of the cluster includes the topology collection and the establishment and maintenance of the cluster, the topology collection process and the cluster maintenance process are relatively independent, the topology collection process starts to start before the cluster is established, and the working principle is as follows:

- All devices get the information of neighbor devices through NDP, including software version, host name, MAC address and port name of neighbor devices.
- The management device collects the device information within the specified hop range and the connection information of each device through NTDP, and determines the candidate devices of the cluster from the collected topology information.
- The management device completes the operation of adding the candidate device to the cluster and the member device leaving the cluster according to the candidate device information collected by NTDP.

The messages of the cluster are layer 2 Ethernet messages, the specific format and interaction flow see the national standard < YDT 1692 --2007 Ethernet switch cluster management technical requirements >.

21.1.2 Cluster role

According to the different position and function of each device in the cluster, different roles are formed, and the user can specify the role through the configuration, and all the roles are as follows:

1）Command the switch:

In a cluster, the only switch that can configure and manage the entire cluster is also the only switch with a public network IP address in the cluster.

- Command the switch to create a cluster;
- Command the switch to discover and determine the candidate switch by collecting the information of NDP (Neighbor Discovery Protocol, neighbor discovery protocol and NTDP (Neighbor Topology Discovery Protocol, neighbor topology discovery protocol).
- Command the switch to control the maintenance of the cluster, the candidate switch can be added to the cluster or the member switch can be removed from the cluster.
- After the cluster is established, the switch is ordered to provide a management channel for the cluster.

2）Member switch

Managed switches in a cluster.

Member switches are candidate switches before joining the cluster.

Member switches do not have public network IP;

The management of the member switch is done by commanding the switch agent.

3）Candidate switch

Has the ability to join the cluster, but has not yet joined any cluster of switches.

The switch must first be a candidate switch before it becomes a member switch.

4） Independent switch

Switch without clustering.

Various roles can be converted according to certain rules:

- While the user creates a cluster on the candidate device, the current candidate device is designated as the cluster management device. Each cluster must specify one (and only one) administrative device. After the management device is designated, the management device discovers and determines the candidate device by collecting relevant information. Users can add candidate devices to the cluster through the corresponding configuration.
- And after the candidate equipment is added into the cluster, the candidate equipment is formed into a member device.
- After the member devices in the cluster are deleted, they will be restored to candidate devices.
- The management device can only be restored to the candidate device when the cluster is deleted.

21.1.3 Introduction to NDP

- The NDP is used to obtain information about the directly connected neighbor device, including the connection port, device name, and software version. The working principle is as follows:
- The device running NDP periodically sends the NDP message to the neighbor. The NDP message contains NDP information (including the device name of the current device, software version, connection port and so on) and the aging time of the NDP information on the receiving device. At the same time, it will also receive but not forward the NDP message sent by the neighbor device.
- Devices running NDP store and maintain NDP neighbor information tables, creating a table item for each neighbor device in the NDP neighbor information table. If a new neighbor is found and the NDP message it sends is received for the first time, a table item will be added to the NDP neighbor information table; if the NDP

information received from the neighbor device is different from the old information, the corresponding data item in the NDP table will be updated, if the same, only the aging time will be updated, and if the NDP message sent by the neighbor has not been received beyond the aging time, the corresponding neighbor table item will be automatically deleted.

21.1.4 Brief introduction to NTDP

NTDP is used to collect the information of each device and the connection information between devices in a certain network range. NTDP provides the device information that can be added to the cluster for the management equipment, and collects the topology information of the device within the specified hop number.

NDP provides NTDP with neighbor table information. NTDP sends and transmits NTDP topology collection requests according to adjacent information, and collects NDP information of each device and its connection information with all neighbors in a certain network range. After collecting this information, the management equipment or network management can use this information as needed to complete the required functions. When the NDP on the member device finds that the neighbor has changed, the management device can start the NTDP to collect the specified topology by handshake message to notify the management device of the changed message, so that the NTDP can reflect the change of the network topology in time.

Management devices can regularly collect topology within the network, or users can start a topology collection through manual configuration commands. The process of managing the device to collect topology information is as follows:

- The management device transmits the NTDP topology collection request message from the port timing enabling the NTDP function.
- The device that receives the request message immediately sends the topology response message to the management device, and copies the request message at the port where the NTDP function is enabled and sends it to the adjacent device; the topology response message contains the basic information of the device and the NDP information of all adjacent devices.
- The adjacent device receives the request message and does the same until the topology collection request message spreads to all devices in the specified hop range.

When the topology collection request message spreads in the network, a large number of network devices receive the topology collection request and send the topology response message at the same time. In order to avoid network congestion and the busy task of the management equipment, the following measures can be taken to control the diffusion speed of the topology collection request message:

- After receiving the topology collection request, the device does not immediately forward the topology collection request message, but the delay waits for a certain time to start forwarding the topology collection request message in a port enabling the NTDP function.
- On the same device, except for the first port, each port that enables NTDP function will delay the forwarding of topology collection request message for a certain period of time after the previous port sends the topology collection request message.

21.1.5 Cluster management and maintenance

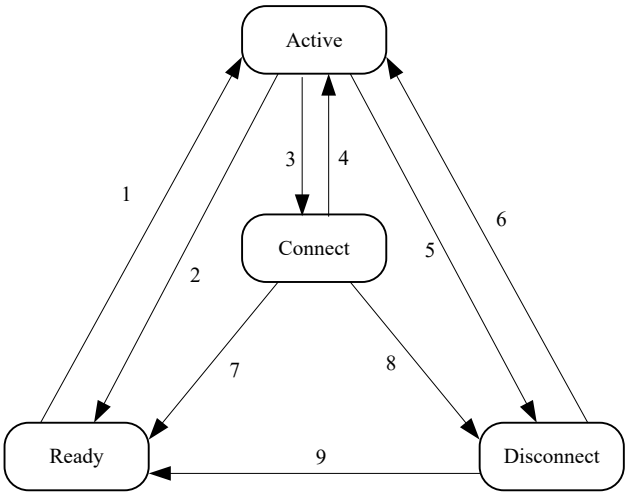
1） Candidate devices join the cluster

Before the user establishes the cluster, the user first specifies the management device, and the management device discovers and determines the candidate device through the NDP and the NTDP protocol, automatically adds the candidate equipment to the cluster, and can add the candidate equipment to the cluster by manual configuration.

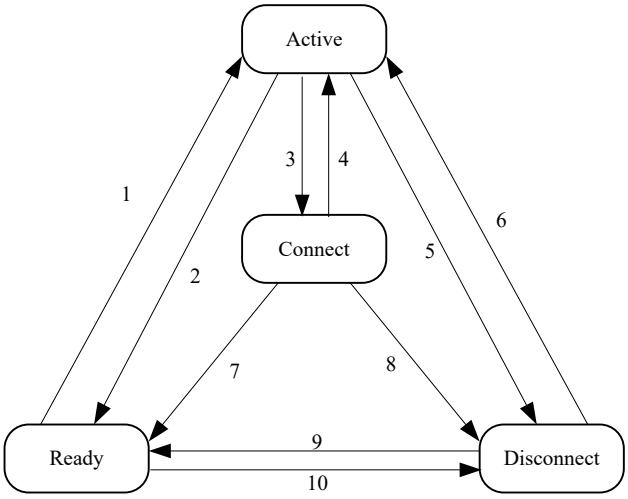
After the candidate device successfully joins the cluster, the cluster member serial number, the cluster management, the private IP address used, and the like assigned by the management device are obtained.

2） Cluster internal communication

In the cluster, the management device and the member device communicate in real time through the handshake message to maintain the connection status between them, and the connection status of the management device and the member device is shown in the following figure.



1 Membership
2 Member delete
3 The handshake signal is not received three times
4 Handshake signal received
5 Receive recovery request
6 Interrupt recovery and re-register through
7 Member deletion
8 Stay in state for more than the specified time
9 Member deletion



Member switch state transition diagram

1 Join the cluster
2 Exit from cluster
3 Handshake signal is not received three times
4 Handshake signal received
5 Request for accession received
6 Interrupt recovery, re-register through
7 Exit from cluster
8 The status is maintained for more than a specified time or a join request message is received.
9 Exit from cluster
10 Configuration recovery

Command the switch to collect the basic information of the device and identify a device as a candidate switch, initially in the Ready state.

If a member operation is deleted in any state, the state of the member switch is migrated back to the Ready state and identified as a candidate switch.

- The cluster was successfully established. After the candidate device joined the cluster to become a member device, the management device saved the status information of the member device to the local, identified the member state as the Active, member device, and saved its own state information to the local, and identified its own state as Active.
- The management device and the member equipment send handshake messages to each other on a regular basis. After the management device receives the handshake message from the member device, it does not reply and keeps the member device in the Active state, and the member device
- If the management device does not receive a handshake message from the member device within the triple handshake message sending interval after sending the handshake message to the member device, the status of the local member device is migrated from Active to Connect; Similarly, if the member device does not receive the handshake message sent by the management device within three times after sending the handshake message to the management device, its own state will be migrated from Active to Connect.
- If the management device receives the handshake message or the management message sent by the member device in the Connect state during the effective retention time, then the state of the member device is migrated back to the Active state, otherwise, the management device is transferred to the Disconnect; If the member device in Connect status has received the handshake message or management message sent

by the management device within the valid retention time, it will be migrated to Active, otherwise it will be migrated to Disconnect.

- When the communication recovery of the management device and the member device is interrupted, the member device in the Disconnect state will rejoin the cluster, and after the join is successful, the member device will be restored to Active in both the management device and the local state.

If a topology change is found, the member device also transmits the change information to the management device through the handshake message.

21.1.6 Manage vlan

Managing VLAN limits the scope of cluster management, and the following functions can be achieved through configuration management VLAN:

- The management messages of the cluster (including NDP,NTDP messages and handshake messages) will be limited to the management VLAN, isolated from other messages, and increased security.
- Manage equipment and member equipment to achieve internal communication through the management of VLAN.

The cluster management requires that the management device is connected to the member/ candidate device, including the cascade port (when the candidate device is connected to the management device through another candidate device, the ports that are connected to each other between the candidate devices) are to allow the management of the VLAN to pass, so:

- If the port does not allow the management VLAN to pass, the device to which the port is connected cannot join the cluster, so it should be determined that the port to which the candidate device is connected to the management device, including the cascade port, allows the management VLAN to pass.
- Only when the management device is connected to the member/ candidate device and the default VLAN ID of the cascade port is the management VLAN, the message of the configuration management VLAN is allowed to pass without the label, otherwise, the message of the management VLAN must pass the label.

See the "Chapter 6 Configuring VLANs" for related knowledge of the VLAN.

21.2 Introduction to Cluster Configuration

Before users configure the cluster, they need to make clear the role and function of each device in the cluster, and also configure the related functions to do a good job of communication planning with the internal equipment of the cluster.

Configuration task		Detailed configuration
Configuration management equipment	NDP functionality of enabling systems and ports	15.3.1
	Configuring NDP Parameters	15.3.2
	Enable the NTDP functionality of the system and port	15.3.3
	Configuring NTDP Parameters	15.3.4
	Configure manual collection of NTDP information	15.3.5

	Enable cluster function	15.3.6
	Set up a cluster	15.3.7
	Configure intercluster member interaction	15.3.8
	Configure cluster member management	15.3.9
Configure member equipment	NDP functionality of enabling systems and ports	15.4.1
	Enable the NTDP functionality of the system and port	15.4.2
	Configure manual collection of NTDP information	15.4.3
	Enable cluster function	15.4.4
Configure cluster member mutual access		15.5

Note:

After the cluster is established, after the NDP or NTDP function is turned off on the management device and the member device, the cluster will not be dissolved, but it will affect the normal operation of the established cluster.

21.3 Configuration management equipment

21.3.1 NDP functionality of enabling systems and ports

Order	Description	CLI mode
ndp global enable	Enables global NDP functionality. Global shutdown by default.	Configuration mode
ndp enable	NDP function of the enable port. All ports by default close NDP.	Interface configuration mode

Note:

- *The NDP function of both the global and the ports must be enabled at the same time, and the NDP can operate normally.*
- *The NDP feature does not support the aggregation port.*
- *In order to prevent management devices from collecting topology information about devices that do not need to join the cluster and adding it to the cluster, it is recommended that the NDP function be turned off on the ports connected to the cluster devices that do not need to join the cluster devices.*

21.3.2 Configuring NDP Parameters

Order	Description	CLI mode
ndp aging-timer <aging-time>	Configure the aging time of the NDP message sent by the device on the receiving device. The default is 180 seconds.	Configuration mode
ndp hello-timer <hello-time>	Configure the interval at which NDP messages are sent. Default 60 seconds.	Configuration mode

Note:

The aging time of NDP message on the receiving device can not be less than the time interval of NDP

transmission, otherwise it will cause the instability of NDP port neighbor information table.

21.3.3 NTDP functions of enabling systems and interfaces

Order	Description	CLI mode
ntdp global enable	Enables global NTDP functionality. Global shutdown by default.	Configuration mode
ntdp enable	The NTDP function of the enabling port. NDP is closed by default for all ports	Interface configuration mode

Note:

- *NTDP must be enabled to both global and port NTDP functionality in order for NTDP to function properly.*
- *The NTDP feature does not support aggregation ports.*
- *In order to prevent management devices from collecting topology information about devices that do not need to join the cluster and adding it to the cluster, it is recommended that the NTDP function be turned off on the ports connected to the cluster devices that do not need to join the cluster devices.*

21.3.4 Configuring NTDP Parameters

Order	Description	CLI mode
ntdp hop <hop-value>	Configure the scope of topology collection. By default, in the collected topology, the furthest device is the largest number of hops from the topology collection device.	Configuration mode
ntdp timer <interval-time>	Configure the time interval for timing topology collection. The default is 1 minute.	Configuration mode
ntdp timer hop-delay <time>	Configure the time that the collection device waits before the first port to forward the topology collection request message. The default is 200 milliseconds.	Configuration mode
ntdp timer port-delay <time>	Configure the port delay time for the current device to forward topology collection requests. The default is 20 milliseconds.	Configuration mode

21.3.5 Configure manual collection of NTDP information

After the cluster is established, the management device will periodically carry out the collection of the topology information. In addition, the user can initiate the collection process of the NTDP information at any time by configuring the manual collection of the NTDP information (regardless of whether the cluster is established), thereby more effectively managing and monitoring the device in real time.

Order	Description	CLI mode
ntdp explore	Manually collect topology information once.	Normal mode; privilege mode

21.3.6 Enable cluster function

Order	Description	CLI mode
cluster enable	Enable cluster function. The default cluster function is off.	Configuration mode

21.3.7 Set up a cluster

- Managing VLAN limits the scope of cluster management, and the following functions can be achieved through configuration management VLAN:
- The management messages of the cluster (including NDP,NTDP messages and handshake messages) will be limited to the management VLAN, isolated from other messages, and increased security.
- Manage equipment and member equipment to achieve internal communication through the management of VLAN.

Order	Description	CLI mode
cluster management-vlan <vlan-id>	Specify administrative VLAN. The default management VLAN is VLAN1	Configuration mode

Note:
Modify the management VLAN is not allowed if the current device is in the cluster.
Situations that are not in the cluster:

1) *Check that the vlan, does not fail directly and that there is a continuation of the next step*
2) *Re-check all of the interfaces, and if the vlan and the management VLAN on which the interface is located are not the same vlan, both the global switches that open the ndp and ntdp are closed and the corresponding closing and emptying operations are turned on and then re-opened.*
3) *Find the layer 3 interface to configure vlan, if not, create a new layer 3 interface corresponding to vlan, if new fails, manage vlan configuration successfully, you can ndp and ntdp, but can not join the cluster.*
4) *Set the mac of the current three-layer interface to dev_id, and if the vlan setting is successful and the new three-layer interface fails, use vlan1 's mac as dev_id.*

If the administrative VLAN, is configured but the user removes the vlan, directly from the vlan database, the administrative VLAN is automatically set to vlan1, and the global switches of both the open ndp,ntdp and the cluster are turned off and emptied accordingly.

Before establishing a cluster, users must first set up the private IP address range used by the member devices in the cluster. When the candidate devices join, the management equipment dynamically allocates a private IP address that can be used in the cluster scope, and sends it to the candidate devices for communication within the

cluster, so as to realize the management and maintenance of the member devices by the management equipment.

Order	Description	CLI mode
cluster ip-pool <IP/MASK>	Configure the private IP address range used by the member devices in the cluster on the devices that you want to set up as administrative devices.	Configuration mode

Note:

- *The IP address of the VLAN interface of the management device and the member device and the cluster address pool cannot be configured on the same network segment, or the cluster will not function properly.*
- *Can be configured only when the device is not in the cluster.*
- *Use management vlan to find out whether there is a corresponding three-layer port, if there is no three-layer port, return directly to failure. (the device cannot be a cluster command switch) if there is a layer 3 interface, the base address of the configuration IP-POOL is to the layer 3 port, and if the configuration fails, the IP-POOL configuration also fails.*

By default, the device is not a management device, the cluster is established:

Order	Description	CLI mode
cluster build <name>	Manually establish a cluster, configure the current device as a management device, and assign a cluster name.	Configuration mode
cluster auto-build <name>	Set up clusters automatically. The automatic clustering feature automatically adds all candidate devices found within the specified hop range to the created cluster.	Configuration mode
cluster delete <name>	Delete the cluster.	Configuration mode
cluster stop auto-add member	Under the automatic establishment of cluster configuration, stop automatically joining the member switch. This operation can only stop adding new devices, and devices that have joined the cluster will remain in the cluster.	Configuration mode

Note:

- *Users can only specify that the management VLAN, device has joined the cluster before the cluster is established, and the user cannot modify the management VLAN. If you need to change the management VLAN, after the cluster is established, you need to delete the cluster on the management device, reassign the management VLAN, and re-establish the cluster.*
- *For security reasons, it is not recommended that the management VLAN be configured to manage the default VLAN ID. of the device connected to the member device and the concatenated port*
- *Only when the port connected to the management device and the member device and the default VLAN ID of all concatenated ports are managed VLAN, the message of the managed VLAN can be allowed to pass without label. Otherwise, the management device, the port connected to the member device and all concatenated ports must be configured to allow the message label of the management VLAN to pass*

through. See "VLAN" for specific configuration.

- *Only when the cluster has not yet been established can the private IP address range of the member devices in the cluster be configured, and can only be configured on the management device. If the cluster is already established, the system is not allowed to modify the IP address range.*

21.3.8 Configure intercluster member interaction

In the cluster, the management device and the member device communicate in real time through the handshake message to maintain the connection state between them. The time interval between the handshake message transmission and the effective retention time of the device can be configured on the management device. This configuration will take effect for all the member devices in the cluster at the same time.

Order	Description	CLI mode
cluster timer <interval-time>	Configure the interval between handshake messages sent. The default is 10 seconds.	Configuration mode
cluster holdtime <hold-time>	The effective retention time of the configuration device default 60 seconds.	Configuration mode

21.3.9 Configure cluster member management

Users can manually specify candidate devices to join the cluster on the management device, or they can manually delete the member devices specified in the cluster. The join / delete operation of the cluster member must be done on the administrative device, otherwise the error prompt message will be returned.

Order	Description	CLI mode
cluster add member mac-address <mac-address>	The candidate device is added to the cluster.	Configuration mode
cluster delete member mac-address <mac-address>	Remove member devices from the cluster.	Configuration mode

21.4 Configuring a Member Device

21.4.1 NDP functionality of enabling systems and ports

See 21.3.1 NDP functionality for enabling systems and ports

21.4.2 Enable the NTDP functionality of the system and port

See 21.3.3 NTDP functionality for enabling systems and ports

21.4.3 Configure manual collection of NTDP information

See 21.3.5 configure manual collection of NTDP information

21.4.4 Enable cluster function

Refer to 21.3.6 Enable Cluster Features

21.5 Configure access to cluster members

After the NDP,NTDP, cluster function is configured correctly, the member devices in the cluster can be configured, managed and monitored through the management equipment. The member device can be configured and managed on the management device to the specified member device operation interface.

Order	Description	CLI mode
cluster switch-to member <member-number>	Switch from the management device operation interface to the member device operation interface.	Normal mode, privileged mode

Note:

The mutual switching between the cluster management device and the member device uses a Telnet connection and needs to be noted when switching:

- *Before performing a switch, the opposite device needs to execute the "telnet server enable" command to enable the telnet function, otherwise the switch will fail.*
- *Switch from the management device to the member device, and if the member number n does not exist, the error message is displayed*

If the requested login device Telnet user is full, the switch will fail.

21.6 Cluster management display and maintenance

Order	Description	CLI mode
show ndp[interface <ifname>]	Display NDP configuration information	Normal mode, privileged mode
reset ndp statistics [interface <ifname>]	Clear NDP statistics.	Configuration view
show ntdp	Display system NTDP information	Normal mode, privileged mode
show ntdp device-list	Display device information collected by NTDP	Normal mode, privileged mode
show ntdp single-device mac-address <mac-address>	Displays NTDP details for the specified device	Normal mode, privileged mode
show cluster	Displays the status and statistics of the cluster to which the device belongs	Normal mode, privileged mode

show cluster topology	Show cluster topology informatio	Normal mode, privileged mode
show cluster candidates [mac-address <mac-address>]	Show Candidate Device Information	Normal mode, privileged mode
show cluster members [<member-number>]	Displays cluster member information.	Normal mode, privileged mode

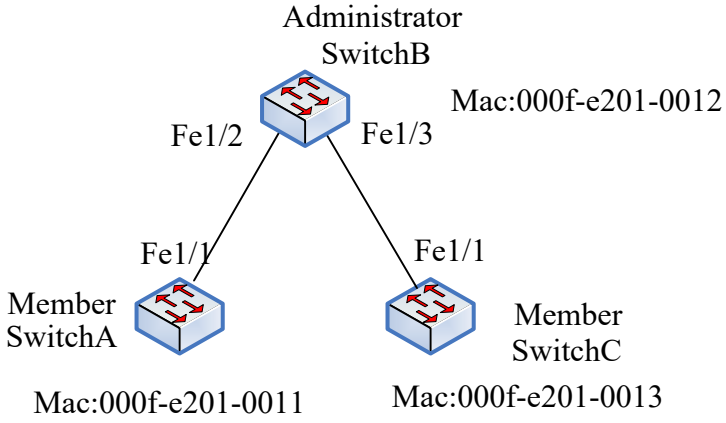
21.7 Examples of typical configuration of Cluster Management

1. Networking requirements:

The cluster ABC consists of three switches, whose management VLAN is VLAN 10. Where, Switch B is the management device (Administrator); Switch A and Switch C are Member devices.

The base address IP of the whole cluster address pool is 10.0.0.1, which supports 8 devices.

2. Group network diagram:



2. Configuration steps:

Configure the member device SwitchA

Configuration Management VLAN.

[SwitchA] cluster management-vlan 10

[SwitchA] interface ge1/1

[SwitchA-ge1/1] switch access vlan 10

Enables global NDP functionality and NDP functionality on port ge1/1.

[SwitchA] ndp enable

[SwitchA] interface ge1/1

[SwitchA-ge1/1] ndp enable

Enables global NTDP functionality and NTDP functionality on port Ethernet1/0/1.

[SwitchA] ntdp enable

[SwitchA] interface ge1/1

[SwitchA-ge1/1] ntdp enable

Enables the cluster

[SwitchA] cluster enable

Configure member device SwitchC

Because the configuration of the member device is the same, the configuration on Switch C is similar to that of Switch A, and the configuration process is slightly.

Configuration management device SwitchB

Configuration Management VLAN.

[SwitchB] cluster management-vlan 10

[SwitchB] interface ge1/2

[SwitchB-ge1/2] switch access vlan 10

[SwitchB] interface ge1/3

[SwitchB-ge1/3] switch access vlan 10

Enable global NDP,NTDP function, and enable port ge1/2 and NDP,NTDP function on ge1/3 respectively.

[SwitchB] ndp enable

[SwitchB] ntdp enable

[SwitchB] interface ge1/1

[SwitchB-ge1/2] ndp enable

[SwitchB-ge1/2] ntdp enable

[SwitchB] interface ge1/3

[SwitchB-ge1/3] ndp enable

[SwitchB-ge1/3] ntdp enable

#The aging time of the NDP message sent by the device is configured to be 200 seconds on the receiving device.

[SwitchB] ndp timer aging 200

#The time interval for configuring the NDP message is 70 seconds.

[SwitchB] ndp timer hello 70

#The maximum number of hops collected by the configuration topology is 2 hops.

[SwitchB] ntdp hop 2

The delay time of configuring the first port of the collected device to forward the topology collection request message is 150ms.

[SwitchB] ntdp timer hop-delay 150

#The delay time of configuring the other ports of the collected device to forward the topology collection request message is 15ms.

[SwitchB] ntdp timer port-delay 15

#The interval for configuring topology collection is 3 minutes.

[SwitchB] ntdp timer 3

#Enables the cluster

[SwitchB] cluster enable

#The private IP address of the configured member device is in the range of 10.0. 0.1 to 10.0. 0.9.

[SwitchB] cluster ip-pool 10.0.0.1 8

#Configure the current device as a management device and establish a cluster called abc, and members automatically join the cluster.

[SwitchB] cluster autobuild abc

After adding all the switches you want to add, you can turn off the auto-join cluster function

[SwitchB]cluster stop auto-add member

Chapter 22 System log configuration

This chapter mainly includes the following:

- Introduction to system log
- System log configuration

22.1 Introduction to system log

The system log module is an important part of the switch, which is used to record the operation of the whole system, the abnormal behavior and the operation behavior of the user, and help the administrator to know and monitor the operation of the system in time. The syslog module management system collects, classifies, stores, and displays the log information from the log information of the various modules that are running.

There is also an important debugging feature in the log system. The syslog is in conjunction with debugging to help the administrator or other technician to monitor the network's operation, debug, and troubleshoot failures in the network. The administrator can conveniently select the content that needs to be debugged and to locate and resolve the failure of the device or network by observing the log information output by the debugging.

This section mainly includes the following:

- The format of the log information
- Storage of logs
- Display of logs
- Debugging tool

22.1.1 The format of the log information

The format of the log information is as follows:

Timestamp priority: module name: log content

There is a space between the timestamp and the priority, a colon and a space between the priority and the module name, a colon and a space between the module name and the log content.

Examples of the format of log information are as follows:

2006/05/20 13:56:34 Warning: MSTP: Port up notification received for port ge1/2

In this log information, the timestamp is 2006/05/20 13:56:34; the priority is Warning; the module name is MSTP; the log content is Port up notification recovery for port ge1/2.

1）Time stamp

Timestamp format: year / month / day　hour: minutes: seconds.

The hours are made on a 24-hour basis, from 0 to 23.

The timestamp records the time when this log information was generated, using the system time of the switch. The system time has been set when the switch leaves the factory, the administrator can also modify, the system time can still run after the equipment is out of power.

2）Priority

According to the importance of the log information, the log information is divided into four levels according to

the importance of the log information. The order of priority from high to low is Critical,Warning,Informational and Debugging.. The priority is described in the following table:

Priority	Description
Critical	Serious error
Warning	General errors, warnings, very important tips
Informational	Important tips, general tips, diagnostic information
Debugging	Debug information

3）Module name

The module name records the module that this log information produces, and the following table lists some of the main modules that generate log information:

Module name	Description
CLI	Command line interface module
MSTP	Multi - instance spanning tree protocol module
VLAN	VLAN function module
ARP	ARP protocol module
IP	IP protocol module
ICMP	ICMP protocol module
UDP	UDP protocol module
TCP	TCP protocol module

4）Log content

The log content is a phrase or sentence, which represents the main idea of the log information. By reading the log content, the administrator can know what is going on in the system.

22.1.2 Storage of the log

There are generally three ways to store logs:

- The log is stored in memory.
- The log is stored in the NVM.
- The log is stored on the server.

According to the priority of the log, there are four log tables in memory, each table stores a kind of priority log information, that is, according to the priority of the log, the log is divided into four categories, and each type of log is stored in a separate log table. Each log table has 1K entries, which can store 1K log information, and the log information that is overwritten for the longest time when the log table is full. There is a problem with this storage

mode. When the system restarts, these log information is gone, and the administrator can not see the log information and can not locate the problem when the system crashes.

For important log information, such as Critical and Warning, this log information can be stored in the NVM of the system. After the system restarts, the log information in NVM can still be retained, which is convenient for the administrator to locate the problem when the system crashes. However, one problem with this storage method is that due to the capacity limit of NVM, the log information entries stored in NVM are very limited.

There is also a better way to store the log information in the server, which can be implemented using the SYSLOG protocol, and the log information can be sent to the server in real time and the server saves the log information and is displayed on an interface. This way of storage not only allows the user to view the log information, but also has a large capacity to store a large amount of log information on the server.

At present, the system only supports storing log information in memory, but not in NVM or server.

22.1.3 Display of logs

There are two ways to display logs: manual display and real-time display. Manual display is that the user displays the log information by inputting the command, and the real-time display is that when the log information is generated, the log information is output directly to the terminal, and the user can see it in time.

For manual display, users can view all log information, or view a priority log information. The order in which the log information is displayed is that the last generated log information is placed at the top, so that the user can first see the nearest running status of the switch.

For real-time display mode, the user must open the terminal real-time display switch. If the switch is open, the generated log information is not only written to the log table, but also the log information is output to the terminal, and if the switch is closed, the log information is not displayed on the terminal in real time. The system can only output log information to the Console terminal in real time, and does not support the output of log information to the Telnet terminal.

22.1.4 Debugging tool

Debugging is a diagnostic tool for devices and networks, which tracks the data packets of the system and the module, the changes of the state machine of the module, etc., which can enable the administrator to understand and monitor the running process of the system and the module. If the network or device has an abnormal situation, it can be traced through the debugging tool.

The debugging tool provides a wealth of switches that administrators can track what they are interested in by

controlling them. When an exception occurs on a device or network, the administrator can turn on the debugging switch associated with this exception and find the problem by tracking the execution of the system and module.

When a debugging switch is turned on, the system generates relevant log information, which is written to the corresponding log table. In general, the priority of log information generated by debugging is Informational. When the terminal displays the switch in real time, the log information is output to the terminal in real time. When the debugging switch is turned off, the system does not generate relevant log information.

22.2 System log configuration

The Syslog configuration includes the following:

- Configure terminal real-time display switch
- View log information
- Configure the debugging switch
- View debugging information

22.2.1 Configure terminal real-time display switch

By default, the terminal real-time display switch is off, and the log information generated by the system is written to the log table, but will not be displayed on the terminal in real time. There are also log information in the system that is not restricted by this switch and is always output to the console in real time.

The terminal real-time display switch corresponds to the priority of the system log. If the terminal display switch of a certain priority is turned on, the log information of that priority will be displayed on the terminal in real time. If the terminal real-time display switch of a certain priority is not turned on, the log information of the priority will not be displayed on the terminal in real time.

At present, the switch can only display the log information on the Console terminal in real time, but can not display the log information on the Telnet terminal in real time.

When the user uses the write command to store the current configuration of the system to the configuration file, the configuration of the terminal real-time display switch will not be stored in the configuration file of the system. When the system restarts, these configurations will be lost and need to be reconfigured.

The commands to configure the terminal to display the switch in real time are as follows:

Order	Description	CLI mode
log display [critical | warning | informational | debugging]	Turn on the terminal real-time display switch. If no parameters are entered, all priority terminal real-time display switches are turned on, and if one of the parameters is entered, the specified priority terminal real-time display switch is turned on.	Privileged mode
no log display [critical	Close the terminal real-time display switch. If the	Privileged mode

| warning | informational | debugging]	parameter is not entered, the terminal real-time display switch of all the priority is turned off, and if one of the parameters is input, the terminal of the designated priority is turned off to display the switch in real time.	

22.2.2 View log information

Commands to view log information are as follows:

Order	Description	CLI mode
show log display	Configure the configuration of the real-time display switch for all the priority terminals	Normal mode, privileged mode
show log [critical | warning | informational | debugging]	Display log information in the log table. If no parameters are entered, the log information of all log tables is displayed. If one of the parameters is entered, the log information of the log table of the specified priority is displayed.	Normal mode, privileged mode

22.2.3 Configure the debugging switch

The system provides a wealth of debugging switches, involving multiple modules, here only listed the schematic commands for each module, the complete format of the command see the command manual.

When the user uses the write command to store the current configuration of the system to the configuration file, the configuration of the debugging switch is not stored in the configuration file of the system. When the system restarts, these configurations will be lost and need to be reconfigured.

The schematic command for configuring the debugging switch is as follows:

Order	Description	CLI mode
debug ip …	Turn on the relevant debugging switch for the system to send and receive IP packets.	Privileged mode
no debug ip …	Shut down the system to send and receive the relevant debugging switch of the IP packet.	Privileged mode
debug ip icmp …	Turn on the relevant debugging switch for the system to send and receive ICMP packets.	Privileged mode
no debug ip icmp …	Shut down the system to send and receive the relevant debugging switch of the ICMP packet.	Privileged mode

debug ip arp …	Open the relevant debugging switch for the system to send and receive the ARP package.	Privileged mode
no debug ip arp …	Shut down the system to send and receive the relevant debugging switch of the ARP package.	Privileged mode
debug ip udp …	Open the relevant debugging switch for the system to send and receive UDP packets.	Privileged mode
no debug ip udp …	Shut down the system to send and receive the relevant debugging switch of the UDP packet.	Privileged mode
debug ip tcp …	Open the relevant debugging switch for the system to send and receive TCP packets.	Privileged mode
no debug ip tcp …	Shut down the system to send and receive the relevant debugging switch of the TCP packet.	Privileged mode
debug mstp …	Turn on the relevant debugging switch for MSTP protocol diagnosis.	Privileged mode
no debug mstp …	Turn off the related debugging switch for MSTP protocol diagnosis.	Privileged mode
debug igmp snooping …	Turn on the relevant debugging switch for IGMP SNOOPING feature diagnosis.	Privileged mode
no debug igmp snooping …	Turn off the IGMP SNOOPING function diagnosis related debugging switch.	Privileged mode
debug dhcp snooping …	Turn on the related debugging switch for DHCP SNOOPIN protocol diagnosis	Privileged mode
no debug dhcp snooping …	Close the relevant debugging switch for the DHCP SNOOPIN protocol diagnostics	Privileged mode
no debug all	Shut down all the debugging switches on the system.	Privileged mode

22.2.4 View debugging information

The commands to view debugging information are as follows:

Order	Description	CLI mode
show debugging [ip | mstp | igmp snooping | dhcp snooping]	View the debugging switch configuration. If you do not enter a parameter, view the debugging switch configuration for all the modules, and if only one of the parameters is entered, only the debugging switch configuration of one module is viewed. If the input parameter is ip, the debugging switch configuration of the IP, ICMP, ARP, UDP, and TCP	Normal mode, privileged mode

	modules is viewed.	

22.3 Configuring the SYSLOG Configure SYSLOG

The SYSLOG includes the following:

- SYSLOG introduction
- SYSLOG configuration
- SYSLOG configuration example

22.3.1 SYSLOG introduction

SYSLOG is a standard protocol for device log information management, which has been greatly applied due to its simplicity. In the SYSLOG system, it is divided into three parts. One is to define each sub-module to distinguish the log information generated by different modules; define different log information levels to observe the device health. Various types of log information of the device are collected according to this convention. The second is the configuration file. How to process the customized collected log information can be saved locally. It can be sent to the specified server on the network, distributed to the specified login user, etc. The configuration file determines how to save the device. Log information. The third is to send SYSLOG protocol packets according to the packet format defined by the RFC. It can be seen that in our switch system, the entire SYSLOG work contract is the system log module. The first part of the SYSLOG protocol is completed by each function sub-module in the switch, and sends log information of each level to the system log module. Four levels of log tables are maintained in the system log module. The second part of the SYSLOG protocol distributes log information uniformly by the system log module. One is to display the serial port terminal in real time or manually through the terminal display switch; the other is to store four levels of log tables in the memory. The third is to save the high value on the NVM. Level log information to avoid losing important log records when power failure occurs. Fourth, the logs are sent to the remote server for storage, collection, and sorting through SYSLOG messages. The SYSLOG submodule in the system log module implements only the third part of the function, transferring the system log to the server.

22.3.2 SYSLOG configuration

The SYSLOG configuration command includes:

- Open the syslog protocol
- Shut down the syslog protocol
- Set the syslog transmission level
- Restore the syslog send level to the default

Order	Description	CLI mode
syslog open <server-ip> [udp-port]	Open syslog protocol; parameter server-ip is server ip address, must fill; parameter udp-port is the destination port number of protocol message, optional, if not set, default value 514; if the setting needs to be consistent with server configuration.	Global configuration mode
syslog close	Shut down the syslog protocol	Global configuration mode
syslog level <critical | warning | informational | debugging>	Set the send level of the log, if set to the debugging level, all logs are sent to the server.	Global configuration mode
no syslog level	Restore the transmission level to the default value debugging	Global configuration mode

22.3.3 SYSLOG configuration example

（1） Configure

Configure syslog server ip address is 192.168.2.2.01, configure server software receive syslog message the udp destination port is 200; connect ge1/3 port to server; server only keep log record up to two levels. The switch is configured as follows:

Switch#configure terminal
Switch(config)#vlan database
Switch(config-vlan)#vlan 2
Switch(config-vlan)#vlan 3
Switch(config-vlan)#exit
Switch(config)#interface ge1/3
Switch(config-ge1/3)#switchport access vlan 2
Switch(config-ge1/3)#interface ge1/4
Switch(config-ge1/4)#switchport access vlan 2
Switch(config-ge1/4)#interface ge1/5
Switch(config-ge1/5)#switchport access vlan 3
Switch(config-ge1/5)#interface ge1/6
Switch(config-ge1/6)#switchport access vlan 3
Switch(config-ge1/6)#interface vlan2
Switch(config-vlan2)#ip address 192.168.2.1/24
Switch(config-vlan2)#exit
Switch(config)#syslog open 192.168.2.201 200
Switch(config)#syslog level warning

（2） Test and verify

```
Switch#show running-config
!
syslog open 192.168.2.201 200
syslog level warning
!
……
!
line vty
!
end

Switch#show syslog
Syslog is opened!
   server ip address: 192.168.2.201
   udp destination port: 200
   severity level: warning
   local device name: Switch
```

Chapter 23 Port loop

This chapter mainly includes the following:

- Introduce
- Protocol principle
- Configuration introduction

23.1 Brief introduction

When a loop appears under one port of the switch, it will cause a broadcast storm under this port, and the source MAC address of all broadcast packets will be learned to this loop port, which will cause the device forwarding to not proceed properly.

23.2 Protocol principle

Ethernet loop detection protocol (Ethernet Loopback Detection, (ELD) can detect the loop through the interaction of data packets, and block the port where the loop occurs. Eld protocol is based on port computing protocol, which can only detect the loop that occurs on this port.

23.2.1 Detection process

When a port is enabled with the ELD protocol, a timer is enabled on this port, the loop detection packet is sent when the timer expires, The operation of blocking the loop is performed on this port and the FDB table for this port is cleared.

If a port belongs to a port member of multiple VLANs, the port automatically sends a loop detection packet to all of the VLANs. That is, the port automatically detects the presence of a loop for all the VLANs that it belongs to.

23.2.2 Recovery mode

As mentioned above, this port will be blocked when a port loop is present. The ELD protocol has two recovery modes that can be configured by two users: automatic recovery and manual recovery.

Automatic recovery is when a port is blocked, the ELD protocol enables a recovery timer, when the timer expires, it performs a reverse operation of the blocking loop, and the loop detection timer is enabled again on this port.

Manual recovery is that after the port is blocked, the protocol no longer enables the timer to restore the port, and the user has to enter his own command to perform the reverse operation of the blocking loop.

23.2.3 Protocol security

The ELD protocol is vulnerable to attack in the network, which means that users can send an ELD protocol packet to an ELD-enabled port according to the packet format of the ELD protocol, resulting in the wrong decision that the port may be blocked without a loop.

The ELD protocol uses two strategies to prevent similar attacks and minimize the error.

Decision 1, first of all, the ELD protocol is a protocol without interaction, that is to say, it does not depend on other devices, then the packet itself can be simply encrypted. Our operation here is to send the ELD protocol packet with a key, the user can not camouflage the protocol packet without a key.

The second decision is to prevent the attacker from reflecting the protocol packet by grasping the packet attack, and can configure the format of the packet received by the switch to prevent the attack, which requires the user to configure.

23.3 Configuration introduction

ELD protocol is based on port implementation, there is no unified enabled command.

23.3.1 Global configuration

Global configuration is a unified attribute of the configuration protocol.

Order	Description	Mode
loop-detection detection-time <1-65535>	Configure the loop detection time period, twice this time must be less than the recovery time period, the default value is 5 seconds.	Global configuration mode
loop-detection resume-time <10-65535>	Configure the automatic recovery time period, the automatic recovery time must be more than 2 of the loop check time, if automatic recovery is enabled, this configuration will take effect. The default recovery time is 600 seconds.	Global configuration mode
loop-detection protocol-safety	Enable protocol security checking, which is turned off by default.	Global configuration mode
loop-detection respond-packets	Configure the number of packages that must be received over a certain period of time, and if protocol security check is enabled, the configuration will take effect, with a default of 10.	Global configuration mode

23.3.2 Interface configuration

Interface configuration is the configuration for each port.

Order	Description	Mode
Loop-detection enable	Enable the ELD protocol on a port.	Interface configuration mode
Loop-detection resume	Manually restore and restart loop checking.	Interface configuration mode
loop-detection resume-mode {automation | manual}	Configure the recovery mode, select either manual or automatic recovery, and the default is automatic recovery.	Interface configuration mode
loopback-detection shutdown-mode {no-shutdown | shutdown}	The command is configured to see if the port is shutdown when a loop is present.	Interface configuration mode

23.3.3 Display configuration

Show loop-detection [ifname]

Displays all configurations of the protocol and the configuration of an interface.

Chapter 24 SNTP configuration

This chapter mainly includes the following:

- Introduce
- Configure SNTP
- Show SNTP

24.1 SNTP Introduction

At present, communication protocol is widely used to realize network time synchronization, that is, NTP (Network Time Protocol network time protocol, and another protocol is the simplified version of NTP protocol, that is, SNTP (Simple Network Time Protocol simple network time protocol).

NTP protocol can span various platforms and operating systems, using very precise algorithms, so it can provide 1-50ms accuracy almost unaffected by network delay and jitter. NTP provides authentication mechanism at the same time, and the security level is very high. However, the NTP algorithm is complex and requires a high system.

The SNTP (Simple Network Time Protocol) is a simplified version of NTP. In the implementation, the calculation time is simple and the performance is high. And the precision can also be up to about 1 second, and can basically meet the needs of the vast majority of occasions.

Because the message of SNTP and the message of NTP are completely consistent, the SNTP Client implemented by this switch can be fully compatible with NTP Server.

24.2 Configure SNTP

24.2.1 Default SNTP settings

Project	Default value
SNTP state	Disable shuts down SNTP service
NTP Server	The default for three NTP Server, is: 211.115.194.21 203.109.252.5 192.43.244.18
The interval of the synchronization time of the SNTP.	1800 seconds
Local time zone	+ 8, that is, the east eight areas

Turn SNTP on and off

The configuration is as follows:

Switch# configure terminal

Enter global configuration mode

Switch(config)# sntp enable

Open SNTP

Switch(config)# sntp disable

Shut down SNTP

24.2.2 Configure the SNTP Server address

Because the message of SNTP is completely consistent with the message of NTP, SNTP Client is fully compatible with NTP Server.. There are more NTP Server, on the network. You can choose one with less network delay as the NTP Server. on the switch.

Specific NTP server addresses can be obtained on http://www.time.edu.cn/ or http://www.ntp.org/.

such as, for example, 43.244.18 (time.nist.gov)

The switch defaults to three Server addresses, 211.115.194.21, 203.109.252.5, and 1443.244.18. The switch first uses the first server address to synchronize the time, if not, using the second server address, and so on. In general, the user does not need to configure the server address and simply use the default server address. if you have a special case to configure that serv address, you need to delete the default serv address before adding a new Server address.

The configuration of adding one server address is as follows:

Switch# configure terminal

Enter global configuration mode

Switch(config)# sntp server 210.72.145.44

Adding SNTP server IP, if the switch already has three Server addresses, it will fail and need to delete the address and then join.

The configuration for deleting the Server address is as follows:

Switch(config)# no sntp server

Delete all Server addresses

Switch(config)# no sntp server 210.72.145.44

Delete one of the Server addresses.

The configuration of setting the server address back to the default address is as follows:

Switch(config)# sntp server default

The server address is reset to the default address, that is, address 211.115.194.21, 203.109.252.5, and address 43.244.18

24.2.3 Configure the interval of the SNTP synchronization clock

SNTP Client needs to synchronize the clock with NTP Server in order to timing the positive clock.

The configuration is as follows:

Switch# configure terminal

Switch(config)# sntp interval 60

Sets the interval between timing and synchronization clocks in seconds, ranging from 60 seconds to 65535 seconds. The default value is 1800 seconds, which is set here to 60 seconds

Switch(config)# no sntp interval

The interval of the timing synchronization clock is restored to default 1800 seconds.

24.2.4 Configure the local time zone

The time obtained after communication through SNTP protocol is Greenwich mean time ((GMT),). In order to prepare the hunting local time, it is necessary to set up the local area to correct the standard time. By default, the switch sets the local time zone for East 8, which is also the time zone for China.

The configuration is as follows:

Switch# configure terminal
Switch(config)# sntp time-zone -8
Set the local time zone to West 8
Switch(config)# no sntp time-zone
The local time zone is restored to East 8.

24.3 Information display of SNTP

The configuration is as follows:
Switch# show sntp
Switch# show running-config

Chapter 25 OAM configuration

This chapter mainly includes the following:

- OAM introduction
- Configure OAM
- Examples of the typical configuration of OAM

25.1 OAM introduction

Ethernet OAM (Operations, Administration and Maintenance) is a tool for monitoring network problems. It operates at the data link layer, and reports the state of the network by using the OAM Protocol Data Units (OAM protocol data units) between the devices so that the network administrator can manage the network more effectively.

At present, Ethernet OAM mainly solves the common link problem of "last kilometer" in Ethernet access. The link status between two devices can be monitored by enabling Ethernet OAM on two point-to-point connected devices.

- This section focuses on the main features of Ethernet OAM, including:
- Link performance monitoring: link failure can be detected;
- Fault detection and alarm: the network administrator can be notified in time when the link fails;
- Loop test: detect link failure by returning a non-OAMPDU loop.

25.1.1 Link performance monitoring

Link monitoring is used to detect and discover link layer failures in a variety of environments.

The Ethernet OAM uses the interaction of the Event Notification OAMPDU for link monitoring. When the link failure occurs, the local link monitors the failure and sends the Event Notification OAMPDU to the peer-to-peer Ethernet OAM entity to inform the normal link event. The administrator can dynamically grasp the status of the network by observing the log information.

Event type	Chinese meaning	Description
Errored Symbol Event	Error signal event	The number of error signals exceeds the threshold in unit time
Errored Frame Event	Error frame event	In unit time, the number of error frames exceeds the threshold
Errored Frame Period Event	Error frame cycle event	The number of error frames exceeds the threshold within the time the specified number of frames is received
Errored Frame Seconds Summary Event	Total number of error frame seconds event	The number of error frame seconds exceeds the threshold within the specified time

25.1.2 Remote fault detection

It is very difficult to detect the fault of Ethernet, especially when the network physical communication is not interrupted and the network performance is slow down.

OAMPDU defines a flag (Flag domain) that allows Ethernet OAM entities to transmit the fault information to the opposite end. This flag can indicate the following emergency link events:

Table 5 Emergency Link Events

Event type	Chinese meaning	Description	OAMPDU transmission frequency
Link Fault	Link failure	End-to-end link signal loss	Sent once per second
Dying Gasp	Critical failure	Unpredictable local failures, such as power outages	Uninterrupted transmission
Critical Event	Emergencies	An unspecified emergency, such as a single link.	Uninterrupted transmission

In the process of Ethernet OAM connection, Information OAMPDU is continuously sent. The local OAM entity can tell the remote OAM entity the emergency link event information that occurs at the local end through Information OAMPDU. In this way, the administrator can dynamically understand the status of the link and deal with the corresponding errors in a timely manner.

25.1.3 Remote loop

The remote loopback function refers to the fact that when the OAM entity in active mode sends all the messages except OAMPDU to the opposite end (remote), the opposite end receives the message and loops it directly to the local end. It can be used to locate link failures and detect link quality: network administrators can judge link performance (including packet loss rate, delay, jitter, etc.) by observing the return of non-OAMPDU messages.

25.2 Configure OAM

Order	Description	CLI mode
oam errored-frame period <1-60>	Configure the period value of the Ethernet port for error frame event detection. The default error frame event has a period of 1 s.	Privilege mode
no oam errored-frame period	The value of the period in which the Ethernet port is reset for error frame event detection. The default error frame event has a period of 1 s.	Privilege mode
oam errored-frame threshold <0-4294967295>	Configure the threshold for error frame event detection. The threshold for the default error frame event is 1.	Privilege mode
no oam errored-frame threshold	Resets the threshold of error frame event detection. The threshold of the default error frame event is 1.	Privilege mode

oam errored-frame-period period <100-6000>	Configure the period value of the Ethernet port for the error frame period event detection. The period of the default error frame period event is 1000 milliseconds.	Privilege mode
no oam errored-frame-period period	The period value of the error frame period event detection is reset for the Ethernet port. The period of the default error frame period event is 1000 milliseconds.	Privilege mode
oam errored-frame-period threshold <0-4294967295>	Configure the threshold for the error frame period event detection. The threshold for the default error frame event is 1.	Privilege mode
no oam errored-frame-period threshold	Reset the threshold for the error frame period event detection. The threshold for the default error frame event is 1.	Privilege mode
oam errored-frame-seconds period <10-90>	Configure the Ethernet port for the periodic value of error frame second event detection. The period of the default error frame event is 60s.	Privilege mode
no oam errored-frame-seconds period	Resets the periodic value of the Ethernet port for error frame second event detection. The period of the default error frame event is 60s.	Privilege mode
oam errored-frame-seconds threshold <0-900>	Configure the threshold for error frame second event detection. The threshold for the default error frame number of seconds event is 1.	Privilege mode
no oam errored-frame-seconds threshold	Reset the threshold for the error frame number of seconds event detection. The threshold for the default error frame number of seconds events is 1.	Privilege mode
oam mode (active| passive)	The operation mode of the Ethernet OAM is configured, and the link mode of the default Ethernet OAM is the active mode.	Interface configuration mode
oam enable	The Ethernet OAM function is turned on and the default Ethernet OAM function is turned off.	Interface configuration mode
oam loopback	Enables the Ethernet OAM loopback function. The default Ethernet OAM loopback function is closed.	Interface configuration mode
no oam loopback	Turn off the Ethernet OAM loopback function. The default Ethernet OAM loopback function is closed.	Interface configuration mode
show oam configuration	Displays windows and threshold values for general link events.	Privilege mode
show oam local-state (IFNAME|)	View OAM local information	Privilege mode
show oam remote-state (IFNAME|)	View OAM end-to-end information	Privilege mode
show oam link-event (IFNAME|)	View OAM link event information	Privilege mode
show oam-loopback IFNAME	Displays a port loopback information.	Privilege mode

25.3 Examples of the typical configuration of OAM

1 Networking requirements
The data link layer is managed by configuring Ethernet OAM protocol on Device A and Device B. (Device A port: fe1/1,Device B port: fe1/1)

(1) Configure Device A:

```
Switch>enable
Switch#configure terminal
Switch(config)# interface fe1/1
```

On port Ethernet1/0/1, the connection mode of its Ethernet OAM is passive mode, and the Ethernet OAM function is enabled.

```
Switch(config-fe1/1)#oam mode passive
Switch(config-fe1/1)#oam enable
```

(2) configure Device B:

```
Switch>enable
Switch#configure terminal
Switch(config)# interface fe1/1
```

The Ethernet OAM working mode of configuring port Ethernet1/0/1 is the default mode active, and enables Ethernet OAM functionality.
Switch(config-fe1/1)#oam enable

(3) (Device A) verify the configuration effect:

```
Switch>enable
Switch#show oam local-state ge1/2
```

Chapter 26 CFM configuration

The switch provides the CFM feature, which is mainly used to detect link connectivity in layer 2 networks, confirm failures, and determine where failures occur, including the following:

- Introduction to CFM
- Configure CFM Basic Settings
- CFM function configuration
- CFM display and maintenance
- Example of a typical configuration of CFM

26.1 Brief introduction to CFM

CFM is the abbreviation of Connectivity Fault Management (connectivity error management. The CFM of this switch mainly refers to connectivity error detection and follows the CFM protocol defined by IEEE 802.1ag. It is an end-to-end OAM (Operations, Administration and Maintenance, operation, management and maintenance mechanism based on VLAN on layer 2 links, which is mainly used to detect link connectivity, confirm faults and determine the location of faults in layer 2 networks.

26.1.1 Basic concept of CFM

1 Maintenance domain

The Maintenance Domain (MD) indicates the network covered by the connectivity error detection, whose boundary is defined by a series of maintenance endpoints configured on the port. The maintenance domain is identified in "Maintaining a Domain Name".

In order to locate the fault point accurately, the concept of level (hierarchy) is introduced into the maintenance domain. The maintenance domain is divided into eight levels, which is represented by integer 0 ≤ 7. The larger the number is, the larger the range of maintenance domain is. Different maintenance domains can be adjacent or nesting, but can not cross, and can only be nesting from high-level maintenance domain to low-level maintenance domain when nesting, that is to say, low-level maintenance domain must be included in high-level maintenance domain. The CFM PDU of the low-level maintenance domain is discarded when it enters the high-level maintenance domain; the CFM PDU of the high-level maintenance domain can traverse the low-level maintenance domain; and the CFM of the same level of maintenance domain PDU cannot cross with each other.

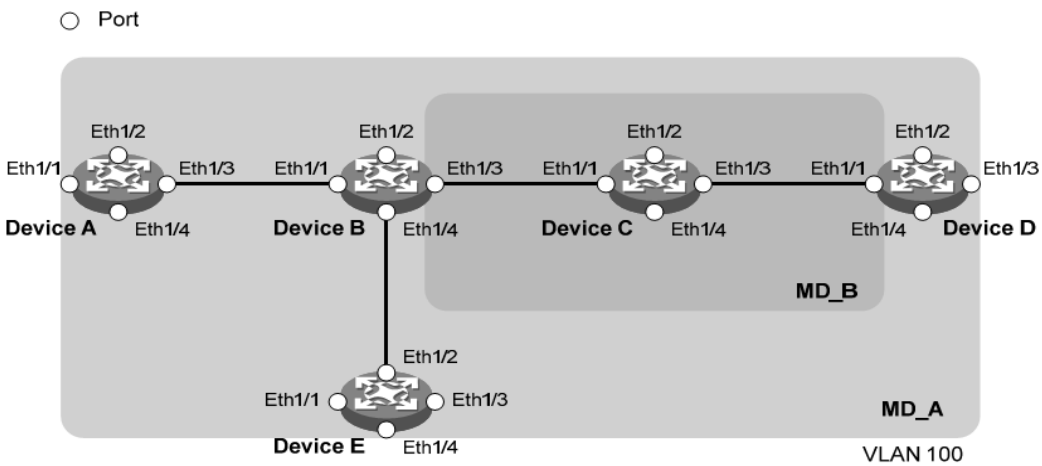


Figure 1-1

In practical application, it is necessary to plan the maintenance domain reasonably: as shown in figure 1, the maintenance domain MD_B is nesting in the maintenance domain MD_A, and in order to detect connectivity in MD_A, the CFM PDU of MD_A is required to traverse MD_B, so the level of MD_A needs to be configured higher than that of MD_B. In this way, the CFM PDU of MD_A can traverse the MD_B, to achieve the connectivity fault management of the whole MD_A, while the CFM PDU of MD_B does not spread into MD_A.

The classification of the maintenance domain makes the fault location more convenient and accurate, as shown in Figure 1-1, the maintenance domain MD _ B is nested in the maintenance domain MD _ A. If the link is not found on the boundary of the MD _ A, it is indicated that the device in the domain has failed and the failure may appear on the Device A-Device E. At this time, if the link is not found on the boundary of the MD _ B, the failure range is reduced to the three devices of Device B to Device D; on the contrary, if the device in the MD _ B is working properly, at least the Device can be determined C is free from malfunction.

2 Maintenance set

Multiple maintenance sets (Maintenance Association,MA) can be configured as needed in the maintenance domain, each of which is a collection of maintenance points in the maintenance domain. The maintenance set is identified by maintenance Domain name + maintenance set name.

The messages sent by the maintenance set serving the maintenance point of a VLAN, maintenance set have the label of the VLAN, and the maintenance point of the maintenance set can receive the messages sent by other maintenance points in the maintenance set.

3 Maintenance point

The maintenance point (Maintenance Point,MP) is configured on the port and belongs to a maintenance set, which can be divided into maintenance endpoint (Maintenance association End Point,MEP and maintenance intermediate point (Maintenance association Intermediate Point,MIP).

1) Maintenance of the endpoint

The maintenance endpoint is identified as an integer called MEP ID, which determines the scope and boundaries of the maintenance domain. The maintenance set

and maintenance domain to which the maintenance endpoint belongs determine the VLAN attribute and level of the message sent by the maintenance endpoint.

The level of the maintenance endpoint determines the level of the message it can handle, and the level of the message sent by the maintenance endpoint is the level of the maintenance endpoint. when the maintenance end point receives the message which is higher than the own level, the maintenance end point is not processed, and the message is forwarded according to the original path; and when the maintenance end point receives the message which is less than or equal to the own level, the maintenance end point carries out corresponding processing, To ensure that messages within the low-level maintenance domain do not diffuse into the high-level maintenance domain.

The maintenance end point is directional, which can be divided into extroverted MEP and introverted MEP. The direction of the maintenance endpoint indicates the location of the maintenance domain relative to the port.

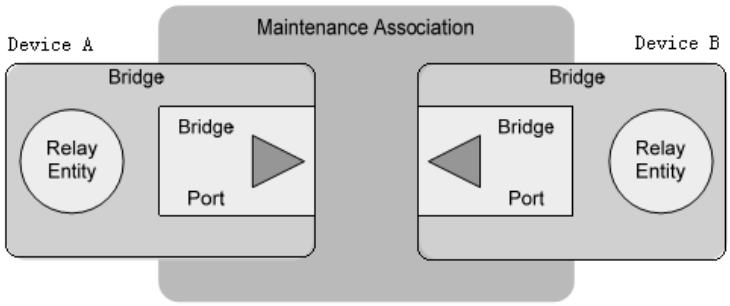


Figure 1-2 Schematic diagram of the outward MEP

As shown in Figure 1-2, outbound maintenance endpoints send messages outward through their ports

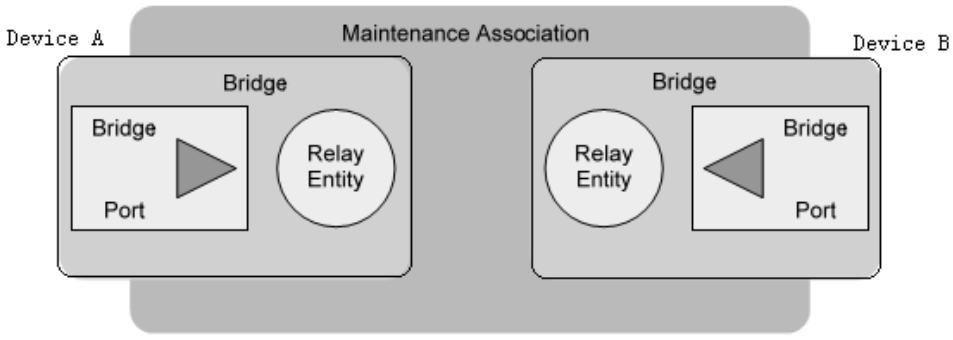


Figure 1-3

As shown in figure 1 / 3, the inward maintenance endpoint does not send messages outward through its port, but through other ports on the device.

2) Maintenance of the middle point

The maintenance center point is located inside the maintenance domain, and the CFM protocol message cannot be actively sent, but the CFM protocol message can be processed and responded. The maintenance set and the maintenance domain to which the intermediate point belongs are maintained, and the VLAN attribute and the level of the message received by the maintenance intermediate point are determined. The maintenance center point can work with the maintenance endpoint to perform the functions similar to the ping and tracert. Similar to the maintenance endpoint, when the maintenance intermediate point receives the message above its own level, it will not be processed, but it is forwarded according to the original path; and when the maintenance intermediate point receives the message that is less than or equal to its own level, it will be processed.

As shown in figure 1 / 4, it is a hierarchical configuration of CFM, assuming that all six devices have only two ports, and that maintenance endpoints and maintenance midpoints are configured on some of these ports, such as the maintenance points on port 1 of Device B as follows: maintenance midpoint at level 5, inward maintenance endpoint at level 3, inward maintenance endpoint at level 2 and outgoing maintenance endpoint at level 0. There are four levels of maintenance domain in the figure, the level of maintenance domain with large identification number is high and the control range is wide, and the level of maintenance domain with small identification number is low and the control range is small.

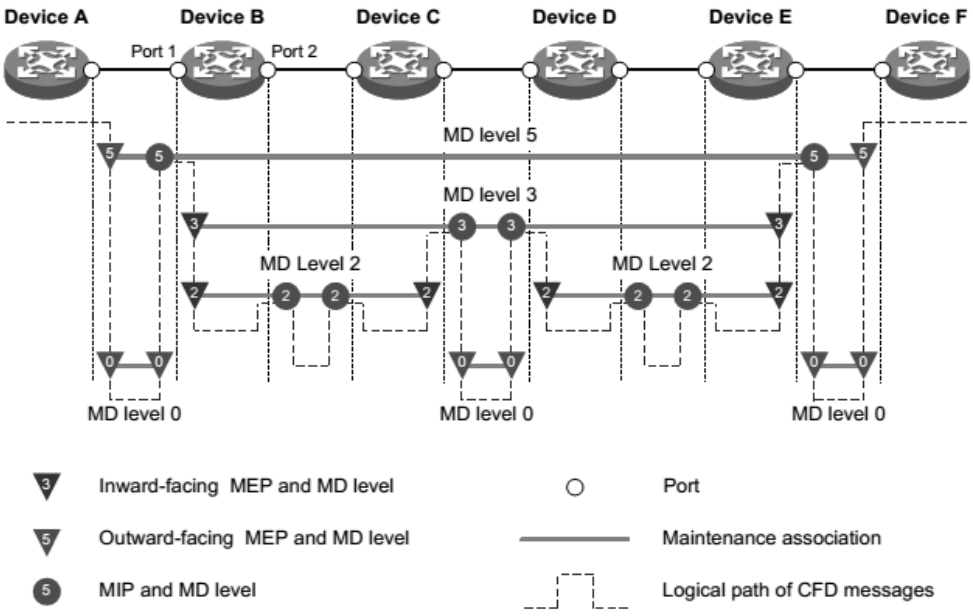


Figure 1-4 Hierarchical configuration of maintenance point

4 Maintain the list of end points

The maintenance endpoint list is a collection of local maintenance endpoints that are allowed to be configured in the same maintenance set and remote maintenance endpoints to be monitored. It limits the selection range of maintenance terminals in the maintenance set: all maintenance terminals in the same maintenance set on different devices should be included in this list, and MEP ID does not repeat each other. If the maintenance endpoint receives a CCM (Continuity Check Message, continuity detection message from the remote device) the maintenance endpoint carried by the message is not in the maintenance endpoint list of the same maintenance set, the message is discarded.

5 Service instance

A service instance is represented by an integer and represents a maintenance set within a maintenance domain. The maintenance domain and maintenance set determine the level attributes and VLAN attributes of the messages processed by the maintenance points within the service instance.

26.1.2 CFM function

The effective application of communication error detection is based on a reasonable network deployment and configuration. Its function is implemented between the configured maintenance points, including:

- （Continuity Check，CC）
- （Loopback，LB）
- （Linktrace，LT）

1. Continuity detection function

The continuity detection function is used to detect the communication state between the maintenance endpoints. The connectivity failure may be caused by a device failure or a configuration error. The implementation mode of the function is that the CCM message is periodically sent by the maintenance endpoint, the message is a multicast message, and other maintenance endpoints of the same maintenance set receive the message, and thus the remote state is known. If the maintenance endpoint does not receive the CCM message from the remote maintenance endpoint within the 3.5 CCM message transmission period, the link has a problem and the log report will be output. when a plurality of maintenance endpoints in the maintenance domain are sending a CCM

message, the link detection between the multi-point and the multi-point is realized.

2. Loopback function

The loopback function is similar to the ping function of the IP layer, which is used to verify the connection status between the local device and the remote device. The implementation of this function is to send the LBM (Loopback Message, loopback message by the maintenance endpoint to the remote maintenance point, and to verify the link state according to whether the LBR (Loopback Reply, loopback reply message can be received from the opposite end. LBM and LBR are unicast messages.

3. Link tracking function

The link tracking function is used for determining the path of the source end to the target maintenance end point, And the source end of the link tracking response message is sent to the source end, and the source end determines the path to the target maintenance end point according to the received LTR. LTM is a multicast message, and the LTR is a unicast message.

26.2 Introduction to CFM Configuration Tasks

Before configuring the CFM feature, the network should be planned as follows:

- The maintenance domain of the whole network is graded and the boundary of each dimension protection domain is determined.
- The name of each maintenance domain is determined and the same maintenance domain is the same name on the different device.
- Determine the maintenance set within each maintenance domain according to the VLAN, that needs to be monitored.
- The name of each maintenance set is determined, and the name of the same maintenance set on different devices is the same in the same maintenance domain.
- Maintenance end points should be planned on the boundary ports of the maintenance domain and maintenance set, and maintenance midpoints can be planned on the non-boundary devices or ports.
- Determines the end-of-end maintenance endpoint list for the maintenance endpoint.

After completing the network planning, make the following configuration.

Configuration task		Explain	Detailed configuration
CFM Foundation Configuration	Enable CFM functionality		0
	Configure Service Instances		0
	Configure maintenance endpoints		錯誤! 找不到參照來源。
	Configure maintenance center point		0
Configure CFM functions	Configuration continuity detection function		錯誤! 找不到參照來源。

	Configure Loopback		錯誤! 找不到參照來源。
	Configure Link Tracking		錯誤! 找不到參照來源。

Note:

- The port blocked by STP protocol can not receive, send and respond to CFM protocol message, but if the port is configured as outgoing MEP, it will still receive and send CCM message even if the port is blocked by STP protocol.
- Only Ethernet ports support configuring CFM functionality.

26.3 CFM Foundation Configuration

26.3.1 Enable CFM function

Order	Description	CLI mode
cfm enable	Enable CFM function. Closed by default.	Configuration mode

26.3.2 Configure Service Instances

The service instance must be configured first before configuring the maintenance endpoint and maintaining the intermediate point. A service instance is represented by an integer representing a maintenance set within a maintenance domain. The maintenance domain and the maintenance set determine the level and VLAN properties of the message handled by the maintenance point within the service instance.
Use the following order to create a maintenance domain, a maintenance set, and a service instance in this order.

Order	Description	CLI mode
cfm md <md-name> level <level-value>	Create a maintenance domain. There is no maintenance domain by default.	Configuration mode
cfm ma <ma-name> md <md-name> vlan <vlan-id>	Create a maintenance set. The maintenance set was not created by default	Configuration mode
cfm service-instance <instance-id> md <md-name> ma <ma-name>	Create a service instance. The default does not create a service instance.	Configuration mode

26.3.3 Configure maintenance endpoints

The maintenance endpoint is the functional entity in the service instance. The CFM function is mainly embodied in the operation of the maintenance endpoint, which

implements the functions of CC, LB and LT, and alarms the error CCM message and the cross connection. Since the maintenance endpoint is configured on the service instance, the level of the maintenance domain represented by the service instance and the VLAN properties naturally become the attributes of the maintenance endpoint.
After the maintenance endpoint is created, you need to configure the list of remote maintenance endpoints that specify the maintenance endpoint, which is a collection of remote maintenance endpoints that need to be monitored within the same maintenance set.

Order	Description	CLI mode
cfm mep <mep-id> service-instance <instance-id> {inbound | outbound}	Create a maintenance endpoint. There is no maintenance endpoint on the default port.	Interface mode
cfm remote-meplist <mep-list> service-instance <instance-id> mep <mep-id>	Configure the remote maintenance endpoint list for the specified maintenance endpoint. The default port does not have a list of maintenance endpoints.	Interface mode
cfm mep service-instance <instance-id> mep <mep-id> enable	Enable the maintenance endpoint. The default maintenance endpoint is in a closed state.	Interface mode

Note:
- When the endpoint is enabled, the maintenance endpoint processes the received CCM message.

26.3.4 Configure maintenance center point

The maintenance midpoint is a functional entity in the service instance that responds to LBM and LTM messages.

The maintenance midpoint is automatically created on each port according to the rules, and its creation rules are as follows: if there is no maintenance midpoint on the port, check the maintenance set in each maintenance domain in order from low to high, and decide whether to create the maintenance midpoint (within the same VLAN) according to the process shown in figure 1 / 5.

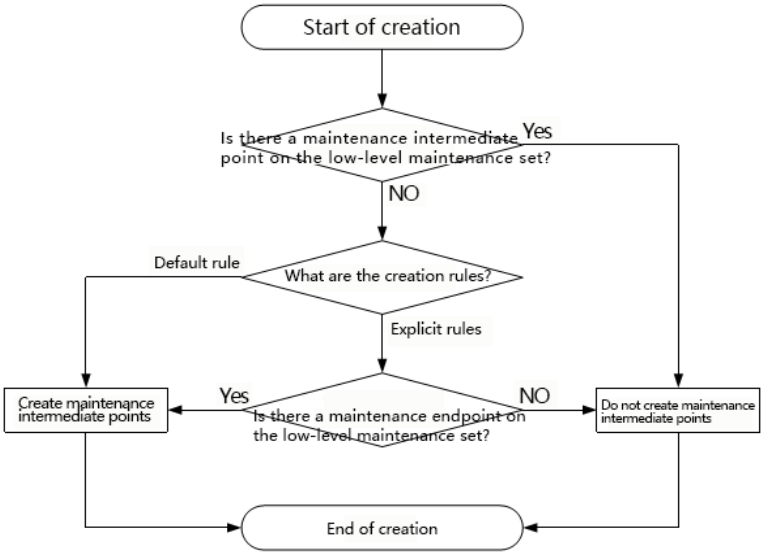


Figure 1 / 5 maintenance midpoint creation process

Please maintain the creation rules of the midpoint according to the planning configuration of the network.

Order	Description	CLI mode
cfm mip-rule {explicit | default} service-instance <instance-id>	Configure the creation rules for maintaining midpoints. By default, there are no creation rules to maintain midpoints, nor do they exist to create maintenance midpoints.	Configuration mode

Note:

After you configure the creation rules for maintaining midpoints, any of the following conditions can trigger the creation or deletion of maintenance midpoints:

- Enable CFM functionality
- Create or remove maintenance endpoints on a port
- The VLAN property of the port changes
- The creation rule for maintaining an intermediate point changes

26.4 Configure CFM function

The CFM's basic configuration needs to be completed before the CFM features are configured.

26.4.1 Configuration continuity detection function

By configuring the continuity detection function, the CCM messages can be sent between the maintenance terminals to detect the connectivity between these maintenance terminals, so as to realize the management of link connectivity.

Order	Description	CLI mode
cfm cc interval <interval-value> service-instance <instance-id>	Enables the maintenance of the CCM message sending function of the endpoint. By default, the CCM message sending function of the maintenance endpoint is turned off.	Configuration mode
cfm cc service-instance <instance-id> mep <mep-id> enable	Configure the value of the time interval field in the CCM message sent by the maintenance endpoint. By default, the value of the time interval field in the CCM message sent by the maintenance endpoint is 4.	Interface mode

The relationship between the value of the interval domain (interval domain) in the CCM message sent by the endpoint and the CCM sending time is maintained, and the relationship between the remote MEP timeout is shown in Table 26 ≤ 1.

Time interval field value	CCM sending time interval	Remote MEP timeout time
3	100 milliseconds	350milliseconds
4	1 second	3.5 second
5	10 second	35 second
6	60 second	210 second
7	600 second	2100 second

Table 26-1 The relationship between the value of the time interval field and the CCM transmission time interval and the remote MEP time-out time.

Note:

- When different devices are in the same maintenance domain and maintenance center, the interval between sending CCM messages must be the same.
- If the value of the time interval domain in which the CCM message is sent by the configuration maintenance endpoint is 3, it is recommended that too many maintenance terminals should not be configured in the same maintenance domain and maintenance set, otherwise the performance of the whole machine will be affected.

26.4.2 Configure Loopback

By configuring the loopback function, the link status can be checked to verify the link connectivity.

Order	Description	CLI mode
cfm loopback service-instance <instance-id> mep <mep-id> { target-mep <target-mep-id> | target-mac <mac-address> } [number <number>]	Enable loopback to check link status.	Privilege mode

26.4.3 Configure Link Tracking

By configuring the link tracking feature, you can find the path between the specified maintenance endpoint and the destination maintenance endpoint to locate the link failure. It includes the following two functions:

- Find the path from the specified maintenance endpoint to the destination maintenance endpoint: determine the path between devices by sending LTM messages from the specified maintenance endpoint to the destination maintenance endpoint and detecting the responding LTR message.
- Automatic link tracking message: after enabling this function, when the maintenance endpoint does not receive the CCM message from the remote maintenance endpoint in the 3.5 CCM message sending cycle, so as to determine that the connection between the remote maintenance endpoint and the remote maintenance endpoint is wrong, the LTM message will be sent (the target of the LTM message is the remote maintenance endpoint, and the TTL field in the LTM message is the maximum value of 255. the fault will be located by detecting the LTR message of the response).

Order	Description	CLI mode
cfm linktrace service-instance <instance-id> mep <mep-id> {target-mep <target-mep-id> | target-mac <mac-address> } [ttl <ttl-value>] [hw-only]	Finds the path from the specified maintenance endpoint to the destination maintenance endpoint.	Privilege mode
cfm linktrace auto-detection [size <size-value>]	And the automatic transmission link tracking message function is enabled. By default, the automatic transmission link tracking message function is in the off state.	Configuration mode

26.5 CFM display and maintenance

After completing the above configuration, executing the show command in any view can display the operation of the CFM after the configuration, and verify the effect of the configuration by viewing the display information.

Order	Description	CLI mode
show cfm status	Displays the enabled state of the CFM.	Privilege mode
show cfm md	Display configuration information for the maintenance domain	Privilege mode
show cfm ma [[<ma-name>] md <md-name>]	Display configuration information for the maintenance set	Privilege mode

show cfm service-instance [<instance-id>]	Display configuration information for the service instance	Privilege mode
show cfm mp [interface <interface-name>]	Display information about maintenance points	Privilege mode
show cfm mep <mep-id> service-instance <instance-id>	Displays the properties and operation information for the maintenance endpoint	Privilege mode
show cfm linktrace-reply [service-instance <instance-id> [mep <mep-id>]]	Displays the LTR message information obtained on the maintenance endpoint	Privilege mode
show cfm remote-mep service-instance <instance-id> mep <mep-id>	Displays information for the remote maintenance endpoint	Privilege mode
show cfm linktrace-reply auto-detection [size <size-value>]	The content of the LTR message received by the automatic transmission of the LTM message is displayed	Privilege mode

26.6 Typical configuration example

Networking requirements:

The network composed of five devices is divided into two maintenance domains of MD _ A and MD _ B. The levels are 5 and 3, respectively. The respective ports, Ethernet1/0/1-Ethernet1/0/4 of each device belong to VLAN 100, and the maintenance set in each maintenance domain is served on the VLAN.

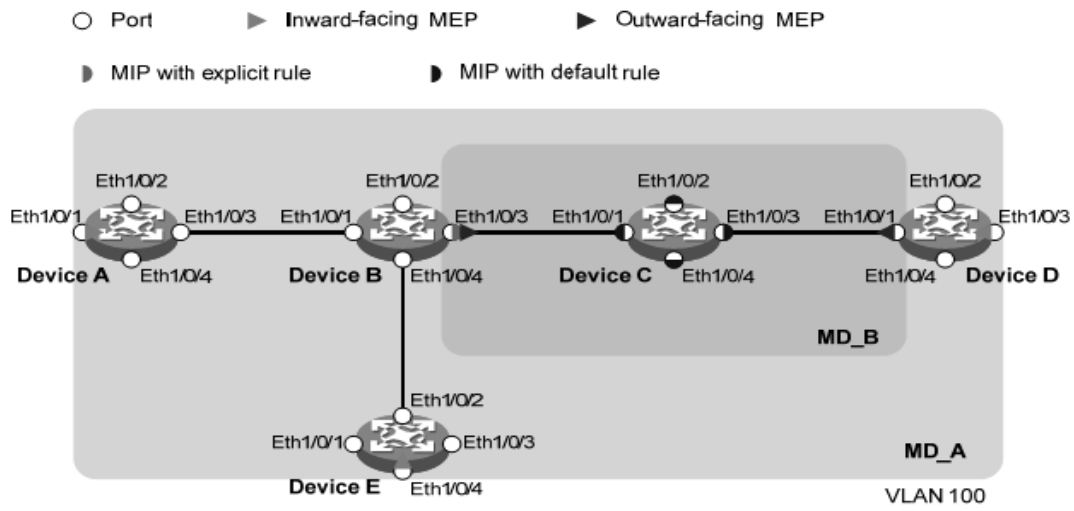
The boundary port of MD _ A is the Ethernet1/0/1 of Device A, and the Ethernet1/0/4 of Device D, and the inward maintenance endpoint is configured on these ports; the boundary port of MD _ B is Ethernet1/0/3 of Device B and Ethernet1/0/1 of Device D, and the outgoing maintenance endpoint is configured on these ports.

The maintenance midpoint of MD_A is required to be planned on Device B and configured only if there is a low-level maintenance endpoint on the port. According to this plan, because the maintenance endpoint of MD_B is configured on the Ethernet1/0/3 of Device B, the maintenance midpoint of MD_A needs to be configured on Device B, and its creation rule is Explicit rule.

The maintenance center point of MD _ B is required to be planned on Device C and configured on all of its ports. According to this plan, configure the maintenance center point for MD _ B on Device C, and its creation rule is the Default rule.

It is required to detect the connectivity between all maintenance endpoints in MD_A and MD_B by using the continuity detection function, to use the loopback function for fault location when a link fault is detected, or to use the link tracking function for path finding or fault location after obtaining the status of the entire network.

Networking diagram:



Configuration steps:

Configuring VLANs and Ports

1）Create VLAN 100 on each device and configure port Ethernet1/0/1 to Ethernet1/0/4 to belong to VLAN 100.

2）Enable CFM functionality

Enable CFM functionality on Device A.

```
DeviceA> config t
[DeviceA] cfm enable
```

The configuration of Device B ~ Device E is similar to Device A and the configuration process is omitted.

3) Configure Service Instances

Create maintenance domain MD _ A with level 5 on Device A, create maintenance set MA _ A for VLAN 100 in MD _ A, and create service instance 1 for MD _ A and MA _ A

```
[DeviceA] cfm md MD_A level 5
[DeviceA] cfm ma MA_A md MD_A vlan 100
[DeviceA] cfm service-instance 1 md MD_A ma MA_A
```

The configuration of Device E is similar to Device A and the configuration process is omitted.

Create a maintenance domain MD_A, with level 5 on Device B to create a maintenance set MA_A, serving VLAN 100 in MD_A and create service instances 1 for MD_A and MA_A; then create a maintenance domain MD_B, with level 3 to create a maintenance set MA_B, serving VLAN 100 in MD_B and create service

instances for MD_B and MA_B.
[DeviceB] cfm md MD_A level 5
[DeviceB] cfm ma MA_A md MD_A vlan 100
[DeviceB] cfm service-instance 1 md MD_A ma MA_A
[DeviceB] cfm md MD_B level 3
[DeviceB] cfm ma MA_B md MD_B vlan 100
[DeviceB] cfm service-instance 2 md MD_B ma MA_B
The configuration of Device D is similar to that of Device B, and the configuration process is slightly.

Create maintenance domain MD_B, with level 3 on Device C create maintenance set MA_B, serving VLAN 100 in MD_B and create service instances 2 for MD_B and MA_B
[DeviceC] cfm md MD_B level 3
[DeviceC] cfm ma MA_B md MD_B vlan 100
[DeviceC] cfm service-instance 2 md MD_B ma MA_B

4) Configure and maintain the endpoint
Create an inward maintenance endpoint 1001 within service instance 1 on the DeviceA port Ethernet1/0/1, configure the remote maintenance endpoint list corresponding to the maintenance endpoint 1001, and then enable the maintenance endpoint 100.1.
[DeviceA] interface ethernet 1/0/1
[DeviceA-Ethernet1/0/1] cfm mep 1001 service-instance 1 inbound
[DeviceA-Ethernet1/0/1] cfm remote-meplist 4002 5001 service-instance 1 mep 1001
[DeviceA-Ethernet1/0/1] cfm mep service-instance 1 mep 1001 enable
[DeviceA-Ethernet1/0/1] quit
Create the outbound maintenance endpoint 2001 within the service instance 2 on the DeviceB port, Ethernet1/0/3, configure the remote maintenance endpoint list corresponding to the maintenance endpoint 2001, and then enable the maintenance endpoint 2001.
[DeviceB] interface ethernet 1/0/3
[DeviceB-Ethernet1/0/3] cfm mep 2001 service-instance 2 outbound
[DeviceB-Ethernet1/0/3] cfm remote-meplist 2001 4001 service-instance 2 mep 2001
[DeviceB-Ethernet1/0/3] cfm mep service-instance 2 mep 2001 enable
[DeviceB-Ethernet1/0/3] quit
Create the outbound maintenance endpoint 4001 within the service instance 2 on the port Ethernet1/0/1 on Device D, configure the remote maintenance endpoint list corresponding to the maintenance endpoint 4001, and then enable the maintenance endpoint 4001.

Create and enable introversion maintenance endpoint 4002 within service instance 1 on port Ethernet1/0/3, while creating a list of remote maintenance endpoints for 4002.
[DeviceD] interface ethernet 1/0/1
[DeviceD-Ethernet1/0/1] cfm mep 4001 service-instance 2 outbound
[DeviceD-Ethernet1/0/1] cfm remote-meplist 2001 service-instance 2 mep 4001
[DeviceD-Ethernet1/0/1] cfm mep service-instance 2 mep 4001 enable
[DeviceD-Ethernet1/0/1] quit
[DeviceD] interface ethernet 1/0/3
[DeviceD-Ethernet1/0/3] cfm mep 4002 service-instance 1 inbound
[DeviceD-Ethernet1/0/3] cfm remote-meplist 1001 5001 service-instance 1 mep 4002
[DeviceD-Ethernet1/0/3] cfm mep service-instance 1 mep 4002 enable
[DeviceD-Ethernet1/0/3] quit
On the port Ethernet1/0/4 of Device E, create and enable the inward maintenance endpoint 5001 in service instance 1 and configure the remote maintenance endpoint

list in service instance 1.

```
[DeviceE] interface ethernet 1/0/4
[DeviceE-Ethernet1/0/4] cfm mep 5001 service-instance 1 inbound
[DeviceE-Ethernet1/0/4] cfm remote-meplist 1001 service-instance 1 mep 5001
[DeviceE-Ethernet1/0/4] cfm mep service-instance 1 mep 5001 enable
[DeviceE-Ethernet1/0/4] quit
```

5) Configure maintenance center point

Within service instance 1 of Device B, configure the creation rule for the maintenance midpoint to be the Explicit rule.

```
[DeviceB] cfm mip-rule explicit service-instance 1
```

within service instance 2 of Device C, configure the creation rule for maintenance midpoint to be Default rule.

```
[DeviceC] cfm mip-rule default service-instance 2
```

6) Configuration continuity detection function

The CCM message sending function of endpoint 1001 is maintained on port Ethernet1/0/1 of Device A on service instance 1.

```
[DeviceA] interface ethernet 1/0/1
[DeviceA-Ethernet1/0/1] cfm cc service-instance 1 mep 1001 enable
[DeviceA-Ethernet1/0/1] quit
```

The CCM message sending function of the maintenance endpoint 2001 in the service instance 2 is enabled on the port Ethernet1/0/3 of the Device B.

```
[DeviceB] interface ethernet 1/0/3
[DeviceB-Ethernet1/0/3] cfm cc service-instance 2 mep 2001 enable
[DeviceB-Ethernet1/0/3] quit
```

Maintains the CCM message sending function of endpoint 4001 in port Ethernet1/0/1 of Device D and the CCM message sending function of endpoint 4002 in port Ethernet1/0/3.

```
[DeviceD] interface ethernet 1/0/1
[DeviceD-Ethernet1/0/1] cfm cc service-instance 2 mep 4001 enable
[DeviceD-Ethernet1/0/1] quit
[DeviceD] interface ethernet 1/0/3
[DeviceD-Ethernet1/0/3] cfm cc service-instance 1 mep 4002 enable
[DeviceD-Ethernet1/0/3] quit
```

The CCM message sending function of endpoint 5001 is maintained on port Ethernet1/0/4 of Device E.

```
[DeviceE] interface ethernet 1/0/4
[DeviceE-Ethernet1/0/4] cfm cc service-instance 1 mep 5001 enable
[DeviceE-Ethernet1/0/4] quit
```

7) Check the configuration effect

When link failure is detected by continuity detection function, loopback function can be used for fault location. For example:

Enable loopback on Device A to check the link status of the maintenance endpoint 1001 to 5001 within service instance 1.

```
[DeviceA] cfm loopback service-instance 1 mep 1001 target-mep 5001
Loopback to 0010-FC00-6512 with the sequence number start from 43404:
Reply from 0010-FC00-6512: sequence number = 43404
Reply from 0010-FC00-6512: sequence number=43405
Reply from 0010-FC00-6512: sequence number=43406
Reply from 0010-FC00-6512: sequence number=43407
Reply from 0010-FC00-6512: sequence number=43408
Send:5 Received:5 Lost:0
```

After obtaining the status of the whole network through the continuity detection function, the link tracking function can be used for path finding or fault location.

For example: # Find the path to maintain endpoints 1001 to 5001 in service instance 1 of Device A.

```
[DeviceA] cfm linktrace service-instance 1 mep 1001 target-mep 5001
Linktrace to MEP 5001 with the sequence number 1001-43462
MAC Address          TTL          Last MAC          Relay Action
0010-FC00-6512       63           0010-FC00-6511    Hit
0010-FC00-6511       62           0010-FC00-6510    FDB
```

Chapter 27 IPv6 Basic Configuration

The switch supports basic IPv6 features, including IPv6 2-layer forwarding, and IPv6 ND features. This chapter describes how to configure IPv6, mainly including the following:

- Introduction to IPv6
- Configure basic IPv6 functions
- Configure IPv6 neighbor Discovery Protocol
- Display and maintenance of IPv6

27.1 Brief introduction to IPv6

IPv6 (Internet Protocol Version 6, Internet Protocol version 6) is the second generation standard protocol of Network layer Protocol, also known as IPng (IP Next Generation, next Generation Internet). It is a set of specifications designed by the IETF (Internet Engineering Task Force,Internet Engineering Task Force and is an upgraded version of IPv4. The most significant difference between IP and IPv4 is that the length of IP address increases from 32 bits. Add to 128 bits.

27.1.1 IPv6 protocol features

1 Simplified message header format

By reducing or moving some fields in the IPv4 header to the extended header, the length of the IPv6 basic header is reduced. IPv6 uses a fixed length basic header, which simplifies the processing of the IPv6 message by the forwarding device and improves the forwarding efficiency. Although the length of the IPv6 address is four times the length of the IPv4 address, the length of the IPv6 base header is only 40 bytes, twice the length of the IPv4 header (excluding option fields).

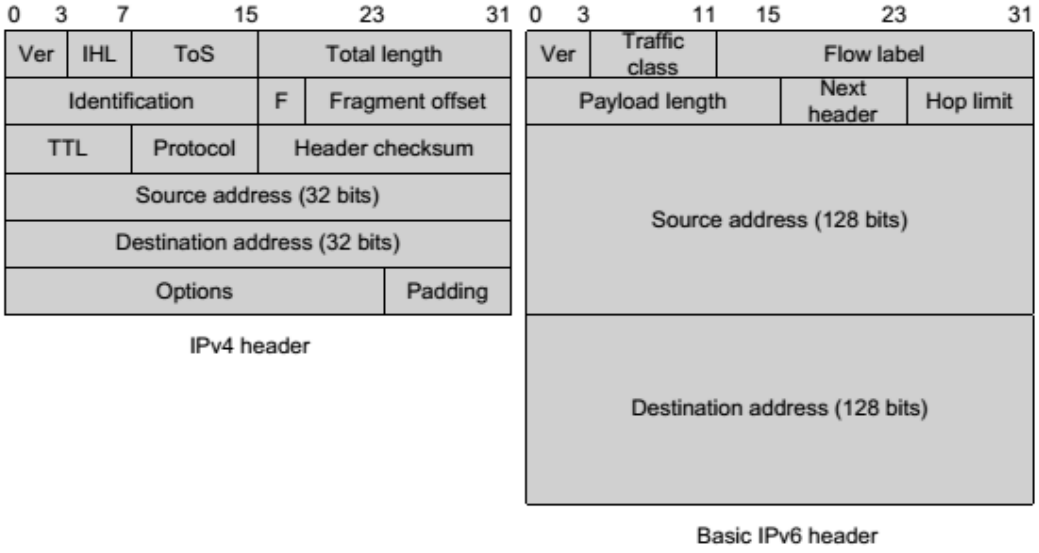


Figure 1 comparison of IPv4 header and IPv6 basic header format

2 Adequate address space

The MTU option is used in RA messages to ensure that all nodes on the link use the

same MTU value, mainly when the node may not be aware of the link MTU. Other Neighbor Discovery messages must silently ignore this option.

3 Hierarchical address structure

The address space of IPv6 adopts hierarchical address structure, which is beneficial to fast routing lookup. at the same time, it can effectively reduce the system resources occupied by IPv6 routing table with the help of routing aggregation.

4 Address automatic configuration

To simplify host configuration, IPv6 supports stateful address configuration and stateful address configuration:

1) Stateful address configuration refers to obtaining IPv6 address and related information from server (such as DHCP server);

2) Stateless address configuration refers to the automatic configuration of IPv6 address and related information by the host according to its own link layer address and the prefix information published by the router.

At the same time, the host may also form a link local address based on its own link layer address and the default prefix (FE80::/10) to enable communication with other hosts on the link.

5 Built-in security

IPv6 uses IPSec as its standard extension to provide end-to-end security features. This feature also provides standards for addressing network security issues and improves interoperability between different IPv6 applications.

6 Support QoS

The flow label field of IPv6 header realizes the identification of traffic, which allows the device to identify the message in a certain class and provide special processing.

7 Enhanced neighbor discovery mechanism

The neighbor discovery protocol of IPv6 is implemented by a set of ICMPv6 (Internet Control Message Protocol for IPv6,IPv6 Internet control message protocols, which manages the interaction of information between neighbor nodes (that is, nodes on the same link). It replaces ARP (Address Resolution Protocol, address resolution protocol), ICMPv4 routers discover and ICMPv4 redirect messages, and provide a series of other

features.

8 Flexible extended header

IPv6 cancels the option field in IPv4 header and introduces a variety of extended header, which not only improves the processing efficiency, but also greatly enhances the flexibility of IPv6 and provides a good extension ability for IP protocol. The option field in IP header is only 40 bytes at most, while the size of IPv6 extension header is only limited by the size of IP message.

27.1.2 IPv6 Address Introduction

1. IPv6 address representation

The IPv6 address is expressed as a series of 16-bit hexadecimal numbers separated by a colon (:). Each IPv6 address is divided into 8 groups, and 16 bits of each group are represented by 4 hexadecimal numbers, and the groups are separated by colons, such as 2001:0000: 130F:0000:0000: 09C0: 876A: 130B.

To simplify the representation of IPv6 addresses,"0" in IPv6 addresses can be handled as follows:

1) The leading "0" in each group can be omitted, that is, the above address can be written as 2001 / 0130F / 009C0 / 876A / 130B.

2) If the address contains two or more consecutive groups of 0, it can be replaced by a double colon "::", that is, the above address can be written as 2001 / 0130F / 9C0 / 876A / 130B.

Note:

Only one double colon "::" can be used in an IPv6 address, otherwise the number of "::" represented by "::" will not be determined when the device converts "::" to 0 to restore the 128-bit address.

IPv6 address consists of two parts: address prefix and interface identification. The address prefix is equivalent to the network number field part of the IPv4 address, and the interface identity is equivalent to the host number part of the IPv4 address.

The address prefix is represented by: IPv6 address / prefix length. Where the IPv6 address is any of the forms listed earlier, and the prefix length is a decimal number,

indicating how many leftmost bits of the IPv6 address are the address prefix.

2 Address classification of 2 IPv6

IPv6 has three types of addresses: unicast, multicast, and anycast addresses.

unicast address: used to uniquely identify an interface, similar to the unicast address of IPv4. The data message sent to the unicast address will be transmitted to the interface identified by the address.

Multicast address: used to identify a set of interfaces (usually this group of interfaces belong to different nodes), similar to the multicast address of IPv4. Data messages sent to a multicast address are transmitted to all interfaces identified by this address.

anycast address: used to identify a set of interfaces (usually this group of interfaces belong to different nodes). A data message sent to an anycast address is transmitted to an interface in a set of interfaces identified by this address that is nearest to the source node (measured according to the routing protocol used).

There is no broadcast address in IPv6, and the function of broadcast address is realized by multicast address.

The IPv6 address type is specified by the first few bits of the address (called format prefix). The corresponding relationship between the main address type and the format prefix is shown in Table 1.

Address type		Format Prefix (binary)	IPv6 Prefix Identification
Unicast address	Unspecified address	000...0(128bits)	::/128
	The loopback address	000...1(128bits)	::1/128
	Link-local address	1111111010	FE80::/10
	Site local address	1111111011	FEC0::/10
	Global unicast address		-
Multicast address		11111111	FF00::/8
As a multicast address		Assignment from a unicast address space using the unicast address format	

Table 1-1 correspondence between address Type and format prefix

3 Type of unicast address

There are many types of IPv6 unicast addresses, including global unicast addresses, link local addresses and site local addresses.

1) The global unicast address is equivalent to the IPv4 public network address and is provided to the network service provider. This type of address allows the aggregation of routing prefixes, thus limiting the number of global routing table items.

2) The link local address is used for communication between the neighbor discovery protocol and the node on the link local in the stateless automatic configuration. Data messages using link local addresses as source or destination addresses are not forwarded to other links.

3) The site local address is similar to the private address in the IPv4. The data message using the site local address as the source or destination address is not forwarded to other sites outside the site (equivalent to a private network).

4) Loopback address: unicast address 0:0:0:0:0:0:0:1 (simplified representation is:1) is called a loopback address and cannot be assigned to any physical interface. Its role is the same as the loopback address in IPv4, that is, the node is used to send an IPv6 message to itself.

5) The address is not specified: The address "::" is called an unspecified address and cannot be assigned to any node. Before the node obtains a valid IPv6 address, the address can be filled in the source address field of the sent IPv6 message, but cannot be used as the destination address in the IPv6 message.

4 Multicasting address

The multicast address shown in Table 1 / 2 is the reserved special purpose multicast address.

Address	Application
FF01::1	Node Local range Multicast address of all nodes
FF02::1	Multicast address of all nodes in the link-local range
FF01::2	Multicast addresses of all routers in the local range of the node
FF02::2	Link-local range multicast addresses of all routers
FF05::2	Multicast addresses of all routers in the local range of the site

Table 1 / 2 list of IPv6 multicast addresses reserved.

In addition, there is a kind of multicast address: requested node (Solicited-Node) address. The address is mainly used to obtain the link layer address of the neighbor node on the same link and to realize duplicate address detection. Each unicast or anycast IPv6 address has a corresponding requested node address. The format is: FF02:0:0:0:0:1:FFXX:XXXX

Where FF02:0:0:0:0:1: FF is a 104-bit fixed format; XX: XXXX is the last 24 bits of the unicast or anycast IPv6 address.

5 IEEE EUI-64-format interface identifier

The interface identifiers in the IPv6 unicast address are used to identify a unique interface on the link. At present, IPv6 unicast addresses basically require that the interface identifiers be 64 bits. The interface identifiers in IEEE EUI-64 format are changed from the link layer address (MAC address) of the interface. The interface identifiers in the MAC address are 64 bits, while the MAC address is 48 bits, so it is necessary to insert the hexadecimal number FFFE (1111111111111110) in the middle of the MAC address (after the 24th bit from the high level). To make sure this comes from the MAC The interface identifiers obtained by the address are unique, and the Universal/Local (U ≤ L) bit (the seventh bit from the high level) is set to "1". The final set of numbers is used as interface identifiers in EUI-64 format.

Figure 1 / 2 conversion of MAC addresses to EUI-64 format interface identifiers

27.1.3 IPv6 Neighbor Discovery Protocol Introduction

The IPv6 neighbor discovery protocol uses five types of ICMPv6 messages to implement some of the following features: address resolution, verify neighbor access, repeat address detection, router discovery/ prefix discovery, address auto-configuration, and redirection.

The type and role of ICMPv6 messages used by the neighbor discovery protocol are shown in Table 1-3.

ICMPv6 message	Type no	role
NeighborSolicitation (NS)	135	Obtain the link layer address of the neighbor
		Verify that the neighbor is reachable
		Repeat address detection
Neighbor Advertisement (NA)	136	Responds to NS messages
		When the link layer changes, a node proactively sends an NA message to notify its neighbor node of the change
Router Solicitation (RS)	133	After the node is started, it sends a request to the router via RS message, requesting the prefix and other configuration information for automatic configuration of the node
Router Advertisement (RA)	134	Respond to RS messages
		If RA messages are not suppressed, the router periodically advertises RA messages, including prefix information options and flag bits
Redirect Messages	137	When certain conditions are met, the default gateway sends a redirection message to the source host to enable the host to select a correct next hop address for sending subsequent packets

Table 1 / 3 types and functions of ICMPv6 messages used by neighbor Discovery Protocol

The main functions provided by the neighbor discovery protocol are as follows:

1 Address resolution

Get the link layer address of the neighbor node on the same link (the same function as the ARP of IPv4), and implement it through the neighbor request message NS and the neighbor notification message NA. As shown in figure 1 / 3, Node A wants to get the link layer address of Node B.

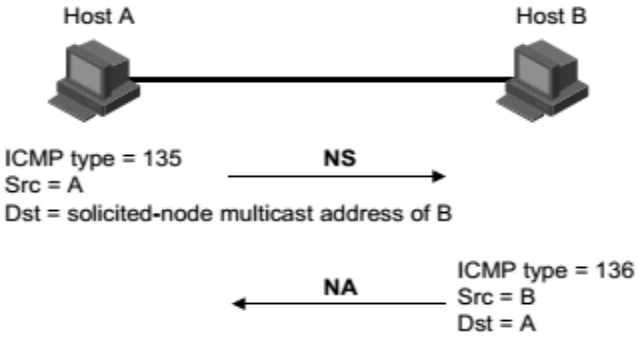


Figure 1 / 3 address resolution schematic diagram

(1) Node A sends NS message by multicasting. The source address of NS message is the interface IPv6 address of node A, and the destination address is the requested node multicast address of node B. the message content contains the link layer address of node A.

(2) after node B receives the NS message, it determines whether the destination address of the message is the requested node multicast address corresponding to its own IPv6 address. If so, node B can learn the link layer address of node A and return the NA message as unicast, which contains its own link layer address.

(3) The node A can obtain the link layer address of the node B from the received NA message.

2 Verify that neighbors are reachable

After obtaining the link layer address of the neighbor node, the neighbor node can be verified by the neighbor request message NS and the neighbor notification message NA.

(1) The node sends an NS message, where the destination address is the IPv6 address of the neighbor node.

(2) If the acknowledgement message of the neighbor node is received, the neighbor is considered reachable; otherwise, the neighbor is considered to be unreachable.

3 Duplicate address detection

When a node has acquired an IPv6 address, it is necessary to use the duplicate address detection function to determine if the address has been used by other nodes (similar to the free ARP feature of IPv4). Duplicate address detection can be achieved by NS and NA, as shown in Figure 1-4.

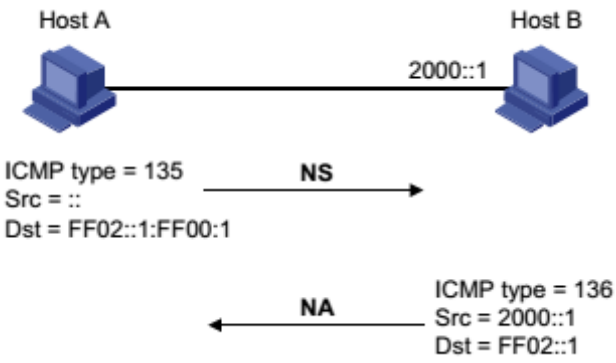


Figure 1-4 Schematic diagram of duplicate address detection

(1) The node A sends the NS message, the source address of the NS message is the unspecified address:, the destination address is the requested node multicast address corresponding to the IPv6 address to be detected, and the message content contains the IPv6 address to be detected.

(2) If node B already uses this IPv6 address, the NA message is returned. It contains its own IPv6 address.

(3) Node A receives the NA message from Node B and knows that the IPv6 address has been used. On the contrary, the address is not used and node A can use this IPv6 address.

4 Router discovery/ prefix discovery and address auto-configuration

The router discovery/ prefix discovery is the prefix of the neighbor router and the network in which the node is derived from the received RA message, as well as other configuration parameters.

The address-free automatic configuration means that the node automatically configures the IPv6 address based on the information acquired by the router discovery/ prefix discovery. The router discovery/ prefix discovery is implemented by the router request message RS and the router advertisement message RA, as follows:

(1) when the node starts, a request is made to the router through the RS message to request the prefix and other configuration information for the configuration of the node.

(2) the router returns the RA message, including the prefix information option (the router also publishes the RA message periodically).

(3) the node automatically configure the IPv6 address and other information of the interface by using the address prefix and other configuration parameters in the RA message returned by the router.

- The prefix information option includes not only address prefix information, but also preferred lifetime (preferred lifetime) and valid lifetime (valid lifetime). For the address prefix When a periodically sent RA message is received, the preferred

lifetime and valid lifetime of the prefix are updated according to the message.

- During the effective lifetime, the automatically generated address can be used normally; after the effective life period expires, the automatically generated address will be deleted.

5 Redirection function

When the host is started, it may have only one default route to the default gateway in its routing table. When certain conditions are met, the default gateway sends an ICMPv6 redirect message to the source host informing the host to select a better next hop for subsequent message transmission (the same function as the ICMP redirect message for IPv4).

- The device sends an ICMPv6 redirect message to the host when the following conditions are met;
- The interface of receiving and forwarding the data message is the same interface;
- The selected route itself has not been created or modified by the ICMPv6 redirect message;
- The selected route is not the default route;
- The forwarded IPv6 data message does not contain routing extension header.

27.1.4 IPv6 PMTU discovery

The links passing through the transmission path from the source end to the destination end may have different mtu. In the IPv6, when the length of the message is larger than the MTU of the link, the fragment of the message is carried out at the source end, so that the processing pressure of the intermediate forwarding device is reduced, and the network resource is reasonably utilized.

The purpose of the PMTU (Path MTU, path MTU) discovery mechanism is to find the working process of the smallest MTU.PMTU on the path from the source to the destination, as shown in figure 1 and 5.

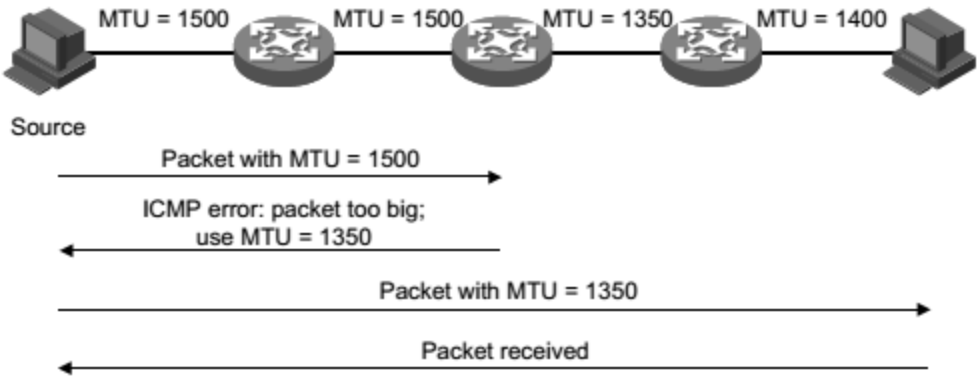


Figure 1 / 5 PMTU Discovery work process

(1) The source host uses its own MTU to fragment the message, and then sends the message to the destination host.
(2) When the intermediate forwarding device receives the message for forwarding, the message is discarded if the MTU value supported by the interface of the forwarding message is found to be smaller than the message length, and an ICMPv6 error message is returned to the source end, and the MTU of the interface of the forwarding failure is included.
(3) After the source host receives the error message, the MTU of the message carried in the message is segmented and sent.
(4) Repeating the message until the destination host receives the message, thereby determining the minimum MTU of the message from the source end to the destination end path.

27.1.5 Protocol specifications

The protocol specifications related to the IPv6 base are:

- RFC 1881：IPv6 Address Allocation Management
- RFC 1887：An Architecture for IPv6 Unicast Address Allocation
- RFC 1981：Path MTU Discovery for IP version 6
- RFC 2375：IPv6 Multicast Address Assignments
- RFC 2460：Internet Protocol, Version 6 (IPv6) Specification.
- RFC 2461：Neighbor Discovery for IP Version 6 (IPv6)
- RFC 2462：IPv6 Stateless Address Autoconfiguration
- RFC 2463：Internet Control Message Protocol (ICMPv6)for the Internet Protocol Version 6
- (IPv6) Specification
- RFC 2464：Transmission of IPv6 Packets over Ethernet Networks
- RFC 2526：Reserved IPv6 Subnet Anycast Addresses
- RFC 3307：Allocation Guidelines for IPv6 Multicast Addresses
- RFC 3513：Internet Protocol Version 6 (IPv6) Addressing Architecture
- RFC 3596：DNS Extensions to Support IP Version 6

27.2 Brief introduction of IPv6 basic configuration Task

Configure the basic functions of IPv6
Configure IPv6 neighbor Discovery Protocol
Configure PMTU Discovery
Configure ICMPv6 message sending

27.3 Configure the basic functions of IPv6v

27.3.1 Configure the IPv6 unicast address

IPv6 global unicast address is obtained by hand

The IPv6 link local address is obtained in two ways:

- Automatic generation: in the VLAN port UP, the device automatically generates the link local address for the interface according to the link local address prefix (FE80::/10) and the link layer address of the interface;
- Manual specification: users manually configure IPv6 link local addresses.

Order	Description	CLI mode
ipv6 address <ipv6-address>/<prefix-length>	Manually specify the IPv6 address. By default, link local addresses are automatically generated based on VLAN interface MAC addresses under layer 3 interfaces.	Configuration mode

27.4 Configure IPv6 neighbor Discovery Protocol

27.4.1 Configure parameters related to RA messages

According to the actual situation, users can configure whether the interface sends RA messages and the interval between sending RA messages, and can configure the relevant parameters in RA messages to notify the host. When the host receives the RA message, these parameters can be used to operate accordingly. The parameters and meanings in the RA message that can be configured are shown in Table 1 / 4.

Table 1 / 4 parameters and descriptions in RA messages

Parameter	Description
(Cur Hop Limit)	When the host sends an IPv6 message, it populates the Hop Limit field in the IPv6 header with this parameter value. At the same time, the parameter value is also used as the Hop Limit field value in the device reply message.
(Prefix Information)	After the host on the same link receives the prefix information released by the device, it is possible to perform the operation without state automatic

	configuration and the like.
(M flag)	Used to determine if the host is automatically configured to obtain an IPv6 address. If that flag bit is set to 1, the host will acquire the IPv6 address by a stateful automatic configuration (e. g., a DHCP server); otherwise, the IPv6 address will be acquire by stateless autoconfiguration, i. e., generate an IPv6 address in accordance with its own link layer address and the prefix information issued by the router.
(O flag)	Used to determine whether the host uses stateful automatic configuration to obtain information other than IPv6 addresses. If the other configuration flag is set to 1, the host will obtain other information besides the IPv6 address through stateful autoconfiguration (such as a DHCP server); otherwise, other information will be obtained through stateless autoconfiguration.
(Router Lifetime)	Used to set the time when the router that publishes the RA message is the default router for the host. Based on the router lifetime parameter value in the received RA message, the host can determine whether to use the router that publishes the RA message as the default router.
(Retrans Timer)	After the device sends an NS message, if the response is not received within the specified time interval, the NS message is retransmitted.
(Reachable Time)	When the neighbor reachability test confirms that the neighbor is reachable, the device thinks that the neighbor is reachable within the set reachability time; after exceeding the set time, if a message needs to be sent to the neighbor, it will reconfirm whether the neighbor is reachable.
(Link MTU)	The MTU option is used in RA messages to ensure that all nodes on the link use the same MTU value, mainly when the node may not be aware of the link MTU. Other Neighbor Discovery messages must silently ignore this option.

Configure hop limit

Order: ipv6 nd cur-hop-limit *value*

View mode: VLAN interface mode

Default configuration: by default, the number of hops published by the router is limited to 64 hops

Unsuppress RA message publishing

Order:ipv6 nd send-ra

View mode: VLAN interface mode

Default configuration: by default, suppress the publication of RA messages

Configure the maximum and minimum interval for RA message publishing

Order: ipv6 nd max-ra-interval *value*

View mode: VLAN interface mode

Default configuration: By default, the maximum interval between the RA messages is 600 seconds

Order:ipv6 nd min-ra-interval *value*

View mode: VLAN interface mode

Default configuration: By default, the maximum interval between the RA messages is 198 seconds

Note:

- When the RA message is periodically released, the time interval between the two adjacent times is to randomly select a value between the maximum time interval and the minimum time interval as the time interval for periodically issuing the RA message.
- The minimum time interval configured should be less than 0.75 times the maximum interval.

Configure the prefix information in the RA message

Order: ipv6 nd prefix X:X::X:X/M (*valid-lifetime preferred-lifetime* (off-link | no-autoconfig))

View mode: VLAN interface mode

Default configuration: by default, the prefix information in the RA message is not configured, and the interface IPv6 address that sends the RA message is used as the prefix information in the RA message.

Set the managed address configuration flag bit

Order: ipv6 nd managed-config-flag

View mode: VLAN interface mode

Default configuration: By default, the managed address flag bit is 0, that is, the host acquires the IPv6 address by stateless auto-configuration.

Set additional configuration flag bits.

Order: ipv6 nd other-config-flag

View mode: VLAN interface mode

Default configuration: by default, the other configuration flag bit is 0, that is, the host obtains other information through stateless automatic configuration.

Configure the lifetime of the router in the RA message

Order: ipv6 nd ra-lifetime *value*

View mode: VLAN interface mode

Default configuration: by default, the lifetime of the router in the RA message is 1800 seconds.

Configure neighbor request message retransmission interval

Order:ipv6 nd base retrans-timer *value*

View mode: VLAN interface mode

Default configuration: by default, the interface sends NS messages at an interval of 1000 milliseconds.

Configure the router retransmission interval in RA messages

Order: ipv6 nd retrans-timer *value*

View mode: VLAN interface mode

Default configuration: by default, the value of the Retrans Timer field in the RA message issued by the interface is 0

Configure the time to keep the neighbor reachable

Order: ipv6 nd base reachable-time *value*

View mode: VLAN interface mode

Default configuration: by default, the interface keeps the neighbor accessible for 30000 milliseconds

Configure the time to keep the neighbor reachable

Order: ipv6 nd reachable-time *value*

View mode: VLAN interface mode

Default configuration: By default, the value of the Reachable Timer field in the RA message issued by the interface is 0.

Configure link MTU size

Order: ipv6 nd link-mtu *value*

View mode: VLAN interface configuration mode

Default configuration: By default, the value of the link mtu field in RA message advertised by the interface is 0.

When the source host sends a message from the interface, the MTU of the interface is compared with the Link MTU, and if the length of the message is greater than the minimum value in both, the message is sliced with the minimum value.

27.4.2 Configure the number of times neighbor request messages are sent when duplicate address detection

After the interface obtains the IPv6 address, it sends a neighbor request message for duplicate address detection. If no response is received within the specified time (configured by the ipv6 nd retrans-timer command), the neighbor request message continues to be sent. After the number of times has been set, the response is still not received and the address is considered available.

Order	Description	CLI mode

ipv6 nd dad attempts <value>	By default, the number of times a neighbor request message is sent when repeated address detection is 1, and when the value value is 0, duplicate address detection is prohibited.	Configuration mode

27.5 IPv6 static route configuration

Order	Description	CLI mode
ipv6 route <X:X::X:X/M> (<X:X::X:X> | <ifName>) <distance>	Configure IPv6 static routing.	Configuration mode

27.6 IPv6 display and maintenance

After the configuration is complete, run the show command in the privilege view to display the IPv6 running status after the configuration.

Order	Description	CLI mode
show ipv6 ndp nc	Display neighbor information	Privilege mode
show ipv6 interface (<ifName>) brief	Displays IPv6 information for interfaces that can be configured with IPv6 addresses	Privilege mode
show ipv6 route (database)	Display IPv6 routing	Privilege mode

Chapter 28 Basic POE Configuration

The switch supports Poe configuration function to query the POE port status and port policy service of each port.

- POE Configuration
- POE Policy configuration
- PD Query configuration

28.1 POE Configuration

- Set maximum total power
- Turn on and off interface Poe power supply
- Display Poe information

Order	Description	CLI mode
poe max-power <power>	Set the maximum total Poe power of the system.	Configuration mode
[no] poe enable	Turn on or off the interface Poe power supply. The default interface power supply status is on.	Interface mode
show poe	Display Poe information of all interfaces.	User mode or privileged user mode

28.2 POE Policy Configuration

The commands for POE policy configuration are as follows:

- Turns on or off the POE policy of the interface
- Set Poe policy entry for interface
- Display Poe policy information

Order	Description	CLI mode
[no] poe policy enable	Open or close the interface Poe policy. The POE policy of the default interface is closed.	Interface mode
[no] poe policy shutdown clock <clock-value> week-day <day-value>	Set or cancel the POE policy entry of the interface. This command can be set multiple times. The POE policy entry is not set by default. Clock value is the time or time range in 24-hour system. If the value is 1, it means 1 point (i.e. between 1 and 2 points), and 20-23 means 20 to 23 points (i.e. between 20 and 0 points). Day value is the day of the week, which means a day or consecutive days. For example, 3 means Wednesday and 1-7 means Monday to Sunday. The POE policy can take effect only when the POE policy of the interface is on.	Interface mode
show poe policy <if-name>	Display Poe policy information of an interface.	User mode or privileged user mode

28.2 POE Query Configuration

The commands for PD query configuration are as follows:

- Set the IP address of PD
- Set the time interval for querying PD
- Set the timeout times of PD query
- Set the start time of PD
- Display PD information

Order	Description	CLI mode
poe pd-ip-address <ip-address> no poe pd-ip-address	Set or clear the IP address of the PD connected to the interface. By default, the IP address of the PD is not configured. If the IP address of PD is configured, the system will query this IP address regularly. If PD does not respond for a given number of times, it will restart PD through Poe control.	Interface mode
poe pd-query-interval <interval> no poe pd-query-interval	Set the time interval for querying PD. The default time interval for querying PD is 5 seconds.	Interface mode
poe pd-timeout-number <number> no poe pd-timeout-number	Set the timeout times of querying PD. The default timeout times of querying PD is 3.	Interface mode
poe pd-boot-time <time> no poe pd-boot-time	Set the startup time of PD. The default startup time of PD is 120 seconds.	Interface mode
show poe pd-information	Displays information for all configured PDs	User mode or privileged user mode