SAN Telequip (P) Ltd.,
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27293455, 8793779568
email : info@santelequip.com

CLI COMMAND USER MANUAL FOR

IESMGR 308-16S Hi

Managed Giga Industrial Ethernet Switch

SAN Telequip (P) Ltd.,
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27293455, 8793779568
email : info@santelequip.com

Contents

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

- Access the switch's CLI
- Introduction to CLI mode
- Command syntax introduction
- Command line shortcuts
- History command

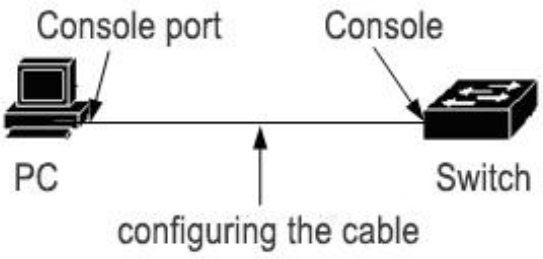
1.1 CLI to access the switch

The CLI command line interface of the switch provides an interface for users to manage the switch. Users can access the CLI command line interface of the switch through two terminals, Console port and Telnet.

1.1.1 Users access the CLI through the console port

The operation steps are as follows:

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



Step 2: Start the terminal emulation program on the PC (such as the Windows HyperTerminal, etc.) and configure the communication parameters of the terminal emulation program. The communication parameter configuration of the terminal is as follows:

Baud rate: 38400

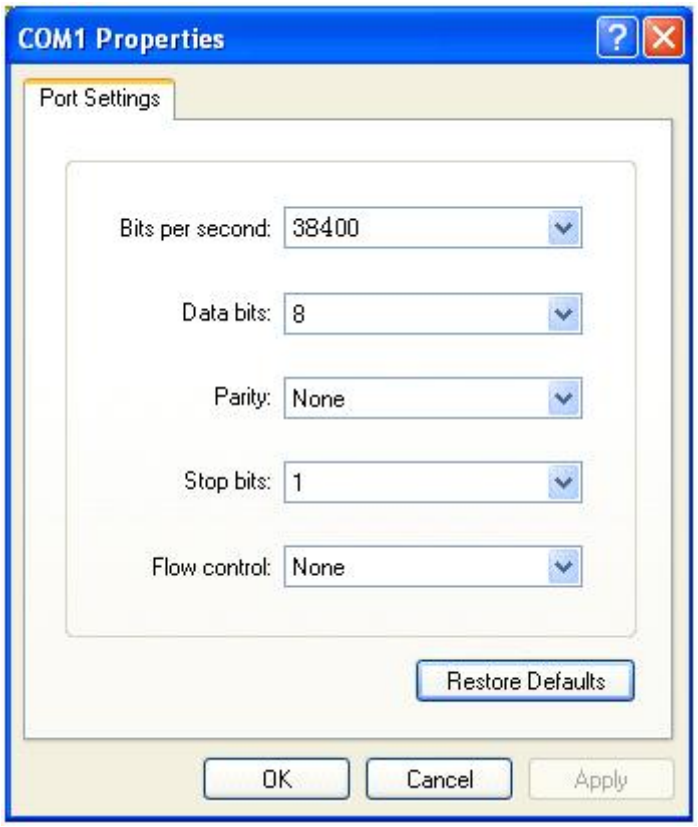
Data bits: 8

Parity: None

Stop bit: 1

Data flow control: None

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



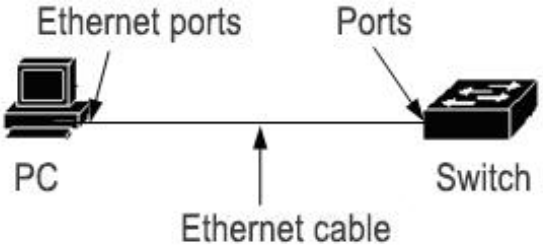
Step 3: Start the switch. After the switch is started, a CLI prompt will be displayed on the terminal (default is Switch>). The user can enter commands at this prompt so that the user can access the CLI of the switch.

1.1.2 Users access the CLI through TELNET

Users can access the switch through the port of the switch.

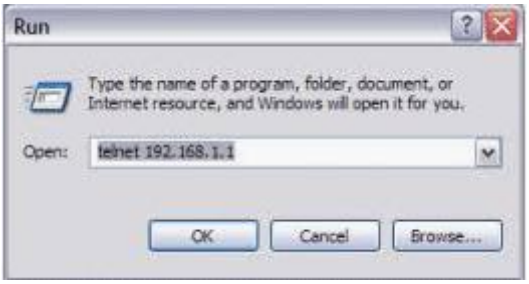
The IP address of the port of the switch is 192.168.0.1 by default. The steps to access the switch through the port are as follows:

Step 1: Connect the Ethernet port of the PC and the port of the switch through an Ethernet cable. As shown below:



Step 2: Set the IP address of the Ethernet port of the PC. The IP address must be in the 192.168.0.0/24 segment (such as the IP address 192.168.0.100). Determine the connectivity between the PC and the switch by ping 192.168.0.1.

Step 3: If the PC is connected to the switch, Telnet 192.168.0.1 enters the Telnet terminal interface. As shown below:



Step 4: Enter the user name and password on the Telnet interface and enter the CLI. The CLI prompt appears (the default is Switch>). The system default user name and password are both admin;

There are two points to pay special attention to:

- The IP address of the switch port is built on the VLAN layer 3 interface. Before accessing the switch, you must set the IP address of a VLAN interface. The default IP address of VLAN 1 is 192.168.0.1, which can be used directly. The IP address of the VLAN interface can be configured through the console port.
- Users access the switch through the port, you can directly connect the PC and the port through the Ethernet cable, or you can connect through a network, as long as the PC can communicate with a certain VLAN of the switch.

1.2 Introduction to CLI Mode

1.2.1 The role of CLI mode

The role of the CLI mode mainly has the following two points:

(1), It is convenient to classify users and prevent unauthorized users from illegally using the CLI.

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

Ordinary users can only view some operating status of the switch, and can only use display commands.

In addition to being able to view the operating status of the switch, privileged users can also maintain and configure the switch and change the behavior of the switch.

(2), It is convenient for users to configure the switch

There are many configurations of switches. If you put all the configurations in one mode, it is very inconvenient for users to use. To this end, multiple modes are established on the CLI, and similar commands are placed in one mode, which is convenient for users to understand and use. For example, put the commands related to VLAN in the VLAN configuration mode, and put the commands related to the interface in the interface configuration mode.

1.2.2 CLI mode logo

The CLI prompt is the identifier of the CLI mode. When using the CLI, the user can know the current CLI mode by looking at the CLI prompt.

The CLI prompt consists of two parts, one identifies the host and the other identifies the mode.

The host part of the CLI prompt uses the host name of the system. The host name of the system is configurable, and the default is Switch. Therefore, the CLI prompt starts with Switch by default. The CLI descriptors mentioned later are generally Use the default host name.

The mode part of the CLI prompt is not configurable. Each mode has its own corresponding mode string. Some mode strings are fixed and some mode strings are variable. For example, the mode character string of the VLAN configuration mode is fixed, and the mode character string of the interface configuration mode is variable.

E.g.:

CLI prompt Switch# identifies privileged mode, Switch identifies host, and # identifies mode.

CLI prompt Switch(config-ge1/1) # identifies the interface configuration mode, and configures the ge1/1 port, Switch identifies the host, and (config-ge1/1) # identifies the mode.

CLI prompt Switch(config-vlan2) # identifies the interface configuration mode, and configures the vlan2 interface, Switch identifies the host, and (config-vlan2) # identifies the mode.

1.2.3 Classification of CLI mode

The CLI mode is divided into four categories: normal mode, privileged mode, global configuration mode and configuration sub-mode, and the configuration sub-mode is composed of many CLI modes.

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

The console and Telnet terminal first enter the normal mode. Enter the enable command in the normal mode and successfully verify the password to enter the privileged mode. On the Telnet terminal, ordinary users can only stay in ordinary mode and cannot enter privileged mode. Enter configure terminal in privileged mode and enter the global configuration mode in CLI mode. Enter the relevant commands in the global configuration mode to enter each configuration sub-mode.

The following table lists the main CLI modes of the switch:

Mode	Description	Prompt	Command to enter mode	Commands to exit mode
Normal mode	Provides a display command to view the status information of the switch.	Switch>	The mode that 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 providing display commands to view the status information of the switch, it also provides debugging, version upgrade, and configuration maintenance commands.	Switch#	Enter the enable command in normal mode.	Use the disable command to return to normal mode. Use the exit or quit command on the Console terminal to exit to normal mode, and use the exit or quit command on the Telnet terminal to exit the Telnet terminal。
Global configuration mode	Provides general commands that cannot be implemented in the configuration sub-mode, such as configuring	Switch(config)#	Enter the configure terminal command in privileged mode.	Use the exit, quit or end command to exit to privileged mode.

	static routing commands.			
Interface configuration mode	Provides commands to configure ports and VLAN interfaces.	port: Switch(config-ge1/1)# VLAN interface : Switch(config-vlan1)#	Enter the interface <if-name> command in the global configuration mode.	Use the exit or quit command to exit to global configuration mode, and use the end command to exit to privileged mode.
VLAN configuration mode	Provides commands for configuring VLANs. For example, commands to create and delete VLANs.	Switch(config-vlan)#	Enter the vlan database command in the global configuration mode.	Use the exit or quit command to exit to global configuration mode, and use the end command to exit to privileged mode.
MSTP configuration mode	Provides commands to configure MSTP. For example, commands to create and delete MSTP instances.	Switch(config-mst)#	Enter spanning-tree mst configuration command in global configuration mode.	Use the exit or quit command to exit to global configuration mode, and use the end command to exit to privileged mode.
Terminal configuration mode	Commands for configuring Console and Telnet terminals are provided, such as commands for configuring the timeout period of terminals.	Switch(config-line)#	Enter the line vty command in the global configuration mode.	Use the exit or quit command to exit to global configuration mode, and use the end command to exit to privileged mode.

1.3 Introduction to Command Syntax

1.3.1 Command composition

The CLI command consists of keywords and parameters. The first word must be a keyword. The following words can be keywords or parameters. The keywords and parameters can appear alternately. A command must have keywords, but there can be no parameters.

For example, the command write has only one keyword and no parameters; the command show version has two keywords and no parameters; the command vlan <vlan-id> has a keyword and one parameter; the command instance <instance-id> vlan <vlan -id> There are two keywords and two parameters and the keywords and parameters appear alternately.

1.3.2 Parameter Type

There are two types of parameters for CLI commands: mandatory parameters and optional parameters. The mandatory parameters must be entered when entering the command, and the optional parameters may or may not be entered. For example, the parameter in the command vlan <vlan-id> is a mandatory parameter. This parameter must be entered when entering the command; and the parameter in the command show interface [if-name] is an optional parameter. , Or not.

1.3.3 Command syntax rules

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

1) The keywords are directly expressed in words.

Such as the command show version.

2) Parameters must be enclosed in <>.

Such as the command vlan <vlan-id>

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

Such as the command show vlan [<vlan-id>]

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

Command show vlan [vlan-id]

That is, the parameter vlan-id can be entered or not.

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

4) If there is more than one keyword or parameter, one must be selected. Use {} to enclose the multiple keywords or parameters. Separate the multiple keywords or parameters with |. A space is required before and after |.

Commands that must be selected for multiple keywords:

spanning-tree mst link-type {point-to-point | shared}

You must choose one between point-to-point and shared.

Commands required for multiple parameters:

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

Required commands with mixed keywords and parameters:

Show spanning-tree mst {none|instance <0-15>}ng

5) If one of multiple keywords or parameters can be selected, use [] to enclose multiple keywords or parameters. The multiple keywords or parameters are separated by |, and a space is required before and after |.

The command is as follows:

debug ip tcp [recv | send]

The keywords recv and send can choose one or not.

show ip route [<ip-address> | <ip-prefix>]

show interface [<if-name> | switchport]

6) If there is a keyword or parameter or a group of keywords or parameters, you can select the input repeatedly, and add the symbol "*" after this (group) keyword or parameter.For example, the ping command:

ping <ip-address> [-n <count> | -l <size> | -r <count> | -s <count> | -j <count> <ip-address>* | -k <count> <ip -address>* | -w <timeout>]*

-j <count> <ip-address>* --- You can enter multiple IP addresses repeatedly

-k <count> <ip-address>* --- You can enter multiple IP addresses repeatedly

The entire option can also be entered repeatedly.

6) The parameter is represented by one or more word descriptors. If there are multiple words, separate each word with the symbol "-", and each word is lowercase.

Correct parameter notation: <vlan-id>, <if-name>, <router-id>, <count>, etc.

Wrong parameter notation: <1-255>, <A.B.C.D>, <WORD>, <IFNAME>, etc.

1.3.4 Command abbreviation

When a user enters a command on the CLI interface, the keyword of the command can be abbreviated. The CLI supports the prefix matching function of commands. As long as the entered word matches the keyword prefix uniquely, the CLI parses the entered word into a matching keyword. In this way, the user is very convenient when using the CLI. The user can type few characters to complete a command. For example, the show version command can only type sh ver.

1.3.5 Grammar help

The CLI command line interface is provided with syntax help to support the help function of each level of commands and parameters, which are described as follows:

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

2) Enter the front part of a command, then enter a space and then enter it? Key, all keywords or parameters of the next level and their descriptions will be listed on the terminal. For example Switch#show ?.

3) Enter an incomplete keyword directly? Key, all keywords and their descriptions matching this input prefix will be listed on the terminal. For example Switch#show ver?.

4) Enter the front part of a command, then enter a space and then enter the Tab key, all the keywords of the next level will be listed on the terminal, if the next level is a parameter, it will not be listed.

5) After entering an incomplete keyword, directly enter the Tab key. If only one keyword matches this input prefix, it will be filled in directly. If there are multiple keywords that match this input prefix, all will be listed on the terminal. Matching keywords.

1.3.6 Command line error message

If the command entered by the user does not pass the grammar check, an error message will be displayed on the terminal.

Error message	wrong reason
Invalid input or Unrecognized command	No matching keywords were found. The parameter input is incorrect. You have entered too many keywords or parameters.
Incomplete command	Command input is incomplete, and keywords or parameters are not entered.
Ambiguous command	Keyword input is incomplete, there are multiple keywords that match the input prefix.

1.4 Command line shortcuts

1.4.1 Line editing shortcuts

The CLI command line interface supports the line editing shortcut key function, which can facilitate the input and editing of CLI commands. When users input or edit commands, they can use the line editing shortcut keys to speed up the input of commands. The following table lists all the row editing shortcut keys and the implemented functions:

hot key	Features
Ctrl+p or ↑	Previous command

Ctrl+n or ↓	Next command
Ctrl+u	Delete the entire line
Ctrl+a	The cursor returns to the beginning of the line
Ctrl+f or → key	Move the cursor one space to the right
Ctrl+b or ←	Cursor moves one frame to the left
Ctrl+d	Delete the character under the cursor
Ctrl+h	Delete the character before the cursor
Ctrl+k	Delete all characters at and after the cursor
Ctrl+w	Delete 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 the global configuration mode or the configuration sub-mode, the CLI returns to the privileged mode; if the CLI is in the normal mode or the privileged mode, the CLI mode remains unchanged, but the CLI starts a new line.
Ctrl+z	Same function as Ctrl+c.
Tab	Use this key after entering incomplete keywords. If there is one keyword that matches the entered prefix, this keyword is completed; if there are multiple keywords that match the entered prefix, all matching keywords are listed; If no keywords match, the key is invalid.

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

1.4.2 Display command shortcut keys

The commands beginning with the show keyword are display commands. Some display commands cannot be displayed on one screen due to the large amount of content displayed. The terminal provides the function of split screen display. After displaying a screen, the terminal waits for user input to decide the subsequent processing. The following table lists the display command shortcut keys and their functions.

hot key	Features
Space	Show next screen
Enter	Show next line
Ctrl+c	Interrupt the execution of the command and exit to CLI mode.
Other keys	Same function as Ctrl+c.

1.5 History Command

The CLI command line interface supports the command history recording function, which can remember the 20 recent historical commands used by the user, and save the commands recently entered by the user. You can use show history to display the commands you have entered, or you can use Ctrl+p, Ctrl+n or ↑, ↓ keys to select the history command. The history command function can facilitate users to input commands.

- Before learning the relevant function configuration of the switch, users need to master some basic configuration of the system management and maintenance of the switch. This chapter describes the basic configuration of these system management and maintenance, mainly including the following:
- System security configuration
- System maintenance and debugging
- System monitoring
- Configuration file management
- Software version upgrade

2.1 System security configuration

In order to prevent illegal users from invading the switch, the system provides several system management security measures, including:

- Multi-user management control
- TACACS+ authentication and authorization
- Anonymous user password control
- Enable password control
- TELNET service control
- SNMP service control
- HTTP service control

2.1.1 Multi-user management control

Multi-user management not only ensures the security of the switch system, but also provides the ability for multiple users to manage and maintain the switch at the same time. Multi-user management ensures system security by giving each user a user name, password, and authority. Users must first verify the user name and password when accessing the switch. Only when the user name and password are correct and consistent can they be verified. After passing the authentication, the user can access the switch, but the user's authority limits the user's access to the switch.

Multi-user management divides user rights into two levels: ordinary users and privileged users. Ordinary 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. Privileged

users can access all modes of the CLI command line interface, and can use all commands provided by the CLI to query the switch information and maintain and manage the switch.

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

The default user name and password of the switch are both admin. The admin user must be an administrator, that is, a privileged user, and cannot be configured as a normal user, nor can the admin user be deleted.

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

command	description	CLI mode
username <user-name> password <key> {normal | privilege}	Add a user. If the specified user already exists, modify the user's password and permissions. The first parameter is the user name, and the second parameter is the password. The options indicate permissions, normal indicates ordinary users, and privilege indicates privileged users.	Global configuration mode
no username <user-name>	Delete a user with the specified username.	Global configuration mode
show running-config	View the current configuration of the system, you can view the configuration of multi-user management.	Privileged mode

2.1.2 TACACS+ certification and authorization

TACACS+ authentication and authorization provides stricter user rights management, not only verifying the legitimacy of users, but also authorizing commands. After enabling

TACACS+ authentication, users must first verify the user name and password through the TACACS+ server when accessing the switch. Only when the user name and password are correct and consistent can they be verified. The user can access the switch after passing authentication.

TACACS+ also divides user rights 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. The user must enter a command (except enable, end, and exit) to verify the permission on the TACACS+ server. If the verification fails, it is not executed.

The TACACS+ authentication and authorization function is only applicable to Telnet and SSH terminals, and does not control the Console terminal. When accessing the switch through Telnet or SSH terminals, you need to verify the user name and password. Only after the user name and password are verified can you access the CLI. During SSH access, only privileged users can pass. TACACS+ authentication is also used for WEB login, but it only verifies password privileges and does not perform command authorization.

By default, the switch does not enable the TACACS+ function. At this time, Telnet, SSH, or WEB login all use the multi-user management function. After enabling the TACACS+ function, the multi-user management function can continue to be configured, but it is not actually used.

The commands related to TACACS+ authentication and authorization are as follows:

command	description	CLI mode
tacacsplus enable	Open TACACS+ function	Global configuration mode
tacacsplus disable	Disable TACACS+ function	Global configuration mode
tacacsplus host A.B.C.D	Configure the main server address, it is recommended to use Cisco's ACS	Global configuration mode
tacacsplus key WORD	Configure a shared key, which is used to encrypt and transmit data, and must be consistent with the configuration on the server	Global configuration mode
tacacsplus auth-type (PAP|CHAP)	Select the authentication method. The supported	Global configuration mode

	methods include PAP and CHAP. PAP is the default mode, and the password is encapsulated in the field, while CHAP encapsulates the MD5 check code of the password.	
show tacacsplus	View TACACS+ configuration information	Global configuration mode
no tacacsplus host	Clear the main server address	Global configuration mode
no tacacsplus key	Clear shared key	Global configuration mode

2.1.3 enable password control

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

The enable password does not depend on the user. Any user who logs in to the Console terminal or Telnet terminal must verify the enable password if they want to enter the privileged mode. If the verification is not successful, they can only stay in the normal mode.

Enter the enable command in normal mode, and the terminal will prompt the user to enter the password. At this time, the user can enter the enable password. If the password verification is successful, the terminal enters the privileged mode. Otherwise, it stays in normal mode. For ordinary users, regardless of whether the password is successfully verified None can enter the privileged mode.

The enable password is empty by default. In this case, the terminal enters the privileged mode without prompting for the password after entering the enable command in normal mode.

The related commands for the enable password are as follows:

command	description	CLI mode
enable password <key>	Set the system's enable password.	Global configuration mode
no enable password	Clear the system's enable password, which is empty.	Global configuration mode

show running-config	View the current configuration of the system, you can view the configuration of the enable password.	Privileged mode
enable	Interactive command to verify the system enable password. After successful verification, the terminal enters privileged mode.	Normal mode

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

2.1.4 TELNET Service control

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

The related commands of Telnet service control are as follows:

command	description	CLI mode
security-manage telnet enalbe	Open the Telnet service.	Global configuration mode
security-manage telnet disable	Close Telnet service.	Global configuration mode
security-manage telnet number <1-100>	The number parameter ranges from 1 to 100, and the default is 5.	Global configuration mode
security-manage telnet access-group <1-99>	Specify an ACL group and enable source IP address control. If the specified ACL group does not exist or is not a standard ACL group, the source IP address is not controlled.	Global configuration mode

no security-manage telnet access-group	Turn off source IP address control.	Global configuration mode
show security-manage	You can view the service control configuration.	Privileged mode

2.1.5 SNMP service control

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

The related commands of SNMP service control are as follows:

command	command	CLI mode
security-manage snmp enalbe	Open the SNMP service.	Global configuration mode
security-manage snmp disable	Disable the SNMP service.	Global configuration mode
Security-manage snmp access-group <1-99>	Specify an ACL group and enable source IP address control. If the specified ACL group does not exist or is not a standard ACL group, the source IP address is not controlled.	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 service control configuration.	Privileged mode

2.1.6 HTTP service control

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

The related commands of HTTP service control are as follows:

command	description	CLI mode
security-manage http enalbe	Open the HTTP service.	Global configuration mode
security-manage http disable	Close the HTTP service.	Global configuration mode
security-manage http access-group <1-99>	Specify an ACL group and enable source IP address control. If the specified ACL group does not exist or is not a standard ACL group, the source IP address is not controlled.	Global configuration mode
no security-manage http access-group	Turn off source IP address control.	Global configuration mode
show security-manage	You can view the service control configuration.	Privileged mode

2.1.7 SSH service control

Traditional network service programs such as ftp, pop, and telnet are inherently insecure because they transmit passwords and data in clear text on the network, and people with ulterior motives can easily intercept these passwords and data. Moreover, the security verification methods of these service programs also have their weaknesses, that is, they are very vulnerable to attacks by man-in-the-middle. The so-called "man-in-the-middle" attack method is that the "man-in-the-middle" impersonates the real server to receive the data you pass to the server, and then impersonates you to pass the data to the real server. After the data transfer between the server and you is changed by the "middleman", serious problems will occur. By using SSH, you can encrypt all transmitted data, so that the "man-in-the-middle" attack is impossible, and it can also prevent DNS spoofing and IP spoofing. Using SSH, there is an additional advantage that the transmitted data is compressed, so it can speed up the transmission speed. SSH has many functions. It can replace Telnet and provide a secure "channel" for FTP, PoP, and even PPP.

2.2 System maintenance and debugging

Basic system maintenance and debugging functions mainly include the following:

- Configure the host name of the system
- Configure the system clock
- Configure terminal timeout attributes
- System reset
- View system information
- Network connectivity debugging
- Detect the distance of network cable
- 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 is convenient for users to distinguish between different switches, and the host name of the system is also part of the CLI prompt of the terminal. The default host name of the system is Switch.
The related commands of the system's host name are as follows:

command	description	CLI mode
hostname <name>	Set the host name of the system.	Global configuration mode
no hostname	Clear the host name of the system, that is, the host name returns to the default value Switch.	Global configuration mode
show running-config	View the current configuration of the system, you can view the configuration of the host name of the system.	Privileged mode

2.2.2 Configure the system clock

The switch provides the function of real-time clock. You can set the current clock and view the current clock through commands. The system clock is powered internally to ensure the

continuous operation of the real-time clock when the system is powered off. There is no need to reset the clock after the system starts.

The switch has already set the clock when it leaves the factory, and the user does not need to set it again. If the user finds that the time is not accurate, the user can reset the clock.

The related commands of the system clock are as follows:

command	description	CLI mode
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	Display the current clock of the system.	Normal mode

2.2.3 Configure terminal timeout properties

For the safety of the terminal, when there is no key input in the terminal, the terminal will perform the exit process after a certain period of time. The console terminal and the Telnet terminal have different exit processes. For the Console terminal, when the terminal times out, the CLI mode returns to the normal mode. For the Telnet terminal, when the terminal times out, the Telnet connection is terminated and the Telnet terminal exits.

The terminal timeout time defaults to 10 minutes, and users can also set the terminal to never time out.

The related commands for terminal timeout are as follows:

command	description	CLI mode
exec-timeout <minutes> [seconds]	Set the terminal timeout time. If the parameters are all 0, it means that the terminal will never time out.	Terminal configuration mode
no exec-timeout	Set the terminal timeout time to return to the default, which is 10 minutes.	Terminal configuration mode
show running-config	View the current configuration of the system, you can view the terminal timeout configuration.	Privileged mode

2.2.4 System reset

The system provides a reset method:

- rest the switch

The related commands of system reset are as follows:

command	description	CLI mode
reset	Reset the switch.	Privileged mode

2.2.5 View system information

The system provides a wealth of display commands to view the system's operating status and system information. Here are only a few commonly used display commands for system maintenance, as shown in the following table:

command	description	CLI mode
show version	Display the system version number and the time to execute the file compilation and connection.	Normal mode
show snmp system information	Displays basic information about the system, including how long it has been running since the system was started.	Normal mode
show history	Displays the list of recently entered commands on the CLI command line.	Normal mode

2.2.6 Network connectivity debugging

In order to debug the connectivity between the switch and another device on the network, you need to implement the ping command on the switch and ping the IP address of the other side on the switch. If the switch receives a ping response from the other side, it means that both ends are connected, otherwise it means The two ends cannot communicate.

The switch not only implements the ping command, but also supports many options on the ping command. Users can use these options for more precise and complex debugging.

The ping command is as follows:

command	description	CLI mode
ping <ip-address> [-n <count> | -l <size> | -r <count> | -s <count> | -j <count> <ip-address>* | -k <count> <ip-address>* | -w <timeout>]*	It can be used without any options or one or more options. Without any options, it is the simplest ping command. When the command is executed, you can type Ctrl+c to interrupt the execution of the command.	Privileged mode

2.2.7 Detection of network cable distance

command	description	CLI mode
show cable-diag interface IFNAME	Detect the distance of network cable	Privileged mode

2.2.8 Traceroute debugging

In order to debug the intermediate devices that the switch and another device in the network pass through during communication, you need to implement the trace-route command on the switch. When using the trace-route command on the switch, specify the IP address of the other party, and all the paths in the middle will be displayed during the command execution.

The switch not only implements the trace-route command, but also supports many options on the trace-route command. Users can use these options for more precise and complex debugging.

The trace-route command is as follows:

command	description	CLI mode
trace-route <ip-address> [-h <maximum-hops> | -j <count> <ip-address>* | -w <timeout>]*	It can be used without any options or one or more options. Without any options, it is the simplest trace-route command. When the command is executed, you	Privileged mode

	can type Ctrl+c to interrupt the execution of the command.	

2.2.9 Telnet client

Series switches provide Telnet client function; users can remotely access other devices through Telnet client.

command	description	CLI mode
telnet <ip-address>	The parameter is the IP address of the target device	Privileged mode

2.2.10 UDLD configuration

UDLD (UniDirectional Link Detection): It is a Layer 2 protocol used to monitor the physical configuration of Ethernet links connected by optical fibers or twisted pairs. When a unidirectional link occurs (only one direction can be transmitted, For example, if I can send the data to you, you can also receive it, but when the data you send to me is not received), UDLD can detect this situation, close the corresponding interface and send a warning message. Unidirectional links may cause many problems, especially spanning tree, which may cause loopback. Note: UDLD needs to be supported by devices at both ends of the link to function properly.

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

Normal mode : In this mode, UDLD can detect a unidirectional link and mark the port as undetermined to generate a system log. 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 period of time.

Aggressive mode: In this mode, UDLD can detect unidirectional links. And it will try to rebuild the link and send a UDLD message for 8 seconds continuously. If there is no UDLD echo response, the port will be placed in errdisable state.

command	description	CLI mode
udld enable	Globally enable the UDLD function	Global configuration mode
udld message time <time>	UDLD message transmission interval	Global configuration mode
udld port	Port enable UDLD	Interface configuration mode

udld aggressive	Enable port aggressive mode, default normal mode	Interface configuration mode
show udld <ifname>	View port UDLD information	Privileged mode

2.3 Configuration file management

The configuration is divided into the current configuration and the initial configuration. The current configuration refers to the configuration when the system is running, which is stored in the system's memory, and the initial configuration is the configuration used when the system is started, and is stored in the system's FLASH, that is, the configuration file. When the user executes the relevant command, the current configuration of the system is modified. Only after the save command is executed, the current configuration is written to the initial configuration for the next startup of the system. When the user does not make any configuration after the system is started, the current configuration information of the system is the same as the initial configuration information.

The current configuration and the initial configuration use the same format, both in 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 commands are saved.
- Only the non-default configuration is saved, and the default configuration is not saved.
- The commands are organized according to the CLI mode. The commands in the same CLI mode are organized together to form a segment, and the segments are separated by "!" For commands in the global configuration mode, commands with the same function or similar functions are organized into a paragraph, separated by "!".
- For commands in the configuration sub-mode, there is a space before the command, and for commands in the global configuration mode, there is no need for a space before the command.

Use "end" as the end of configuration.

Configuration file management mainly includes the following:

- View configuration information
- Save configuration
- Delete configuration file
- Download on configuration file

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 there is no configuration file in FLASH, the system uses the default configuration at startup. At this time, if you view the initial configuration of the system, the system will prompt that the configuration file does not exist.

The commands for viewing configuration information are as follows:

command	description	CLI mode
show running-config	View the current configuration of the system.	Privileged mode
show startup-config	View the initial configuration of the system.	Privileged mode

2.3.2 Save configuration

When the user modifies the current configuration of the system, these configurations need to be saved in the configuration file, so that these configurations still exist after the next startup, otherwise, this configuration information will be lost after the restart. Saving the configuration is to save the current configuration to the initial configuration.

The commands to save the configuration are as follows:

command	description	CLI mode
write	Save the current configuration.	Privileged mode

Note: The user needs 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 configuration file

When users want the initial configuration of the system to return to the default configuration, they can delete the configuration file, and deleting the configuration file has no effect on the current configuration. If they want the current configuration of the system to return to the default configuration, they 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,

command	description	CLI mode
delete startup-config	Delete the system	Privileged mode

	configuration file.	

2.3.4 Download on configuration file

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

The commands downloaded on the configuration file are as follows:

command	description	CLI mode
upload configure <ip-address> <file-name>	Upload the configuration file to the PC. The first parameter is the IP address of the PC. The second parameter is the file name of the configuration file stored on the PC.	Privileged mode
download configure <ip-address> <file-name>	Download the configuration file to the PC, the first parameter is the IP address of the PC, the second parameter is the file name of the configuration file stored on the PC.	Privileged mode

The TFTP protocol is used to download the configuration file, the TFTP client software is run on the switch, and the TFTP server software is run on the PC. The steps to download the configuration file are as follows:

The first step: build a network environment.

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

Step 3: Save the configuration on the switch.

Step 4: Run the configuration file upload command on the switch to back up the configuration file to the PC.

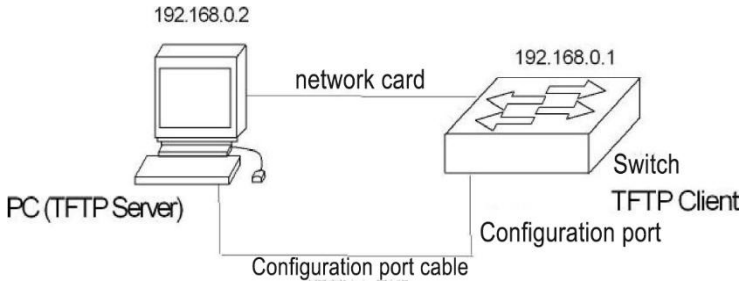
Step 5: When the switch needs the configuration file on the PC, execute the

configuration file download command on the switch to download the configuration file on the PC to the switch.

Step 6: For the configuration to take effect, the switch must be restarted.

Example: A switch that has been configured with VLANs and interface addresses needs to download the configuration file.

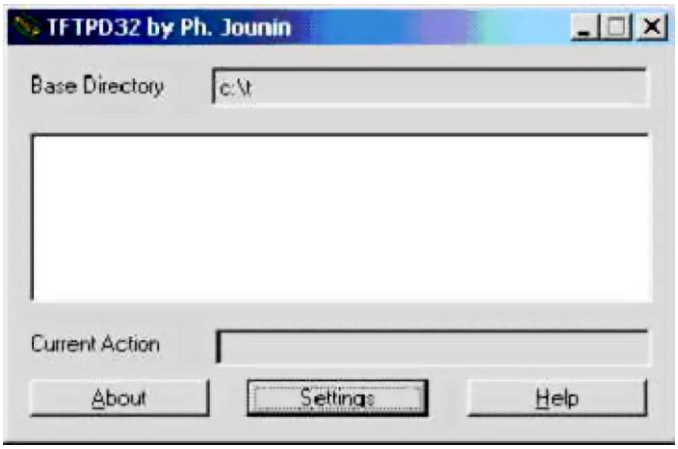
Step 1: Build the network environment as shown below.



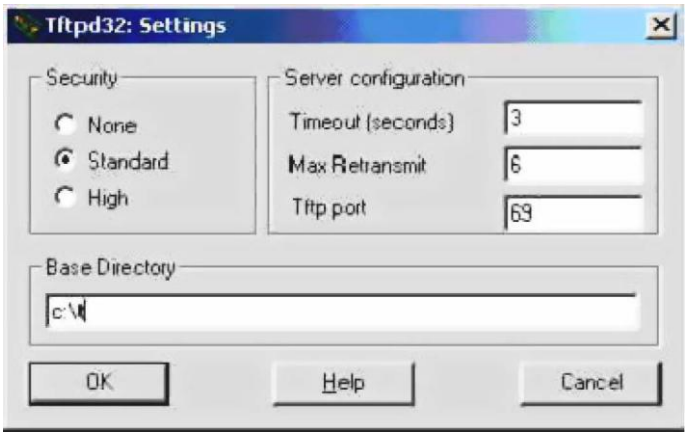
Connect the configuration port of the switch to a configuration terminal via a cable, and connect it to a PC via a network cable. Install TFTP Server on the PC and configure the IP address of the Ethernet port of the PC. Here, it is assumed that the IP address of the PC is 192.168.0.2. Then, configure the IP address of the switch. Here, the IP address of the switch is assumed to be 192.168.0.1 to ensure the connectivity between the PC and the switch.

Step 2: Start TFTP Server and configure TFTP Server parameters.

Run TFTP Server, the window interface is as follows:



Then, set the directory of the backup configuration file. The specific operation is to click the [Settings] button to set the interface, as shown below:



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

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

Step 4: Back up the file to the PC and execute the command Switch#upload configuration 192.168.0.2 beifen.cfg.

Step 5: If necessary, download the backup file to the switch and execute the command Switch#download configuration 192.168.0.2 beifen.cfg.
Step 6: For the downloaded configuration file to take effect, you must restart the switch and execute the command Switch#reset.

2.4 Software version upgrade

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

2.4.1 Software version upgrade commands

To upgrade the image file of the switch in the global configuration mode, the command is as follows:

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 name of the image file saved on the TFTP server.

The power cannot be cut off during the upgrade, otherwise the image file of the switch may be damaged and the switch will not start. After downloading, you need to restart the switch to run the newly downloaded image file program. The entire upgrade process takes a

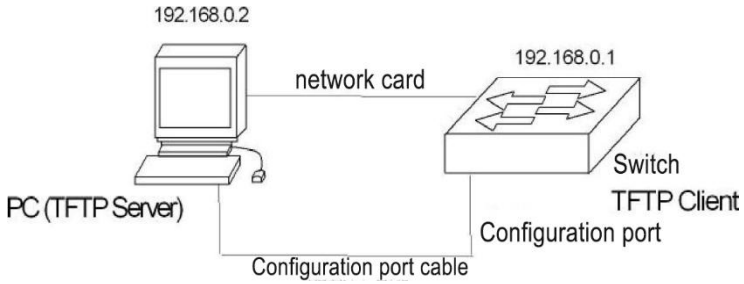
few minutes, please be patient.

The software version can also be upgraded through WEB. For specific operations, please refer to the WEB operation manual.

2.4.2 Software upgrade process

The steps to upgrade the image file are as follows:

The first step: build an upgrade environment. As shown below.



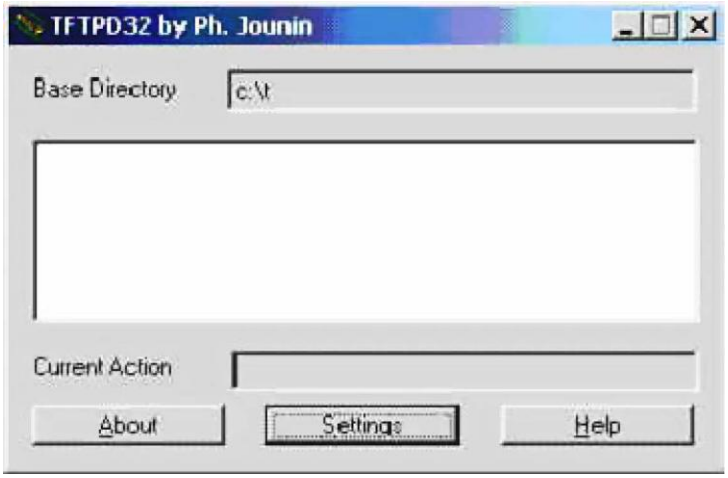
The construction process is as follows:

- Connect the console port of the switch to a configuration terminal (PC) through a cable.
- Install TFTP Server on the PC.
- Copy the new image file to a certain path of the PC, here assume the path is c:\t;
- Configure the IP address of the Ethernet port of the PC. Here, it is assumed that the IP address of the PC is 192.168.0.2.
-

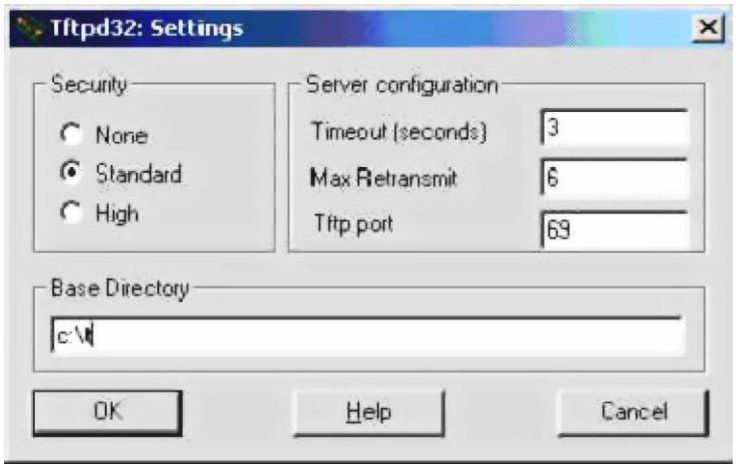
Configure the IP address of the switch, here it is assumed that the IP address of the switch is 192.168.0.1.

Step 2: Run TFTP Server and configure TFTP server.

First: Run TFTP Server. The TFTPD32 window interface is as follows:



Then: Set the TFTP Server file directory. After starting the TFTP Server, reset the TFTP Server file directory and copy the image file to be loaded into this directory. The specific operation is to click the [Settings] button, the TFTPD32 setting interface appears, as shown below.



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

Step 3: Upgrade files.

First: Connect the port of the switch to the PC running the TFTP Server program via an Ethernet cable. And use the ping command to check whether the host is connected to the switch.

Then: Enter the command at the Switch# prompt of the super terminal:

Switch# download image 192.168.0.2 switch.img，Press Enter and wait for the upgrade file to finish.

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

……

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

After the file transfer is completed, the system will prompt you whether you need to restart the switch; under normal circumstances, we recommend that you select'Y' to restart the switch, because the system upgrade will only take effect after the restart; if your configuration file is not saved, you can select'N ', do not restart first; restart the switch after completing other operations such as saving.

Switch#

Note：**The switch cannot be powered off during the upgrade process.**

Step 4: Restart the switch.

Switch# reset

Chapter 3 Port Configuration

This chapter introduces the port-related configuration, mainly including the following:

- General configuration of ports
- Configure MIRROR
- Configure STORM-CONTROL
- Configure STORM-CONSTRAIN
- Configure FLOW-CONTROL
- Configure port bandwidth
- Configure TRUNK
- Configure jumbo frames

3.1 General configuration of port

The administrator configures the port of the switch to control users connected under the port. If the user under the port is not allowed to access the network, the administrator can close the port. This section describes the general configuration of the port, mainly including:

- Port opening and closing
- Port speed configuration
- Display port information

3.1.1 Port speed configuration

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

The following command configures the port rate in interface configuration mode:

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

autonegotiate---Adaptive

full-1000------Full duplex gigabit

full-100--------Full duplex 100M

full-10 --------Full duplex ten trillion

half-100--------Half-duplex 100M

half-10---------Half-duplex ten trillion

For example, the rate of port 1/1 is configured as full duplex 100M:

Switch(config-ge1/1)# speed full-100

3.1.2 Display port information

The following command displays information about one or more ports in normal mode or privileged mode:

show interface [if-name]

For example, display the information of port 1/1:

Switch# show interface ge1/1

For example, display the information of all ports:

Switch# show interface

3.2 Configure MIRROR

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

- Configure MIRROR's listening port and monitored port
- Display MIRROR configuration

3.2.1 Configure MIRROR's listening port and monitored port

When the administrator configures the listening port, you need to enter this interface configuration mode to set the monitored port. For example, to set the port ge1/1 to listen to the port ge1/2, you need to enter the port ge1/1 and type the command:

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

At this time, port ge1/1 is set as the listening port, and ge1/2 is set as 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 time, the port ge1/1 is set as the listening port, and the <if-name> is set as the monitored port, and the following {both | receive | transmit} indicates the direction of monitoring: receive means monitoring the received data packets; transmit monitoring Packets sent; both listen to all packets sent and received. such as:

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

It means to set port ge1/1 to listen to the data packets sent and received by port ge1/2.

If you want to set multiple monitored ports, you need to execute multiple commands.

In interface configuration mode, the administrator can cancel the monitored port, the command is as follows:

Switch(config-ge1/1)#no mirror interface <if-name> direction { receive | transmit}

At this time, <if-name> is the port that is no longer being monitored. {receive | transmit} indicates the direction that is not to be monitored: receive means not to monitor received packets; transmit means not to monitor transmitted packets. such as:

Switch(config-ge1/1)# no mirror interface ge1/2 receive

It means that the port ge1/1 is no longer listening to the data packets received by the port ge1/2.

When all monitored ports are canceled, the monitored ports will also be cleared.

3.2.2 Display MIRROR configuration

The administrator can view the MIRROR configuration that has been set in the normal mode or the privileged mode through the following command:

Switch# show mirror

Need to pay attention to the following points:

- A port cannot be set as a listening port and a monitored port at the same time.
- There can only be one listening port, but there can be multiple listening ports.

3.3 Configure STORM-CONTROL

In real life, a high rate of unicast, multicast, and broadcast packets sent by a NIC card can cause the network to malfunction. In this case, the suppression function on the switch is particularly important, it can prevent the influx of data packets The network is congested. All ports of the switch support the suppression of broadcast packets, multicast packets and DLF packets.

This section describes the configuration of STORM-CONTROL in detail, including the following contents:

- Default configuration
- Broadcast suppression configuration
- Multicast suppression configuration
- DLF suppression configuration

Display STORM-CONTROL configuration

3.3.1 Default configuration

The switch supports setting broadcast, multicast, and dlf switches for each port separately. The three settings have separate rate limits. The rate limit of broadcast packets, multicast packets and DLF packets of the default port is turned off. The purpose of this function is to prevent the network from forming a broadcast storm.

3.3.2 Broadcast suppression configuration

The following command configures broadcast suppression for this port in interface configuration mode:

storm-control broadcast

The following command cancels the broadcast suppression configuration of this port in interface configuration mode:

no storm-control broadcast

3.3.3 Multicast suppression 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 DLF suppression for this port in interface configuration mode:

storm-control dlf

The following command cancels the configuration of DLF suppression for this port in interface configuration mode:

no storm-control dlf

3.3.5 Suppression rate configuration

The following command configures the suppression rate of this port in interface configuration mode:

storm-control ratelimit { broadcast | dlf | multicast } <1- 1048575 >

3.3.6 Display STORM-CONTROL configuration

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

show storm-control

3.4 Configure STORM-CONSTRAIN

The port flow threshold control function is used to control the packet storm on Ethernet. A port enabled with this function will periodically detect the unicast packet traffic, multicast packet traffic and broadcast packet traffic arriving at the port. If a certain type of packet traffic exceeds the preset upper threshold, the user can configure whether to block the port or close the port, and whether to send Trap and Log information.

When the traffic of a certain type of packet exceeds the preset upper threshold of that type of packet, the system provides two processing methods:

(1) Block mode: If the traffic of a certain type of packet on the port is greater than the upper threshold, the port will suspend the forwarding of this type of packet (other types of packets are forwarded as usual). The port is blocked, but the port still counts this Traffic of similar packets. When the traffic of this type of packet is less than the preset lower threshold, the port will resume the forwarding of this type of packet.

(2) Shutdown mode: If the traffic of certain types of packets on the port is greater than the upper threshold, the port will be shut down and the system will stop forwarding all packets. You can restore the port status by executing the undo shutdown command, or by canceling the port traffic threshold configuration.

Note: For certain types of packet traffic, you can use this function or the storm suppression function of the Ethernet port to suppress, but these two functions cannot be configured at the same time, otherwise the suppression effect is uncertain. For example, you cannot configure the unicast packet flow threshold control function and unicast storm suppression function of the port at the same time.

The CLI configuration commands are as follows:

command	description	CLI mode
storm-constrain (broadcast|multicast|unicast) min-rate <1-1488100> max-rate <1-1488100>	Storm control of broadcast, multicast or unknown unicast packets under the interface	Interface configuration mode
no storm-constrain (broadcast|multicast|unicast|all)	Cancel storm control	Interface configuration mode

storm-constrain action (block|shutdown)	Configure the action of storm control. By default, no storm control is performed on packets	Interface configuration mode
no storm-constrain action	Cancel the configured storm control action	Interface configuration mode
storm-constrain enable (log|trap)	Switch to record log or report alarm when storm control is turned on	Interface configuration mode
no storm-constrain enable (log|trap|all)	Switch to record log or report alarm when storm control is turned off	Interface configuration mode
storm-constrain interval <6-180>	Configure the storm control detection interval. By default, the storm control detection interval is 5 seconds	Interface configuration mode
no storm-constrain interval	Restore the storm control detection interval to the default value	Interface configuration mode
no storm-constrain	Remove the storm control function of the interface	Interface configuration mode
show storm-constrain	View storm control information for all interfaces	Privileged mode
show storm-constrain interface IFNAME	View storm control information on the interface	Privileged mode

Configuration instructions:

(1) View the storm control information description table of the interface

project	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	Storm control actions, including (1) block-block message; (2) shutdown-shutdown interface

punish-status	Packet status of the current interface, including (1) block-when the rate is greater than max-rate and the storm control action is blocked, the status is blocked; (2) Normal-normal forwarding; (3) shutdown-when When it is greater than max-rate and the storm control action is to close the interface, the status is to close the interface
trap	Alarm switch status, on/off
log	Log switch status, on/off
interval	Storm control detection time interval, the unit is second, the default value is 5 seconds
last-punish-time	Last time to implement storm control penalties

(2) By executing the storm- constrain action command to configure storm control actions and the storm- constrain command to configure storm control high and low thresholds, you can control storm packets to prevent flooding. During the storm control detection interval, when the average rate of receiving broadcast, multicast, or unicast packets on an interface is greater than the specified high threshold, Storm Control will block the interface or shut down the interface according to the configured action. When the storm control action is a blocking packet, if the traffic is below the minimum threshold, the interface returns to the normal forwarding state; when the storm control action is to shut down the interface, the interface cannot be automatically restored, you need to manually execute the no shutdown command to restore, you can cancel Port storm control shutdown action configuration to restore.
(3)The port traffic exceeds the upper threshold or falls back from the upper threshold to the lower threshold and outputs log/trap information

3.5 Configure FLOW-CONTROL

FLOW-CONTROL (flow control) is used to prevent data loss when the port is blocked. In half-duplex mode, flow control is achieved through Backpressure technology, which causes the information source to reduce the sending rate. In full-duplex mode, flow control follows the IEEE802.3x standard, and the blocked port sends a "Pause" packet to the information source to suspend its transmission.

This section describes the configuration of FLOW-CONTROL in detail, including the following contents:

- Default configuration
- Set the port side flow control
- Set the flow control on the receiving side of the port
- Turn off port flow control

- Display flow control information

3.5.1 Default configuration

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

3.5.2 Set port receive and send side flow control

The following command configures the port to receive and send flow control to open in interface configuration mode:

flowcontrol

3.5.3Turn off port flow control

The following command disables flow control on the sending and receiving sides of the port in interface configuration mode:

no flowcontrol

3.5.4 Display flow control information

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

show flowcontrol

The following command displays the flow control information of a certain port in normal mode or privileged mode:

show flowcontrol interface <if-name>

Among them, <if-name> is the name of the port to query flow control information.

3.6 Configure port bandwidth

Port bandwidth control is used to control the rate at which ports are sent and received. This section describes the configuration of port bandwidth in detail, including the following contents:

- Default configuration
- Set the port to send or receive bandwidth control

- Cancel port send or receive bandwidth control
  Display the bandwidth control of the port configuration

3.6.1 Default configuration

The switch supports setting the sending and receiving bandwidth separately for each port. There is no bandwidth control on the default port.

3.6.2 Set port send or receive bandwidth control

The following command sets the port transmit or receive bandwidth control in interface configuration mode:

portrate {egress | ingress} <rate>

egress means to control the bandwidth of the sent data packets.

ingress means to control the bandwidth of the received data packets.

<rate> indicates the value of the bandwidth to be set, the range is 1-1024000, and the unit is kbits.

3.6.3 Cancel port sending or receiving bandwidth control

The following command cancels the port bandwidth control in interface configuration mode:

no portrate {egress | ingress}

egress means to cancel the bandwidth control of sending data packets.

ingress means cancel the bandwidth control of the received data packet.

3.6.4 Display the bandwidth control of the port configuration

The following command checks the bandwidth control of the port configuration in normal mode or privileged mode:

show portrate interface <if-name>

Where <if-name> is the name of the port whose bandwidth control information is to be queried.

3.7 Configure TRUNK

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

All ports in the TRUNK group must be configured for the same speed and in full-duplex mode. The switch can support up to 8 groups of TRUNK, each group of TRUNK members can be up to 8. It is important to note that each port can only belong to a trunk group.

The LACP protocol is a protocol based on the IEEE802.3ad standard. The LACP protocol exchanges information with the peer through LACPDU (Link Aggregation Control Protocol Data Unit).

The LACP protocol is enabled on the interface in the aggregation group. The interface will notify the peer of its system LACP protocol priority, system MAC, port LACP protocol priority, port number, and operation key by sending LACPDUs. After receiving the LACPDU, the peer compares the information in it with the information received by other interfaces to select the interface that can be in the Selected state, so that both parties can reach an agreement that the interface is in the Selected state.

The operation key is a configuration combination that is automatically generated according to certain configurations of member ports during link aggregation, including port rate, duplex mode, up/down status, allowed VLANs on the port, and default VLAN ID of the port, The link type of the port (ie Trunk, Hybrid, Access type), etc. In the aggregation group, the member ports in the Selected state have the same operation key.

This section describes the configuration of TRUNK in detail, including the following contents:

- LACP protocol configuration
- Configuration of TRUNK group
- TRUNK member port configuration
- TRUNK load balancing strategy configuration

TRUNK display

3.7.1 LACPprotocol configuration

command	description	CLI mode
lacp system-priority <1-65535>	Set the priority of lacp system	Global configuration mode
no lacp system-priority	Restore the default value of system priority 32768	Global configuration mode
lacp max-active-link-number <1-8>	Set the upper limit of LACP active aggregation port	Global configuration mode
no lacp max-active-link-number	Restore the default upper limit of the LACP active aggregation port 8	Global configuration mode
lacp port-priority <1-65535>	Set the priority of lacp port	Interface

		configuration mode
no lacp port-priority	Restore the default port priority 32768	Interface configuration mode
lacp timeout (short|long)	Set lacp port timeout, default long timeout	Interface configuration mode
show lacp summary	Show a simple situation of all lacp aggregation	Privileged mode
show lacp detail	Show all lacp aggregation	Privileged mode
show lacp <1-8>	Display the details of the lacp aggregation port	Privileged mode
show lacp port IFNAME	Display the details of the lacp port	Privileged mode
show lacp system-id	Display the status of lacp system	Privileged mode
show lacp counter <1-8>	Display statistics of lacp aggregation port	Privileged mode
show lacp counter	Display statistics of all lacp aggregation ports	Privileged mode
clear lacp <1-8> counters	Clear the statistics of lacp aggregation port	Privileged mode
clear lacp counters	Clear statistics of all lacp aggregation ports	Privileged mode

3.7.2 Configuration of the TRUNK group

The following command creates a manual trunk group in global configuration mode:
trunk <trunk-id>

Create a TRUNK group. The value range of <trunk-id> is 1-8, indicating the ID of the TRUNK group to be created. Up to 8 groups of TRUNK can be configured; after successful creation, the interface name of the TRUNK group is trunk+id, such as the group ID The interface of the TRUNK group with the number 1 is named trunk1. In the configuration mode, you can use the "interface trunk+id number" command to enter the interface configuration mode, and then operate the trunk group. For example, use the command interface trunk1 to enter the trunk mode of trunk 1, and configure trunk 1.

The following command creates a static LACP TRUNK group in global configuration mode:

trunk <1-8> dynamic

The following command deletes a trunk group in global configuration mode:

no trunk <trunk-id>

When deleting the TRUNK group, you must ensure that the TRUNK group has no member ports.

3.7.3 TRUNK group member port configuration

The following command adds a member port of the trunk group in interface configuration mode:

trunk interface IFNAME (passive|)

<if-name> is the name of the port that needs to be added to the trunk group, and must be a Layer 2 interface. Each group of TRUNK can add up to 8 Layer 2 interfaces. If the TRUNK group is a static LACP TRUNK group, the added interface defaults to the active state, and can also be configured in the passive state.

The following command deletes all member ports of the trunk group in interface configuration mode:

no trunk interface

The following command deletes the specified trunk group member port in interface configuration mode:

no trunk interface <if-name>

You can use this command multiple times to delete multiple member ports of the trunk group.

3.7.4 TRUNK load balancing strategy configuration

The following command sets TRUNK's load balancing strategy in 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 destination 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 strategy in interface

configuration mode:

no trunk load-balance

The default port load balancing strategy is src-dst-mac (a balancing strategy based on source MAC and destination MAC).

3.7.5 TRUNK's display

The following command checks all trunk group configurations in normal mode or privileged mode:

show trunk

The following command checks the configuration of the specified trunk group in normal mode or privileged mode:

show trunk <trunk-id>

Where <trunk-id> is the ID number of the TRUNK group to be queried.

3.8 Configuring Jumbo Frames

3.8.1 Introduction to Jumbo Frames

In order to realize that the port can receive jumbo frames, the port can be set to support a specific jumbo frame length.

3.8.2 Jumbo frame configuration

Configure the port to support jumbo frame length. In config mode, enter the port configuration mode, such as interface ge1/1, execute the following command:

Switch(config-ge1/1)# jumbo frame 2000

Jumbo frame length supported by display port

Switch#show jumbo frame ge1/1

Port	Jumbo frame(bytes)
ge1/1	2000

3.9 Configure redundant ports

In some special circumstances, such as the need to focus on ensuring the stability of certain servers linked to the network, the redundant ports of the switch can provide two ports to link to this server, and ensure that the server has only one LINK UP port link network at a time In the case of LINK DOWN on one port, the system immediately activates the other port.

When a port is in the LINK UP in the redundant port group, we call it the Active state;

conversely, if a port is in the LINK DOWN in the redundant port group, we call it the Disable state.

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

- Redundant port configuration
- Display of redundant ports

3.9.1 Redundant port configuration

The switch can be configured with 8 groups of redundant ports, and a group of redundant ports can only be configured with 2 ports; one port can only be configured into one redundant port group.

A redundant port group can be configured with a primary-port and secondary-port. When the configuration enables redundant port groups:

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 is set to the Disable state;

2. If only one port is in LINK UP state, put the current LINK UP port into Active state, and the other port is in Disable state;

3.Otherwise, both ports are in Disable state.

If a LINK DOWN event occurs on a port in the Active state, another port will be tried to be placed in the Active state.

Another configuration parameter is the force-switch, which is when the secondary-port is Active and the primary-port is in the Disable state. If a LINK UP event occurs in the primary-port at this time, it is decided whether to switch to the primary-port again. Active, secondary-port is Disabled. If force-switch is configured as enable, then it is forced to switch, otherwise the port status of the original redundant port group will be retained.

command	description	CLI mode
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 primary port interface, secondary-port IFNAME is the name of the secondary port interface, Whether force-switch enables the force switch.	Global configuration mode
redundant-port <1-8> force-switch	Enable the forced switch of the redundant port.	Global configuration mode

no redundant-port <1-8>	Delete the redundant port group.	Global configuration mode
no redundant-port <1-8> force-switch	Turn off the forced switch of the redundant port.	Global configuration mode

3.9.2 Display of redundant ports

Commands to display redundant ports

command	description	CLI mode
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 types of network devices and their respective configurations are intricate. In order to enable devices of different manufacturers to discover and interact with their systems and configuration information on the network, a standard information exchange platform is required.

LLDP (Link Layer Discovery Protocol, Link Layer Discovery Protocol) was created in this context, it provides a standard link layer discovery method, you can the main capabilities of the local device, management address, device identification , Interface identification and other information are organized into different TLV (Type/Length/Value, type/length/value), and encapsulated in LLDPDU (Link Layer Discovery Protocol Data Unit, link layer discovery protocol data unit) and released to direct After receiving this information, the neighbor saves it in the form of a 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, mainly including the following:

- LLDP configuration
- LLDP display

3.10.1 LLDP configuration

There are 4 working modes of LLDP port:

TxRx: Both send and receive LLDP packets.

Tx: Only send and do not receive LLDP packets.

Rx：Only receive and do not send LLDP packets.

Disable：Neither sends nor receives LLDP messages.

When the LLDP working mode of the port changes, the port will initialize the protocol state machine. In order to avoid frequent changes in the working mode of the port and cause the port to continuously perform the initialization operation, you can configure the port initialization delay time. When the working mode of the port changes, the initialization operation is performed after a delay.

command	description	CLI mode
lldp global enable	LLDP global enable command.	Global configuration mode
lldp hold-multiplier <num>	Lldp TTL multiple.	Global configuration mode
lldp timer [<reinit-delay><time>][< tx-delay><time>][< tx-interval ><time>]	Configure various LLDP timers.	Global configuration mode
lldp enable	Enable interface LLDP	Interface configuration mode
lldp admin-status{ disable| rx|tx|rxtx}	Configure the working mode of the LLDP port.	Interface configuration mode
lldp check-change-interval <time>	Configure the interval for refreshing interface information	Interface configuration mode
lldp management-address <A.B.C.D>	Configure the interface LLDP management address	Interface configuration mode
lldp tlv-enable{ dot1-tlv| dot3-tlv|med-tlv }	Configure interface LLDP extended capability set switch	Interface configuration mode

3.10.2 Display of LLDP

LLDP commands

command	description	CLI mode
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 packet statistics	Privileged mode
show lldp status [ifname]	Display lldp status information	Privileged mode

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

- Introduction
- MAC binding configuration
- MAC filtering configuration

Port learning limit 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 simultaneously Bind multiple MAC addresses. MAC binding can be applied to a designated port at the same time as 802.1x. This function is very useful for some devices that do not have 802.1x functions or devices that are inconvenient to use 802.1x, such as printers and file servers.

MAC filtering can prevent some specified MAC addresses from accessing the network. The main purpose is to prevent illegal devices from accessing the network. When a MAC address is configured for MAC filtering, the MAC address cannot access the network at any port of the switch, nor can it receive packets whose destination MAC is the specified MAC address. Like MAC binding, a port can be configured with multiple MAC address for MAC filtering. In the application, if some virus software attacks the network through the forged MAC address, in addition to the ACL, it can also access and control these forged data packet attacks through MAC filtering.

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 this port is equal to the number configured for this port, it will no longer learn new MAC addresses. For these new MAC addresses, The packet will be dropped.

It should be noted that the MAC address referred to here is actually MAC+VID, and the description later in this chapter will not be repeated. In addition, the MAC binding function and 802.1x can be configured on one port at the same time; MAC filtering and port learning limit can be configured on one port at the same time; MAC binding function, 802.1x and MAC filtering, port learning limit can not be simultaneously Configured to the same port.

4.2 MAC binding configuration

MAC binding configuration supports manual binding of MAC addresses and automatic binding of MAC addresses. Manually binding the MAC address is that the user enters the MAC address one by one through the command to bind to the port. The automatic MAC address binding is to read the existing entry of the port in the layer 2 hardware forwarding table and directly perform MAC address binding. The command to read the second layer hardware table is Show bridge fdb.

Configuration commands

command	description	CLI Mode
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>	Automatically convert the specified number of MAC addresses of an interface into MAC binding configuration.	Interface configuration mode
switchport-security mac-bind auto-conversion vlan <1-4094>	Automatically convert the MAC address of a specified VLAN of an interface into MAC binding configuration.	Interface configuration mode
show port-security mac-bind [IFNAME]	Display MAC binding configuration	Privileged mode

Note:

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

The port has been configured with 802.1x

The port has been configured with MAC filtering or port learning restrictions;

The MAC address has been bound to another port, or MAC filtering is configured;

The L2 table of the switch is full.

4.3 MAC filtering configuration

MAC filtering configuration supports manual binding of MAC addresses and automatic binding of MAC addresses. Manual configuration of MAC filtering is to bind MACs and ports by entering the MACs to be filtered one by one through commands. The automatic configuration of MAC filtering is to read out the existing entries of the port in the layer 2 hardware forwarding table and directly perform MAC filtering configuration. The command to read the second layer hardware table is Show bridge fdb.

Configuration commands

command	description	CLI mode
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- filter auto-conversion number <1-	Automatically convert the specified number of MAC	Interface configuration

16383>	addresses of an interface to MAC filtering configuration	mode
switch port-security mac-filter HHHH.HHHH.HHHH vlan <1-4094>	Automatically convert the MAC address of a specified VLAN of an interface to MAC filtering configuration	Interface configuration mode
show port-security mac-filter [IFNAME]	Display MAC binding configuration	Privileged mode

Note:

The reasons for invalid or failed MAC filtering configuration may be as follows:

The port has been configured with MAC binding or enabled 802.1x protocol function;

The MAC address has been bound to another port, or MAC binding is configured;

The L2 table of the switch is full.

4.4 Port Learning Limit Configuration

The switch can configure the maximum number of dynamic learning addresses for each port. If a port is configured to dynamically learn the number of MAC addresses, then the port can only learn the corresponding number of MAC addresses. When the MAC address exceeds this number, it cannot learn and forward on this port.

If no learning limit is configured, a port can learn up to 16,383 MAC addresses.

Configuration commands

command	description	CLI mode
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

Configure port ge1/5 to learn only 7 MAC addresses

Switch#configure terminal

Switch(config)interface ge1/5

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

Note:

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

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

Chapter5 Port IP and MAC binding

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

- Introduction
- IP and MAC binding configuration
- Configuration example

Configuration troubleshooting

5.1 Introduction

Configuring IP and MAC binding on the Layer 2 switch port is a static defense measure against ARP attacks. The ARP attacker attacks the user by sending an ARP message carrying a false MAC address, causing the user's local ARP cache table to be overwritten by the attacker's MAC address, and normal data flows to the attacker. Configuration commands on the switch port can be used to statically bind user IP addresses and MAC addresses to effectively filter ARP attack packets.

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

The four functions of IP MAC binding, ACL, 802.1x anti-ARP spoofing and DHCP SNOOPING all use the same system resource CFP. When configuring, pay attention to whether the CFP resource is exhausted. At the time of design, we formulated the compatibility relationship between them. The following table:

	IP MAC binding	ACL	802.1x	DHCP SNOOPING
IP MAC binding	compatible	Not compatible	compatible	compatible
ACL	Not compatible	compatible	Not compatible	Not compatible
802.1x	compatible	Not compatible	compatible	Not compatible
DHCP SNOOPING	compatible	Not compatible	Not compatible	compatible

CFP is a limited hardware resource. On average, only 16 IP MAC binding entries can be configured per port. Therefore, if there are only a few ports or a few IP and MAC addresses to be controlled in a network with many access hosts, static can be used. IP MAC binding function. To avoid the data forwarding failure due to CFP exhaustion.

In addition, as to whether to use 802.1x or DHCP SNOOPING protocol, it depends on the current situation. If you use a static IP address configuration and use 802.1x protocol to access the network, you must use 801.1x anti-ARP spoofing to be effective. If you use dynamic acquisition of IP address Case, you need to use the DHCP SNOOPING protocol.

5.2 IP and MAC binding configuration

IP and MAC binding configured in interface mode

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 and MAC binding

Switch#configure terminal

Switch(config)#interface ge1/1

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

Display configuration

Display binding entries for all ports

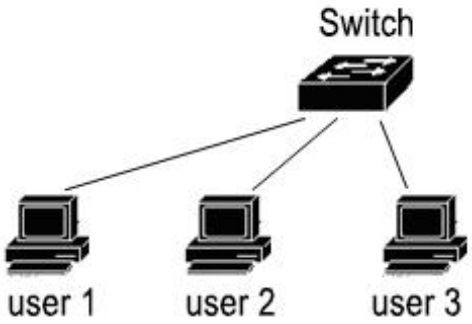
show ip mac-bind

Display binding entries for an interface

show ip mac-bind IFNAME

5.3 Configuration example

There are user 1, user 2, and user 3 in the network, and the user's IP and MAC are bound to the port to prevent ARP attacks.



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 192.168.0.1/24
!
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 Layer 3 interface or a trunk interface.

Chapter 6 VLAN Configuration

VLAN is an important concept in switches, and it is widely used in practical applications. It is the basis for dividing multiple networks internally. VLAN is short for Virtual Local Area Network. It is a network that logically organizes multiple devices together, regardless of the physical location of the devices. Each VLAN is a logical network, which has all the functions and attributes of a traditional physical network. Each VLAN is a broadcast domain. Broadcast packets can only be forwarded in one VLAN, and cannot cross VLANs. Data communication between VLANs must be forwarded through Layer 3.

This chapter mainly includes the following:

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

6.1 Introduction to VLAN

This section gives a detailed introduction to VLAN, mainly including the following:

- Benefits of VLAN
- VLAN ID
- VLAN port member type
- The default VLAN of the port
- Port VLAN mode
- VLAN trunking
- Data flow forwarding in VLAN

VLAN subnet

6.1.1 Benefits of VLAN

VLAN greatly expands the size of the physical network. The traditional physical network can only have a very small scale, which can accommodate thousands of devices at most, and the physical network divided by VLAN can accommodate tens of thousands or even hundreds of thousands of devices. VLANs have the same functions and attributes as traditional physical networks.

Using VLAN has the following benefits:VLAN can effectively control the traffic in the network. In a traditional network, regardless of whether it is necessary or not, all broadcast packets are

transmitted to all devices, which increases the load on the network and devices. The VLAN can organize devices in a logical network as needed. A VLAN is a broadcast domain, and broadcast packets are transmitted only within the VLAN, and do not cross the VLAN. By dividing VLANs, you can effectively control the traffic in the network.

- VLAN can improve the security of the network.

The devices in a VLAN can only communicate with devices in the same VLAN at Layer 2. If you want to communicate with another VLAN, you must use Layer 3 forwarding. If you do not establish Layer 3 forwarding between VLANs, communication between VLANs will be completely impossible. The role of isolation ensures data security in each VLAN. For example, if a company's R&D department does not want to share data with the marketing department, the R&D department can establish a VLAN, the marketing department can establish a VLAN, and there is no Layer 3 communication channel between the two VLANs.

VLAN makes the movement of equipment convenient.

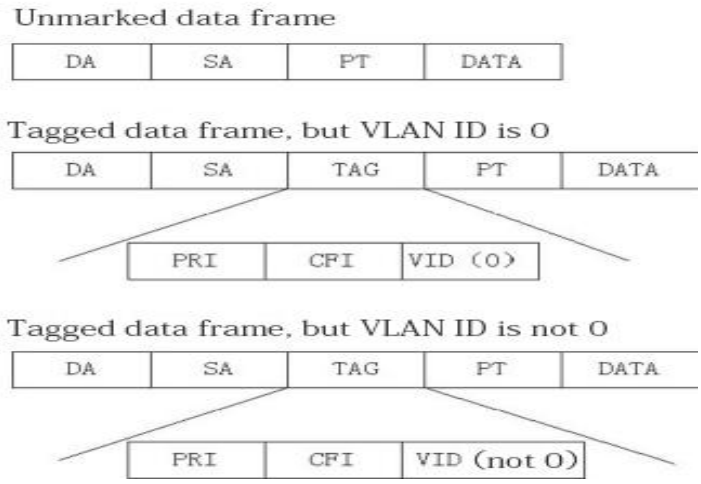
If a device in a traditional network moves from one location to another and belongs to a different network, the network configuration of the mobile device needs to be modified, which is very inconvenient for users. A VLAN is a logical network. Devices that are not in the same physical location can be placed on the same network. When the device moves, the device can also belong to this VLAN, so that the mobile device does not need to modify any configuration.

6.1.2 VLAN ID

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

The switch supports 4094 VLANs. When creating a VLAN, a VLAN ID must be selected, ranging from 2 to 4094. The switch creates VLAN 1 by default, and VLAN 1 cannot be deleted.

There are three kinds of data frames transmitted in a VLAN in the network: data frames without tags, data frames with tags with VID of 0, and data frames with tags with VID other than 0. The following figure shows three different data frame formats.



All data frames inside the switch are marked. If a untagged data frame is entered into the switch, the switch adds a tag to the data frame and selects a VLAN ID value to fill in the tagged VID. If a tagged data frame with a VID of 0 enters the switch, the switch selects a VLAN ID value to fill in the tagged VID. If a data frame with a VID other than 0 is input to the switch, the frame remains unchanged.

6.1.3 VLAN port member type

The switch supports port-based VLAN and 802.1Q-based VLAN. A VLAN includes two types of port members: untagged members and tagged members. A VLAN can include both untagged port members and tagged port members.

A VLAN can have no port members or one or more port members. When a port belongs to a VLAN, it can be an untagged or tagged member of the VLAN.

A port can belong to tagged or untagged members of one or more VLANs. If a port belongs to tagged members of two or more VLANs, this port is also called a VLAN trunk port. A port can belong to untagged members of one or more VLANs and tagged members of one or more VLANs at the same time.

6.1.4 The default VLAN of the port

There is one and only one default VLAN for a port. The default VLAN is used to determine the VLAN to which untagged or tagged packets with a VID of 0 enter. The default VLAN is also called port VID or PVID. By default, the default VLAN of a port is 1.

6.1.5 VLAN mode of port

There are three VLAN modes on the port: ACCESS mode, TRUNK mode and HYBRID mode. The user must first specify the port's VLAN mode when configuring the port's VLAN.
The port in ACCESS mode is an access port that directly faces the user. The port can only belong to an untagged member of a VLAN. The default VLAN is the VLAN specified by the user. When the port belongs to only one untagged member of a VLAN, you can specify the

VLAN mode of the port as ACCESS mode.

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

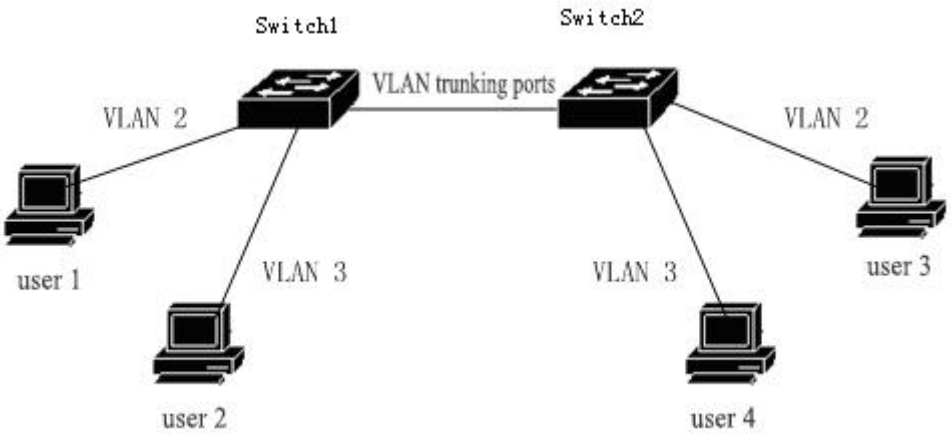
The port in HYBRID mode is a trunk port that is directly connected to the switch. The port can belong to one or more VLAN tagged members and/or one or more VLAN tagged members. The default VLAN of this port can be changed.

In actual application, the user can select the VLAN mode of the port according to the specific situation.

6.1.6 VLAN trunking

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

The following figure is an example of VLAN trunking. Two switches are connected by VLAN trunk ports, which are trunk ports of VLAN 2 and VLAN 3. Each switch is divided into two VLANs, namely VLAN 2 and VLAN 3. There is one user in each VLAN. 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 Data flow forwarding in VLAN

When the switch receives a packet from a port, it performs Layer 2 forwarding according to the following steps:

- Determine 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 according to different data packets (can be zero, one or

more output ports), if there is no output port, discard the data packet.

- According to the member type of the output port in the VLAN, decide whether the outgoing packet is tagged.
- Sent 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 not tagged or tagged but the VID value in the tag is 0, the VLAN to which the packet belongs is the default VLAN of the port.

2) How to determine the type of packet:

If the destination MAC address of the received data packet is FF:FF:FF:FF:FF:FF, the data packet is a broadcast data packet.

If the received packet is not a broadcast packet and the 40th bit of its destination MAC address is 1, the packet is a multicast packet.

If it is neither a broadcast data packet nor a multicast data packet, the data packet is a unicast data packet.

3) How to determine the output port of the data 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 packet is a multicast packet, first look up the Layer 2 hardware multicast forwarding table based on the destination multicast MAC address and the VLAN to which it belongs. If a matching multicast entry is found, the output port and the VLAN to which the multicast entry belongs The common port (and operation) in the member ports in is the output port of the packet. If there is no common port, the packet is discarded. If no matching multicast entry is found in the Layer 2 hardware multicast forwarding table, the output port is determined according to the forwarding mode of the Layer 2 hardware multicast forwarding table. If the multicast forwarding mode is not registered, multicast packets are treated as broadcast. All member ports of the VLAN to which they belong are the output port of the packet. If it is in the registered forwarding mode, there is no output port and the packet is dropped.

If the input data packet is a unicast data packet, first look up the Layer 2 hardware forwarding table based on the destination MAC address and the VLAN to which it belongs. If a matching entry is found, the output port in the entry is a common port among the member ports of the VLAN AND operation) is the output port of the packet. 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 treated as a broadcast packet, and all member ports of the VLAN to which it belongs are the output port of the packet.

4) Send data packet:

After deciding the output port of the input data packet, the data packet should be sent out from all output ports.

If an output port is an untagged member of the VLAN to which the packet belongs, the packet is sent out of the output port without tag.

If an output port is a tagged member of the VLAN to which the packet belongs, the packet is tagged 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 VLAN configuration, mainly including the following:

- Create and delete VLANs
- Configure the VLAN mode of the port
- VLAN configuration in ACCESS mode
- TRUNK mode VLAN configuration
- VLAN configuration in HYBRID mode
- VLAN subnet configuration

View VLAN information

6.2.1 Create and delete VLAN

Before creating and deleting VLANs, users need to use the vlan database command in the global configuration mode to enter the VLAN configuration mode, and create and delete VLANs in this mode.

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

command	description	CLI mode
vlan <vlan-id>	Create a VLAN. If the VLAN already exists, no processing is done, otherwise the VLAN is created. The parameters range from 2 to 4094.	VLAN configuration mode
no vlan <vlan-id>	Delete a VLAN, if the VLAN does not exist, it will not be processed, otherwise delete the VLAN. The parameters range from 2 to 4094.	VLAN configuration mode

6.2.2 Configure the VLAN mode of the port

Before configuring a port's VLAN, you need to specify the port's VLAN mode. By default, the port's VLAN mode is ACCESS. The commands for specifying the VLAN mode of the port are as follows:

command	description	CLI mode
switchport mode access	The VLAN mode of the designated port is ACCESS mode. After this command is executed, the port is an untagged member of VLAN 1, and the default VLAN of the port is 1.	Interface configuration mode
switchport mode trunk	The VLAN mode of the designated 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 the TRUNK mode, and returns to the default situation, namely the ACCESS mode.	Interface configuration mode
switchport mode hybrid	The VLAN mode of the designated port is HYBRID mode. After this command is executed, the port is an untagged member of VLAN 1, and the default VLAN of the port is 1.	Interface configuration mode
no switchport hybrid	The VLAN mode of the port is no longer HYBRID mode, and returns to the default situation, namely ACCESS mode.	Interface configuration mode

6.2.3 VLAN configuration in ACCESS mode

Before configuring the port for VLAN, you need to specify the VLAN mode of the port as ACCESS mode. In this VLAN mode, the port is the untagged member of VLAN 1 by default, and the default VLAN of the port is 1. The VLAN configuration commands in ACCESS mode are as follows:

command	description	CLI mode
switchport access vlan <vlan-id>	Configure the port as an 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 default, that is, the port is an untagged member of VLAN 1, and the default VLAN of the port is 1.	Interface configuration mode

6.2.4 TVLAN configuration in RUNK mode

Before configuring the port for VLAN, you need to specify the VLAN mode of the port as TRUNK mode. In this VLAN mode, the port is the tagged member of VLAN 1 by default, and the default VLAN of the port is 1. The VLAN configuration commands in TRUNK mode are as follows:

command	description	CLI mode
switchport trunk native vlan <vlan-id>	Configure the default VLAN of the port, which is pvid. The parameters range from 2 to 4094.	Interface configuration mode
switchport trunk allowed vlan all	The configuration port is a tagged member of all VLANs. For newly created VLANs, the port is also a tagged member of these VLANs.	Interface configuration mode

switchport trunk allowed vlan none	Except for VLAN1, this port is no longer a tagged member of all other VLANs.	Interface configuration mode
switchport trunk allowed vlan add <vlan-list>	Configure the port to become a tagged member of one or more VLANs. The parameter <vlan-list> can be a VLAN, a VLAN range, or multiple VLANs. For example, the parameter can be "1", "2-4" or "1,3,5".	Interface configuration mode
switchport trunk allowed vlan remove <vlan-list>	Remove the port from the specified VLAN or VLANs and no longer be a tagged member of these VLANs. The parameter <vlan-list> can be a VLAN, a VLAN range, or multiple VLANs. For example, the parameter can be "1", "2-4" or "1,3,5".	Interface configuration mode

6.2.5 VLAN configuration in HYBRID mode

Before configuring the port for VLAN, you need to specify the VLAN mode of the port as HYBRID mode. In this VLAN mode, the port is the untagged member of VLAN 1 by default, and the default VLAN of the port is 1. The VLAN configuration commands in HYBRID mode are as follows:

command	description	CLI mode
switchport hybrid native vlan <vlan-id>	Configure the port as an untagged member of the specified VLAN and the default VLAN of the port as the specified VLAN. The parameters range from 2 to 4094.	Interface configuration mode
no switchport hybrid vlan	Remove the port from the default VLAN and no longer	Interface configuration

	be a tagged or untagged member of the default VLAN. The default VLAN of the port returns to 1.	mode
switchport hybrid allowed vlan all	The configuration port is a tagged member of all VLANs (except VLAN 1). For newly created VLANs, the port is also a tagged member of these VLANs.	Interface configuration mode
switchport hybrid allowed vlan none	Except for VLAN1, the port is no longer a tagged or untagged member of all other VLANs, and the default VLAN of the port returns to 1.	Interface configuration mode
switchport hybrid allowed vlan add <vlan-list> egress-tagged enable	Configure the port to become a tagged member of one or more VLANs. The parameter <vlan-list> can be a VLAN, a VLAN range, or multiple VLANs. For example, the parameter can be "1", "2-4" or "1,3,5".	Interface configuration mode
switchport hybrid allowed vlan add <vlan-list> egress-tagged disable	Configure the port to become an untagged member of the specified VLAN or VLANs. The parameter <vlan-list> can be a VLAN, a VLAN range, or multiple VLANs. For example, the parameter can be "1", "2-4" or "1,3,5".	Interface configuration mode
switchport hybrid allowed vlan remove <vlan-list>	Remove the port from the specified VLAN or VLANs and no longer be a tagged or untagged member of these VLANs If the default VLAN of the port belongs to the	Interface configuration mode

	specified VLAN, the default VLAN returns to 1.	

6.2.6 View VLAN information

The commands for viewing VLAN information are as follows:

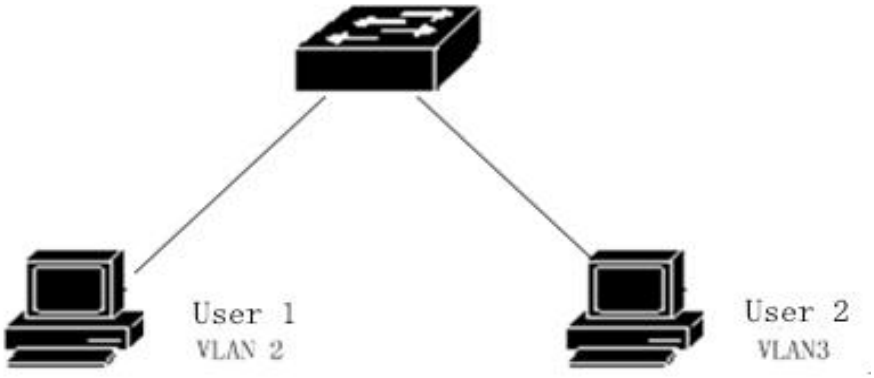
command	description	CLI mode
show vlan [vlan-id]	If no parameters are entered, all VLAN information is displayed, and if parameters are entered, the information of a specified VLAN is displayed. The parameters range from 1 to 4094.	Normal mode
show interface switchport	Display the VLAN related information of all ports of the system, such as VLAN mode, default VLAN, etc.	Normal mode
show running-config	View the current configuration of the system, you can view the VLAN configuration.	Privileged mode

6.3 VLAN configuration example

6.3.1 PORT-based VLAN

1) Configuration

There are two users, user 1 and user 2. The two users need to be in different VLANs due to 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 configuration of the switch is as follows:

Create VLAN

Switch#config t

Switch(config)#vlan database

Switch(config-vlan)#vlan 2

Switch(config-vlan)#vlan 3

Assign ports to VLANs

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) Debug

If, after configuration, it is found that PCs in different VLANs cannot communicate, this is normal, because communication between different VLANs must go through Layer 3 routing and forwarding. If PCs in the same VLAN cannot communicate, the following verification must be made:

show vlan

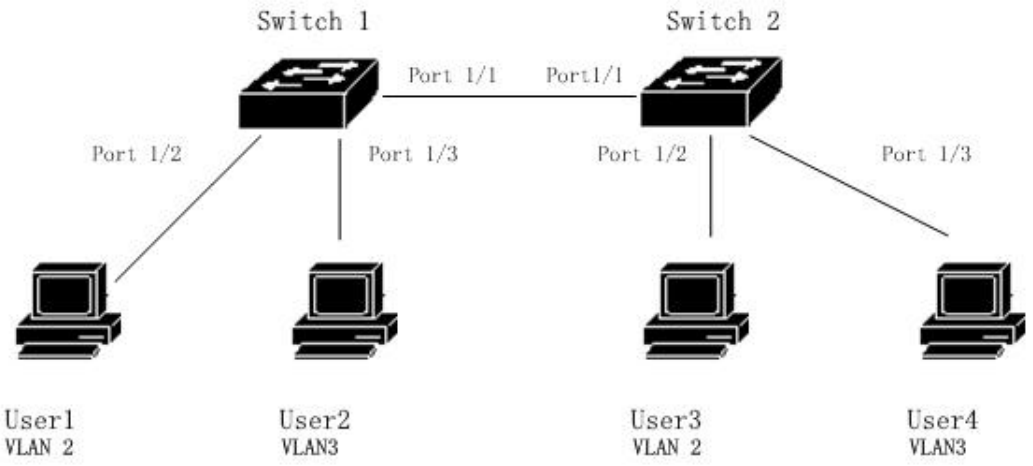
View the status of all VLAN member ports

show vlan <vlan-id>

Check whether the port connected to a specific PC is in the specified VLAN

6.3.2 802.1Q-based VLAN

1) Configuration



There are two switches to connect two users：

User	VLAN	Connecting port	Switches	Cascade port
User1	2	1/2	Switch1	1/1
User2	3	1/3	Switch1	1/1
User3	2	1/2	Switch2	1/1
User4	3	1/3	Switch2	1/1

Need to configure on two 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) Debug

Cross-switch vlan, PCs in the same vlan can communicate. If not, please check the following：

- Whether the port connected to the PC belongs to the corresponding VLAN, and apply the ACCESS mode to join this 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

MAC-based VLANs are divided according to the source MAC address of the message. After receiving the untagged (or tag is 0) packet from the port, the device determines the VLAN to which the packet belongs according to the source MAC address of the packet, and then automatically divides the packet into the designated VLAN for transmission;

VLANs based on IP subnets are divided according to the source IP address and subnet mask of the message. After receiving the untagged packet from the port, the device determines the VLAN to which the packet belongs according to the source address of the packet, and then automatically divides the packet into the designated VLAN for transmission.

This feature is mainly used to transmit the packets sent by the specified network segment or IP address in the specified VLAN;

Protocol-based VLANs assign different VLAN IDs to packets based on the protocol type to which the packets received by the port belong. The protocols that can be used to divide VLANs are IP, IPV6, IPX, etc.

Before configuring a VLAN based on MAC, IP subnet, or protocol, you must first create the corresponding VLAN.

command	description	CLI mode
mac-vlan mac WORD vlan <1-4094>	Create a VLAN based on the source MAC address	Interface configuration mode
no mac-vlan mac WORD	Delete a VLAN based on source MAC address	Interface configuration mode
no mac-vlan	Delete all VLANs based on source MAC address	Interface configuration mode
show mac-vlan	Display all VLANs based on source MAC address	Privileged mode
ip-subnet-vlan ip A.B.C.D A.B.C.D vlan <1-4094>	Create a VLAN based on the source IP subnet	Interface configuration mode
no ip-subnet-vlan ip A.B.C.D A.B.C.D	Delete a VLAN based on the source IP subnet	Interface configuration mode
no ip-subnet-vlan	Delete all VLANs based on the source IP subnet	Interface configuration mode
show ip-subnet-vlan	Display all VLANs based on source IP subnet	Privileged 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 VLANs	Interface configuration mode
show protocol-vlan	Show all protocol-based VLANs	Privileged mode
show vlan-partition interface IFNAME	Display the status of VLAN based on MAC, IP subnet and protocol on the interface	Privileged mode

6.5 Voice VLAN

Voice VLAN is a VLAN specially divided for users' voice data flow. By dividing the Voice VLAN and adding the port connected to the voice device to the Voice VLAN, you can configure QoS (Quality of Service) parameters for voice data to improve the priority of voice data packets and ensure 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 packet entering the port. Packets whose source MAC address matches the OUI address of the voice device set by the system are considered as voice data streams and are divided into Voice VLANs for transmission.

The user can set the OUI address in advance, or use the default OUI address as the judgment criterion, as follows

Serial 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 manually. Then, by identifying the source MAC of the message and matching the OUI address, after the match is successful, the system will issue ACL rules and configure the priority of the message.

Voice VLAN security mode and normal mode, security mode: only allow OUI matching language flow transmission in Voice VLAN, while OUI mismatching data flow is not allowed in Voice VLAN; normal mode: all data flow can be in Voice Transmission in VLAN.

Before configuring Voice VLAN, you must first create the corresponding VLAN.

command	description	CLI mode
voice-vlan security (enable|disable)	Voice VLAN security mode is enabled	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 by OUI address and mask	Global configuration mode

no voice-vlan oui description WORD	Delete user OUI configuration by naming	Global configuration mode
no voice-vlan oui	Delete all user OUI configuration	Global configuration mode
no voice-vlan default-oui WORD mask WORD	Delete defualt OUI configuration by OUI address and mask	Global configuration mode
no voice-vlan default-oui description WORD	Delete defualt OUI configuration by naming	Global configuration mode
no voice-vlan default-oui	Delete all defualt OUI configuration	Global configuration mode
voice-vlan default-oui resume	Restore all defualt OUI configuration	Global configuration mode
show voice-vlan oui	Display all defualt and user OUI configuration	Privileged mode
voice vlan <1-4094> (enable|disable)	Voice VLAN enabled on the interface	Interface configuration mode
voice vlan qos map-queue <0-7> remark-dscp <0-63>	The interface configures the qos priority, the default queue is 6, dscp is 46	Interface configuration mode
no voice vlan qos	Restore the default configuration of interface qos priority	Interface configuration mode
no voice vlan	Delete interface configuration Voice VLAN	Interface configuration mode
show voice-vlan state	Display the configuration of Voice VLAN on all interfaces	Privileged mode

6.6 VLAN mapping

The VLAN mapping (that is, VLAN Mapping) function can modify the VLAN Tag carried in the packet and provide the following mapping relationship: 1:1 VLAN mapping: Modify the VLAN ID in the VLAN Tag carried in the packet to another VLAN ID.

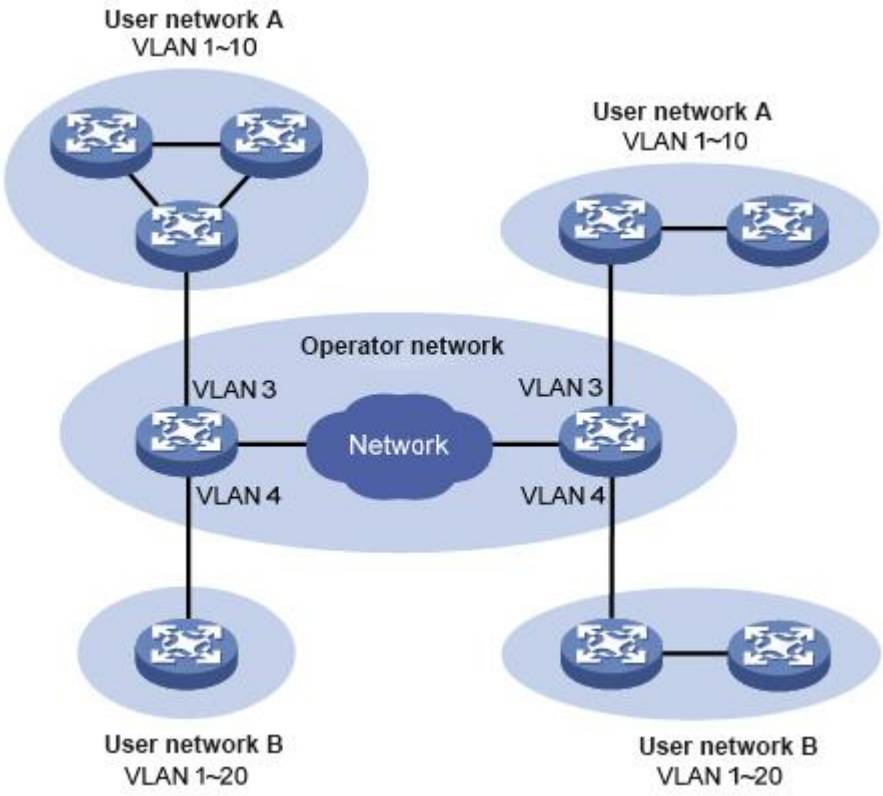
Before configuring VLAN mapping, you must first create the corresponding VLAN.

command	description	CLI mode
vlan-mapping vlan <1-4094>	Configure a VLAN mapping	Interface

map-vlan <1-4094>	relationship for the port	configuration mode
no vlan-mapping vlan <1-4094>	Delete a VLAN mapping relationship of the port	Interface configuration mode
no vlan-mapping	Delete all VLAN mappings of the port	Interface configuration mode
show vlan-mapping	Display all configured VLAN mappings	Privileged mode

6.7 QinQ

The port QinQ feature provided by the device is a simple and flexible Layer 2 VPN technology. It encapsulates the outer VLAN Tag for the user's private network packet on the edge device of the operator's network, so that the packet carries two Layer VLAN Tag through the operation Backbone's backbone network (public network). In the public network, the device only forwards the packet according to the outer VLAN tag, and learns the source MAC address entry of the packet into the MAC address table of the VLAN where the outer tag is located, while the user's private network VLAN tag is being transmitted. In the process, it will be transmitted as the data part of the message.
The QinQ feature allows operators to use one VLAN to serve user networks with multiple VLANs. As shown in the following figure, the private network VLAN of user network A is VLAN 1 to 10, and the private network VLAN of user network B is VLAN 1 to 20. The VLAN assigned by the operator to user network A is VLAN 3, and the VLAN assigned to user network B is VLAN 4. When packets with VLAN Tag of user network A enter the operator's network, the packets will be encapsulated with a layer of VLAN Tag with VLAN ID 3; when packets with VLAN Tag of user network B enter the operator's network , The packet will be encapsulated with a layer of VLAN tag with VLAN ID 4. In this way, the packets of different user networks are completely separated when they are transmitted on the public network. Even if the VLAN ranges of the two user networks overlap, there will be no confusion when the public networks are transmitted.



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

(1) Alleviate the problem of increasingly scarce public network VLAN ID resources.

(2) Users can plan their own private network VLAN ID without conflicting with the public network VLAN ID.

(3) Provide a relatively simple Layer 2 VPN solution for small metropolitan area networks or enterprise networks.

QinQ can be divided into two types: basic QinQ and flexible QinQ.

(1) Basic QinQ: Basic QinQ is implemented based on the port method. After the basic QinQ function of the port is enabled, when the port receives a packet, the device will tag the packet with the VLAN tag of the default VLAN of the port. If a packet with a VLAN tag is received, the packet becomes a double-tag packet; if a packet without a VLAN tag is received, the packet becomes a default VLAN tag with a port Message.

(2) Flexible QinQ: Flexible QinQ is a more flexible implementation of QinQ, which is implemented based on the combination of ports and VLANs. In addition to all basic QinQ functions, packets received on the same port can also perform different actions based on different VLANs, adding different outer VLAN tags to packets with different inner VLAN IDs.

command	description	CLI mode
qinq tpid WORD	Configure the tpid value carried in the VLAN tag of the port, the default is 0x8100	Interface configuration mode
no qinq tpid	Restore port default tpid	Interface configuration mode
qinq uplink	Configure the port as an uplink port	Interface configuration mode
no qinq uplink	Cancel the uplink configuration of the port	Interface configuration mode
qinq customer	Configure the port as a 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 translation for the interface	Interface configuration mode
no qinq inner-vid VLAN_ID	Delete a VLAN translation of the interface	Interface configuration mode
no qinq outer-vid <1-4094>	Delete a VLAN translation of the interface	Interface configuration mode
show qinq	Display all configured qinq conditions	Privileged mode

SAN Telequip (P) Ltd.,
504 & 505 Deron Heights, Baner Road
Pune 411045, India
Phone : +91-20-27293455, 8793779568
email : info@santelequip.com

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

- QoS introduction
- QoS configuration

QoS configuration example

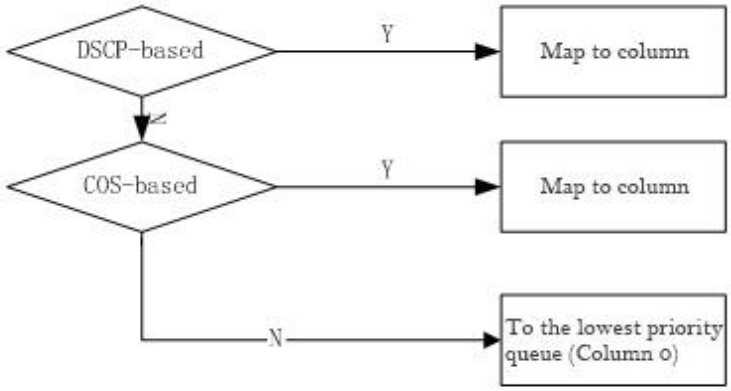
7.1 Introduction to QoS

Using the switch's QoS feature, you can prioritize important data streams forwarded through the switch, making your network's bandwidth utilization more reasonable and network performance predictable.

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

The switch implements QoS based on COS (802.1p), QoS based on DSCP (DiffServ) and QoS based on MAC. DSCP-based QoS can be configured on a physical port; COS-based QoS is enabled by default on physical ports.

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



The switch supports eight priority queues from 0 to 7, with queue 7 having the highest priority and queue 0 having the lowest priority. There are three types of scheduling for priority queues: SP, WRR, and WFQ. SP is strictly priority scheduling, that is, the packets of queue 7 are always forwarded preferentially. The packets of queue 6 are not forwarded until the packets of queue 7 are forwarded, and the packets of queue 5 are not forwarded until the packets of queue 6 are forwarded. And finally forward the data packets of queue 0. WRR refers to weighted priority polling. When forwarding data packets, the switch polls and forwards the data packets from the high priority queue to the low priority queue according to the configuration of the weight, and then forwards the right number of data packets from the high priority. When forwarding the next highest priority packet of weights, until the lowest priority queue is forwarded, it is

forwarded again from the highest priority, and so on. WFQ and WRR queue scheduling algorithms are similar, both support byte-count and weight in the weight algorithm, and also support SP grouping, which can be replaced with each other. The difference between the two is as follows: WRR supports the maximum delay, which can ensure that the maximum time for the packets in the configured queue from entering the queue to leave the queue does not exceed the maximum delay set; WFQ supports bandwidth guarantee, which can ensure that the port traffic is congested The minimum queue bandwidth that can be obtained.

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

QosProfile	802.1p (CoS) value	Priority queue
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 QoS

The port enables COS-based QoS by default. The switch will obtain the priority value of the VLAN TAG in the data packet entering the port, and determine the output queue of the data packet according to the user-configured COS value and the mapping relationship of the queue. If the data packet does not have VLAN TAG or the VID of VLAN TAG is 0, the switch will fill the data packet according to the default VID of the port configured by the user and the default priority of the port, and then determine the data packet according to the default priority Output queue.

7.1.2 DSCP-based QoS

If DSCP-based QoS is enabled for a port, the switch will obtain the DSCP value of the IP packet entering the port and determine the output queue of the packet according to the mapping relationship between the user-configured DSCP value and the queue.

The cos-dscp type is an extension based on the dscp type cos type, and its essence is one of the dscp type or the cos type. If the cos-dscp type is now used, the ip message system will

automatically match the dscp priority, and the non-ip message system will be based on the cos priority. According to the priority type (dscp/cos) for the corresponding scheduling.

7.1.3 Policy-based QOS

QoS strategy includes class and strategy action. Classes are used to identify flows. Users can use commands to define a series of rules to classify data packets; policy actions are used to define QoS actions performed by packets that match the rules. If policy-based QoS is enabled for a port, the switch will classify the packets entering the port. For the packets that meet the classification requirements, the switch will process the packets of the port according to the corresponding policy actions. For those that do not meet the classification requirements The data packet is not processed, and then the output queue of the data packet is determined according to the priority mapping relationship.

7.2 QoS configuration

7.2.1 Default configuration of QoS

Configuration item	value	Is it configurable
Queue number	8	NO
Scheduling method	WRR	YES
Whether to enable SP scheduling	disable	YES
Whether to enable WFQ scheduling mode	disable	YES
Queue weight	qp0[1],qp1[2],qp2[4],qp3[8],qp4[16] qp5[32],qp6[64],qp7[127]	YES
The mapping relationship between COS and qosprofile	COS0[qp0] COS1[qp1] COS2[qp2] COS3[qp3] COS4[qp4] COS5[qp5] COS6[qp6] COS7[qp7]	NO
The mapping relationship between DSCP and qosprofile	DSCP0~DSCP7[qp0] DSCP8~DSCP15[qp1]	YES

	DSCP16~DSCP23[qp2] DSCP24~DSCP31[qp3] DSCP32~DSCP39qp4] DSCP40~DSCP47[qp5] DSCP48~DSCP55[qp6] DSCP56~DSCP64[qp7]	
Qosprofile properties	qp0 cos[0] 队列0 qp1 cos[1] 队列1 qp2 cos[2] 队列2 qp3 cos[3] 队列3 qp5 cos[4] 队列4 qp5 cos[5] 队列5 qp6 cos[6] 队列6 qp7 cos[7] 队列7	NO
Whether the interface enables qos based on DSCP	disable	NO
Whether the interface enables COS-based qos	enable	NO
Interface user priority (COS value)	0	YES

7.2.2 Configure scheduling mode

The default scheduling mode of the switch is WRR. The SP and WFQ scheduling modes can be configured through commands.

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

7.2.3 Configure queue weight

command	description	CLI mode

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 configuration of the recovery queue is the default configuration	Interface configuration mode

Queue weight refers to the number of packets forwarded by the priority queue in one round of polling and forwarding. Therefore, pay attention to when configuring queue weight: the weight of the low priority queue should not exceed the weight of the high priority queue.

7.2.4 Configure the mapping relationship between DSCP and QosProfile

command	description	CLI mode
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 between DSCP and qosprofile to the default configuration.	Global configuration mode

7.2.4 Configure Port QoS

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

Define class, define a set of flow classification rules:

There are three types of traffic classification rules: 802.1p priority, DSCP, and ACL. A class can only use one set of flow classification rules, and a set of flow classification rules can be used by multiple classes. The default configuration does not match any rules.

command	description	CLI mode
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, can configure 8 rules at the same time	Global configuration mode
qos class <1-256> match dscp <0-63> (<0-63>…)	Define matching DSCP rules, 8 rules can be configured at the same	Global configuration

	time	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>|)	Display information about configured classes	Privileged mode

Define a strategy and a set of QoS actions that match the rules:

There are a total of six QoS actions for mapped message output queue, remark DSCP, statistics, copy to CPU, mirror, and speed limit. Copy to CPU and mirror cannot be configured at the same time. A policy can be connected to multiple classes, and a class can be connected to multiple policies. A group of QoS actions can be used when a policy is connected to a class. In the default configuration, the policy is not connected to any class, nor does it use any QoS actions.

command	description	CLI mode
qos policy <1-256> name WORD	Name the specified strategy	Global configuration mode
qos policy <1-256> class <1-256> remark dscp <0-63>	Match the classification rules and remark the DSCP value of the packet	Global configuration mode
no qos policy <1-256> class <1-256> remark	Action to remove remarked message	Global configuration mode
qos policy <1-256> class <1-256> meter <1-1000000> <1-65535>	Match classification rules to limit the bandwidth and burst traffic of packets	Global configuration mode
no qos policy <1-256> class <1-256> meter	Remove actions that limit packet bandwidth and burst traffic	Global configuration mode
qos policy <1-256> class <1-256> statistic-packets	Match classification rules and count the number of packets	Global configuration mode
no qos policy <1-256> class <1-256> statistic-packets	Action to remove the number of statistical packets	Global configuration mode

qos policy <1-256> class <1-256> mirror-to cpu	Match the classification rules, and the packets are mirrored to the CPU	Global configuration mode
qos policy <1-256> class <1-256> mirror-to monitor-interface	Match the classification rule, the packet is mirrored to the mirror port (the mirror port is configured and effective)	Global configuration mode
no qos policy <1-256> class <1-256> mirror	Remove the action of mirroring the message	Global configuration mode
no qos policy <1-256> (class <1-256>|)	Strategy 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 distribute the packets to the corresponding output queue	Global configuration mode
no qos policy <1-256> class <1-256> map-queue	Match classification rules, assign packets to the default output queue 0	Global configuration mode
clear interface IFNAME qos policy statistic-packets	Clear statistics of interface qos policy	Global configuration mode
show qos policy (<1-256>|)	Display information about configured policies	Privileged mode
show qos	Display the information of the configured qos	Privileged mode

Application strategy, apply the corresponding strategy to the interface;

It only affects the flow in the ingress direction. An interface can only have one policy, and a policy can be used by multiple interfaces.

Only one QoS can be selected for a port. The QoS function can only be configured on the physical port, not on the trunk group or Layer 3 interface.

command	description	CLI mode
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-	Interface

	based.	configuration mode
show qos	Display all qos configuration information	Privileged mode
show qos interface IFNAME	Display the information of qos configured on the interface	Privileged mode
show qos interface	Display qos information for all interfaces	Privileged mode

7.2.5 Configure port user priority (COS value)

command	description	CLI mode
qos user-priority <0-7>	Configure the user priority of the port (COS value)	Interface configuration mode
no qos user-priority	Restore the user priority (COS value) of the port to 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 function is activated by default:

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

Configure interface ge1/3 to enable DSCP-based QoS, and DSCP value 3 is mapped 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 ACL to capture the data flow of source MAC1, MAC2, MAC3 respectively

(Acl rules can be modified as needed, here are just simple examples)

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 flows of the source MAC1, MAC2, and MAC3 respectively

(You can modify the matching rules cos or dscp according to your needs, here are just simple examples)

qos class 10 match acl 700

qos class 11 match acl 701

qos class 12 match acl 702

Configure the QOS policy to re-mark the 802.1p priority of the data flows with the source MAC1, MAC2, and MAC3 respectively

(The strategy can be modified according to demand, 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

Deliver QOS policy to the port

interface ge1/23

qos apply-policy 10

View configuration information, test result analysis on G1/24 port packet capture

Switch#show qos interface ge1/23

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

- Introduction of MSTP
- MSTP configuration

MSTP configuration example

8.1 Introduction to MSTP

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

8.1.1 Overview

MSTP uses RSTP to quickly converge and aggregate multiple VLANs into a spanning tree instance. Each instance 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 spanning tree instances that are required to support a large number of VLANs.

8.1.2 Multiple spanning tree domains

For instances participating in multiple spanning tree (MST) calculations, the same MST configuration information of the switch must be configured consistently. The set of connected switches with the same MST configuration constitutes the MST region.

The MST configuration determines the domain to which each switch belongs. The configuration includes the domain name, revision number, and MST instance and VLAN assignment mapping; this information will generate a unique digest in the MST configuration. The digests in the same domain are the same, and they must be the same. You can view these information with 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 BPDUs. There is no limit to the number of MST regions in a network, but each region supports up to 16 instances. You can only assign one VLAN to a spanning tree instance at a time.

8.1.3 IST, CIST, and CST

Internal spanning tree (IST), a spanning tree running in the MST region.

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

This IST is just a spanning tree instance that receives and sends BPDUs; all other spanning tree instance information is compressed in MSTI BPDUs. Because MSTI BPDUs

carry information for all instances, the number of BPDUs that need to be processed by a switch that supports multiple spanning 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 consumption, and so on. By default, all VLANs are assigned to IST.

A common and internal spanning tree (CIST) is a collection of all ISTs in each MST region and a common spanning tree (connecting the MST region to a single spanning tree).

The spanning tree calculated in a domain looks like a subtree of CSTs containing all switch domains. CIST is formed by the result of spanning tree calculation between switches supporting 802.1W and 802.1D. The CIST in the MST region is the same as the CST outside the region.

Common spanning tree (CST), a spanning tree running between MST regions.

8.1.4 Operation in the domain

IST connects 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 region and the path cost to the CST root. If there is only one domain in the network, the IST master is also the CST root. If the CST root is outside the domain, an MSTP switch at the boundary of the domain is selected as the IST master.

When an MSTP switch is initialized, it sends BPDUs to request itself as the CST root and IST master, and the path cost to the CST root and IST master is set to 0. The switch also initializes all MST instances and requires to be their root. If the MST root information received by the switch has priority over the information stored on the current port (low bridge ID, low path cost elimination, etc.), it abandons its requirement to become an IST master.

During 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 and joins the new subdomain that may contain the real IST master. Therefore, all subdomains are shrunk, with the exception of those containing real IST masters.

For correct operation, all switches in the MST region must recognize the same IST master. Therefore, the switches in any two domains synchronize the roles of the ports of one of their MST instances, only if they converge to a common IST master.

8.1.5 Inter-domain operations

If there are multiple domains or early 802.1D switches in the network, MSTP establishes and maintains CST, which includes all MST domains and all early STP switches in the network. The MST instance joins the IST at the boundary of the domain to become the CST.

IST connects all the switches in the MSTP domain and looks like a subtree of CST (surrounding all switch domains). The root of the subtree becomes the IST master. The MST region looks like a virtual switch adjacent to the STP switch and MST region.

It's just that the CST instance sends and receives BPDUs, and the MST instance adds their spanning tree information to the BPDU to affect neighbor switches and calculate the final spanning tree topology. Because of 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 do not affect all MST instances. Parameters related to spanning tree topology (for example: switch priority, port VLAN cost, port VLAN priority) can be configured in the CST instance and MST instance.

MSTP switches use version 3 RSTP BPDUs or 802.1D BPDUs to communicate with 802.1D switches. MSTP switches use MSTP BPDUs to communicate with MSTP switches.

8.1.6 Count of hops

Message-age and maximum-age information is not used for IST and MST instances in BPDUs configured with spanning tree topology calculation. Instead, it uses the path cost to the root and a hop-count mechanism equivalent to IP TTL.

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

In a domain, the Message-age and maximum-age information in the RSTP BPDU part remains the same, and the same value is propagated on the designated port of the boundary domain.

8.1.7 Border port

A boundary port is a spanning tree domain that connects the MST region to a single RSTP running, or a separate spanning tree region of 801.1D, or another MST region with different configurations. A border port is also connected to a LAN. The designated switch for this LAN is either a separate spanning tree switch or a switch with different MST region configurations.

At the border port, the role of the MST port is not important, and their status is forced to be the same as the status of the IST port (when the IST port is forwarding, the MST port at the border is forwarding). An IST port at the border can have any role except the backup port.

On a shared border connection, the MST port waits for the forward-delay time to expire in the blocking state before transitioning to the learning state. The MST port waits for another forward-delay time to expire before switching to forwarding.

If the boundary port is a point-to-point connection and is the root port of the IST, the MST port transitions to the forwarding state as soon as the IST port transitions to the forwarding state.

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

8.1.8 Interoperability of MSTP and 802.1d STP

A switch running MSTP supports a built-in protocol migration mechanism, which enables him to coordinate with 802.1D. If the switch receives an 802.1D configured BPDU from a port, it sends an 802.1D BPDU on that port. When a border port of a domain receives an 802.1D BPDU or a MSTP BPDU or RSTP BPDU from a different domain, the MSTP switch can detect it.

However, if the switch no longer receives 802.1D BPDUs, it will not automatically return to MSTP mode because it cannot determine whether the other party's switch has been deleted from the connection unless the other party's switch is the designated switch. Similarly, when the switch connected to this switch has been added to this domain, the switch may continue to assign a border port role to a port. Restart the protocol migration process (force to negotiate with neighbor switch).

If all the connected peer switches are RSTP switches, they can process MSTP BPDUs and RSTP BPDUs. Therefore, the MSTP switch either sends a version 0 configuration and TCN BPDU or version 3 MSTP BPDU on the border port. A boundary port connected to the LAN, his designated switch is either a separate spanning tree switch or a switch with a different MST configuration.

8.1.9 Port role

MSTP uses RSTP's fast convergence algorithm. The following briefly introduces the role of MSTP ports and rapid convergence in conjunction with RSTP.

RSTP provides fast convergence of designated port roles and decision of active topology. RSTP is based on IEEE802.1D STP and selects a high-priority switch as the root switch. When RSTP assigns a port role to a port:

Root port-Provides optimal path consumption when the switch forwards packets to the root switch.

Designated port-Connect to the designated switch. When forwarding packets from the LAN to the root switch, the lowest path cost is generated. The port through which the designated switch connects to the LAN is called the designated port.

Alternate port-Provides an alternate path from the current root port to the root switch.

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

Disable port-There is no port role in spanning tree operation.

Master port-Located on the shortest path to the root of the domain or the root, it is the port connecting the domain to the root of the master.

The root port or designated port role is included in the active topology. The role of replacement port or backup port is not included in the active topology.

In a network with a stable topology and a fixed port role, RSTP ensures that each root port and designated port immediately transition 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 rapid recovery under the following conditions: switch failure, port failure, or LAN failure, which provides rapid recovery for edge ports, new root ports, and connections to a point-to-point connection:

Edge ports-If you configure a port as an edge port, the edge port immediately transitions to the forwarding state. You can open it as a boundary port only when the port is connected to a separate terminal or to determine the device that does not need to calculate the spanning tree.

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

Point-to-point links-If you connect a port to other ports through a point-to-point connection and the local port becomes a designated port, it negotiates a fast migration with other ports through a proposal-agreement handshake to determine a fast convergence without loop -free) topology.

Topology change

This section describes the difference between RSTP and 802.1D in handling spanning-tree topology changes.

Detection-Unlike 802.1D, any transition between the blocking and forwarding states will cause a topology change. Only the transition from blocking to the forwarding state causes a RSTP topology change (only the topology change is considered to increase connectivity). A state change on an edge port will not cause a topology change. When a RSTP switch detects

a topology change, it floods it to learn all non-edge ports (nonedge ports) except the ports that receive TC information.

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

Acknowledgement-When an RSTP switch receives a TCN message from an 802.1D switch on a designated port, it responds with an 802.1D BPDU and sets the TCA flag. However, if the TC-while timer (same as the topology-change timer of 802.1D) is active, connect to the 802.1D switch at the root port and receive a configuration BPDU with TCA, the TC-while timer resets (reset) . This behavior is only required to support 802.1D switches. RSTP BPDU never has TCA flag.

Propagation-When an RSTP switch receives a TC message from another switch through a designated port or root port, it propagates to all non-edge ports, designated ports, and root ports (other than the receiving port). All such ports of the switch start the TC-while timer and flood the information they learned.

Protocol migration-For backward compatibility with 802.1D switches, RSTP selectively sends 802.1D configuration BPDUs and TCN BPDUs based on each port.

When one has been initialized, the migrate-delay timer starts (the specified minimum value is during the RSTP BPDU is sent), the RSTP BPDU is sent. When this timer is active, the switch processes all BPDUs received from the port and ignores the protocol type.

After the port's migration-delay timer has been suspended, 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 BPDUs on a port and receives a RSTP BPDU after the timer is suspended, it restarts the timer on that port and starts using RSTP BPDUs.

8.1.10 802.1D Introduction to Spanning Tree

The spanning tree protocol is based on the following:

1) There is a unique group address (01-80-C2-00-00-00) to identify all the switches on a particular LAN. This group address can be recognized by all switches;

2) Each switch has a unique identifier (Brideg Identifier);

3) The port of each switch has a unique port identifier (Port Identifier). Management of the spanning tree configuration 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. The root path cost is the sum of the path costs from the switch to the various network segments traversed by the root switch. The port with the lowest root path cost in a switch is called the root port. If multiple ports have the same root path cost, the port with the highest priority is the root port.

There is a switch in each LAN called a designated switch, which belongs to the switch with the least root path cost in the LAN. The port connecting the LAN to the designated switch is the designated port of the LAN. If more than two ports in the designated switch are connected to this LAN, the port with the highest priority is selected as the designated port.

The elements that must be determined to form a spanning tree:

1) Determine the root switch

A. At the beginning, all the switches consider themselves as root switches;

B. The switch sends a configuration BPDU to the LAN broadcast connected to it. The root_id and bridge_id have the same value;

c. When the switch receives the configuration BPDU from another switch, if 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 and root of the switch are updated The path costs the values of parameters such as root_path_cost, and the switch will continue to broadcast configuration BPDUs with new values.

2) Determine the root port

The port with the lowest root path cost in a switch is called the root port.

If there are multiple ports with the same lowest root path cost, the port with the highest priority is the root port. If two or more ports have the same lowest root path cost and highest priority, the port with the smallest port number is the default root port.

3) Designated LAN authorized switch

a. At the beginning, all switches consider themselves to be designated switches for the LAN.

b. When the switch receives BPDUs from other switches with the lower root path cost (in the same LAN), the switch no longer claims to be the designated switch. If there are two or more switches with the same root path cost in a LAN, the switch with the highest priority is selected as the designated switch.

c. If the designated switch receives a configuration BPDU from another switch on the LAN due to competition for the designated switch at a certain time, the designated switch will send a response configuration BPDU to re-determine the designated switch.

4) Decide to designate the port

The designated switch of the LAN is connected to the LAN as the designated port. If the designated switch has two or more ports connected to the LAN, the port with the lowest identification is the designated port.

Except for the root port and designated ports, all other ports will be placed in the blocked state. In this way, after determining the root switch, the root port of the switch, and the

designated switch and designated port of each LAN, the topology of a spanning tree is also determined.

8.2 MSTP configuration

8.2.1 Default configuration

Command parameters	Default value
spanning-tree mst enable(Start mstp)	shut down
Spanning-tree mst priority(Switch cist priority)	32768
spanning-tree mst hello-time(Switch cist hello-time)	2 seconds
spanning-tree mst forward-time(Switch cist forward-time)	15 seconds
spanning-tree mst max-age(Switch cist max-age)	20 seconds
spanning-tree mst max-hops(Switch cist max-hops)	20 seconds
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

MSTP is turned off by default when the system is started.

The configuration process to start 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

Configuration max-age is the configuration for all instances. max-age is the number of seconds the switch waits to receive spanning tree configuration information before triggering 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 field before the BPDU is discarded.

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. According to the generating number protocol, forward-time must meet the following conditions: 2*(forward-time – 1) >= max-age.

Configuration process:

Switch#configure terminal

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

Configure hello-time

Configuring hello-time is the configuration for all instances. The hello-time is the interval at which the root switch generates 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 of the CIST bridge (priority)

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

Configuration process:

Switch#configure terminal

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

Configuration compatible with CISCO

The switch uses the MSTP protocol based on 802.1s, the length of each MSTI message is 16 bytes; and the length of each MSTI message of the BPDU of the CISCO switch is 26 bytes. In order to interoperate with CISCO switches, switches that are compatible with CISCO must be activated when configuring the switch.

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

The default system does not enable this function.

Open and CISCO compatible:

Switch#configure terminal

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

Close and compatible with CISCO:

Switch#configure terminal

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

The

Reset protocol check task

In order to be compatible with the 802.1D STP protocol, the system can automatically detect the protocol that the opposing system is running. Determine the protocol that this port runs according to the protocol that the other party runs.

In some cases, the protocol needs to be reset. For example, after the system negotiates a port to run the STP protocol, after a period of time, the other party's device running the STP protocol has been replaced with a host. At this time, I need to configure this port as a fast port, but the port is already running the stp protocol, and the task of protocol negotiation has stopped; at this time, I need to reset the task of this protocol negotiation to let it renegotiate the protocol between it and the host.

Reset the reconnaissance mission of the entire device:

Switch#clear spanning-tree detected protocols

Reset the protocol reconnaissance task of a port:

Switch#clear spanning-tree detected protocols interface <if-name>

8.2.3 Domain configuration

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

A domain has one or more members with the same MST configuration, and each member can handle RSTP BPDUS capability. 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 'Instance Configuration'. Here only the domain name configuration and revision number configuration are introduced.

Configure the domain name:

Switch#configure terminal
Switch(config)#spanning-tree mst configuration
Switch(config-mst)#region <region-name>

Configure the 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 instance ID numbers is 0-15. Only one spanning tree instance can be assigned to a VLAN at a time.

By default, there is only one instance 0, and all VLANs belong 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 of the MSTI bridge

The default configuration is 32768, and 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 following describes MSTP-related port configuration information. Only the simple

configuration part is introduced here, port fast and root guard are introduced separately later.

The process of configuring a port to join an instance:

Switch#configure terminal

Switch(config)#interface <if-name>

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

Configure the priority of the CIST port (priority)

The default configuration is 128, and the configuration range is <0-240>. The priority value 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 CIST port (priority)

The default configuration is 128, and the configuration range is <0-240>. The priority value 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 instance <instance-id> priority <priority>

Configure path cost for CIST ports (path-cost)

The default configuration is 20000000, and the configuration range is 1-200000000. The following is the bandwidth and path cost elimination mapping table:

Bandwidth (bps)	Path 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 process

Switch#configure terminal

Switch(config)#interface <if-name>

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

Configure path cost for MSTI ports (path-cost)

The default configuration is 20000000, and the configuration range is 1-200000000. The bandwidth and path consumption are the same as the table above.

Configuration process

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 sent protocol packet

The default configuration is to send MSTP protocol packets. The configuration range is 0-3 and the mapping relationship is 0-stp, 2-rstp, 3-mstp.

Configuration process:

Switch#configure terminal

Switch(config)#interface <if-name>

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

Configure connection type

If a port is connected to other ports in a point-to-point manner, and the local port becomes a designated port (specified port), RSTP negotiates a rapid migration through the proposal-agreement process and the port it is connected to becomes the root port To determine an acyclic topology.

The following briefly introduces the proposal-agreement negotiation process.

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 superior root information received from the root port, the switch is synchronized.

When RSTP forces it to synchronize new root information, if a designated port is in forwarding state and is not configured as an edge port, it transitions to the blocking state. Normally, when RSTP forces a port to synchronize new root messages and the port cannot meet the above conditions, the port status is set to blocking.

When ensuring that all ports are synchronized, the switch sends an agreement message to the designated port corresponding to the root port. When the switch connects to a point-to-point connection in agreement on their port role, RSTP immediately migrates the port state to forwarding.

If it is a shared connection, it is necessary to go through the calculation process of 802.1D to determine the status of the port.

The default port connection type is 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 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 an 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 a single workstation and server, allowing these devices to connect to the network immediately without waiting for the spanning tree to converge.

Configure a port as a 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 based on the switch or based on each port, but their characteristics are different.

At the global level, you can use the spanning-tree mst portfast bpdu-filter command to enable the BPDU filtering function for ports in the portfast bpdu-filter default state.

At the port layer, you can use spanning-tree mst portfast bpdu-filter enable to enable 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

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

At the global level, you can use spanning-tree mst portfast bpdu-guard to enable the BPDU guard function for ports in the portfast bpdu-gurad default state.

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

When a port configured with BPDU gurad receives a BPDU, the spanning tree will shut down this port. In a valid configuration, Port Fast-enabled ports do not receive BPDUs. A BPDU received on a Port Fast-enabled port indicates an invalid configuration, such as an unauthorized device connection, and the BPDU guard enters an error-disabled state.

Error-disabled is when the port that starts the BPDU gurad receives the BPDU, if the system configures the error-disable mechanism, it will start the error-disable timer. error-disable will restart this port after the system configured timeout.

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

An SP's Layer 2 network can contain many switches that are not connected to them. In such a topology, spanning tree can reconfigure itself and select a customer switch as the root

switch. You can avoid this situation by configuring the root guard on the SP switch to connect to the switch port on the customer network. If spanning tree calculation causes the port on the customer network to be selected as the root port, the root guard configures the port as root-inconsistent (blocked) to prevent the customer switch from becoming the root switch or having a path to the root.

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 will not become the root switch and there is no path to the root.

If the switch is operating in MST mode, the root guard forces the port to become the designated port. If a border port is blocked in the IST instance because of root guard, this port is blocked in all MST instances. A border port is a port connected to a LAN, and the designated switch is either an 802.1D switch or a switch configured in a different MST region.

When a port is opened, the root guard is applied to all VLANs to which the port belongs. VLANs can be aggregated and mapped to an MST instance.

Configuration process

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 in a ring. You need to open the spanning tree protocol of each switch to avoid loops. Perform configuration on each switch separately.

Switch 1 configuration:

Switch>en

Switch#configure terminal

Switch(config)#spanning mst enable

Switch 2 configuration:

Switch>en

Switch#configure terminal

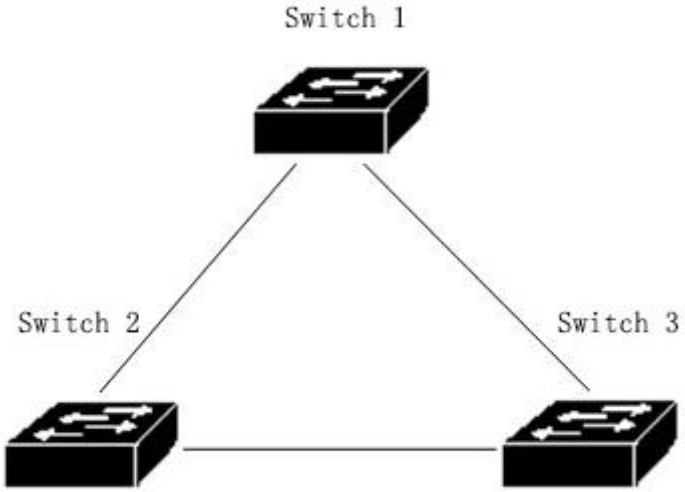
Switch(config)#spanning mst enable

Switch 3 configuration:

Switch>en

Switch#configure terminal

Switch(config)#spanning mst enable



(2)Troubleshooting:

Check which switch is selected as the root bridge:

Run show spanning-tree mst and observe that the value of CISTRoot is the smallest MAC address among the three switches, that is, the root election result is correct.

Switch#show spanning-tree mst

View the port status of the switches in the spanning tree:

Execute the show spanning-tree mst interface ge1/1 command and observe the State value of PORT ge1/1 in instance 0

Switch#show spanning-tree mst interface ge1/1

Chapter 9 EAPS Configuration

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

- Introduction to EAPS
- Basic concepts of EAPS
- EAPS protocol introduction
- EAPS configuration
- Restrictions
- Configuration example

9.1 Introduction to EAPS

EAPS is short for Ethernet Automatic Protecting Switching. EAPS utilizes standard Ethernet and VLAN technologies to provide loop topology and loop recovery mechanisms. EAPS has the ability to resume data communication within 1 second when a fault occurs in the ring. 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 depend on other devices, which means that there can be devices that do not support the EAPS protocol in the EAPS ring.

9.2 Basic concepts of EAPS

Here are some basic concepts involved in EAPS:
1. EAPS Domain, in a network, an EAPS Domain runs in a separate ring. It is a series of node devices that form a single loop. An EAPS Domain contains a Master Node and one or more Transit Nodes.
2. Master Node, a switch running EAPS or called EAPS node device, an EAPS Domain has only one Master Node.
3. Transit Node, a switch running EAPS or called EAPS node device, other nodes except Master Node in an EAPS Domain.
4. Primary Port, a port in EAPS Domain that connects to EAPS node devices. A node device in an EAPS Domain has only one Primary Port connected to this ring.
5. Secondary Port, a port in the EAPS Domain that connects to EAPS node devices. A node device has only one Secondary Port connected to this ring in an EAPS Domain.
6. Control VLAN, control VLAN, the VLAN responsible for the transmission of EAPS Domain protocol packets. There is only one Control VLAN in an EAPS Domain.
7. Protected VLAN, protected VLAN, a VLAN that transmits business data in EAPS Domain. There must be one Protected VLAN in an EAPS Domain, or more than one Protected VLAN.

9.3 Introduction to EAPS protocol

An EAPS Domain runs on an EAPS ring. An EAPS Domain contains a Master Node and one or more Transit Nodes; each EAPS node contains the same Control VLAN and multiple Protected VLANs; each EAPS node contains a Primary Port and a Secondary Port in an EAPS Domain, Both ports belong to the Control VLAN and all Protected VLANs of this ring.

Connect all the nodes in this EAPS Domain through the Primary Port and Secondary Port of each EAPS node device to form an EAPS ring.

Under normal circumstances, when all Primary Ports and Secondary Ports in the EAPS Domain are LINK UP, the Secondary Port of the Master Node is blocked (setting the Secondary Port's port status to Blocking) to eliminate the loop of business data in the EAPS Domain. When the EAPS Domain fails, immediately open the Secondary port of the Master Node (set the status of the Secondary Port to Forwarding) to allow it to forward business data and restore normal forwarding of business data.

Transit Node has no difference between Primary Port and Secondary Port processing. The following introduces two kinds of fault detection and loop recovery of EAPS:

9.3.1 Link-Down alarm

When the Transit Node finds that LINK DOWN appears in its Primary Port or Secondary Port, it will immediately send a LINK-DOWN protocol packet from the Control VLAN to the Master Node through another LINK UP port.

When the Master Node receives this LINK-DOWN protocol packet:

The Master Node immediately enters the Failed state from the Complete state, opens the Secondary Port (sets the status of the Secondary Port to Forwarding), refreshes its Layer 2 and Layer 3 forwarding tables, and sends a RING-DOWN-FLUSH-FDB to notify EAPS Domain that other Transit refresh its own Forwarding table, re-learning Layer 2 and Layer 3 forwarding tables.

When the Master Node finds that a LINK DOWN occurs in the local Primary Port, its operation is the same as the operation of receiving the LINK-DOWN protocol packet.

When the Master Node discovers that the local Secondary Port has a LINK DOWN, the Master Node immediately enters the Failed state from the Complete state, refreshes its own Layer 2 and Layer 3 forwarding tables, and sends the RING-DOWN-FLUSH-FDB protocol packet to notify EAPS Domain of other Transit refresh Re-learn the Layer 2 and Layer 3 forwarding table with your own forwarding table.

9.3.2 Loop check

The Master Node will periodically send HEALTH protocol packets from the Primary Port. If the ring is complete, the Master Node can receive this HEALTH protocol packet in its Secondary Port. At this time, the Master Node will restart its Fail-period timer, and the status of the Master Node is Complete.

If the fail-period does not receive its own HEALTH protocol package, the Master Node will leave the Complete state, enter the Failed state, open the Secondary Port (set the Secondary Port state to Forwarding), refresh its own Layer 2 and 3 forwarding table, and send RING-DsOWN-FLUSH-FDB informs EAPS Domain other Transit to refresh its forwarding table and re-learn the Layer 2 and Layer 3 forwarding table.

9.3.3 Ring recovery

9.3.4

The Master Node sends HEALTH protocol 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 packet is received from its Secondary Port, the ring will return to the Complete state. At this time, the Master Node will set the status of the Secondary Port to blocking, refresh its own Layer 2 and Layer 3 forwarding table, and send a RING-UP-FLUSH-FDB packet to notify other devices to refresh its Layer 2 and Layer 3 forwarding table and restart Learn the Layer 2 and Layer 3 forwarding tables.

During the transition of the Transit Node's port from LINK DOWN back to LINK UP and the recovery of the Master Node discovery ring, the Secondary Port of the Master Node may still be in the Forwarding state. In this case, a temporary ring may be created. Therefore, when the Transit Node is in the LINK UP state on one port and the other LINK DOWN port also becomes LINK UP, the Transit Node must enter a "pre-Forwarding state" (PRE-FORWARDING). In this state, the LINK UP The port will also be in the Pre-forwarding state and cannot forward service data, interrupting possible data loops. When Master Node recovers and sends RING-UP-FLUSH-FDB, Transit Node will switch the node state to LINK-UP state after receiving this protocol packet, set the port in Pre-forwarding state to Forwarding state, and restore the service data. Forward normally.

If the Transit Node cannot receive the RING-UP-FLUSH-FDB protocol packet, it will be set to the Forwarding state by the port in the Pre-forwarding state after double the fail-time.

9.3.5 Extreme EAPS compatible

Extreme's products are the earliest manufacturers that support EAPS. The EAPS protocol supported by the switch follows the RFC3619 standard; the Extreme equipment's EAPS protocol package and RFC3619 protocol package definition have some differences. The EAPS protocol supported by the switch is fully compatible with Extreme equipment, and the compatibility switch is turned on by default.

Multiple EAPS Domain

The switch can support multiple EAPS Domains, supporting a total of 16.

9.4 EAPS configuration

The basic configuration of the EAPS protocol includes the following basic elements: Control VLAN, node mode, Primary Port, Secondary Port, Protected VLAN, Hello Time, and Fail Time. There are default configurations for Hello Time and Fail Time. Hello Time is 1

second and Fail Timer is 3 seconds.

9.5 Restrictions

1、The Primary Port must belong to the Control VLAN of an EAPS Domain and the TRUNK mode members of all Protected VLANs.

2、The EAPS protocol cannot run simultaneously with the MSTP protocol. If MSTP is started or an MSTP instance is configured, the EAPS protocol cannot be started.

3、A VLAN can not be configured as the Control VLAN or Protected VLAN of EAPS after the VLLP protocol is activated.

4、The Control VLAN of EAPS can only contain Primary Port and Secondary Port, and it can only be the VLAN TRUNK mode.

5、If a VLAN is configured as the Control VLAN of the EAPS Domain, and this Domain has been activated, then this VLAN cannot be deleted and its port members cannot be modified or deleted. Control VLAN cannot be configured with Layer 3 interfaces.

6、The Primary Port and Secondary Port in Protected VLAN can only be in TRUNK mode. Other member ports are not restricted.

7、A port can only be configured as a Primary Port or Secondary Port of an EAPS Domain.

8、The same VLAN can only belong to the Control VLAN or Protected VLAN of an EAPS Domain.

9、The control VLANs of all nodes in an EAPS Domain must be the same.

9.6 A brief introduction to the EAPS command

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

There are certain sequence requirements for configuring EAPS. You must first create an EAPS Domain. Before starting EAPS Domain, you must configure other parameters according to the previous requirements; otherwise, the startup will not succeed. If you want to change the hello time to a value greater than the current fail time, you must first modify the fail time to a larger number; otherwise, the configuration will be unsuccessful. There are no special requirements for other configuration sequences.

When an EAPS Domain has been started, control-vlan, mode, primary-port, and

secondary-port cannot be modified; protected-vlan, fail-timer, hello-time, extreme-interoperability can be modified.

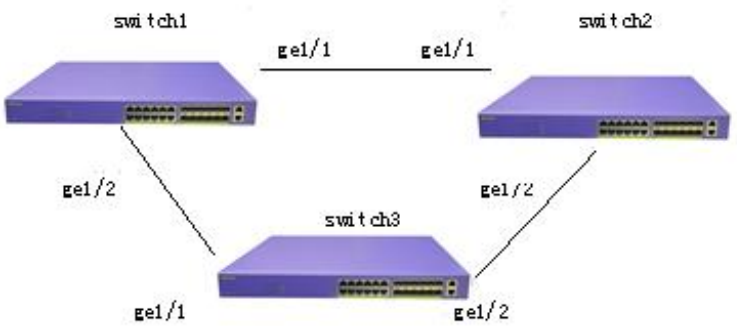
Primary-port and secondary-port support LACP port (that is, TRUNK group).

9.6.1 EAPS configuration commands

command	description	mode
eaps create <ring-id>	Create an 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 the running node mode of an EAPS Domain.	Global configuration mode
eaps primary-port <ring-id> <ifname>	Configure an EAPS Domain Primary Port.	Global configuration mode
eaps secondary-port <ring-id> <ifname>	Configure a secondary port for EAPS Domain.	Global configuration mode
eaps data-span <ring-id>	Configuring EAPS ring data forwarding across rings	Global configuration mode
eaps fail-time <ring-id> <secs>	Configure a timeout period for the fail-period timer of an EAPS Domain. The default is 3 seconds. The unit is seconds.	Global configuration mode
eaps hello-time <ring-id> <secs>	Configure an EAPS Domain to send HEALTH packets regularly. 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>	It is compatible with Extreme equipment when it is turned on or off. The default is to be compatible.	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	Display the information of EAPS Domain started in the system	Normal mode/privileged mode
Show eaps <ring-id>	Display detailed information of an EAPSDomain	Normal mode/privileged mode

9.7 Single ring configuration example

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



Switch1 configuration:

Switch1 is configured as the master of EAPS Domain ring 1, the control VLAN is VLAN 2, the protected VLAN is VLAN 1, the primary-port is ge1/1, the secondary-port is ge1/2, and other configurations use the 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 a trunk member 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 a trunk member 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 an EAPS Domain ring 1
Switch(config)#eaps create 1

#Configure VLAN 2 as the control VLAN
Switch(config)#eaps control-vlan 1 2
#Configure VLAN 1 as the protected VLAN
Switch(config)#eaps protected-vlan 1 1

#Configure 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
```

Switch2 configuration

Switch2 is configured as the transit of EAPS Domain ring 1, the control VLAN is VLAN 2, the protected VLAN is VLAN 1, the primary-port is ge1/1, the secondary-port is ge1/2, and other configurations use the 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 a trunk member 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 a trunk member 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 an EAPS Domain ring 1
Switch(config)#eaps create 1

#Configure VLAN 2 as the control VLAN
Switch(config)#eaps control-vlan 1 2

#Configure VLAN 1 as the 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

Switch3 configuration

Switch3 is configured as the transit of EAPS Domain ring 1, the control VLAN is VLAN 2, the protected VLAN is VLAN 1, the primary-port is ge1/1, the secondary-port is ge1/2, and 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 a trunk member 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 a trunk member 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 an EAPS Domain ring 1

Switch(config)#eaps create 1

#Configure VLAN 2 as the control VLAN

Switch(config)#eaps control-vlan 1 2

#Configure VLAN 1 as the 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

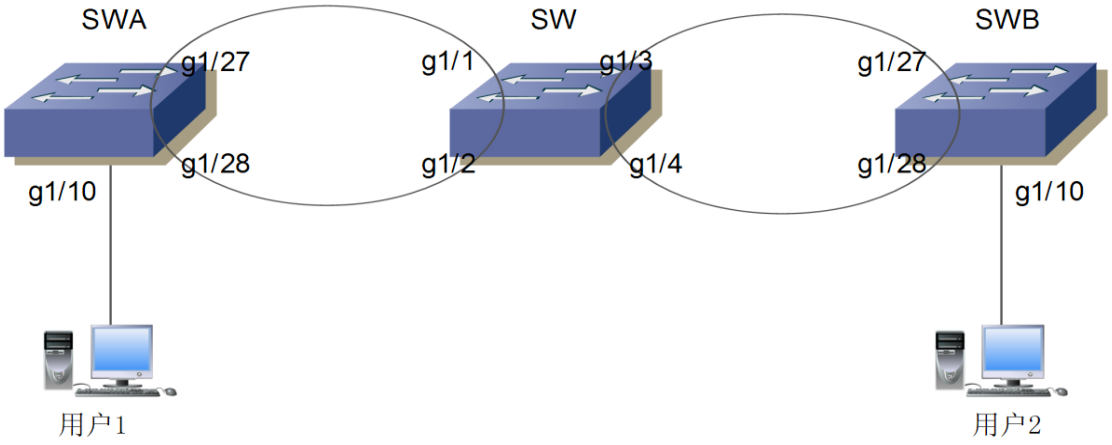
Switch(config)#eaps secondary-port 1 ge1/2

#Start EAPS Domain ring 1

Switch(config)#eaps enable 1

9.8 Cross-ring data forwarding configuration example

There are three switches SWA, SW, and SWB, which implement vlan1 vlan2 inter-ring inter-ring through the EAPS protocol. The topology is as follows:



SWA ring 1 controls vlan111 and protects vlan1 and 2, the configuration is 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 connects with SWA to control vlan111 and protect vlan1,2. Ring 2 is connected to the SWB to control vlan222 and protect vlan3333 (virtual vlan, and the interface needs to be added). If you want to implement ring 1 and ring 2 data forwarding across rings, 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 vla 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              ###This is a virtual protection vlan
eaps data-span 2
eaps enable 2
```

SWB ring 2 connects with SW ring 2 to control vlan222 and 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 is completed, user 1 and user 2 communicate with each other, and vlan1 data also communicates. The Eaps node mode can be modified as required.

10.1 Overview of ERPS

ERPS (Ethernet Ring Protection Switching, Ethernet Ring Protection Switching Protocol) is a ring network protection protocol developed by ITU, also known as G.8032. It is a link layer protocol specifically applied to the Ethernet ring network. It can prevent the broadcast storm caused by the data loop when the Ethernet ring network is complete, and can quickly restore the communication between each node on the ring network when a link on the Ethernet ring network is disconnected. The ERPS protocol provides a fast Ethernet ring network protection mechanism, which can quickly restore network transmission when the ring network fails, thereby ensuring high availability and high reliability of the switch in the case of ring network topology.

10.2 Introduction to ERPS technology

10.2.1 ERPS ring

The ERPS ring is based on the principle of minimizing the ring. Each ring must be the smallest ring, which is divided into a main ring and a sub-ring: the main ring is a closed ring; the sub-ring is a non-closed ring or a closed ring; both need to be configured by commands. Each ERPS ring (whether it is a main ring or a sub-ring) has five states: (1) Idle state: when each physical link of the ring network is connected; (2) Protection state: a certain one in the ring network Or the state when multiple physical links are disconnected; (3) Manual switch state: manually change the state of the ring; (4) Forced switch state: forcefully change the state of the ring; (5) Pending state: pending intermediate state.

10.2.2 ERPS node

The layer 2 switching equipment that joins the ERPS ring is called a node. Each node cannot add more than two ports to the same ERPS ring. One port is an RPL port, and the other port is an ordinary ring port.

For the overall situation, the role of nodes is divided into the following two types: (1) Intersecting nodes: in intersecting ERPS rings, nodes that belong to multiple rings at the same time are called intersecting nodes; (2) Non-intersecting nodes: in intersecting ERPS rings In, nodes that only belong to a certain ERPS ring are called non-intersecting nodes.

The node modes specified in the ERPS protocol mainly include three types: RPL owner node, RPL neighbour node and ordinary ring node. (1) RPL owner node: There is only one RPL

owner node in an ERPS ring, which is determined by user configuration. Blocking the RPL port prevents loops in the ERPS ring. When the RPL owner node receives a fault message, it learns about other nodes on the ERPS ring Or, when the link fails, the RPL port will be automatically opened. This port resumes the reception and transmission of traffic to ensure that the traffic will not be interrupted; (2) RPL neighbour node: a node directly connected to the RPL port of the RPL owner node, under normal circumstances , The RPL port of the RPL owner node and the RPL port of the RPL neighbour node are blocked to prevent loops. When the ERPS ring fails, both the RPL port of the RPL owner node and the RPL port of the RPL neighbour node will be released; (3) Normal ring node: In the ERPS ring, all nodes except the RPL owner node and the RPL neighbour node are Ordinary ring node, the RPL port of the ordinary ring node is not different from the ordinary ring port, the ring port of the ordinary ring node is responsible for monitoring the link status of its directly connected ERPS protocol, and notifying other nodes of the link status change message in time;

10.2.3 Links and channels

(1) RPL (Ring Protection Link): Each ERPS ring has one and only one RPL, that is, the link where the RPL port of the RPL owner node is located. When the Ethernet ring is in the Idle state, the RPL link is in a blocked state, and data packets are not forwarded to avoid loops;

(2)Sub-ring link: Among intersecting rings, the link belongs to the sub-ring and is controlled by the sub-ring;

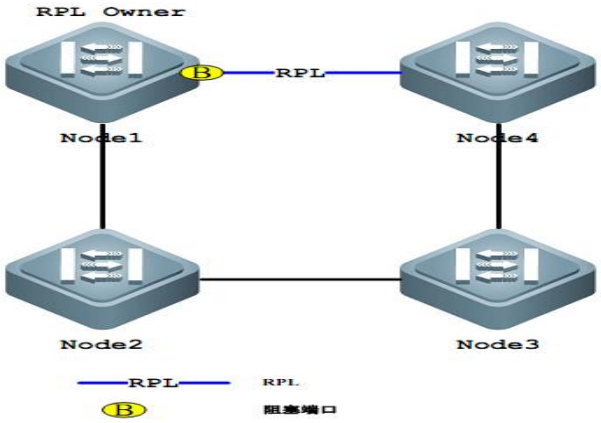
(3)RAPS (Ring Auto Protection Switch) virtual channel: In an intersecting ring, the inter-nodes are used to transmit sub-ring protocol packets, but the path that does not belong to the sub-ring is called the sub-ring's RAPS virtual channel.

10.2.4 ERPS VLAN

There are two types of VLANs in ERPS: (1) RAPS VLAN: used to transmit ERPS protocol packets. The ports on the device that access the ERPS ring belong to the RAPS VLAN, and only the ports that access the ERP ring can join this VLAN. The RAPS VLAN of different rings must be different. It is not allowed to configure an IP address on the interface of the RAPS VLAN; (2) Data VLAN: In contrast to the RAPS VLAN, the data VLAN is used to transmit data packets. The data VLAN can contain both ERP ring ports and non-ERP ring ports.

10.3 Working Principle of ERPS

10.3.1 Normal state

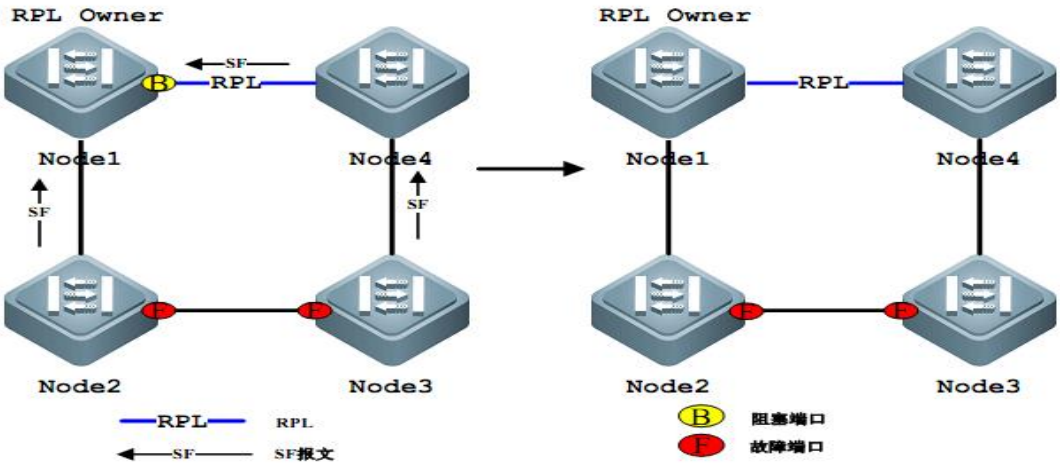


(1)All nodes are connected in a ring on the physical topology;

(2)The loop protection protocol ensures that no loops are formed by blocking RPL links. As shown in the figure above, the link between Node1 and Node4 is an RPL link;

(3)Perform fault detection on each link between adjacent nodes.

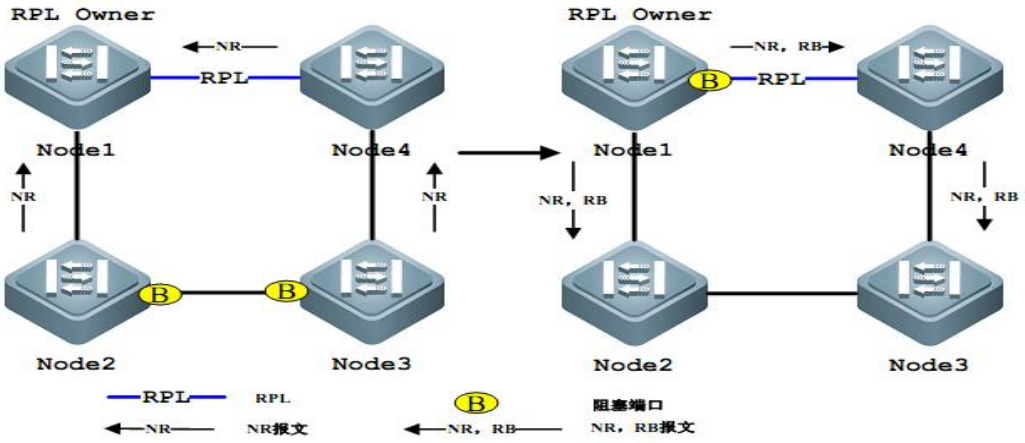
10.3.2 Link failure



(1)The node adjacent to the failed link blocks the failed link and uses RAPS (SF) messages to report the failure to other nodes on the ring. As shown in the figure above, assuming that the link between Node2 and Node3 fails, Node2 and After Node3 waits for the holdoff timer to expire, it will block the faulty link and send RAPS (SF) messages to each node on the ring network;

(2)The RAPS (SF) message triggers the RPL owner node to open the RPL port. The RAPS (SF) message also triggers all nodes to update their MAC entries, and then the node enters the protection state.

10.3.3 Link recovery



(1)When the fault is recovered, the node adjacent to the fault continues to remain blocked and sends a RAPS (NR) message, indicating that there is no local fault;

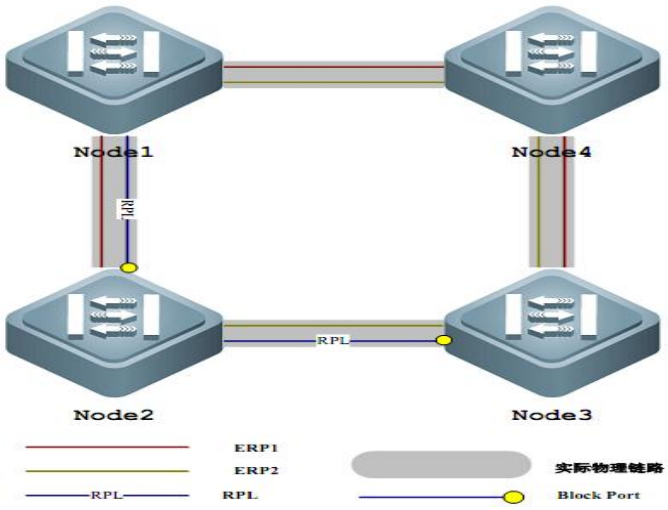
(2)After the guard timer expires, the RPL Owner node starts the WTR timer after receiving the first RAPS (NR) message;

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

(4)After receiving this message, the other nodes update their MAC entries, the node that sent the RAPS (NR) message stops periodically sending the message, and opens the originally blocked port. The ring network has returned to its original normal state.

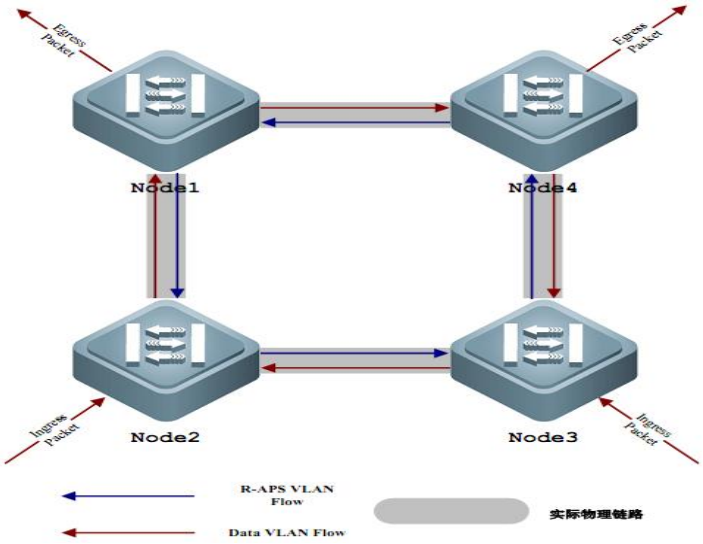
10.4 ERPS technical characteristics

10.4.1 ERPS load balancing



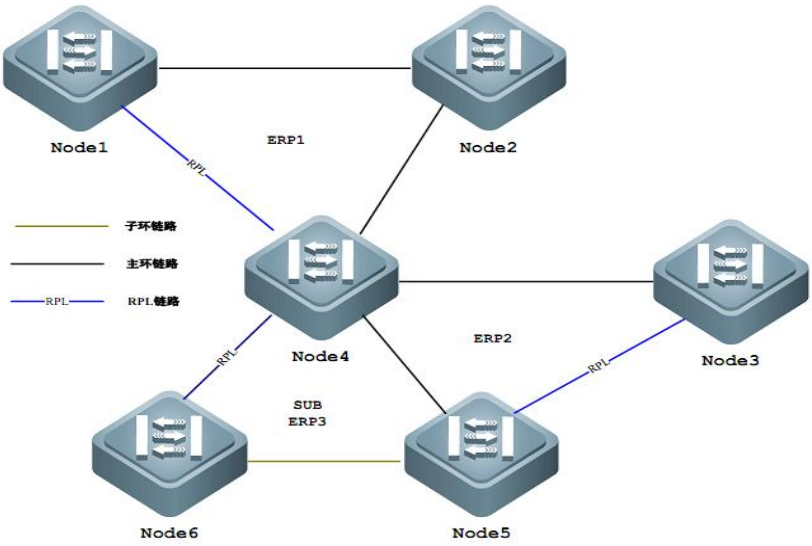
By configuring multiple instances and multiple ERPS rings on the same physical ring network, different ERPS rings send traffic in different VLANs (called protection VLANs) to achieve different topology of data traffic in different VLANs in the ring network, thereby achieving load sharing the goal of. As shown in the figure above, a physical ring network corresponds to two instances and two ERPS rings. The two ERPS rings protect different VLANs. Node2 is the RPL owner node of ERP1, and Node3 is the RPL owner node of ERP2. Through configuration, different VLANs can be used to block different links, thereby achieving load sharing for a single ring.

10.4.2 Good security



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

10.4.3 Support multi-ring intersection and tangent



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

10.5 ERPS protocol commands

command	description	CLI Mode
erps <1-8>	Create an ERPS instance	Global configuration mode
no erps <1-8>	Delete an ERPS instance	Global configuration mode
node-role (interconnection | none-interconnection)	Configure the role of nodes in the ERPS ring, interconnected nodes or non-interconnected nodes	ERPS model
ring <1-32>	Create an ERPS ring	ERPS model
no ring <1-32>	Delete an ERPS ring	ERPS model
ring <1-32> ring-mode (major-ring | sub-ring)	Configure ERPS ring mode, major ring or sub-ring	ERPS model
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 ordinary ring node	ERPS model

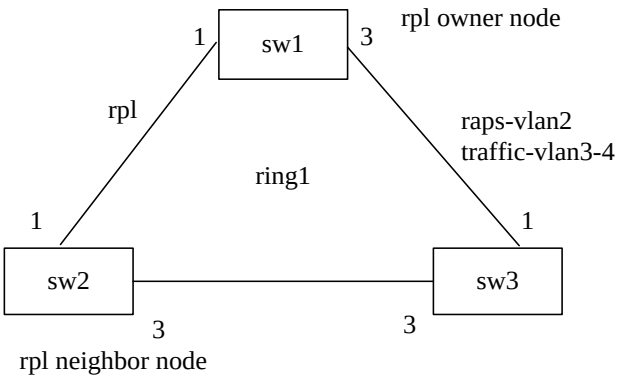
ring <1-32> raps-vlan <2-4094>	Configure ERPS ring protocol VLAN	ERPS model
no ring <1-32> raps-vlan	Delete ERPS ring protocol VLAN	ERPS model
ring <1-32> traffic-vlan <1-4094>	Configure ERPS ring data VLAN	ERPS model
no ring <1-32> traffic-vlan <1-4094>	Delete the ERPS ring data VLAN	ERPS model
ring <1-32> (rpl-port|rl-port) IFNAME	Configure ERPS ring port, RPL port or ordinary ring port	ERPS model
no ring <1-32> (rpl-port|rl-port)	Delete ERPS ring port	ERPS model
ring <1-32> revertive-behaviour (revertive|non-revertive)	Configure ERPS ring recovery behavior, recoverable or non-recoverable	ERPS model
ring <1-32> hold-off-time <0-10000>	Configure ERPS ring hold-off time	ERPS model
no ring <1-32> hold-off-time	Restore ERPS ring hold-off default time	ERPS model
ring <1-32> guard-time <10-2000>	Configure ERPS ring guard time	ERPS model
no ring <1-32> guard-time	Restore ERPS ring guard default time	ERPS model
ring <1-32> wtr-time <1-12>	Configure ERPS ring wtr time	ERPS model
no ring <1-32> wtr-time	Restore ERPS ring wtr default time	ERPS model
ring <1-32> wtb-time <1-10>	Configure ERPS ring wtb time	ERPS model
no ring <1-32> wtb-time	Restore ERPS ring wtb default time	ERPS model
ring <1-32> raps-send-time <1-10>	Configure the ERPS ring protocol packet sending time	ERPS model
no ring <1-32> raps-send-time	Restore the default sending time of ERPS ring protocol packets	ERPS model
ring <1-32> (enable|disable)	Open or close ERPS ring	ERPS model
ring <1-32> forced-switch	Forcibly switch ERPS ring	ERPS model

IFNAME	ports	
ring <1-32> clear forced-switch	Clear forced switching of ERPS ring	ERPS model
ring <1-32> manual-switch IFNAME	Manually switch ERPS ring ports	ERPS model
ring <1-32> clear manual-switch	Clear manual switching of ERPS ring	ERPS model
ring <1-32> clear recovery	Manual recovery when clearing unrecoverable behavior of ERPS ring or manual recovery before WTR/WTB expiration	ERPS model
show erps	Display a brief overview of all ERPS instances and rings of the device	Privileged mode
show erps <1-8>	Display the details of a single ERPS instance and ring of the device	Privileged mode

10.6 Typical application of ERPS

10.6.1 Single ring example

As shown in the figure below, the sw1, sw2 and sw3 nodes form an erps single ring ring1. The 1, 3 ports of each node are used as erps ring ports. The protocol vlan of the ring is 2, the data vlan is 3, 4, the sw1 node is the rpl owner node, sw2 The node is an rpl neighbor node, and the link between sw1 and sw2 is an 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 the ring port vlan mode to trunk, add erps protocol and data vlan

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 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 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) Configure sw2:

(3) 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 the ring port vlan mode to trunk, add erps protocol and data vlan

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 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-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

(4) Configure sw3:

(5) 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 the ring port vlan mode to trunk, add erps protocol and data vlan

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 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 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

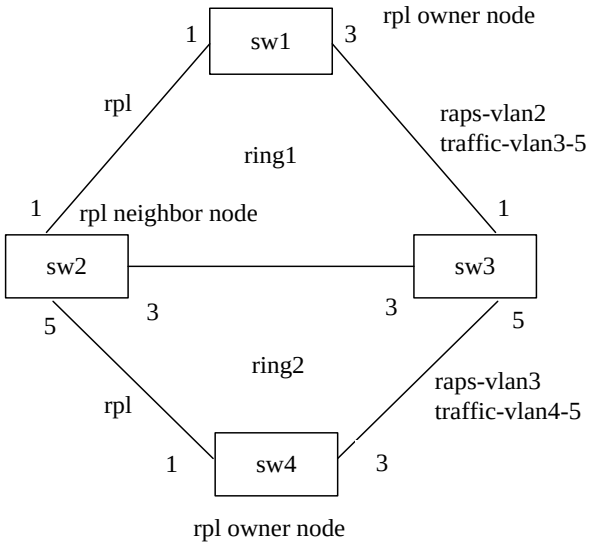
Switch(config-erps-1)# ring 1 enable

Switch(config-erps-1)#exit

10.6.2 Multi-ring example

As shown in the following figure, the sw1, sw2, and sw3 nodes form an erps main ring ring1, and the ports 1 and 3 of the sw1, sw2, and sw3 nodes are used as the main ring ring1 ring port, the protocol vlan of the main ring ring1 is 2, the data vlan is 3, 4, 5. The sw1 node is the primary ring1 rpl owner node, the sw2 node is the primary ring1 rpl neighbor node, and the link between sw1 and sw2 is the primary ring ring1 rpl link.

The sw2, sw3, and sw4 nodes form an erps sub-ring ring2. The 5 ports of the sw2 and sw3 nodes and the 1 and 3 ports of the sw4 node serve as the sub-ring ring2 ring ports. The protocol vlan of the sub-ring ring2 is 3, and the data vlan is 4, 5. The sw4 node is the subring ring2 rpl owner node, and the link between sw2 and sw4 is the subring 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 the ring port vlan mode to trunk, add erps protocol and data vlan

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) Configure sw2:

(3) 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 the ring port vlan mode to trunk, add erps protocol and data vlan

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

(4) Configure sw3:

(5) 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 the ring port vlan mode to trunk, add erps protocol and data vlan

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 terminal

Create erps protocol and data VLAN

Switch(config)#vlan database

Switch(config-vlan)#vlan 3-5

Switch(config-vlan)#exit

Configure the ring port vlan mode to trunk, add erps protocol and data vlan

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 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

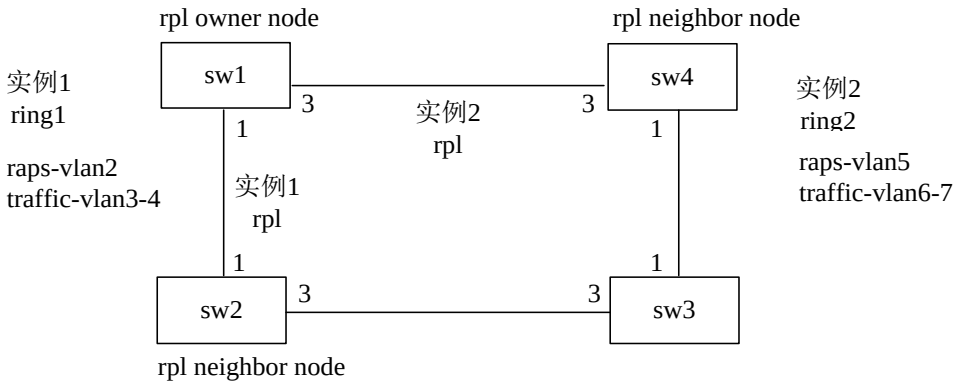
Switch(config-erps-1)# ring 2 rl-port xe1/3

Switch(config-erps-1)# ring 2 enable

Switch(config-erps-1)#exit

10.6.3 Multi-instance load balancing example

As shown in the figure below, the sw1, sw2, sw3, and sw4 nodes form an erps instance 1 single ring ring1, the ports 1 and 3 of each node are used as erps ring ports, the protocol vlan of the ring is 2, the data vlan is 3, 4, and the sw1 node is rpl The owner node and sw2 node are rpl neighbor nodes, and the link between sw1 and sw2 is the rpl link.
The sw1, sw2, sw3, and sw4 nodes form an erps instance 2 single ring ring2, and the ports 1 and 3 of each node are used as erps ring ports. The protocol vlan of the ring is 5, the data vlan is 6, 7, and the sw1 node is the rpl owner node. The sw4 node is an rpl neighbor node, and the link between sw1 and sw4 is an rpl link.



(1)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 the ring port vlan mode to trunk, add erps protocol and data vlan

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 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 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 the ring port vlan mode to trunk, add erps protocol and data vlan

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 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-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 the ring port vlan mode to trunk, add erps protocol and data vlan

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 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 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

Configure 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 the ring port vlan mode to trunk, add erps protocol and data vlan

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 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 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 the ring port vlan mode to trunk, add erps protocol and data vlan

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 ring 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 the ring port vlan mode to trunk, add erps protocol and data vlan

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 ring 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 the ring port vlan mode to trunk, add erps protocol and data vlan

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 ring 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 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 the ring port vlan mode to trunk, add erps protocol and data vlan

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 ring 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

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

- Introduction to 802.1x
- Introduction to RADIUS
- Configure 802.1x

Configure RADIUS

AAA is short for Authentication, Authorization, and Accounting. It provides a consistent framework for configuring the three security functions of authentication, authorization, and accounting. The configuration of AAA is actually a management of network security. Network security here mainly refers to access control. Including who can access the network? What services can users with access rights get? How to account for users who are using network resources?

Authentication: To verify whether the user can gain access.

Authorization (Authorization): Authorized users can use which services.

Accounting (Accounting): record the user's use of network resources.

The company has launched a complete set of AAA solutions. Its products include 802.1x clients, various switches and authentication and accounting systems that support authentication. The 802.1x client is installed on the PC where users access the Internet. When users need to access the network, they need to use the 802.1x client for authentication. Only users who pass the authentication can use the network. This is a switch that supports authentication. It receives the client's authentication request and transmits the user name and password to the authentication and accounting system. The switch itself does not do the actual authentication. The authentication and charging system receives the authentication request sent by the switch to perform the actual authentication, and performs accounting processing on the user who has successfully authenticated.The 802.1x protocol is used for communication between the 802.1x client and the switch, and the RADIUS protocol is used for communication between the switch and the authentication and accounting system.

11.1 802.1x Introduction

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

802.1x is a Layer 2 protocol. The authenticated switch and the user's PC must be on the same subnet, and protocol packets cannot cross network segments. 802.1x authentication uses a client server model, and there must be a server to authenticate all users.

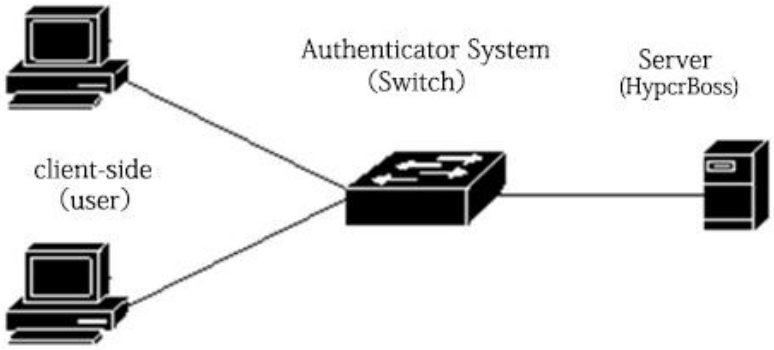
In MAC mode, before the user passes the authentication, only the authentication flow can pass through the port of the switch. After the authentication is successful, the data flow can pass through the port of the switch, that is, the user must access the network after passing the authentication. In port mode, you can enable the Guest Vlan function, which is disabled by default. When Guest Vlan is turned off, the data passing method is the same as MAC mode, but the port is opened after the authentication is passed, instead of registering the MAC address; when Guest Vlan is turned on, the data can pass Guest Vlan before the user passes the authentication, and after the authentication is successful, the pass Auth Vlan, this method can be used to limit the user to access the specified limited range before authentication, and to access the public network after authentication.

This section mainly includes the following:

- 802.1x device composition
- Brief introduction of protocol package
- Protocol flow interaction
- 802.1x port status

11.1.1 802.1xdevice composition

An 802.1x device is composed of three parts: a client (Supplicant System), an authentication system (Authenticator System), and an authentication server (Authentication Server System). As shown below.



802.1x devices

The client refers to a device requesting access to the network, which is generally a user terminal system, such as a user's PC. An 802.1x client software must be installed on the user terminal system, 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 user name 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 state of the user's logical port (referred to as the MAC address). If the user's logical port state is unauthorized, the user cannot access the network. If the user's logical port state is authorized, Then the user can access the network.

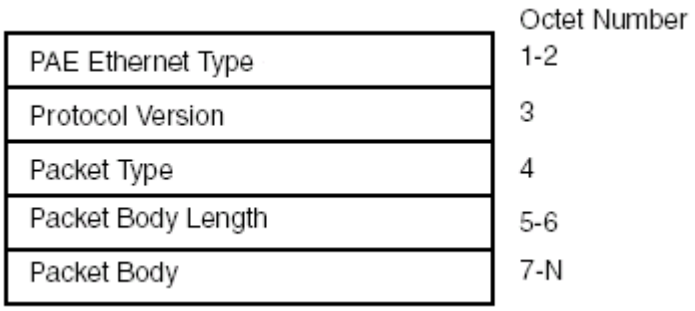
The authentication system is a relay between the client and the authentication server. The authentication system requests the user's identity information, and forwards the user's identity information to the authentication server, and forwards the authentication result from the authentication server to the client. The authentication system needs to implement the server part of the 802.1x protocol near the user side, and the client part of the RADIUS protocol near the authentication server side. The RADIUS protocol client of the authentication system encapsulates the 802.1x client with EAP information in RADIUS It is sent to the authentication server, and the EAP information is decapsulated in 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 users. The authentication server receives the identity information of the user from the authentication system and verifies it. If the authentication succeeds, the authentication server authorizes the authentication system to allow the user to access the network. If the authentication fails, the authentication server tells the authentication system that the user failed authentication and the user cannot access the network . The authentication server and the authentication system communicate through the RADIUS protocol extended by EAP. The company provides an authentication and charging system to authenticate and charge users.

11.1.2 Introduction to Protocol Package

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

The format of the EAPOL frame is shown below. PAE Ethernet Type is EAPOL's Ethernet protocol type number, with a value of 0x888E. Protocol Version is the EAPOL version number, with 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.



vEAPOL frame format

The switch uses three EAPOL protocol frames, namely:

EAPOL-Start: The value of Packet Type is 1, an authentication initiation frame. When a user needs to authenticate, this frame is first initiated and sent by the client to the switch.

EAPOL-Logoff: The value of Packet Type is 2 to exit the request frame. This frame is sent to the switch when the user does not need to use the network.

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

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

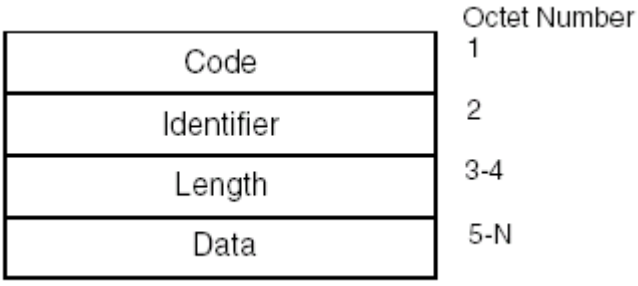
The EAP package includes the following four types:

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

EAP-Response: Code value is 2, EAP response packets are sent from the client to the switch, and the user name and/or password are sent to the switch.

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

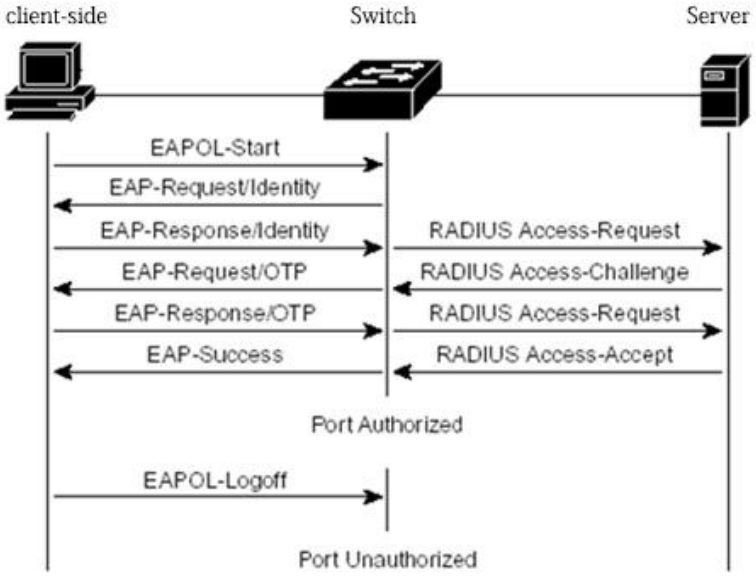
EAP-Failure: Code value is 4, EAP failure packet is sent from the switch to the client, telling the client that the user authentication failed.



EAP packet format

11.1.3 Protocol flow interaction

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



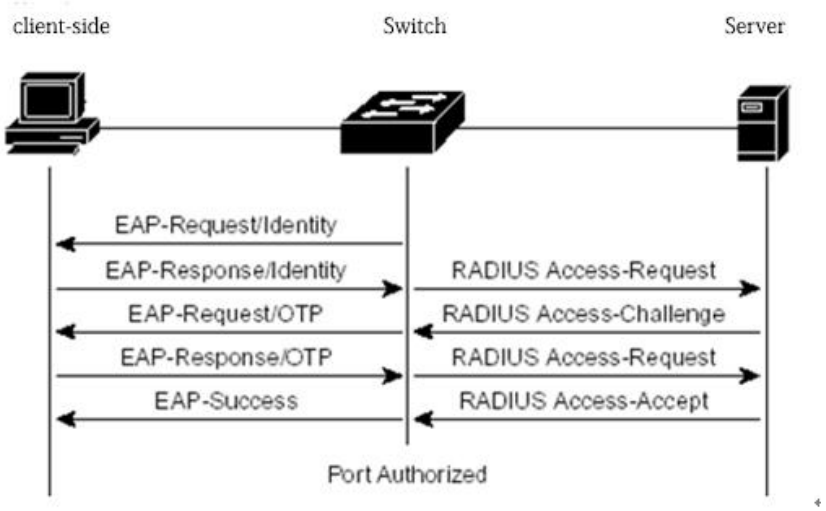
Client initiates authentication protocol interaction

When the user needs to access the network, the client first sends EAPOL-Start to the switch to request authentication. After the switch receives the authentication request, it sends an EAP-Request to request the user's username. The client sends back EAP-Response. The switch extracts the EAP information and encapsulates it in The RADIUS packet is sent to the authentication server. 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 sends back EAP-Response. The switch encapsulates the EAP information in the RADIUS packet and sends it to the authentication server. The server authenticates the user based on the user name and password. If the authentication is successful, the authentication server notifies the switch, and the switch sends EAP-Success to the client and puts the user's logical port in the authorized state. When the client receives the EAP-Success, the authentication is successful, and the user can access the network.

When the user no longer needs to use the network, the client sends EAPOL-Logoff to the switch, and the switch changes the user's logical port status to the unauthorized state, at which time the user cannot access the network.

In order to prevent the client from going offline abnormally, the switch provides a re-authentication mechanism. You can set the re-authentication interval on the switch. When the authentication time arrives, the switch initiates re-authentication. If the authentication is

successful, the user can continue to use the network. Failure, users will not be able to use the network. The protocol interaction is shown below.



Re-authentication protocol

11.1.4 802.1xport status

The port status here refers to the physical port status of the switch. There are four states of the physical port of the switch: N/A state, Auto state, Force-authorized state and Force-unauthorized state. When the switch does not open 802.1x, all ports are in N/A state. When the switch port is set to the Auto state, Force-authorized state, or Force-unauthorized state, you must first enable 802.1x on the switch.

When the port of the switch 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, it discards these protocol packets.

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 an EAP-Success packet, and when the switch receives other 802.1x protocol packets from the port, it discards these protocol packets.

When the port of the switch is in Force-unauthorized state, all users under the port cannot always access the network, and the authentication request will never pass. When the switch receives 802.1x protocol packets from this port, it discards these protocol packets.

When the port of the switch is in the Auto state, it is necessary to distinguish the authentication mode. In port mode, if Guest Vlan is not configured, users under the port must pass authentication to access the network, and the port is closed when not authenticated; if

Guest Vlan is configured, users under the port can access Auth Vlan after authentication, when unauthenticated Can visit Guest Vlan. All users under the port must pass authentication before they can access the network. The 802.1x protocol interaction is shown in the figure. If the user needs to do authentication, the port should generally be set to the Auto state.

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 only the data packets of the source MAC and source IP of the IP packet that meet the information provided by the client during authentication and the sender IP of the ARP packet Data packets that match the sender's MAC and the information provided by the client during 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 obtained dynamically through the DHCP protocol, the DHCP SNOOPING protocol can be enabled to achieve this function; if you need a more detailed introduction, please refer to the IP MAC binding configuration.

11.2 Introduction to RADIUS

When the user performs authentication, the RADIUS protocol that supports EAP extension is used for interaction between the switch and the authentication server. The RADIUS protocol uses a client/server model. The switch needs to implement a RADIUS client, and the authentication server needs to implement a RADIUS server.

In order 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 must authenticate each other. The switch and the authentication server need the same key. When the switch or the authentication server sends a RADIUS protocol packet, all protocol packets use the HMAC algorithm to generate a message digest based on the key. When the switch and the authentication server receive the RADIUS protocol packet, all The message digest of the protocol package must be verified with the key. If the verification is passed, it is considered to be a legitimate RADIUS protocol package, otherwise it is an illegal RADIUS protocol package and discarded.

This section mainly includes the following:

Brief introduction of protocol package

- Protocol flow interaction

User authentication method

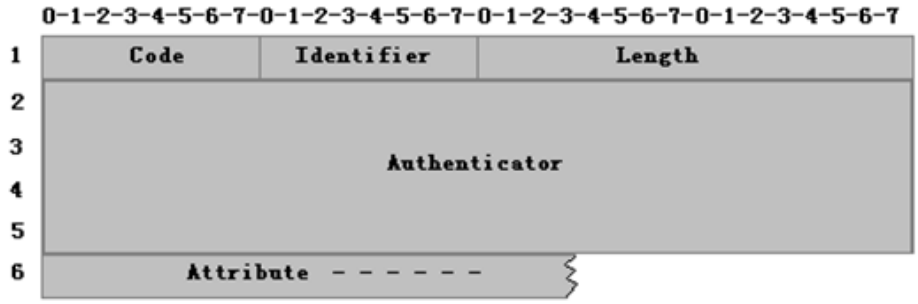
11.2.1 Introduction to the protocol package

RADIUS is a protocol built on UDP. RADIUS can encapsulate authentication information

and accounting information. The early RADIUS authentication port is 1645, currently using port 1812, the early RADIUS accounting port is 1646, and currently using port 1813.

Because RADIUS is carried on UDP, RADIUS must have a timeout retransmission mechanism. At the same time, in order to improve the reliability of the communication between the authentication system and the RADIUS server, two RADIUS server schemes are generally adopted, that is, a backup server mechanism.

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



RADIUS packet format

The switch uses the following RADIUS protocol packages:

Access-Request: Code value is 1, an authentication request packet sent from the authentication system to the authentication server, and the user name and password are encapsulated in this packet.

Access-Accept: Code value is 2, a response packet sent from the authentication server to the authentication system, indicating that the user authentication is successful.

Access-Reject: Code value is 3, a response packet sent from the authentication server to the authentication system, indicating user authentication failure.

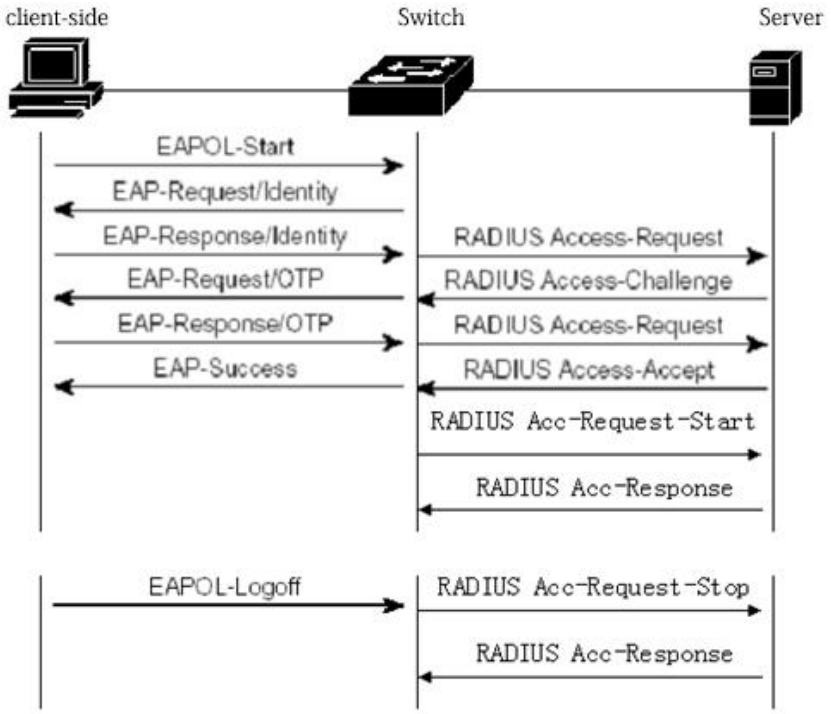
Access-Challenge: Code value 11, a response packet sent from the authentication server to the authentication system, indicating that the authentication server needs further information of the user, such as a password.

Accounting-Request: The Code value is 4, and the accounting request packet sent from the authentication system to the authentication server includes the start accounting and end accounting packets, and the accounting information is encapsulated in this packet.

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

11.2.2 Protocol flow interaction

When the user initiates authentication, the authentication system and the authentication server interact through the RADIUS protocol. The following figure shows the protocol flow interaction of the authentication system without sending RADIUS accounting packets. Generally, after the user authentication is successful or when the user goes offline, the authentication system needs to send a RADIUS accounting packet to the authentication server. The protocol flow interaction is shown in the figure below.



When the user performs authentication, the switch encapsulates the user name in an Access-Request message and sends it to the authentication server. The server responds to the Access-Challenge request for the user's password. The switch requests the client user's password. The client encapsulates the password in the EAP. The switch After obtaining this EAP, it is encapsulated in Access-Request and sent to the authentication server. The authentication server authenticates the user. If the authentication is successful, it returns Access-Accept to the switch. After receiving this message, the switch notifies the client that the authentication is successful and sends Accounting- Request informs the authentication server to start charging, and the authentication server sends back Accounting-Response.

When the user does not want to use the network, the switch user is notified to go offline, and the switch sends an Accounting-Request to notify the authentication server to end accounting. The accounting information is encapsulated in this package, and the authentication server sends back Accounting-Response.

11.2.3 User authentication method

RADIUS has three user authentication methods, as follows:

- PAP (Password Authentication Protocol). 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 package. The RADIUS server searches the database. If the same user name and password exist, the authentication is passed, otherwise the authentication is not passed.
- CHAP (Challenge Handshake Authentication Protocol). When a user requests Internet access, the switch generates a 16-byte random code to the user. The user encrypts the random code, password and other domains to generate a response, and transmits the user name and response to the switch. The switch transmits the user name, response and the original 16-byte random code to the RADIUS server. RADIU looks up the database on the exchange side according to the user name, obtains the same password used for encryption at the user side, and then encrypts it according to the 16-byte random code transmitted, and compares the result with the response received. If the same indicates The verification is passed. If they are different, the verification fails.
-

EAP (Extensible Authentication Protocol). With this authentication method, the switch does not really participate in the authentication, but only serves as a forwarding function between the user and the RADIUS server. When a user requests Internet access, 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 for the user and stores the random code. The user pairs the random code, password, and other fields. Encryption generates a response, passes the user name and response to the switch, and the switch forwards it to the RADIUS server. RADIU looks up the database on the switch side according to the user name, obtains the same password used for encryption at the user side, and then encrypts according to the stored 16-byte random code, and compares the result with the response received. If the same indicates verification Passed, if not the same, it means that the verification failed.

The company's authentication and billing solution uses the EAP user authentication method.

11.3 Configure 802.1x

This section describes the configuration of 802.1x in detail, including the following contents:

- 802.1x default configuration

- Start and shut down 802.1x
- Configure 802.1x port status
- Configure re-authentication mechanism
- Configure the maximum number of port access hosts
- Configure interval time and retransmission times
- Configure the port as a transmission port
- Configure the 802.1x client version number
- Configure whether to check the client version number
- Configure authentication method
- Configure whether to check the client's timing package
- Display 802.1x information

11.3.1 802.1x default configuration

The default configuration of the switch 802.1x is as follows:

- 802.1x is closed.
- 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.
- The number of times to retransmit EAP-Request is 3 times.
- The waiting time for user authentication failure is 60 seconds.
- The timeout interval of the server overtime retransmission is 10 seconds.

The switch provides a command in the global CONFIG mode to return all configurations to the default state. The command is as follows:

Switch(config)#dot1x default

11.3.2 Turning 802.1x on and off

The first step in configuring 802.1x is to start 802.1x. Enter the following command in global CONFIG mode to start 802.1x:

Switch(config)#dot1x

When 802.1x is turned off, all ports return to N/A state. Enter the following command in global CONFIG mode to close 802.1x:

Switch(config)#no dot1x

11.3.3 Configure 802.1x port status

Before setting the 802.1x port status, be sure to enable 802.1x. If all users under the port must pass authentication before they can access the network, the port must be set to the Auto state.

The following command sets port ge1/1 to Auto state in interface configuration mode and enables anti-ARP spoofing function:

Switch(config-ge1/1)dot1x control auto

If the anti-ARP spoofing 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 DHCP SNOOPING function is enabled on the current interface.
4. The configured interface is a Layer 3 interface or a trunk interface.

The following command sets the port ge1/1 to Force-authorized state in interface configuration mode:

Switch(config-ge1/1)dot1x control force-authorized

The following command sets the port ge1/1 to Force-unauthorized state in interface configuration mode:

Switch(config-ge1/1)dot1x control force-unauthorized

The following command sets port ge1/1 to 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 Method

Before setting the 802.1x port authentication method, be sure to enable 802.1x. If only one user who needs to be authenticated is connected to the port, the port must be opened if the authentication is passed, and the port must be set to portbase. If MAC address-based

authentication is to be implemented, it must be set to macbase. The default state is macbase.

The following command sets port ge1/1 to portbase state in interface configuration mode:

Switch(config-ge1/1)dot1x method portbase

The following command sets 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

Before setting the guest VLAN for the 802.1x port, be sure to enable 802.1x and configure the port for the Auto state and the portbase state. If you want the user under the port to be able to access the guest vlan before passing the authentication and accessing the configuration vlan after passing the authentication, the guest vlan must be configured on the port.

It must be noted that guest vlan only supports access mode and does not support trunk. Once a guest VLAN is configured on a port, its mode cannot be modified, nor can guest VLAN be configured in non-access mode. When configuring a 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

To prevent the switch and the authentication server from being noticed after the client goes offline abnormally, the switch provides a re-authentication mechanism. The switch initiates authentication every re-authentication interval.

The following command starts the re-authentication mechanism in global CONFIG mode:

Switch(config)#dot1x reauthenticate

The following command turns off the re-authentication mechanism in global CONFIG mode:

Switch(config)#no dot1x reauthenticate

The following command sets the re-authentication interval in global CONFIG mode:

Switch(config)#dot1x timeout re-authperiod <interval>

Note: Do not set the re-authentication interval too short, otherwise the network bandwidth and the CPU resource consumption of the switch will be 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 that can be accessed. This function can restrict users from using multiple hosts to illegally access the network. The maximum number of port access hosts is 100 by default, and the maximum number can be set to 100. If the maximum number of access hosts on a port is set to 0, then the port denies any user access.

The following command sets the maximum number of access hosts on port ge1/1 in interface configuration mode:

Switch(config-ge1/1)dot1x support-host <number>

11.3.8 Configure Interval Time and Retransmission Times

The 802.1x protocol standard specifies some intervals and retransmission times of the protocol interaction and protocol state machine. The switch uses standard intervals and retransmission times. It is recommended that users do not change these intervals and retransmission times when using them.

tx-period indicates the interval between the switch retransmitting EAP-Request protocol packets; max-req indicates the number of times the switch retransmits EAP-Request; quiet-period indicates the interval between waiting for re-authentication when user authentication fails; server-timeout indicates Interval time for the switch to resend the RADIUS packet to the authentication server; supp-timeout indicates the time interval for the switch to resend the eap request packet to the client.

The following command configures these intervals and retransmission times in 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 Configure the port as a transmission port

When the switch does not have 802.1x authentication turned on, and other switches in

the subnet have 802.1x authentication turned on, you can configure the port connecting the client to the authentication switch as the transmission port, and forward eapol between the client and the 802.1x authentication switch Certification package. In order to achieve the 802.1x authentication of the client by other switches.

The following command sets port ge1/1 as a transmission port in interface configuration mode:

Switch(config-ge1/1)dot1x transmit-port

The following command sets port ge1/1 as a non-transport port in interface configuration mode:

Switch(config-ge1/1)no dot1x transmit-port

11.3.10 Configure the 802.1x client version number

Configure the version number of the 802.1x client. Only clients whose version is not lower 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 to check the client version number

Configure whether to check the version number of the 802.1x client. If it is configured to check, the switch must first check the client version number when doing authentication. The default is configured to check.

The following command configures to enable checking the client version number in global CONFIG mode:

Switch(config)# dot1x check-version open

11.3.12 Configure Authentication Method

Configure the switch's authentication method for 802.1x packets. The authentication method initiated by the client is divided into general authentication and extended authentication. The switch can be configured to authenticate first. If the authentication method initiated by the client is inconsistent with the authentication method configured on the switch, the client will switch to another authentication method to initiate authentication after a certain number of authentication failures.

The following command configures the authentication mode of the switch as the extended authentication mode in the global CONFIG mode:

Switch(config)# dot1x extended

11.3.13 Configure whether to check the client's timing package

Configure whether the switch checks the client's timed packets. After the authentication is successful, the switch will ask the client to send 802.1x packets at regular intervals, but not all clients will send 802.1x packets at regular intervals after passing the authentication. End timing packet.

The following command is configured for the switch to check the client's timing packets in global CONFIG mode:

Switch(config)# dot1x check-client

11.3.14 Display 802.1x information

The following command displays 802.1x information in normal mode/privileged mode. When the command is show dot1x, it displays all 802.1x configuration information, including all port configuration information; when the command is show dot1x interface, it displays Information of all access users:

Switch#show dot1x

Switch#show dot1x interface

11.4 Configure RADIUS

This section describes the RADIUS configuration in detail, including the following contents:

- Default configuration of RADIUS
- Configure the IP address of the authentication server
- Configure shared key
- Starting and closing billing
- Configure RADIUS port and attribute information
- Configure RADIUS roaming function

Display RADIUS information

11.4.1 RADIUS default configuration

The default configuration of the switch RADIUS is as follows:

- The IP addresses of the primary authentication server and the backup authentication server are not configured, that is, the IP address is 0.0.0.0.
- No shared key is configured, that is, the shared key string is empty.
- Billing is enabled by default.
- The UDP port for RADIUS authentication is 1812, and the UDP port for accounting is 1813.
-

The value of the RADIUS attribute NASPort is 0xc353, the value of NASPortType is 0x0f, and the value of NASPortServer is 0x02.

11.4.2 Configure the IP address of the authentication server

To enable RADIUS communication between the switch and the authentication server, you need to configure the IP address of the authentication server on the switch. In practical applications, one authentication server or two authentication servers can be used, 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 communicating with the backup authentication server when the switch disconnects from the main authentication server.

The following command configures the IP address of the primary authentication server in global CONFIG mode:

Switch(config)#radius-server host <ip-address>

The following command configures the IP address of the backup authentication server in global CONFIG mode:

Switch(config)#radius-server option-host <ip-address>

11.4.3 Configure Shared Key

The switch and the authentication server must authenticate each other. Both the switch and the authentication server need to be set with the same shared key. Note that the shared key on the switch must be the same as the authentication server.

The following command configures the shared key of the switch in global CONFIG mode:

Switch(config)#radius-server key <string>

11.4.4 Turn billing on and off

If accounting is disabled on the switch, the switch will not send RADIUS accounting

packets to the authentication server after the authentication is successful or the user goes offline. Generally, in practical applications, billing is turned on.

The following command starts accounting in global CONFIG mode:

Switch(config)#radius-server accounting

The following command turns off accounting in global CONFIG mode:

Switch(config)#no radius-server accounting

11.4.5 Configuring RADIUS Port and Attribute Information

It is recommended that users do not modify the RADIUS port and attribute information configuration.

The following command modifies the RADIUS authentication UDP port in global CONFIG mode:

Switch(config)#radius-server udp-port <port-number>

The following command modifies RADIUS attribute 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 performed on the client, and when the client is moved to another location, the bound client cannot perform 802.1x authentication because the MAC address, IP address, or VLAN of the client changes. Turning on the radius roaming function will ignore the client's MAC, IP or VLAN binding, thus continuing to implement 802.1x authentication.

The following command configures the RADIUS roaming function in global CONFIG mode:

Switch(config)#radius-server roam

The following command disables 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 mode/privileged mode:

Switch#show radius-server

11.5 Configuration example

Open the 802.1x protocol, configure port ge1/1 as Auto, configure the main authentication server as 198.168.80.111, and configure the shared key of the switch as 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

This chapter mainly includes the following:

- GMRP introduction
- Configure GMRP
- Display GMRP

12.1 Introduction of GMRP

At present, GMRP (GARP Multicast Registration Protocol, GARP Multicast Registration Protocol) is a multicast registration protocol based on GARP, used to maintain multicast registration information in the switch. All switches that support GMRP can receive multicast registration information from other switches, and dynamically update local multicast registration information, and can also propagate local multicast registration information to other switches. This information exchange mechanism ensures the consistency of the multicast information maintained by all GMRP-enabled devices in the same switching network.

When a host wants to join a multicast group, it will send a GMRP join message. The switch joins the port that receives the GMRP join message to the multicast group, and broadcasts the GMRP join message in the VLAN where the receiving port is located, so that the multicast source in the VLAN can know the existence of the multicast member. When a multicast source sends a multicast message to a multicast group, the switch only forwards the multicast message to the port connected to the member of the multicast group, thereby implementing Layer 2 multicast in the VLAN.

12.2 Configuring GMRP

The main configuration of GMRP includes:
Turn on GMRP
View GMRP
In the configuration task, you must enable global GMRP before you can enable port GMRP.

12.2.1 Open GMRP settings

command	description	Configuration mode
set gmrp enable | disable	Enable/disable all global vlan gmrp	Global configuration mode
set gmrp enable vlan <vlan-id>	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 the port GMRP function	Global configuration mode

12.2.2 View GMRP information

After completing the above configuration, execute the show command in any view to display the running status of GMRP after configuration, and verify the effect of the configuration by viewing the displayed information.

command	description	Configuration mode
show gmrp configuration	View GMRP configuration information	Privileged mode
show gmrp machine	View GMRP state machine information	Privileged mode
show gmrp statistics vlanid	View specific vlanid's gmrp statistics	Privileged mode
show gmrp timer <ifname>	View timer information for specific ports	Privileged mode

12.3 GMRP typical configuration example

1. Networking requirements
In order to achieve dynamic registration and update of multicast information between switches, GMRP needs to be started on the switch
2. Network diagram

GMRP example network diagram

3.Configuration steps

Configure SW1

Start global GMRP

Switch(config)# set gmrp enable

Start port GMRP on the Gigabit Ethernet port ge1/1

Switch(config)# set port gmrp enable ge1/1

Switch(config)#

Configure SW2

Start global GMRP

Switch(config)# set gmrp enable

Start port GMRP on Gigabit Ethernet port ge1/28

Switch(config)# set port gmrp enable ge1/28

Switch(config)#

In the metropolitan area network/Internet, when unicast is used to send the same data packet to multiple but not all receivers in the network, since the packet needs to be copied to each receiving endpoint, as the number of receivers increases, the need The number of packets sent will also increase linearly, which makes the overall burden on the host, switching routing equipment, and network bandwidth resources heavier, and the efficiency is greatly affected. With the increasing demand for multi-point video conferencing, video-on-demand, and group communication applications, in order to improve resource utilization, the multicast method has increasingly become a commonly used transmission method in multi-point communication.

The switch implements the IGMP SNOOPING function and serves multicast applications. IGMP SNOOPING monitors IGMP packets on the network to achieve dynamic learning of IP multicast MAC addresses.

This chapter describes the concept and configuration of IGMP SNOOPING, including the following contents:

- IGMP SNOOPING introduction
- IGMP SNOOPING configuration、
- IGMP SNOOPING configuration example

13.1 Introduction to IGMP SNOOPING

In a traditional network, multicast data packets are treated as broadcasts in a subnet, which easily causes large network traffic and causes network congestion. When IGMP SNOOPING is implemented on the switch, IGMP SNOOPING can dynamically learn the IP multicast MAC address and maintain the output port list of the IP 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:

- 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 that listens for IGMP protocol packets passing through the switch, maintains a multicast group based on the receiving ports, VLAN IDs, and multicast addresses of these IGMP protocol packets, and then forwards these IGMP protocol packets. Only ports that have joined the multicast group can receive multicast data

streams; this reduces network traffic and saves network bandwidth.

The multicast group includes the multicast group address, member port, VLAN ID, and Age time.

The formation of 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 received the IGMP QUERY also joins the multicast group, otherwise it just forwards the IGMP QUERY packet. IGMP SNOOPING also supports the IGMP V2 Leave mechanism; if IGMP SNOOPING is configured with fast-leave as ENABLE, the receiving port can immediately leave the multicast group when receiving the IGMP V2 leave packet; if fast-leave leave wait time is configured (fast-leave-timeout), then the multicast group waits for this time to expire before leaving the multicast group.

IGMP SNOOPING has two update mechanisms. One is the leave mechanism introduced above. In most cases, IGMP SNOOPING deletes expired multicast groups by age time. When a multicast group joins IGMP SNOOPING, the time of joining is recorded. When the multicast group stays in the switch for more than a configured age time, the switch deletes the multicast group.

When a port receives the Leave protocol packet, the port will be immediately deleted from the multicast group to which it belongs. This situation may affect the continuity of the network data flow; because the port may be connected to a HUB or no IGMP SNOOPING A functional network device, a lot of devices for receiving multicast data streams are connected to this device. If a device sends a Leave, other devices may not receive the multicast data stream. The fast-leave-timeout mechanism can prevent this from happening. Configure a leave-wait time through Fast-leave-timeout. After the port receives the leave packet, it waits for Fast-leave-timeout for a long time and then it will leave the multicast group to which it belongs. Delete in the middle, may guarantee the continuity of the network multicast stream.

13.1.2 Layer 2 Dynamic Multicast

The multicast MAC address entries in the Layer 2 hardware multicast forwarding table can be dynamically learned through IGMP SNOOPING. What I learned dynamically through IGMP SNOOPING is the IP multicast MAC address.

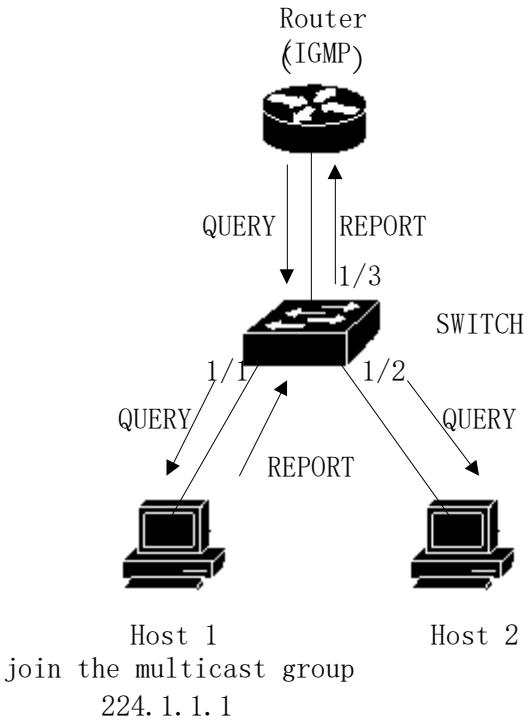
When the switch turns off IGMP SNOOPING, the Layer 2 hardware multicast forwarding table is in unregistered forwarding mode, the multicast MAC address cannot be learned dynamically, there is no entry in the Layer 2 hardware multicast forwarding table, and all Layer 2 multicast data streams are treated as Broadcast processing.

When the network has a multicast environment, in order to effectively control the multicast traffic of the network, the switch can turn on IGMP SNOOPING. At this time, the Layer 2

hardware multicast forwarding table is in the registered forwarding mode. The switch can learn the group by listening to the IGMP protocol packets on the network Only the MAC address can be forwarded if the layer 2 multicast stream matches the entry in the layer 2 hardware multicast forwarding table.

13.1.3 Join a group

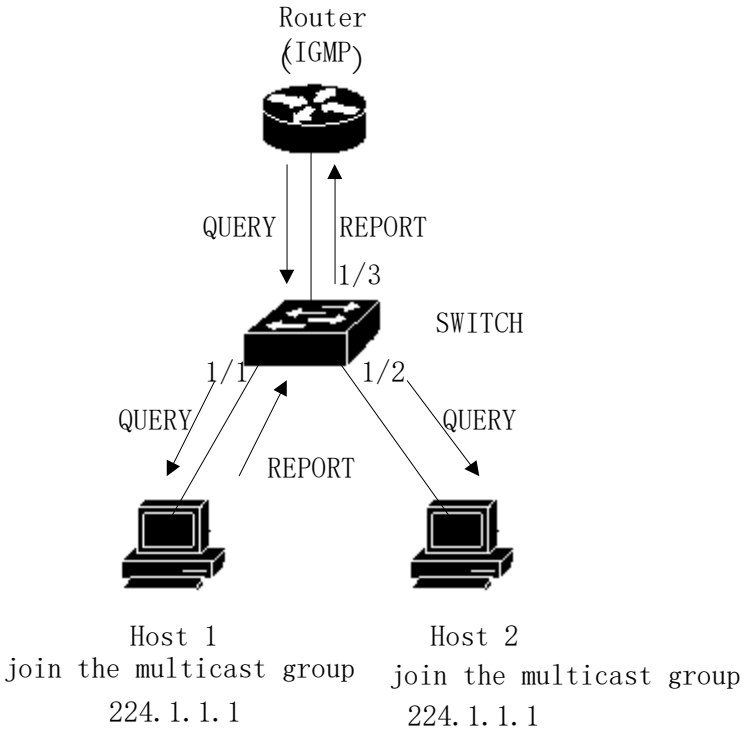
When a host wants to join a multicast group, the host sends an IGMP REPORT packet, which specifies the multicast group the host wants to join. When the switch receives an IGMP QUERY packet, the switch will forward the packet to all other ports in the same VLAN. When the host under the port who wants to join the multicast group receives the IGMP QUERY packet, it will return an IGMP REPORT packet. When the switch receives an IGMP REPORT packet, it will create a Layer 2 multicast entry. The port that receives the IGMP QUERY packet and the port of the IGMP REPORT packet will be added to the Layer 2 multicast entry and become its output port.



As shown above, all the devices are in a subnet, assuming that the VLAN of this subnet is 2. The router runs the IGMPv2 protocol and regularly sends IGMP QUERY packets. Host 1 wants to join the multicast group 224.1.1.1. After receiving the IGMP QUERY packet from port 1/3, the switch records this port and forwards the packet to ports 1/1 and 1/2. Host 1 sends back an IGMP REPORT packet after receiving the IGMP QUERY packet. Host 2 does not send the IGMP REPORT packet because it does not want to join the multicast group. After receiving

the IGMP REPORT packet from port 1/1, the switch forwards the packet from query port 1/3 and creates a Layer 2 multicast entry (assuming that the entry does not exist). The Layer 2 multicast entry 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 shown in the above picture, the conditions are the same as in Figure 1. Host 1 has joined the multicast group 224.1.1.1, and now host 2 wants to join the multicast group 224.1.1.1. When host 2 receives an IGMP QUERY packet and sends back an IGMP REPORT packet, the switch forwards the packet from query port 1/3 after receiving the IGMP REPORT from port 1/2 and adds the packet port 1/2 to the Layer 2 group In the broadcast entry, the layer 2 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 Leaving 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. The host that has joined the multicast group or wants to join the multicast group will send back 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 leaving means that the host sends an IGMP LEAVE packet to the router. Passive leaving means that the host does not send back 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 leave the Layer 2 multicast entry on the switch port: leave overtime and leave after receiving the IGMP LEAVE packet.

When the switch does not receive an IGMP REPORT packet of a multicast group from a port for more than a certain time, the port should be cleared from the corresponding layer 2 multicast entry. If the layer 2 multicast entry has no port, delete the two Layer multicast entry.

When the switch's fast-leave 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 has no port , Then delete the Layer 2 multicast entry.

Fast-leave is generally used when a host is connected to a port; if there is more than one host under a port, the fast-leave-timeout latency can be configured to ensure the continuity and reliability of the multicast stream in the network.

13.2 IGMP SNOOPING configuration

13.2.1 IGMP SNOOPING default configuration

IGMP SNOOPING is off by default, and the Layer 2 hardware multicast forwarding table is in unregistered forwarding mode.

Fast-leave is off by default.

Fast-leave-timeout time is 300 seconds.

The age of the REPORT port of a multicast group defaults to 400 seconds.

The age of the QUERY port of the multicast group defaults to 300 seconds.

13.2.2 Turning on and off IGMP SNOOPING

The IGMP SNOOPING protocol can be opened globally or some VLANs can be opened individually; only if IGMP SNOOPING is turned on globally can IGMP SNOOPING of a VLAN be turned on or off.

Turn on global IGMP SNOOPING

Switch#configure terminal

Switch(config)#ip igmp snooping

Turn on 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

Disable IGMP SNOOPING for a VLAN

Switch#configure terminal

Switch(config)#no ip igmp snooping vlan <vlan-id>

13.2.3 Configuring Time to Live

Configure the time to live for multicast groups

Switch#configure terminal

Switch(config)#ip igmp snooping group-membership-timeout <interval> vlan <vlan-id>

The unit of Interval is milliseconds.

Configure the time to live for a 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-leave

Start a VLAN fast-leave

Switch#configure terminal

Switch(config)#ip igmp snooping fast-leave vlan <vlan-id>

Close 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 the default fast-leave wait time

Switch#configure terminal

Switch(config)#no ip igmp snooping fast-leave-timeout vlan <vlan-id>

13.2.5 Configuring MROUTER

Configure a static query port

Switch#configure terminal

Switch#interface ge1/6

Switch(config-ge1/6) #ip igmp snooping mrouter vlan [vlan-id]

13.2.6 Display information

Display IGMP SNOOPING configuration information

Switch#show ip igmp snooping

Display configuration information of a VLAN

Switch#show ip igmp snooping vlan <vlan-id>

Display REPORT multicast group aging information

Switch#show ip igmp snooping age-table group-membership

Display QUERY's aging information

Switch#show ip igmp snooping age-table query-membership

Display the forwarding information of the multicast group

Switch#show ip igmp snooping forwarding-table

Display MROUTER information

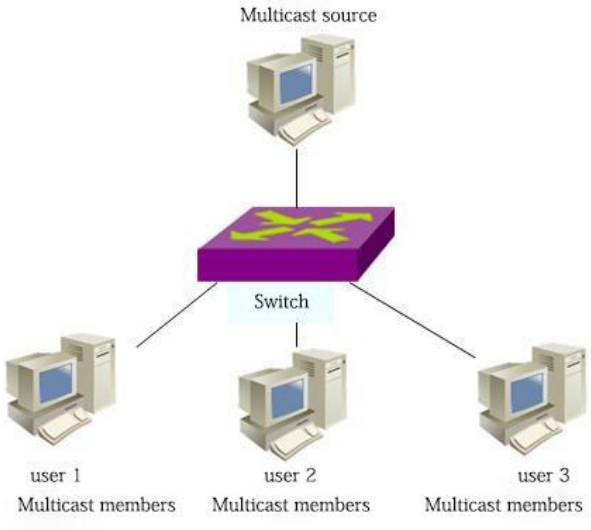
Switch#show ip igmp snooping mrouter

Display 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, and user 3 can join 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 mainly includes the following:

- MVR Introduction
- Configure MVR

14.1 Introduction to MVR

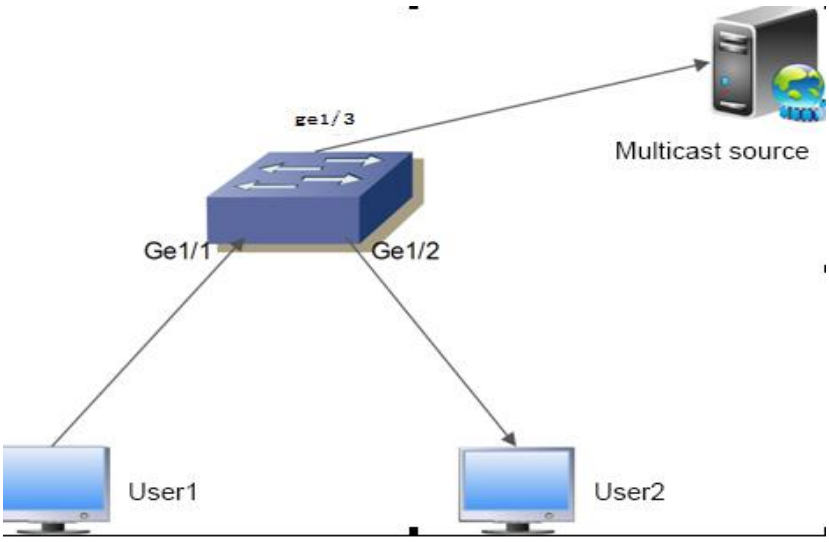
Multicast VLAN registration (MVR) is used for multicast streaming applications in service provider networks, such as TV on demand. MVR allows subscribers on a port to subscribe to or cancel multicast streams in a multicast VLAN, and allows data streams in a multicast VLAN to be shared by other VLANs. MVR has two purposes: (1) Through simple configuration, it can effectively and safely transfer multicast streams between VLANs; (2) Support dynamic joining and leaving of multicast groups;
The operation mode of MVR is similar to IGMP snooping. Both functions can be started at the same time. MVR only handles 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 multicast streams in IGMP snooping can only be forwarded in one VLAN, while MVR multicast streams can be forwarded in different VLANs.

14.2 Configuring MVR

command	description	CLI mode
mvr (enable|disable)	Start global MVR	Global configuration mode
no mvr	Clear all MVR configuration	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 an IP multicast address and a continuous MVR group address	Global configuration mode
mvr vlan <1-4094>	Specify the VLAN to receive multicast data	Global configuration mode
no mvr vlan	Restore the default VLAN1 for receiving multicast data	Global configuration mode
mvr-interface (enable|disable)	Start interface MVR	Interface configuration mode
show mvr	Display MVR configuration information	Privileged mode

14.3 MVR Configuration examples

The network topology is shown in the following figure. User 1 and user 2 belong to vlan10 and vlan20 respectively. User 1 and user 2 watch the same program. The program range is 225.1.1.1~225.1.1.64, and mvr vlan is 100:



Configure vlan, enable global IGMP snooping, configure mvr vlan, mvr program group range, and enable mvr globally:
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 the switch user port Ge1/1 Ge1/2 and upstream 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)#

15.1 DHCP V6CLIENT presentation

The dynamic host configuration protocol (DHCP) was designed to handle IP address and other network information assigned to the computer so that the computer can communicate automatically on the network. Using IPv6 network, you don't actually need DHCP to configure the address, but there are good reasons to use it. DHCP for IPv6(dhcpv6) can provide IPv6 hosts with stateful address configurations or stateless configuration settings. IPv6 hosts can configure addresses in a variety of ways:

The stateless address is automatically configured to configure both the linked local address and other non-linked local addresses by exchanging router requests and router announcement messages with adjacent routers.

Automatic configuration of stateful addresses is used to configure non-linked local addresses by using configuration protocols such as DHCP.

IPv6 host automatically performs stateless address automatic configuration and uses a configuration protocol (e.g. DHCPv6) based on the following tags in router announcement messages sent by adjacent routers:

Host address configuration tags, also known as M tags. When set to 1, this tag indicates that the host uses a configuration protocol to obtain a state address.

Other stateful configuration tags, also known as O tags. When set to 1, this tag indicates that the host uses the configuration protocol to get other configuration settings.

This section mainly includes the following:

- DHCPV6CLIENT configuration

15.2 DHCP V6CLIENT configuration

DHCPV6client the configuration command

Command	Description	CLI mode
dhcp v6client enable	Boot dhcpv6client function to get interface address	vlanif Configuration Mode
dhcpv6client renew	Retrieve IP address for interface	vlanif Configuration Mode
dhcpv6client release	Address IP Release Interface	vlanif Configuration Mode
show dhcp v6client	Check current dhcp v6client information	Privilege mode

16.1 ZTP presentation

ZTP (Zero Touch Provisioning) is a function that automatically loads configuration files when a new factory or empty configuration device is powered on. When deploying the network equipment, after the installation of the equipment hardware is completed, the administrator is required to go to the installation site to debug the software for the equipment. When the number of devices is large and the distribution is wide, the administrator needs to do manual configuration on each device, which not only affects the efficiency of deployment, but also requires high labor costs. Equipment running ZTP function, can obtain configuration from the file server, realize the equipment without on-site configuration, deployment, thereby reducing labor costs, improve deployment efficiency

ZTP implementation process is divided into the following stages:

1. power on the device start stage.

   After the device is powered on, if the device has a configuration file, it starts normally with that configuration file; if it is an empty configuration device, it enters the ZTP process.

2. DHCP information acquisition phase.

   Complete automatic deployment by DHCP. The device broadcasts a DHCP v6 request message (containing option 59,) on the Ethernet interface option 60). DHCP server sends DHCP reply messages to the device, ip address, are the Option options in the message option 59, option60 wait for information.

3. Gets the profile phase.

   According to the information obtained in the DHCP reply message, the device downloads the profile from the profile server.

4. Restart phase.

   The device sets the downloaded configuration file to the next boot file, then restarts, completes automatic deployment

16.2 ZTP configuration

ZTP configuration includes the configuration of the dhcpv6(already described in the dhcpv6client) and the start-up of parameters related to the ZTP.

ZTP commands are as follows:

Command	Description	CLI mode
ip dhcpv6bootfile-add-mac	get the profile name by DHCPv6 protocol and rename it. create a new file name by merging the original file name and the mac address on the ZTP device, i.e ." file name - mac".	Global Configuration Mode
ip dhcpv6tftp-download	DHCPv6 carry option 59option 60 in the request protocol to get the TFTP server address and profile name.	Global Configuration Mode
ip dhcpv6duid-type {en |ll |llt}	Type of duit for DHCPv6 protocol packages	Global Configuration Mode
ztp enable	Boot ZTP function	Interface Configuration Mode

In a dynamically connected network environment, the host obtains the IP address and network parameters through the DHCP server. DHCP SNOOPING is a listening protocol proposed for ARP attacks. By listening to DHCP packets, the IP address and client MAC address assigned by the DHCP server to the client are dynamically bound to filter ARP attack packets on the switch.

The switch supports DHCP SNOOPING function, which can effectively prevent ARP attacks. DHCP SNOOPING listens for DHCP messages on the network and binds port ARP information.

Four physical ports of the DHCP server can be configured to prevent unknown servers from interfering with the network to a certain extent.

When the switch is powered off and restarted, the binding table will be lost and need to be learned again; the switch provides the binding table upload and download function, which can save the binding table on the tftp server.

This chapter describes the concept and configuration of DHCP SNOOPING, including the following contents:

- DHCP SNOOPING introduction
- DHCP SNOOPING configuration
- DHCP SNOOPING configuration example

17.1 Introduction to DHCP SNOOPING

The ARP protocol has created a loophole in network security due to a simple trust mechanism. When an ARP attack packet carrying false MAC information reaches the host, it will directly cover the local ARP cache table without restriction, resulting in normal data flow to the attacker. To this end, the port's 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 an unpredictable DHCP server enters the network, the IP address allocation will be confused. The DHCP SNOOPING protocol provides a physical port for binding the link server. Unspecified physical ports cannot forward DHCP protocol packets sent by the DHCP server, which can reduce this unknown. The opportunity for the server to enter the network.

This section mainly includes the following:

- DHCP SNOOPING Process
- DHCP SNOOPING Binding table
- DHCP SNOOPING is bound to the physical port of the server
- DHCP SNOOPING binding table upload and download

17.1.1 DHCP SNOOPING process

The DHCP SNOOPING protocol only listens to DHCPrequest, DHCPack, and DHCPrelease packets, does not receive other types of DHCP packets, and binds the mapping relationship between IP and MAC according to these packets.

The global DHCP SNOOPING switch is responsible for turning on the switch to receive DHCP messages, that is, IP messages with UDP ports 67 and 68.

17.1.2 DHCP SNOOPING binding table

The DHCP SNOOPING binding table entries are indexed by the MAC address and include the entry type, IP address, MAC address, interface information, delay timer, and lease timer. There are two types of REQ and ACK. The REQ type entry indicates that a DHCPrequest message has been received and a DHCPack message has not been received. At this time, a delay timer is started. The default interval is 10 seconds. If the DHCPack message is not received in 10 seconds The REQ type binding table entry is deleted; the ACK type entry indicates that the DHCPack message is received, the recorded IP address is the IP address assigned by the server, the lease timer is started at this time, and the time interval is in the DHCPack message Contains the lease value provided by the DHCP server. When the lease is renewed, the timer is restarted. When the lease expires, the binding table entry is deleted. The interface information records the interface where the client is located, that is, the interface corresponding to the binding relationship between the IP address and the MAC address.

When a DHCPrequest message is received, a binding table entry is created, the entry type is REQ, the IP address, MAC address, interface information is recorded, and a 10-second delay timer is started.

When a DHCPrequest message is received, there is already a REQ type binding table entry, the entry is updated, and the delay timer is restarted.

When a DHCPrequest message is received and an ACK type binding table entry already exists, the interface information is recorded.

When a DHCPack message is received, if there is a REQ type binding table entry, 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, there is no REQ type binding table entry, the message is discarded.

When a DHCPack message is received, a binding table entry of the ACK type already exists. If the interface has changed, the binding table entry of the original interface is deleted and the entry is updated.

If the interface has not changed and the IP address assigned by the server has changed, delete the binding table entry of the original interface and update the entry.

If the interface has not changed and the IP address has not changed, it indicates that it is a renewal process, and the lease timer can be restarted.

When the delay timer expires, the REQ type binding table entry is deleted.

When the lease timer expires, the ACK type binding table entry is deleted.

17.1.3 DHCP SNOOPING specifies the physical port of the link server

DHCP SNOOPING specifies the physical port of the link server, and DHCP messages can only be received on the specified port. If there are multiple DHCP servers in the network, the OFFER provided by the server from a non-specified port will be filtered, and the client cannot be assigned an IP address. The designated port is conducive to the unified allocation of IP addresses in the network, to avoid that the address pool of unknown servers is not in the IP planning, and some clients cannot connect to the network normally. To a certain extent, the probability of abnormal network communication caused by private access to the server is reduced.

17.1.4 DHCP SNOOPING binding table upload and download

DHCP SNOOPING records the binding relationship between IP and MAC by monitoring DHCP messages and maintains its binding table. When the switch is powered off and restarted or a fault or unexpected power failure occurs, the binding table is lost. After restarting, the switch needs to learn the binding table entries again. In the network topology, if the hosts that are not directly connected are difficult to recognize the interruption of the network connection and restart the DHCP discover process, the switch will have difficulty learning the binding information again. To this end, save the binding table on the tftp server, and download the binding table after the switch restarts, which can solve the short-term memory blank that appears on the switch during restart. The switch provides the binding table upload and download function. The administrator can manually upload or download the binding table through the command, and can also configure the automatic upload command to periodically upload the binding table; the automatic download binding table command at restart is downloaded from the tftp server during the startup process The binding table file that has been backed up is written into the binding table of the DHCP SNOOPING protocol module.

17.2 DHCP SNOOPING configuration

17.2.1 DHCP SNOOPING default configuration

DHCP SNOOPING is off by default.

The default timer interval of the REQ entry in the DHCP SNOOPING binding table is 10 seconds.

17.2.2 Turning DHCP SNOOPING on and off globally

The DHCP SNOOPING of an interface can be turned on or off only after the DHCP SNOOPING is turned on globally. The DHCP SNOOPING must be turned off before all the interfaces can be turned off.

Turn on global DHCP SNOOPING

Switch#configure terminal

Switch(config)#ip dhcp snooping [IF_LIST]

The 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 "," signs, such as: ge1/1, ge1/25, ge1/26

Turn off global DHCP SNOOPING

Switch#configure terminal

Switch(config)#no ip dhcp snooping

17.2.3 Interface to turn DHCP SNOOPING on and off

Turn on DHCP SNOOPING for an interface

Switch#configure terminal

Switch(config)#interface ge1/1

Switch(config-ge1/1)#dhcp snooping

Turn off DHCP SNOOPING for an interface

Switch#configure terminal

Switch(config)#interface ge1/1

Switch(config-ge1/1)#no dhcp snooping

17.2.4 DHCP SNOOPING binding table upload and 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

Parameters: A.B.C.D IP address of tftp server; FILE_NAME is the name of the binding table file saved on 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 to periodically upload the 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 timed upload interval, ranging from 1 minute to one day.

Cancel the configuration of regularly uploading the DHCP SNOOPING binding table to the TFTP server

Switch#configure terminal

Switch(config)#no dhcp snooping auto-upload

Automatically download the DHCP SNOOPING binding table from the 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 when restarting

Switch#configure terminal

Switch(config)#no dhcp snooping reset-download

17.2.5 Display information

Display DHCP SNOOPING configuration information

Switch#show dhcp snooping

Display DHCP SNOOPING binding table information

Switch#show dhcp snooping binding-table

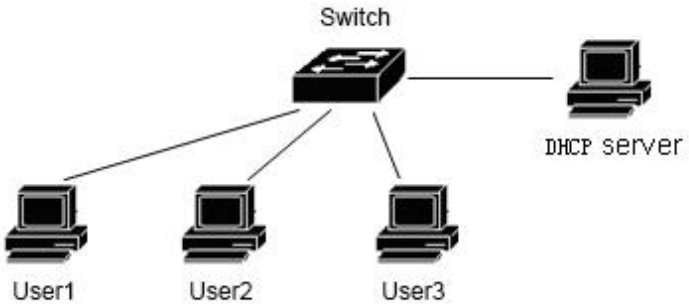
Display the current configuration of the system, including DHCP SNOOPING configuration.

Switch#show running-config

17.3 DHCP SNOOPING configuration example

17.3.1 Configuration

Enable the DHCP SNOOPING function on the Layer 2 switch. User 1, User 2, and User 3 dynamically obtain IP addresses and network parameters through the DHCP server. The interface where user 1, user 2, and user 3 are located starts the DHCP SNOOPING function, and dynamically binds ARP information to the interface.




```
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 192.168.0.1/24
!
```

```
interface ge1/1
 dhcp snooping
!
interface 1/2
 dhcp snooping
!
interface 1/3
 dhcp snooping
!
line vty
!
End
Switch#
```

17.4 DHCP SNOOPING configuration troubleshooting

If DHCP snooping configuration fails, it may be caused by the following reasons:

1. The system CFP resources are exhausted.
2. If an interface is configured with ACL filtering function, DHCP SNOOPING fails to be enabled globally
3. If an interface is configured with IP and MAC binding, the global opening of DHCP SNOOPING fails
4. The current interface is configured with ACL filtering.
5. The current interface is enabled with 802.1x anti-ARP spoofing function.
6. The configured interface is a Layer 3 interface or a trunk interface.

18.1 Introduction to DHCP CLIENT

DHCP (Dynamic Host Configuration Protocol, Dynamic Host Configuration Protocol), based on the Client/Server working mode, DHCP CLIENT function is the layer 3 interface address of the switch can obtain the address and gateway through the DHCP server.

This section mainly includes the following:

- Configuration of DHCP CLIENT

18.2 DHCP CLIENT configuration

Open the dhcp client function of interface vlan1

switch(config)#

Switch(config)#interface vlan1

Switch(config-vlan1)#dhcp client enable

Reacquire an IP address for interface vlan1

switch(config)#

Switch(config)#interface vlan1

Switch(config-vlan1)#dhcp client renew

Release the IP address of interface vlan1

switch(config)#

Switch(config)#interface vlan1

Switch(config-vlan1)#dhcp client release

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 the packet needs to be copied to each receiving endpoint, as the number of receivers increases, the need The number of packets sent will also increase linearly, which makes the overall burden on the host, switching routing equipment and network bandwidth resources heavier and the efficiency greatly affected. With the increasing demand for multi-point video conferencing, video-on-demand, and group communication applications, in order to improve resource utilization, the multicast method has increasingly become a commonly used transmission method in multi-point communication.

The switch implements the MLD SNOOPING function and serves multicast applications. MLD SNOOPING monitors MLD packets on the network to achieve dynamic learning of IPV6 multicast MAC addresses.

This chapter describes the concept and configuration of MLD SNOOPING, including the following contents:

- MLD SNOOPING introduction
- MLD SNOOPING configuration
- MLD SNOOPING configuration example

19.1 Introduction to MLD SNOOPING

In a traditional network, multicast data packets are treated as broadcasts in a subnet, which can easily cause heavy network traffic and cause network congestion. When MLD SNOOPING is implemented on the switch, MLD SNOOPING can dynamically learn the IPV6 multicast MAC address and maintain the output port list of the 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 multicast
- Join a group
- Leave a group

19.1.1 MLD SNOOPING process

MLD SNOOPING is a Layer 2 network protocol that monitors MLD protocol packets passing through the switch, maintains a multicast group based on the receiving ports, VLAN IDs, and multicast addresses of these MLD protocol packets, and then forwards these MLD protocol packets. Only ports that have joined the multicast group can receive multicast data streams; this reduces network traffic and saves network bandwidth.

The multicast group includes the multicast group address, member port, VLAN ID, and Age time.

The formation of MLD SNOOPING multicast group is a learning process. When a port of the switch receives an MLD REPORT packet, MLD SNOOPING will generate a new multicast group, and the port that receives the MLD REPORT packet will be 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 received the MLD QUERY also joins the multicast group, otherwise it simply forwards the MLD QUERY packet. MLD SNOOPING also supports the MLD V2 Done mechanism; if MLD SNOOPING is configured with fast-leave as ENABLE, the receiving port can immediately leave the multicast group when receiving the MLD V2 Done packet; if fast-leave leave wait time is configured (fast-leave-timeout), then the multicast group waits for this time to expire before leaving the multicast group.

MLD SNOOPING has two update mechanisms. One is the Done mechanism introduced above. In most cases, MLD SNOOPING deletes expired multicast groups by age time. When a multicast group joins MLD SNOOPING, the time of joining is recorded. When the multicast group remains in the switch for more than a configured age time, the switch deletes the multicast group.

When a port receives the Done protocol packet, the port will be immediately deleted from the multicast group to which it belongs. This situation may affect the continuity of the network data flow; because a HUB may be connected below the port or no MLD SNOOPING A functional network device, a lot of devices for receiving multicast data streams are connected to this device. If a device sends Done, it may affect other devices and cannot receive multicast data streams. The fast-leave-timeout mechanism can prevent this from happening. Configure a leave-wait time through Fast-leave-timeout. After the port receives the leave packet, it waits for Fast-leave-timeout for a long time and then it will leave the multicast group to which it belongs. Delete in the middle, may guarantee the continuity of the network multicast stream.

19.1.2 Layer 2 dynamic multicast

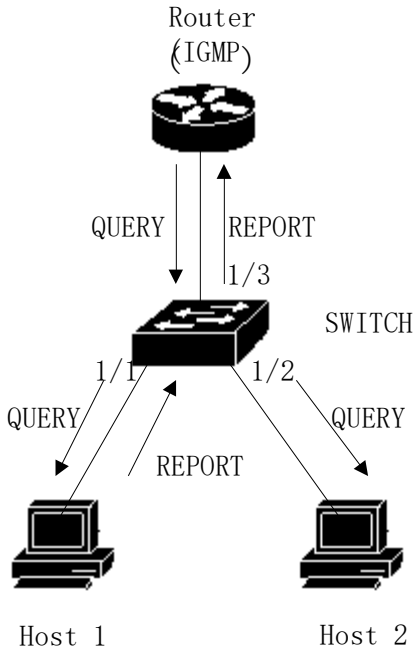
The multicast MAC address entry in the Layer 2 hardware multicast forwarding table can be dynamically learned through MLD SNOOPING. What is learned dynamically through MLD SNOOPING is the IPV6 multicast MAC address.

When the switch turns off MLD SNOOPING, the Layer 2 hardware multicast forwarding table is in unregistered forwarding mode, the multicast MAC address cannot 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 processing.

When the network has a multicast environment, in order to effectively control the multicast traffic of the network, the switch can turn on MLD SNOOPING. At this time, the Layer 2 hardware multicast forwarding table is in the registered forwarding mode, and the switch can learn the group by listening to the MLD protocol packets on the network. Only the MAC address can be forwarded if the layer 2 multicast stream matches the entry in the layer 2 hardware multicast forwarding table.

19.1.3 Join a group

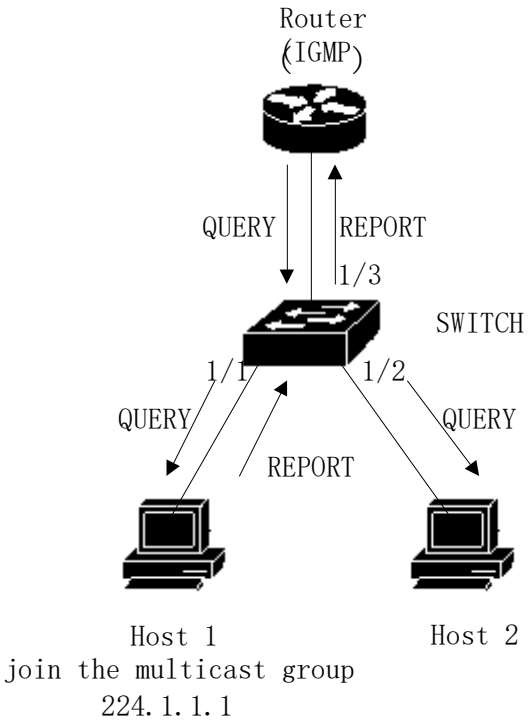
When a host wants to join a multicast group, the host sends an MLD REPORT packet, which specifies the multicast group the host wants to join. When the switch receives an MLD QUERY packet, the switch will forward the packet to all other ports in the same VLAN. When the host under the port that wants to join the multicast group receives the MLD QUERY packet, it will return an MLD QUPORT 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 port of the MLD REPORT packet will join the Layer 2 multicast entry and become its output port.



As shown above, all the devices are in a subnet, assuming that the VLAN of this subnet is 2. The router runs the MLDv2 protocol and regularly sends MLD QUERY packets. Host 1 wants to join the multicast group ff15::1. After receiving the MLD QUERY packet from port 1/3, the switch will record this port and forward 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 send

the MLD REPORT packet because it does not want to join the multicast group. 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 that 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 the above picture, the conditions are the same as in Figure 1. Host 1 has joined the multicast group ff15::1, and now host 2 wants to join the multicast group ff15::1. When the host 2 receives the MLD QUERY packet and sends back an MLD REPORT packet, the switch will forward the packet from the query port 1/3 after receiving the MLD REPORT from port 1/2 and add the packet port 1/2 to the Layer 2 group In the broadcast entry, the layer 2 multicast entry becomes:

Layer 2 multicast address	VLAN ID	Output port list
33:33:5e:00:00:01	2	1/1，1/2，1/3

19.1.4 Leaving 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. The host that has joined the multicast group or wants to join the multicast group will send back an MLD REPORT after receiving the MLD QUERY.

If the host wants to leave a multicast group, there are two ways: active leave and passive leave. Active leaving means that the host sends an MLD LEAVE packet to the router. Passive leaving means that the host does not return the MLD REPORT after receiving the MLD QUERY from the router.

Corresponding to the way that the host leaves the multicast group, there are two ways to leave the Layer 2 multicast entry on the switch: leave overtime and leave after receiving the MLD DONE packet.

When the switch does not receive a MLD REPORT packet of a multicast group from a port for more than a certain time, the port should be cleared from the corresponding layer 2 multicast entry. If the layer 2 multicast entry has no port, delete the two. Layer multicast entry.

When the switch's fast-leave is configured as ENABLE, if a port receives an MLD LEAVE packet from a multicast group, the port is cleared from the corresponding layer 2 multicast entry, and if the layer 2 multicast entry has no port , Then delete the Layer 2 multicast entry.

Fast-leave is generally used when a host is connected to a port; if there is more than one host under a port, fast-leave-timeout latency can be configured to ensure the continuity and reliability of the multicast stream in the network.

19.2 MLD SNOOPING configuration

19.2.1 MLD SNOOPING default configuration

MLD SNOOPING is off by default, and the Layer 2 hardware multicast forwarding table is in unregistered forwarding mode.

Fast-leave is off by default.

Fast-leave-timeout time is 300 seconds.

The age of the REPORT port of a multicast group defaults to 400 seconds.

The age of the QUERY port of the multicast group defaults to 300 seconds.

19.2.2 Turn MLD SNOOPING on and off

The MLD SNOOPING protocol can be opened globally or some VLANs can be opened individually; only MLD SNOOPING can be turned on or off in a VLAN.

Turn on global MLD SNOOPING

Switch#configure terminal

Switch(config)#ipv6 mld snooping

Open MLD SNOOPING for a VLAN

Switch#configure terminal

Switch(config)#ipv6 mld snooping vlan <vlan-id>

Turn off global MLD SNOOPING

Switch#configure terminal

Switch(config)#no ipv6 mld snooping

Turn off MLD SNOOPING for a VLAN

Switch#configure terminal

Switch(config)#no ipv6 mld snooping vlan <vlan-id>

19.2.3 Configure time to live

Configure the time to live for multicast groups

Switch#configure terminal

Switch(config)#ipv6 mld snooping group-membership-timeout <interval> vlan <vlan-id>

The unit of Interval is milliseconds.

Configure the time to live for a query group

Switch#configure terminal

Switch(config)#ipv6 mld snooping query-membership-timeout <interval> vlan <vlan-id>

The unit of Interval is milliseconds.

19.2.4 Configure fast-leave

Start a VLAN fast-leave

Switch#configure terminal

Switch(config)#ipv6 mld snooping fast-leave vlan <vlan-id>

Close 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-leave wait time

Switch#configure terminal

Switch(config)#no ipv6 mld snooping fast-leave-timeout vlan <vlan-id>

19.2.5 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]

19.2.6 Display information

Display MLD SNOOPING configuration information

Switch#show ipv6 mld snooping

Display configuration information of a VLAN

Switch#show ipv6 mld snooping vlan <vlan-id>

Display REPORT multicast group aging information

Switch#show ipv6 mld snooping age-table group-membership

Display QUERY's aging information

Switch#show ipv6 mld snooping age-table query-membership

Display the forwarding information of the multicast group

Switch#show ipv6 mld snooping forwarding-table

Display MROUTER information

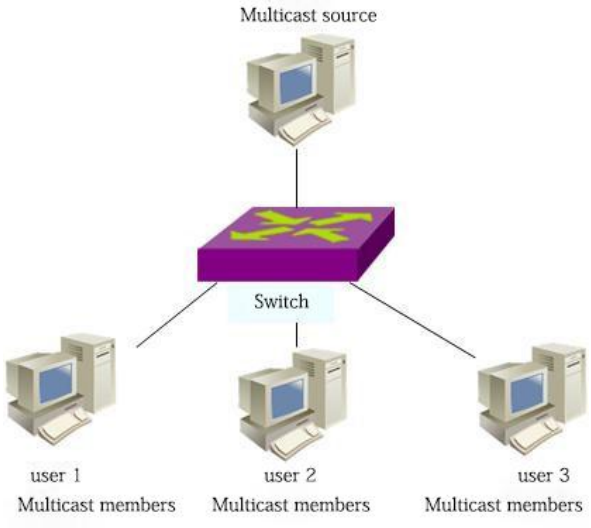
Switch#show ipv6 mld snooping mrouter

Display the current configuration of the system, including the configuration of MLD SNOOPING

Switch#show running-config

19.3 MLD SNOOPING configuration example

Enable MLD SNOOPING on the switch, user 1, user 2, user 3 can join 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 20 ACL configuration

In an actual network, network access security is an issue that administrators are very concerned about. The switch supports ACL filtering to provide network access security. By configuring ACL rules, the switch filters incoming data streams according to these rules to achieve network access security.

This chapter describes how to configure ACL, mainly including the following:

- Introduction of ACL resource library
- Introduction to ACL filtering
- ACL resource library configuration
- ACL based on time period
- ACL filtering configuration
- ACL configuration example

20.1 Introduction to ACL Resource Library

The ACL (Access list control) resource library is a collection of multiple sets of access rules. The ACL resource library does not have the function of controlling data forwarding, but is a set of rules with conflicting sorting. After the ACL resource library is referenced by applications, these applications control the forwarding of data according to the rules provided by the ACL resources. ACL can be applied to port access filtering, service access filtering and QoS, etc.

The ACL resource library has standard IP rule groups (group numbers 1 to 99, 1300 to 1999), extended IP rule groups (group numbers 100 to 199, 2000 to 2699), IP MAC groups <group numbers 700 to 799>, and ARP groups (Group number 1100~1199); each group of rules automatically prioritizes conflict rules. When the user configures an ACL rule, the system will insert the rule into the corresponding position according to the sorting rule.

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 appear to match at the same time, the first rule that matches exactly Effective; this matching rule determines whether the packet is forwarded or dropped. The so-called perfect match is that the value of the field in the rule is exactly equal to the value of the corresponding field in the data packet. Only if it matches a certain rule of ACL exactly, this rule will be used for corresponding deny or permit operation.

In the switch, the rules in the same group are automatically ordered. The automatic sorting of rules is relatively complicated. In the sorting process, the rules with a large range are ranked at the back, and the rules with a small range are ranked at the front. The size of the range is determined by the constraint conditions of the rule; the fewer the constraint conditions of the rule, the larger the range of the rule matching, and the more the constraint

conditions of the rule, the smaller the range of the rule matching. The constraints of the rule are mainly reflected in the wildcard of the address and the number of non-address fields. Wildcard is a bit string. The IP address is four bytes, and the MAC address is six bytes. When bits are '1', no matching is required, and bits are '0', which means matching. The non-address field refers to the protocol type, IP protocol type, and protocol port. These fields also hide a wildcard. Their length is the byte length of the corresponding field, so the length of the same field is uniform, and only the number of fields needs to be calculated. The more wildcard bits are '0', the more constraints.

The following uses port access filtering as an example to illustrate the necessity of rule sequencing and the advantages of automatic sequencing. If the user needs to reject the forwarding of the source address of the 192.168.0.0/16 network segment and allow the forwarding of the source address of the 192.168.1.0/24 network segment, the following two rules can be configured:

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

Hereinafter referred to as Rule 1 and Rule 2.

These two rules are in conflict; because the address of rule 1 is included in the address of rule 2, and one is deny and one is permit; according to the filtering principle of ACL, different orders have different results. If you want to achieve the above requirements, the order of the above two rules must be: Rule 1 is in the front, Rule 2 is in the back. The switch automatically implements the above sorting function. No matter what order the user configures the above rules, the last order is rule 1 in front of rule 2. When a packet with a source address of 192.168.1.1 is forwarded, the first rule is compared first, and then the second rule is compared. Both rules match, and the previous one takes effect (forwarding); if the source address is 192.168. At 0.1, only the first match, then discarded (not forwarded).

If there is no sorting, the user may configure rule 2 first, then configure rule 1; rule 1 is in the back, and rule 2 is in the front.

access-list 1 deny 192.168.0.0 0.0.255.255 - Rule 2

access-list 1 permit 192.168.1.0 0.0.0.255 - Rule 1

Because the previous rule 2 contains the following rule 1, it may lead to the situation that: a packet that completely matches rule 1 also completely matches rule 2, and rule 2 will take effect every time; it cannot meet the needs of the application.

In a switch, '0.0.255.255' is wildcard bits, bits '1' means no match is needed, and bits '0' means match. It can be seen that the wildcard bits of rule 2 is '0.0.255.255', which needs to match two bytes (16 bits); the wildcard bits in rule 1 is '0 0.0.255', which needs to match three bytes (24 bits); so the rule'range' of rule 2 is larger, so it comes in the back. In extended IP, sorting needs to consider more rule fields, such as IP protocol type, communication port, etc.

Their ordering rules are the same, that is, the more the configuration limit, the smaller the "range" of the rule, and conversely, the larger the "range". The ordering of rules is implemented in the background, and user commands can only be displayed in the order of user configuration.

The filter fields supported by ACL include source IP, destination IP, IP protocol type (such as TCP, UDP, OSPF), source port (such as 161), and destination port. Users can configure different rules for access control according to different needs.

In a switch, a set of rules can be applied by multiple applications; for example, a set of rules are referenced by port access filtering and service access filtering at the same time or by port access filtering of two ports at the same time.

20.2 Introduction to ACL filtering

ACL filtering is performed on the input port of the switch, and the data flow input to this port is matched by rules to realize port filtering. ACL filtering is handled at the line speed of the switch and does not affect the forwarding efficiency of the data flow.

When a port of the switch is not configured with ACL filtering, all data flows input through this port will not be matched by rules, and can be forwarded through this port. When ACL filtering is configured on a port of the switch, all input data flows passing through the port will be matched by rules. If the action of the matched rule is permit, the data flow is allowed to be forwarded. If it is deny, the data flow is not allowed to be forwarded. throw away.

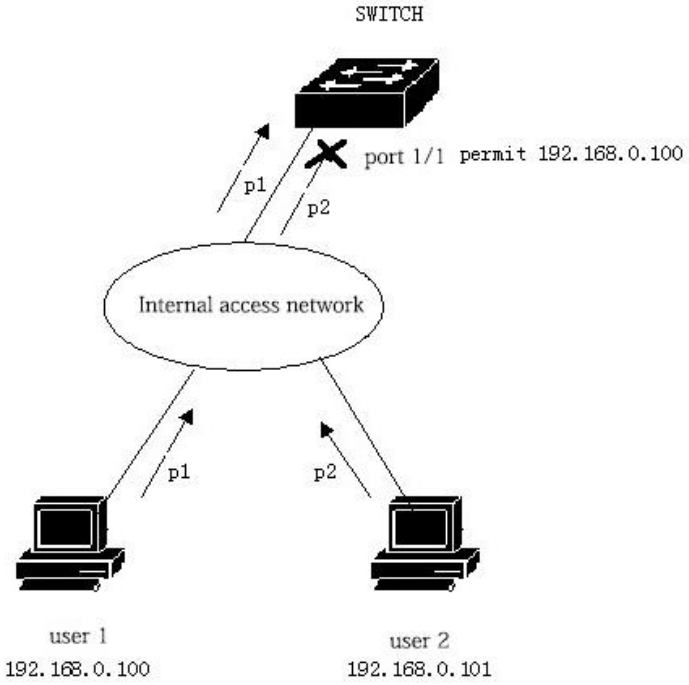
When configuring ACL filtering for a port, multiple ACL rule groups can be selected for a port. After the selection, the rules of the group are imported into the CFP of the port. If there are no rules that reject or allow all IP protocol packets in the group rules, the CFP is written Will add a rule that rejects all IP protocols. When the rules of the ACL resource library change, the rules written in the CFP will 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 rejects all IP protocol packets will be hidden. In fact, there will be two rules imported into the port's CFP. During data flow filtering, only data flows with source addresses from 192.168.1.0 to 192.168.1.255 can be forwarded through this port, and all other data flows are filtered out.

For example, there are two rules in a set of rules: access-list 1 deny 192.168.1.0 0.0.0.255 and access-list 1 permit any. At this time, there is a rule that allows all IP protocol packets. At this time, there is no hidden rule. In fact, there will be two rules imported into the CFP of the port. In data flow filtering, only data flows with source addresses from 192.168.1.0 to 192.168.1.255 are filtered out, and all other data flows can be forwarded.

The following figure is an example of ACL filtering. The port 1/1 of the switch selects an ACL rule group 1. 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 this 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 user 2 cannot access the network through port 1/1 of the switch. The data stream p1 from user 1 can be forwarded through the port 1/1 of the switch, while the data stream p2 from user 2 is discarded at port 1/1 of the switch.



When performing ACL filtering on multiple ports, you can select the same ACL rule group and use the same filtering rule.

Regardless of whether a set of rules or multiple sets of rules are referenced by a port, they will be sorted automatically, even if the sorting between the two sets of rules overlaps.

After a user references a set of rules, if the set of rules changes, the port that references the set of rules will automatically respond to the user's configuration; there is no need to reconfigure the port reference.

20.3 ACL resource library configuration

The switch has no rules by default.

The resource library in the switch supports four types of ACL rules: standard IP rules, extended IP rules, IP MAC groups, and ARP groups. The following are four types of rules to introduce ACL configuration.

Standard IP rules: Standard IP rules control the forwarding of data packets by source IP address.

Command form：access-list <groupId> {deny | permit} <source>

Parameter Description：

groupId：Access control list group number, standard IP ACL supports from 1 to 99 groups or 1300 to 1999.

deny/permit：If there is an exact match, the packet is rejected or allowed to be forwarded.

source：There are three input methods for source IP:

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

wildcard：Decide which bits need to match, '0' means need to match, '1' means don't need to match.

Extended IP rules: Extended IP rules are an extension of standard IP rules. You can control the forwarding of data packets by source IP, destination IP, IP protocol type, and service port.

Command form：access-list <groupId> {deny | permit} <protocol> <source> [eq <srcPort>] <destination> [destPort] <tcp-flag>

Parameter Description：

groupId：Access control list group number, extended IP ACL support from 100 to 199 groups or 2000 to 2699.

deny/permit：If there is an exact match, the packet is rejected or allowed to be forwarded.

protocol：The protocol types above the IP layer, such as: tcp, udp, etc., can also enter the corresponding number 6 (tcp). If you do not need to control these protocols, you can enter ip or 0.

source：There are three input methods for source IP:

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相当于A.B.C.D 0.0.0.0

srcPort: For the case where the protocol is tcp or udp, you can control the source port of the data packet. The input method can be some familiar port service names, such as www or numbers, such as 80.

destination：There are three input methods for the destination IP:

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 equivalent to A.B.C.D 0.0.0.0

destPort: For the case where the protocol is tcp or udp, the destination port of the data packet can be controlled, and the input method is the same as srcPort.

tcp-flag: When the protocol is tcp. You can control the tcp field matching of the data packet. The optional parameters are ack, fin, psh, rst, syn, and urg.

IP MAC rule: The IP MAC group can control the source and destination MAC addresses and source and destination IP addresses of IP packets.

Command form: access-list <groupid> {deny | permit} <src-mac> vid <vlan-id|any> ip <src-ip> <dst-ip>

Parameter Description:

groupId：Access control list group number, extended IP ACL support from 700 to 799 groups.

deny/permit：If there is an exact match, the packet is rejected or allowed to be forwarded.

src-mac：Source MAC address.

There are three ways to enter the MAC address:

1)HHHH.HHHH.HHHH wildcard can control the MAC address from a segment;

2)anyis equivalent to HHHH.HHHH.HHHH FFFF.FFFF.FFFF.

3)host A.B.C.D is equivalent to HHHH.HHHH.HHHH 0000.0000.0000

Vid：Outer vid, can be a vlan-id, or any vlan-id

src-ip：Source IP address.

dst-ip：Destination IP address.

There are three ways to enter the IP address:

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

ARP rules: ARP group can control the operation type of ARP packet, sender MAC and sender IP.

Command form：access-list <groupid> {deny | permit} arp <sender-mac> <sender-ip>

Parameter Description：

groupId：Access control list group number, extended IP ACL supports groups from 1100 to 1199.

deny/permit：If there is an exact match, the packet is rejected or allowed to be forwarded.

sender-mac：The MAC address of the sender of the ARP packet.

There are three ways to enter the MAC address:

1)HHHH.HHHH.HHHH wildcard Can control the MAC address from a segment;

2)any is 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 packet.

There are three ways to enter the IP address:

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

List of other commands:

show access-list [groupId]

Displays the list of rules configured in the current ACL. If groupId is entered, the rule list of the current group; otherwise, all rule lists are displayed.

no access-list <groupId>

Delete the specified rule list. all the rules of groupId group.

20.4 ACL based on time period

The time period is used to describe a special time range. Users may have such a requirement: some ACL rules need to take effect within a certain period or certain periods of time, and they are not used for packet filtering in other time periods, which is commonly referred to as filtering by time period. At this time, the user can first configure one or more time periods, and then refer to the time period by the time period name under the corresponding rule. This rule only takes effect within the specified time period, thereby realizing the ACL based on the time period filter.

If the time period referenced by the rule is not configured, the system gives a prompt message and allows such a rule to be created successfully, but the rule cannot take effect immediately until the user configures the referenced time period and the system time is within the specified time range ACL rule To take effect.

There are two situations for the configuration of the time period:

(1) Configure the relative time period: take the form of a certain time of a certain day to a certain time of a certain time;

(2)Configure an absolute time period: in the form of a certain year, a month, a day, a certain time, and a certain year, a month, a certain day, a certain time, and a minute.

Configure ACL based on time period：

command	description	CLI mode
time-range WORD cycle-time from <0-23> <0-59> to <0-23> <0-59>	Configure a relative time period for time period	Global configuration mode
time-range WORD cycle-time days from <0-6> to <0-6>	Configure a relative time period for the time period	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>	Configure a relative time period for the time period, including time and week	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>	Configure an absolute time period for the time period XX containing the year, month, day, and hour	Global configuration mode
no time-range WORD cycle-time	Delete all relative time periods in a certain time period	Global configuration mode
no time-range WORD utter-time	Delete all absolute time periods	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	Show all relative time periods of a certain time period	Privileged mode

show time-range WORD utter-time	Display all absolute time periods of a certain time period	Privileged mode
show time-range WORD	Display certain time period (including all absolute time periods and absolute time periods)	Privileged mode
show time-range	Show all time periods	Privileged mode
acl (<1-99>|<100-199>|<1300-1999>|<2000-2699>|<700-799>|<1100-1199>) time-range WORD	XX ACL rules are applied for XYZ periods, and are applied when ACL is applied to the interface	Global configuration mode
no acl (<1-99>|<100-199>|<1300-1999>|<2000-2699>|<700-799>|<1100-1199>) time-range (WORD|)	Cancel the application of a certain acl rule to a certain time period or all time periods	Global configuration mode
show acl (<1-99>|<100-199>|<1300-1999>|<2000-2699>|<700-799>|<1100-1199>) time-range	Show all time periods for which XX ACL rules are applied	Privileged mode
show all acl time-range	Display the time period during which all ACL rules are applied	Privileged mode

have to be aware of is:

(1) Configure multiple relative time periods for a certain time period, the relationship between the relative time periods is OR, the system time is in any relative time period, and the time period is in the activated state;

(2) Configure multiple absolute time periods for a certain time period, the relationship between the absolute time periods is OR, the system time is in any absolute time period, the time period is in the activated state;

(3) If a certain time period is configured with a relative time period and an absolute time period at the same time, the relative time period and the absolute time period are related, and the system time is only in the relative time period and the absolute time period at the same time. Is active;

(4) A maximum of 256 time periods can be defined; a time period can be configured with up to 256 relative time periods and absolute time periods; an acl rule can apply up to 256 time periods; when an acl rule associated with a time period is applied to an interface, The time period begins to work.

20.5 ACL filtering configuration

By default, all ports of the switch are not ACL filtered.

Command list:

access-group <groupId>

Mode: Layer 2 interface configuration mode

parameter:

groupId：ACL group number bound to the port

Function: Configure 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 the hardware resources are exhausted or occupied by other applications.

Display ACL port filtering configuration

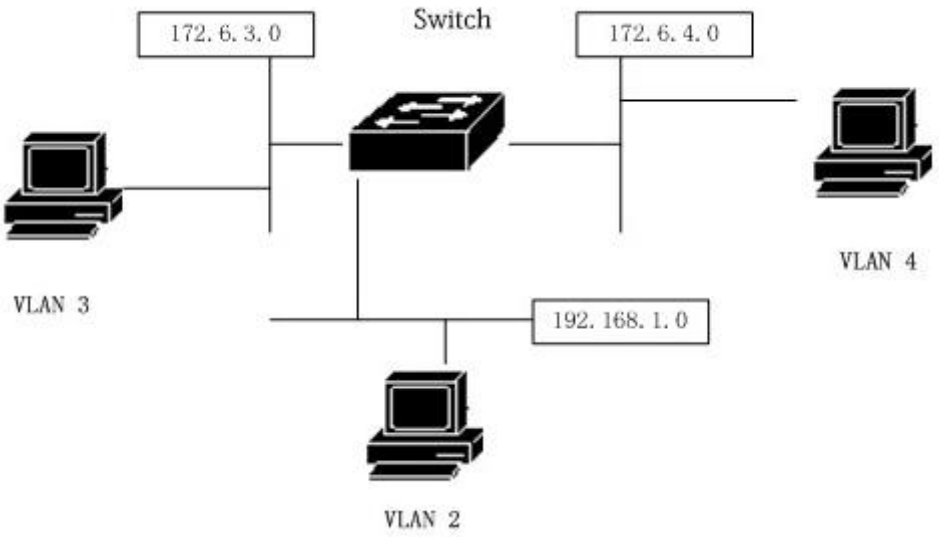
show acccess-group

Delete the configuration related to the current port and ACL port filtering

no acl- group <groupId>

20.6 ACL configuration example

A switch is connected to three subnets, an ACL is designed, and the blocking source address is the 192.168.1.0 network address. It allows traffic from other network addresses to pass through. 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 can be configured according to specific needs. The time period is associated with ACL rules. 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
```

20.7 ACL configuration troubleshooting

If ACL configuration fails, there may be the following reasons:

1. Before configuring the access control list, make sure that all IPs are connected, and then add the access control list. This access control list is blocking the IP data flow of the source address 192.168.1.0 through the switch. Pay attention to the writing of subnet reverse code. Use the show access-list command to list the access control list for viewing. It is important to note that the source and destination addresses are not reversed. Then check the access control list. And the default access control list has an implicit deny any statement at the end. If you want to let all others pass, you need to add a permit any statement, otherwise it will not pass.

2、The system is configured with static IP MAC binding.

3、The current interface is enabled with DHCP SNOOPING protocol.

4、The system CFP resources are exhausted.

For a Layer 2 switch with network management functions, it is necessary to provide basic network configuration for the TCP/IP protocol to achieve communication with other devices.

This chapter mainly includes the following:

- Configure VLAN interface
- Configure ARP
- Configure static routing
- IP routing configuration example

21.1 Configure VLAN Interface

In the switch, each layer 3 interface is attached to a certain VLAN, so the layer 3 interface is also called a VLAN interface. The creation and deletion of VLAN interfaces are done manually. Up to 4094 VLANs can be divided on the switch, but only up to 32 subnets can be established. The creation of the subnet interface can be created according to the needs of the user; the subnet interface can be manually deleted by the user, or can be deleted as the VLAN where the subnet is located is deleted.

Each VLAN interface has a name. The name of the VLAN interface is the string "vlan" followed by the VLAN ID number. For example, the name of the layer 3 interface of VLAN 1 is "vlan1", and the name of the layer 3 interface of VLAN 4094 is "vlan4094" ".

Like ports, VLAN interfaces also have management status and link status. At present, the switch does not provide the configuration of the management status of the VLAN interface. As long as the VLAN interface is created, the management status of the VLAN interface is always UP. The link status of the VLAN interface is related to the port included in the VLAN corresponding to the interface. As long as the link status of a port in the VLAN is RUNNING, the link status of the VLAN interface is RUNNING. If all the ports in the VLAN are If it is not RUNNING, the link status of the VLAN interface is not RUNNING.

You can configure an IP address on the VLAN interface and specify the network prefix of the network segment connected to this interface (which can be converted to a netmask). Currently, the switch only supports one IP address on one VLAN interface. Before configuring an IP address, users need to create a VLAN and add related ports to the VLAN. By default, the switch has a VLAN1 interface, and the IP address 192.168.0.1/24 is set on this interface. You can also modify the IP address of the VLAN1 interface. Interfaces of VLANs other than VLAN 1 have no IP address set by default.

The commands to configure the IP address of the VLAN interface are as follows:

command	description	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>	Set the IP address on the VLAN interface. The 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 first, and then set the specified IP address. The format of the parameter is A.B.C.D/M.	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 during setup, otherwise this command is invalid. The format of the parameter is A.B.C.D/M.	Interface configuration mode

The commands to view the VLAN interface are as follows:

command	description	CLI mode
show interface [if-name]	View the information of the VLAN interface, including the interface's IP address, MAC address, management status, link status, etc. The	Normal mode

	parameter is the interface name of the VLAN interface. If no parameter is specified, the information of all ports and VLAN interfaces is checked.	
show running-config	View the current configuration of the system, you can view the configuration of the VLAN interface.	Privileged mode

example:

Configure the subnet 193.1.1.0 on the VLAN3 interface, the subnet prefix is 24 (that is, the mask is 255.255.255.0), the IP address of the interface is 193.1.1.1, and view the information of the VLAN3 interface. The command 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

21.2 Configuring ARP

The ARP (Address Resolution Protocol) protocol is a protocol for mapping IP addresses to corresponding MAC addresses. When the source sends the Ethernet data frame to the destination in the same VLAN, the destination is determined based on the 48-bit Ethernet MAC address, and the destination determines whether it needs to receive this data based on the destination MAC address of the packet package.

Assume that hosts A and B on two adjacent network segments communicate through the switch. Before sending data to host B, host A first sends an ARP request packet to the interface of the switch directly connected to host A, and sends the data after receiving an ARP reply. Packet to this interface. After receiving the data packet, the switch first broadcasts an ARP request message to host B. After receiving the ARP response message from host B, it sends the data packet to host B.

There is an ARP cache on the switch, called the ARP table, which stores the mapping records of IP addresses to MAC addresses in directly connected networks. Each entry in the ARP table has a time to live. The default is 20 minutes. When the switch does not receive an ARP request or response packet for the IP address during the life time, the ARP entry

corresponding to the IP address will be deleted .

This section includes the following:

- Configure static ARP
- Configure ARP binding
- Configure ARP aging time
- View ARP information

21.2.1 Configuring Static ARP

There are two different ARP entries in the ARP table, one is static ARP and the other is dynamic ARP. Static ARP is an ARP entry configured by the user through commands. The system will not automatically refresh and delete it. You need to manually complete it. Dynamic ARP is the ARP that the system automatically learns based on the received ARP request or response packet. The system automatically creates and deletes, updates and maintains in real time, without user intervention, but users can manually delete dynamic ARP entries.

The switch is not configured with static ARP entries by default. It should be noted that when a VLAN interface is deleted or the IP of the subnet segment of the interface changes, the static and dynamic ARP entries in the original subnet segment are deleted.

The commands for configuring static ARP are as follows:

command	description	CLI mode
arp <ip-address> <mac-address> [if-name]	Configure static ARP entries. The first parameter is the IP address. The IP address must be within a subnet segment. The second parameter is the MAC address. The MAC address must be a unicast MAC address. The format of the MAC address is HHHH.HHHH.HHHH, such as 0010.5cb1.7825. The third parameter is the name of the Layer 2 interface, which is optional, indicating that the static arp entry is associated with a specific Layer 2 interface.	Global configuration mode

no arp {<ip-address> | <ip-prefix> | all | dynamic | static }	Delete ARP entries. Including deleting an ARP entry of an IP; deleting an ARP entry of a network segment; deleting all ARP entries; deleting all dynamic ARP entries; deleting all static ARP entries.	Global configuration mode
arp static {<ip-prefix> | all}	Modify all or all dynamic ARP entries in a network segment to static ARP entries.	Global configuration mode
arp aging <time>	Configure arp aging time, only effective for dynamic learning arp	Global configuration mode

21.2.2 View ARP information

The commands for viewing ARP information are as follows:

command	description	CLI mode
show arp [<ip-prefix> | dynamic | static]	View the ARP entry information in the ARP table, including all ARP entries, ARP entries of a certain network segment, dynamic ARP entries and static ARP entries.	Normal mode
show running-config	View the current configuration of the system, you can view the ARP configuration.	Privileged mode

21.3 Configuring Static Routes

A static route is a route defined by the user that allows a data packet to pass from a source address to a destination address through a specified path. You can configure a static route as the default route to send data packets that cannot be routed to the default gateway.

The static route is manually configured by the administrator. It is suitable for networks with relatively simple networking structure. The administrator only needs to configure static routes to make the switch work normally. Static routes will not consume valuable network bandwidth because there will be no route updates.

The default route is also a static route. Simply put, the default route is the route that is used only when no matching route 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 (with a mask of 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 the source indicating 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. Using the default route 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 simultaneously.

The switch can be configured with multiple static routes to the same destination, but only one of the routes is activated for actual data forwarding. The switch is not configured with static routes by default.

The commands for configuring static routes are as follows:

command	description	CLI mode
ip route <ip-prefix> <nexthop-address>	Set up 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.	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 IP address of the next hop.	Global configuration mode

no ip route <ip-prefix> [nexthop-address]	Delete the 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 matching the specified network segment will be deleted. If there is a second parameter, delete the route that matches both the specified network segment and the next hop.	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 IP address of the next hop. If there is no third parameter, all routes matching the specified network segment will be deleted. If there is a third parameter, delete the route that matches both the specified network segment and the next hop.	Global configuration mode

The commands for viewing routes are as follows:

command	description	CLI mode
show ip route [<ip-address> | <ip-prefix>	View the information of the activated route, you can choose to view all routes, a route, a route of a network segment, and a static route.	Normal mode
show ip route database	View all routing information (including activated and inactive routes), you can	Normal mode

	choose to view all routes.	
show running-config	View the current configuration of the system, you can view the configuration of the 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 the static route whose destination IP address is 200.1.1.0, subnet mask is 255.255.255.0, and next hop is 10.1.1.2. The configuration commands are:

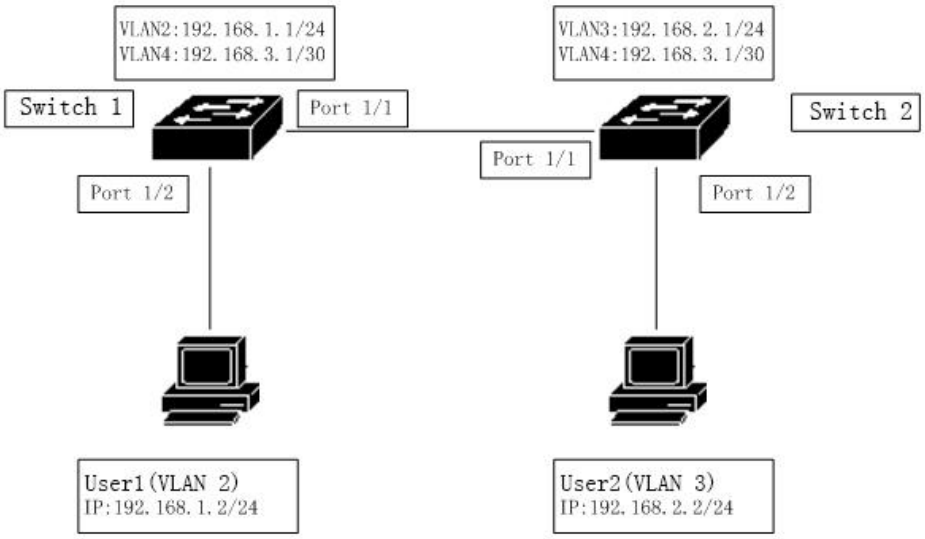
Switch(config)#no ip route 200.1.1.0/24

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

21.4 TCP/IP basic configuration example



In the figure, switch 1 is a layer 2 switch, and switch 2 is a layer 3 switch.

21.4.1 Layer 3 interface

Configure the Layer 3 interface corresponding to VLAN 2 on Switch 1, and assign an IP address of 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

Verification: User 1 can ping the IP address of the Layer 3 interface corresponding to VLAN 2 of switch 1.

21.4.2 Static Routing

To access switch 1, user 2 must access switch 1 through the routing function of switch 2.

The configuration on Switch 1 is as follows:

Switch#config t

Switch(config)#ip route 192.168.2.0 255.255.255.0 192.168.3.2

The configuration on Switch 2 is as follows:

Switch#config t

Switch(config)#ip route 192.168.1.0/24 192.168.3.1

Verification: User 2 can ping General Switch 1.

21.4.3 ARP

Configure static ARP for user 1 to allow only user 1 to access from VLAN 2. Assume that the MAC address of user 1 is

00:00:00:00:00:01。

Switch 1 is configured as follows:

Switch#config t

Switch(config)#arp 192.168.1.2 0000.0000.0001

Verification: User 1 can ping the IP address of the Layer 3 interface corresponding to VLAN 2 of switch 1.

Chapter 22 SNMP Configuration

The switch provides SNMP for remote management of the switch. This chapter describes how to configure SNMP, mainly including the following:

This chapter mainly includes the following:

- Introduction to SNMP
- SNMP configuration
- SNMP configuration example

22.1 Introduction to SNMP

SNMP is a simple network management protocol. It is currently the most widely used network management protocol. It has five major functions: fault management, billing management, configuration management, performance management, and security management. It provides information format for communication between network management application software and network management agent (agent).

There are four major elements of the SNMP network management protocol: management workstation, management agent, management information base, and network management protocol. The management agent is on the switch, which is the server end of the management station to access the switch. The information of the management station to access the network management agent is organized in the form of MIB to form a management information database.

There are three major operations in SNMP: 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 objects in the agent. The TRAP operation enables the agent to notify the management station of events.

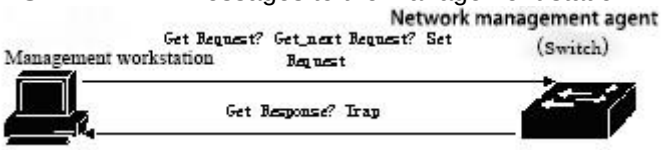
TRAP messages are actively sent to the management workstation when an event occurs on the switch. These messages include cold start, hot start, port link up and link down, common body name authentication failure, and STP state switching.

At present, there are three versions of SNMP: SNMPV1, SNMPV2, and SNMPV3. The later version is an upgraded version of the previous one, with enhanced functions and improved security. The switch supports all three SNMP versions and can parse the three versions of SNMP protocol packets. When sending TRAP messages, you can use any of SNMPV1, SNMPV2 and SNMPV3 to send.

The switch supports RFC, BRIDGE and private MIB objects, and the switch can be completely managed through SNMP. Listed below are some 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,

Common MIBs such as RFC 2674.

The figure is an example of the SNMP protocol interaction between the management station and the management agent. The management station can access the switch management agent by sending SNMP messages of Get Request, GetNext Request, GetBulk Request, and Set Request to obtain or set the value of the MIB object of the switch. The switch management agent returns the SNMP message of Get Response to the management station. When some events occur on the switch, the management agent of the switch actively sends SNMP TRAP messages to the management station.



SNMP protocol interaction between management station and management agent

22.2 SNMP configuration

The SNMP configuration includes the community configuration of the switch, the TRAP workstation, the configuration of the snmp system information and the configuration of the engine id, user and group of the snmpV3. The switch has a read-only community by default, the community name is public, and the switch can be configured with up to 8 communities. The switch does not configure TRAP workstations by default. The switch has a local engine id by default, and the switch can modify the local engine id. The switch has a user name: initialnone by default, which is a non-authentication and non-encrypted user name. The switch can be configured with multiple user names of different levels. The switch defaults to a group name: initial, and the switch can configure different group names according to different user names.

The SNMP commands are as follows:

command	description	CLI mode
snmp community <community-name> {ro | rw}	Configure the community name to access the NMS. This is an interactive command. During configuration, the user can enter the name of the created community and read/write permissions according to the prompt.	Global configuration mode
no snmp community <community-name>	Delete the specified SNMP community name.	Global configuration mode
snmp trap <notify-name>	Add or modify the sending	Global

host <ipaddress> version {1 | 2c | 3}	destination of snmp trap. This is an interactive command. The notify name is unique. 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 by snmpV1, snmpV2c or snmpV3. This command configures the target port as 162 by default.	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. Configurable system information includes: 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-digit hexadecimal number; and if the input is less than 24 digits, it will be automatically filled with 0.	Global configuration mode
snmp user <user-name> <group-name> v3 [auth {md5 | sha} <auth-key>]	The snmp user command is to set a username corresponding to 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	Global configuration mode

	protocol (md5 or sha) and the corresponding authentication password.	
no snmp user <user-name> <group-name> v3	Delete a username corresponding to the local engine ID of 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 to set a group name, the security level is (auth or noauth), the notification, writable or readable view specified by the security model (v3).	Global configuration mode
no snmp group <group-name> v3 {auth | noauth}	Delete a group name, the security level is (auth or noauth), the view specified by the security model (v3).	Global configuration mode
show snmp community	Display all current public body names and corresponding read and write permission information.	Normal mode/privileged mode
show snmp trap	Display all current trap names and the target IP address and version information sent by the corresponding trap.	Normal mode/privileged mode
show snmp system information	Displays the system information set by SNMP.	Normal mode/privileged mode
show snmp engine-id	Displays the local engine-id of SNMPV3.	Normal mode/privileged mode
show snmp user [specify name of user]	Display a username information corresponding to the local engine ID of snmpv3. Including the group name corresponding to the	Normal mode/privileged mode

	user name and the authentication and encryption information supported by the user name.	
show snmp group	Display all group names, security levels (auth or noauth), notifications, writable or readable view information specified by the security model (v3).	Normal mode/privileged mode

22.3 SNMP configuration example

Configure a community name named "private" to operate with read and write permissions.

Configure an SNMP trap named test and send the destination IP as 192.168.0.10; the SNMP version used is 1.

The specific content of the contact to configure the system is: E-mail:networks@abc.com.

The specific content of the location of the configuration system is: Shenzhen, China.

The specific content of the configuration system name is: abcSwitch.

Set a user name initialmd5 that supports md5 authentication, the group name is intia, and the authentication password is abcdefg.

Set the group name to initial, the security level is (auth), and the notification specified by the security model (v3). The view names that can be written or read are internet, internet, and internet.

The configuration of the switch is 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 auth read internet write internet notify internet

Chapter 23 RMON Configuration

This chapter mainly includes the following:

- RMON Introduction
- RMON configuration
- RMON configuration example

23.1 Introduction to RMON

RMON (Remote Monitoring, remote network monitoring) is a standard monitoring specification, mainly used to monitor the data traffic in a network segment or even the entire network, and is one of the widely used network management standards. The RMON specification is extended from the SNMP MIB, so it is also a MIB and is the most important enhancement to the MIB II standard. RMON makes SNMP more effective and proactive in monitoring remote devices.

The RMON monitoring system consists of two parts: a detector (agent or monitor) and a management station. RMON agents store network information in RMON MIB, and they are directly implanted into network devices (such as routers, switches, etc.). The management station uses SNMP to obtain RMON data information.

This device supports the 4 most commonly used groups in RMON:

(1) Statistics: provides statistics for each interface. Most of the objects are counters, which record the information collected by the monitor from the interface.

(2) History: save the data sampled on the specified interface at fixed time intervals.

(3) Alarm group: the specified data of all interfaces are sampled at fixed time intervals, and compared with the set threshold, and the corresponding event is triggered when the conditions are met.

(4) Event group: set an event, you can choose to record a log or send a trap.

23.2 RMON configuration

The RMON command includes 4 groups of configuration, view configuration and view data:

command	description	CLI mode
rmon statistics <1-100> (owner WORD|)	This port is an interactive command to enable the configuration of the statistical group with the specified serial number for	Port configuration mode

	this port. The configuration is that the user can input the serial number and owner according to the prompt, and the owner is optional (the same below). The serial number is the number configured by the statistics group, and the value ranges from 1 to 100.	
no rmon statistics <1-100>	Cancel the configuration of the statistical group with the specified serial number.	Port configuration mode
rmon history <1-100> buckets <1-100> interval <1-3600> (owner WORD|)	It is an interactive command to configure the history group parameter of specified serial number for this port. Configure users to enter the serial number, number of buckets requested, time interval, and owner as prompted. The serial number is the configuration number of the historical group, and 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 interval is in seconds, and the value range is 1 to 3600.	Port configuration mode
no rmon history <1-100>	Cancel the configuration of the historical group with the specified serial number.	Port configuration mode
rmon alarm <1-60> WORD <1-3600> (absolute|delta) rising-threshold <1-2147483647> <1-60> falling-threshold <1-2147483647> <1-60> (owner WORD|)	Configure the alarm group parameters of the specified serial number. This is an interactive command. The configuration user can enter the serial number, monitoring object, time interval, comparison method, upper limit	Global configuration mode

	threshold, upper limit event serial number, lower limit threshold, lower limit time serial number and owner according to the prompt. The serial number is the number of the alarm group configuration, the value range is 1 to 60; the monitoring object is the OID of a MIB node, the sampling interval is in seconds, and the value range is 1 to 3600; the comparison mode can be selected absolute or delta, respectively Represents the absolute value (the value of each sample) and the relative value (the increment of each sample relative to the previous sample); the upper and lower threshold values range from 1 to 2147483647; the event must be configured in advance, and the number value range is 1 to 60.	
no rmon alarm <1-60>	Cancel the configuration of the alarm group with the specified serial number.	Global configuration mode
rmon event <1-60> (log|log-trap WORD|none|trap WORD) (description WORD|) (owner WORD|)	It is an interactive command to configure the event group parameters of the specified serial number. The configuration user can input the serial number, event type, community name, description and owner according to the prompt. The sequence number is the number of the event group configuration, and the value range is 1 to 60; the event type can be selected from log (record log), log-trap (record log and send Trap), none (no action) and trap (issue Trap), When selecting log-trap or trap, you must also	Global configuration mode

	specify the community name (the community name configuration is ignored in this device).	
no rmon event <1-60>	Cancel the configuration of the event group with the specified serial number.	Global configuration mode
show rmon (statistics|history-control|alarm|event) config	View RMON configuration information, this is an interactive command. The configuration user can input the viewing object according to the prompt.	Global configuration mode
show rmon statistics-data interface IFNAME|	To view the RMON statistics group data, the configuration user must enter the interface name.	Global configuration mode
show rmon history-data interface IFNAME|	To view the RMON historical group data, the configuration user must enter the interface name.	Global configuration mode

23.3 RMON configuration example

Enable statistics group configuration on port ge1/1, the serial number is 10, and the owner is tereco.

Enable the historical group data collection on port ge1/8, the serial number is 2, save up to 80 data, the sampling interval is 1 minute, there is no owner.

Configure the event with sequence number 1 to record logs without owner.

Configure the event with sequence number 3, send Trap, the community name is public, and there is no owner.

Enable the alarm group with sequence number 5 to monitor the number of bytes received on each port. When the number of bytes per half minute is greater than 1000, a Trap alarm is issued, and when it is less than 10, a log is recorded. There is no owner.

The switch configuration is 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

The switch provides a cluster management function, which can realize a group of network devices managed by a single device. This chapter describes how to configure cluster management, mainly including the following:

- Introduction to cluster management
- Configuration management equipment
- Configure member devices
- Cluster management display and maintenance
- Typical configuration examples of cluster management

24.1 Introduction to Cluster Management

24.1.1 Cluster definition

A cluster is a collection of network devices that can be managed as a single device.

The purpose of cluster management: to solve the centralized management of a large number of scattered network devices.

Cluster advantages: save public network IP addresses; simplify configuration management tasks. The network administrator 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 management functions is the command switch, and the other managed switches are member switches. The command switch and the member switches form a "cluster".

The cluster configures and manages switches within the cluster through the following three protocols.

- NDP（Neighbor Discovery Protocol）
- NTDP（Neighbor Topology Discovery Protocol）
- Cluster （Cluster Management Protocol）

The working process of the cluster includes 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 before the cluster is established. The working principle is as follows:

- All devices obtain information about neighboring devices through NDP, including information such as the software version, host name, MAC address, and port name of

neighboring devices.

- The management device uses NTDP to collect device information within the user-specified hop range and connection information for each device, and determines cluster candidate devices from the collected topology information.
- The management device completes the operations 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 packets of the cluster are all Layer 2 Ethernet packets. For the specific format and interaction process, see the national standard "YDT 1692-2007 Ethernet Switch Cluster Management Technical Requirements."

24.1.2 Cluster role

According to the different positions and functions of each device in the cluster, different roles are formed. Users can specify roles through configuration. All roles are as follows:

1）Command switch:

In a cluster, the only switch that can configure and manage the entire cluster is also the only switch in the cluster that has a public IP address.

- Command the switch to create a cluster;
- Command switch through the collection NDP（Neighbor Discovery Protocol）和 NTDP（Neighbor Topology Discovery Protocol）Information to discover and determine candidate switches;
- Command switches to control the maintenance of the cluster, you can add candidate switches to the cluster or delete member switches from the cluster;

2）After the cluster is established, the command switch provides a management channel for the cluster.

3） Member switch

Managed switches in the cluster.

Member switches are candidate switches before joining the cluster.

The member switch does not have a public IP;

The management of member switches is done through the command switch agent.

4） Candidate switch

The switch has the ability to join the cluster, but has not joined any cluster.

The switch must be a candidate switch before it can become a member switch.

5）Independent switch

Switches that do not have cluster functions.

Various roles can be converted according to certain rules:

While creating a cluster on the candidate device, the user designates the current candidate device as the cluster management device. Each cluster must specify one (and only one) management device. After the management device is designated, the management device discovers and determines candidate devices by collecting relevant information. Users can add candidate devices to the cluster through corresponding configuration.

After the candidate device joins the cluster, it becomes a member device.

- After the member devices in the cluster are deleted, they will be restored as candidate devices.
- The management device can only be restored as a candidate device when the cluster is deleted.

24.1.3 Introduction to NDP

NDP is used to obtain information about directly connected neighboring devices, including connection port, device name, software version, etc. The working principle is as follows:

- A device running NDP periodically sends NDP messages to neighbors. The NDP message contains NDP information (including the device name, software version, and connection port of the current device) and the aging time of the NDP information on the receiving device. It also receives but does not forward NDP messages sent by neighboring devices.
- A device running NDP periodically sends NDP messages to neighbors. The NDP message contains NDP information (including the device name, software version, and connection port of the current device) and the aging time of the NDP information on the receiving device. It also receives but does not forward NDP messages sent by neighboring devices.

24.1.4 NTDP Introduction

NTDP is used to collect information about each device and connection information between devices within a certain network. NTDP provides device information that can join the cluster for the management device and collects topology information of devices within the specified hop count.

NDP provides adjacency table information for NTDP. NTDP sends and forwards the NTDP topology collection request based on the adjacency information to collect NDP information of each device within a certain network range and its connection information with

all neighbors. After collecting this information, the management device or network management can use this information as needed to complete the required functions. When the NDP on the member device discovers that the neighbor has changed, it informs the management device of the neighbor change through a handshake message. The management device can start NTDP to collect the specified topology, so that NTDP can reflect the network topology change in time.

The management device can periodically perform topology collection in the network, and the user can also initiate a topology collection through manual configuration commands. The process for the management device to collect topology information is as follows:

- The management device periodically sends NTDP topology collection request packets from the NTDP-enabled port.
- The device that receives the request message immediately sends a topology response message to the management device, and copies the request message on the NTDP-enabled port and sends it to the neighboring device; the topology response message contains the basic information of the device and all NDP information of adjacent devices.
- The neighboring device will perform the same operation after receiving the request message, until the topology collection request message spreads to all devices within the specified hop range.

When topology collection request packets are diffused in the network, a large number of network devices simultaneously receive topology collection requests and simultaneously send topology response packets. In order to avoid network congestion and busy management device tasks, the following measures can be taken to control the topology collection request packet proliferation speed:

- After receiving the topology collection request, the device does not immediately forward the topology collection request message, but waits for a certain period of time before it starts to forward the topology collection request message on the NTDP-enabled port.
- On the same device, except for the first port, each NTDP-enabled port sends a topology collection request packet after the previous port delays a certain amount of time before forwarding the topology collection request packet.

24.1.5 Cluster management and maintenance

1) Candidate device joins the cluster

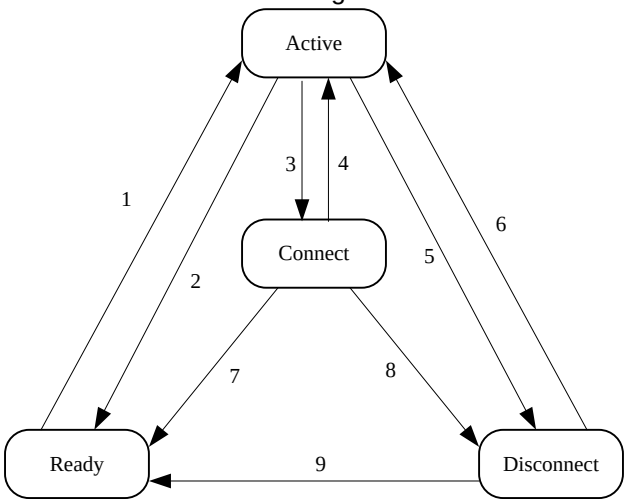
The user should first specify the management device before establishing the cluster. The management device discovers and determines candidate devices through the NDP and NTDP protocols, automatically adds the candidate devices to the cluster, or can manually add the candidate devices to the cluster.

After the candidate device successfully joins the cluster, it will obtain the cluster member serial number and cluster management assigned to it by the management device

Private IP address used, etc.

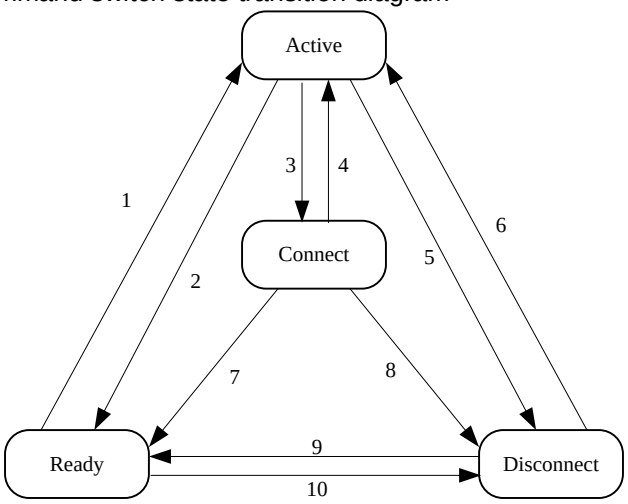
2) Communication within the cluster

Within the cluster, management devices and member devices communicate in real time through handshake messages to maintain
Connection status, the connection status of the management device and member devices is shown in the figure below.



1 ,Member join
2 ,Member deletion
3, Can't receive handshake signal for three consecutive times
4, Receive handshake signal
5,Recover request received
6, Interrupt recovery, re-register through
7 ,Member deletion
8,The state remains longer than the specified time
9, Member deletion

Command switch state transition diagram



1 ,Join the cluster
2, Exit the cluster
3, Can't receive handshake signal for three consecutive times
4, Receive handshake signal
5, Received join request
6, Interrupt recovery, re-register through
7, Exit the cluster
8, The state stays longer than the specified time or receives the join request message
9, Exit the cluster
10 ,Configuration recovery

Member switch state transition diagram

The command switch collects the basic information of the device, identifies a device as a candidate switch, and is initially in the Ready state.

In any state, the operation of deleting a member will move the state of the member switch back to the Ready state and identify it as a candidate switch.

- The cluster is established successfully. After the candidate device joins the cluster and becomes a member device, the management device saves the status information of the member device locally, and marks the member status as Active. The member device also saves its own status information locally and saves its own status The logo is Active.
- The management device and member devices send handshake messages to each other at regular intervals. After receiving the handshake message from the member device, the management device does not respond and keeps the member device in the Active state; the member device also does not reply and keeps its state as Active.
- If the management device does not receive the handshake message sent by the member device within the triple handshake message sending interval after sending the handshake message to the member device, the state of the member device saved locally will be migrated from Active to Connect; the same If the member device does not receive the handshake message sent by the management device within three times of the handshake message transmission interval after sending the handshake message to the management device, its own state will also transition from Active to Connect.
- If the management device receives the handshake message or management message sent by the member device in the Connect state within the effective retention time, it will migrate the state of the member device back to Active, otherwise it will be migrated to Disconnect, and the management device will think The member is disconnected; if the member device in the Connect state receives the handshake message or management message sent by the management device within the effective retention time, it will migrate its state to Active, otherwise it will migrate to Disconnect.
- When the interrupted communication between the management device and the member device is restored, the member device in the Disconnect state will rejoin the cluster. After joining successfully, the member device will return to Active on 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 a handshake message.

24.1.6 Management VLAN

The management VLAN limits the scope of cluster management. By configuring the management VLAN, the following functions can be achieved:

- The management messages of the cluster (including NDP, NTDP messages, and handshake messages) are restricted to the management VLAN, and are isolated from other messages, increasing security.
- The management device and member devices implement internal communication through the management VLAN.
- Cluster management requires the ports connecting the management device and the member/candidate device, including the cascade port (when the candidate device is connected to the management device through another candidate device, the ports connected between the candidate devices are called cascade ports) To allow the management VLAN to pass, therefore:
- If the port does not allow the management VLAN to pass, the device connected to the port cannot join the cluster. Therefore, before the cluster, make sure that the port connected to the candidate device and the management device includes the cascade port to allow the management VLAN to pass.
- Only when the default VLAN ID of the port connecting the management device to the member/candidate device and the cascade port is the management VLAN, the packets of the management VLAN are allowed to pass without a label, otherwise the packets of the management VLAN must be Pass with label.

For the related knowledge of VLAN, please refer to "Chapter 6 Configuring VLAN".

24.2 Introduction to cluster configuration

Before configuring a cluster, users need to clarify the roles and functions of each device in the cluster, and also configure related functions to plan communication with devices in the cluster.

Configuration tasks		Detailed configuration
Configuration management equipment	Enable the NDP function of the system and port	15.3.1
	Configure NDP parameters	15.3.2
	Enable the NTDP function of the system and port	15.3.3
	Configure NTDP parameters	15.3.4
	Configure to manually collect NTDP information	15.3.5
	Enable the cluster function	15.3.6
	Establish a cluster	15.3.7

	Configure member interaction within the cluster	15.3.8
	Configure cluster member management	15.3.9
Configure member devices	Enable the NDP function of the system and port	15.4.1
	Enable the NTDP function of the system and port	15.4.2
	Configure to manually collect NTDP information	15.4.3
	Enable the 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 disabled on the management device and member devices, the cluster will not be disbanded, but it will affect the normal operation of the established cluster.

24.3 Configuration Management Equipment

24.3.1 Enabling the NDP function of the system and port

command	description	CLI mode
ndp global enable	Enable the global NDP function. By default, it is turned off globally.	Configuration mode
ndp enable	Enable the NDP function of the port. NDP is disabled by default on all ports	Interface configuration mode

note:

- *The NDP function of the global and port must be enabled at the same time for NDP to operate normally.*
- *The NDP function does not support aggregated ports.*
- *In order to prevent the management device from collecting topology information of devices that do not need to join the cluster during topology collection and adding it to the cluster, it is recommended to turn off the NDP function on the ports connected to devices that do not need to join the cluster.*

24.3.2 Configuring NDP parameters

command	description	CLI mode
ndp aging-timer <aging-time>	Configure the aging time of NDP packets sent by this device on the receiving device. The default is 180 seconds.	Configuration mode
ndp hello-timer <hello-time>	Configure the interval for sending NDP packets. The default is 60 seconds.	Configuration mode

note

The aging time of NDP packets on the receiving device cannot be less than the NDP sending interval. Otherwise, the NDP port neighbor information table will become unstable.

24.3.3 Enable the NTDP function of the system and interface

command	description	CLI mode
ntdp global enable	Enable the global NTDP function. By default, it is turned off globally.	Configuration mode
ntdp enable	Enable the NTDP function of the port. NDP is disabled by default on all ports	Interface configuration mode

note :

- *Both the global and port NTDP functions must be enabled at the same time for NTDP to function properly.*
- *The NTDP function does not support aggregated ports.*
- *In order to prevent the management device from collecting topology information of devices that do not need to join the cluster during topology collection and add it to the cluster, it is recommended to disable the NTDP function on the ports connected to devices that do not need to join the cluster.*

24.3.4 Configure NTDP parameters

command	description	CLI mode
ntdp hop <hop-value>	Configure the scope of topology collection. By default, in the collected topology, the farthest device is 3 hops away from the topology collection device.	Configuration mode

ntdp timer <interval-time>	Configure the interval for collecting topology information periodically. The default is 1 minute.	Configuration mode
ntdp timer hop-delay <time>	Configure the time that the collected device waits before forwarding the topology collection request packet on the first port. The default is 200 milliseconds.	Configuration mode
ntdp timer port-delay <time>	Configure the port delay time for the current device to forward the topology collection request. The default is 20 milliseconds.	Configuration mode

24.3.5 Configure Manually Collect NTDP Information

After the cluster is established, the management device will periodically collect topology information. In addition, users can manually collect NTDP information through configuration (regardless of whether the cluster is established) or not, and initiate a NTDP information collection process, so as to more effectively manage and monitor the device in real time.

command	description	CLI mode
ntdp explore	Collect topology information manually.	Normal mode, privileged mode

24.3.6 Enabling the cluster function

command	description	CLI mode
cluster enable	Enable the cluster function. The default cluster function is turned off.	Configuration mode

24.3.7 Establish a cluster

The management VLAN limits the scope of cluster management. By configuring the management VLAN, the following functions can be achieved:

- The management messages of the cluster (including NDP, NTDP messages, and handshake messages) are restricted to the management VLAN, and are isolated from other messages, increasing security.

The management device and member devices implement internal communication through the management VLAN.

command	description	CLI mode
cluster management-vlan <vlan-id>	Specify the management VLAN. The default management VLAN is VLAN1.	Configuration mode

note:
If the current device is in a cluster, management VLAN modification is not allowed.
When not in the cluster:

1）Check if the vlan exists, if there is no direct failure, if there is, continue to the next step

2） Check all the interfaces again. If the vlan where the interface is located and the management VLAN are not the same vlan, turn on the global switches of ndp and ntdp and close and clear them accordingly, and then reopen them

3）Find the Layer 3 interface to be configured with VLAN. If not found, create a Layer 3 interface corresponding to VLAN. If the creation fails, the management VLAN configuration is successful. You can use ndp and ntdp, but you cannot join the cluster.

4）Set the mac of the current Layer 3 interface to dev_id. If the VLAN setting is successful and the creation of the Layer 3 interface fails, use the mac of vlan1 as the dev_id

If the management VLAN has been configured, but the user deletes the vlan directly in the vlan database, the management VLAN is automatically set to vlan1, and the opened ndp, ntdp, and global switches of the cluster are all turned off and the corresponding closing and clearing operations are performed.

Before establishing a cluster, the user must first set the private IP address range used by the member devices in the cluster. When a candidate device is added, the management device dynamically allocates a private IP address that can be used within the cluster range and issues it to the candidate device. It is used for communication within the cluster to realize the management and maintenance of member devices by the management device.

command	description	CLI mode
cluster ip-pool <IP/MASK>	Configure the private IP address range used by the member devices in the cluster on the device to be set as the management device.	Configuration mode

note:

- *The IP addresses of the VLAN interfaces of the management device and member devices and the cluster address pool cannot be configured on the same network segment, otherwise the cluster will not work properly.*

- *It can be configured only when the device is not in the cluster.*
- *Use the management VLAN to find whether there is a corresponding layer 3 port. If there is no layer 3 port, directly return failure. (This device cannot be a cluster command switch) If there is a Layer 3 interface, configure the base address of IP-POOL to the Layer 3 port. If the configuration fails, IP-POOL also fails to configure.*

By default, the device is not a management device, and the cluster is established:

command	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>	Automatically establish a cluster. The automatic cluster function 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 cluster configuration, stop automatically joining member switches. This operation can only stop joining new devices. Devices that have already joined the cluster will remain in the cluster.	Configuration mode

note :

- *Users can only specify the management VLAN before establishing the cluster. After the device has joined the cluster, 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 finally re-establish the cluster.*
- *For security reasons, it is recommended not to configure the management VLAN as the default VLAN ID of the port connecting the management device to the member device and the cascade port.*
- *Only when the ports connecting the management device and member devices and the*

default VLAN IDs of all cascade ports are management VLANs, can the packets of the management VLAN be allowed to pass through without tags, otherwise the management device and the member devices must be configured Ports and all cascade ports allow tags of management VLANs to pass through. For details, see "VLAN".

- *The private IP address range of member devices in the cluster can only be configured when the cluster has not been established, and can only be configured on the management device. If the cluster has been established, the system does not allow modification of the IP address range.*

24.3.8 Configuring the interaction of members within the cluster

Within the cluster, the management device and the member devices communicate in real time through handshake messages to maintain the connection status between them. You can configure the time interval for sending handshake messages and the effective retention time of the device on the management device. All member devices in the cluster take effect simultaneously.

command	description	CLI mode
cluster timer <interval-time>	Configure the interval at which handshake packets are sent. The default is 10 seconds.	Configuration mode
cluster holdtime <hold-time>	Configure the effective retention time of the device. 60 seconds by default	Configuration mode

24.3.9 Configure Cluster Member Management

The user can manually specify the candidate devices to join the cluster on the management device, or manually delete the cluster

The specified member device. The joining/deleting operation of cluster members must be performed on the management device, otherwise an error message will be returned.

command	description	CLI mode
cluster add member mac-address <mac-address>	Add candidate devices to the cluster.	Configuration mode
cluster delete member mac-address <mac-address>	Remove member devices from the cluster.	Configuration mode

24.4 Configuring Member Devices

24.4.1 Enabling the NDP function of the system and port

See 21.3.1 Enabling the NDP function of the system and port

24.4.2 Enabling the NTDP function of the system and port

See 21.3.3 Enabling the NTDP function of the system and port

24.4.3 Configuring Manually Collecting NTDP Information

See 21.3.5 Configure Manually Collect NTDP Information

24.4.4 Enable the cluster function

See 21.3.6 Enabling the cluster function

24.5 Configure access to cluster members

After the NDP, NTDP, and cluster functions are correctly configured, the member devices in the cluster can be configured, managed, and monitored through the management device. You can switch to the specified member device operation interface on the management device to configure and manage the member device.

command	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 :

Telnet connection is used for the mutual switching between the cluster management device and the member devices. Note the following when switching:

- *Before performing the switch, the peer 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, if the member number n does not exist, an error message will be displayed*

If the Telnet user of the device requested to log in is full, the switch will fail.

24.6 Cluster management display and maintenance

command	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>	Display detailed NTDP information of the specified device	Normal mode, privileged mode
show cluster	Display the status and statistics of the cluster to which the device belongs	Normal mode, privileged mode
show cluster topology	Display cluster topology information	Normal mode, privileged mode
show cluster candidates [mac-address <mac-address>]	Display candidate device information	Normal mode, privileged mode
show cluster members [<member-number>]	Display cluster member information.	Normal mode, privileged mode

24.7 Typical Configuration Examples of Cluster Management

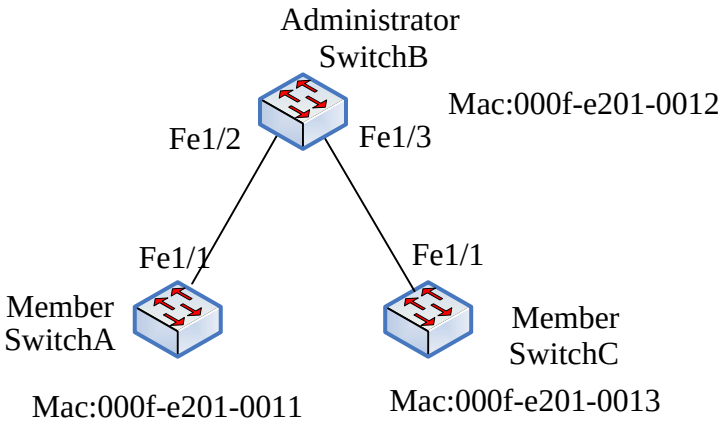
1、Networking requirements：

The cluster abc is composed of three switches, and its management VLAN is VLAN 10. Among them, Switch B is the management device

(Administrator); Switch A and Switch C are member devices (Member).

The base address IP of the entire cluster address pool is 10.0.0.1 and supports 8 devices.

2、Network diagram:



3、Configuration steps:

Configure member device SwitchA

Configure Management VLAN

[SwitchA] cluster management-vlan 10

[SwitchA] interface ge1/1

[SwitchA-ge1/1] switch access vlan 10

Enable the global NDP function and the NDP function on port ge1/1.

[SwitchA] ndp enable

[SwitchA] interface ge1/1

[SwitchA-ge1/1] ndp enable

Enable the global NTDP function and the NTDP function on port Ethernet1/0/1.

[SwitchA] ntdp enable

[SwitchA] interface ge1/1

[SwitchA-ge1/1] ntdp enable

Enable the cluster function.

[SwitchA] cluster enable

Configure member device SwitchC

Because the configuration of member devices is the same, the configuration on Switch C is similar to Switch A, and the configuration process is omitted.

Configure management device SwitchB

Configure the 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 the global NDP and NTDP functions, and enable the NDP and NTDP functions

on ports ge1/2 and 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

Configure the aging time of NDP packets sent by the device on the receiving device to 200 seconds.

[SwitchB] ndp timer aging 200

Set the interval for sending NDP packets to 70 seconds.

[SwitchB] ndp timer hello 70

Configure the maximum hop count for topology collection to 2 hops.

[SwitchB] ntdp hop 2

Configure the delay time for the first port of the collected device to forward topology collection request packets to 150 ms.

[SwitchB] ntdp timer hop-delay 150

Configure the delay time for other ports of the collected device to forward topology collection request packets to 15 ms.

[SwitchB] ntdp timer port-delay 15

Configure the topology collection interval to 3 minutes.

[SwitchB] ntdp timer 3

Enable the cluster function.

[SwitchB] cluster enable

Configure the private IP addresses of member devices to range from 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 named abc, members automatically join the cluster.

[SwitchB] cluster autobuild abc

#When you have added all the switches you want to add, you can turn off the automatic join cluster function

[SwitchB]cluster stop auto-add member

This chapter mainly includes the following:

- System log introduction
- System log configuration

25.1 Introduction to System Log

The system log module is an important part of the switch. It is used to record the operation status, abnormal behavior and user's operation behavior of the entire system, helping administrators to understand and monitor the working status of the system in time. The system log module manages all the log information from the running modules of the system, collects, classifies, stores and displays the log information.

In the logging system, there is also an important debugging function. The cooperation of system logs and debugging can help administrators or other technical personnel to monitor the operation of the network and debug and diagnose faults in the network. Administrators can easily select the content that needs to be debugged, and locate and solve the fault of the device or network by observing the log information output by debugging.

This section mainly includes the following:

- Format of log information
- Log storage
- Log display
- Debugging tool

25.1.1 Format of 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, and a colon and a space between the module name and the log content.

An example of the format of the log information is as follows:

2006/05/20 13:56:34 Warning: MSTP: Port up notification received for port ge1/2

In this log message, the timestamp is 2006/05/20 13:56:34; the priority is Warning; the module name is MSTP; and the log content is Port up notification received for port ge1/2.

1）Timestamp

The format of the time stamp: year/month/day hour:minute:second.

Hours are in 24-hour format, from 0 to 23.

The timestamp records the time when this log information was generated, and uses the system time of the switch. The system time has been set when the switch was shipped from the factory, and the administrator can also modify it. After the device is powered off, the system time can still run.

2）priority

The priority records 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 mistake
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 generated by this log message. 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 content of the log information. The administrator can know what happened to the system by reading the log content.

25.1.2 Log storage

There are generally three ways to store logs, namely:

- The log is stored in memory.
- Logs are stored in NVM.
- Logs are stored in the server.

There are four log tables in memory according to the priority of the logs. Each table stores log information of a priority. That is, the logs are divided into four types according to the priority of the logs. Each type of log exists in a separate log table. Each log table has 1K entries, which can store 1K log messages. When the log table is full, the logs behind it cover the log messages with the longest time. There is a problem with this storage method. After the system restarts, these log messages are gone. The administrator cannot see the log messages when the system crashes, and cannot locate the problem.

For important log information, such as the log information with the priority of Critical and Warning, you can store the log information in the NVM of the system. In this storage method, after the system restarts, the log information in the NVM can also 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 limited capacity of NVM, the log information entries stored in NVM are very limited.

Another better way is to store the log information in the server, which can be achieved using the SYSLOG protocol. The log information can be sent to the server in real time, and the server saves the log information and displays it on an interface. This storage method is not only convenient for users to view log information, but also has a huge capacity. It can store a large amount of log information on the server.

Currently, the system only supports storing log information in memory, and does not support storing log information in NVM or servers.

25.1.3 Log display

There are two ways to display the log: manual display and real-time display. Manual display means that the user displays the log information by inputting commands, and real-time display means that when the log information is generated, the log information is directly output to the terminal, and the user can see it in time.

For the manual display method, the user can view all the log information, and also can view the log information of a priority. The display order of the log information is that the last

generated log information is placed at the forefront, so that the user can first see the latest operating status of the switch.

For the real-time display mode, the user must turn on the terminal real-time display switch. If the switch is turned on, the generated log information is not only written to the log table, but also the log information is output to the terminal. If the switch is turned off, the log information will not be displayed on the terminal in real time. Currently, the system can only output log information to the Console terminal in real time, and does not support output of log information to the Telnet terminal.

25.1.4 debugging tools

Debugging is a diagnostic tool for devices and networks. It can track data packets sent and received by the system and modules, and changes in the state machine of the module. It can allow administrators to understand and monitor the operation of the system and modules. The situation can be tracked through the debugging tool.

The debugging tool provides a wealth of switches. By controlling these switches, the administrator can track what he is interested in. When an abnormality occurs on the device or network, the administrator can turn on the debugging switch related to this abnormality and find the problem by tracking the execution process of the system and modules.

When a debugging switch is turned on, the system will generate related log information, which will be written to the corresponding log table. In general, the priority of the log information generated by debugging is Informational. When the terminal real-time display switch is turned on, these log information will be output to the terminal in real time. When the debugging switch is turned off, the system will not generate related log information.

25.2 System log configuration

The system log configuration includes the following:

- Configure terminal real-time display switch
- View log information
- Configure debugging switch
- View debugging information

25.2.1 Configure terminal real-time display switch

By default, the real-time display switch of the terminal is turned off, and the log information generated by the system is written to the log table, but it will not be displayed on the terminal in real time. There are also some log messages in the system that are not restricted by this switch. These log messages are always output to the Console terminal in real time.

The real-time display switch of the terminal corresponds to the priority of the system log. If the real-time display switch of a certain priority terminal is turned on, the log information of the priority will be displayed on the terminal in real time. If the real-time display switch of a certain priority terminal is displayed If it is not turned on, the log information of this priority will not be displayed on the terminal in real time.

At present, the switch can only display log information in real time on the Console terminal, and cannot display log information in real time on the Telnet terminal.

When the user uses the write command to store the current configuration of the system in the configuration file, the terminal real-time display switch configuration will not be stored in the system configuration file. When the system restarts, these configurations will be lost and need to be reconfigured.

The command to configure the terminal real-time display switch is as follows:

command	description	CLI mode
log display [critical | warning | informational | debugging]	Turn on the terminal real-time display switch. If no parameters are entered, the real-time display switches of all priority terminals are turned on. If one of the parameters is entered, the real-time display switches of the designated priority terminals are turned on.	Privileged mode
no log display [critical | warning | informational | debugging]	Turn off the terminal real-time display switch. If no parameter is entered, the real-time display switch of all priority terminals is turned off. If one of the parameters is entered, the real-time display switch of the specified priority terminal is turned off.	Privileged mode

25.2.2 View log information

The commands for viewing log information are as follows:

command	description	CLI mode
show log display	Display the configuration of real-time display switches of all priority terminals.	Normal mode
show log [critical | warning | informational | debugging]	Display the log information in the log table. If no parameter is entered, the log information of all log tables is displayed. If one of the parameters is entered, the log information of the specified priority log table is displayed.	Normal mode

25.2.3 Configure the debugging switch

The system provides a variety of debugging switches, involving multiple modules, here only lists the schematic commands of each module, for 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 is restarted, these configurations will be lost and need to be reconfigured.

The schematic commands for configuring the debugging switch are as follows:

command	description	CLI mode
debug ip …	Turn on the debugging switch for the system to send and receive IP packets.	Privileged mode
no debug ip …	Turn off the debugging switch for sending and receiving IP packets in the system.	Privileged mode
debug ip icmp …	Turn on the debugging switch that the system	Privileged mode

	sends and receives ICMP packets.	
no debug ip icmp …	Turn off the debugging switch for sending and receiving ICMP packets in the system.	Privileged mode
debug ip arp …	Turn on the debugging switch for the system to send and receive ARP packets.	Privileged mode
no debug ip arp …	Turn off the debugging switch for the system to send and receive ARP packets.	Privileged mode
debug ip udp …	Turn on the debugging switch for the system to send and receive UDP packets.	Privileged mode
no debug ip udp …	Turn off the debugging switch for sending and receiving UDP packets in the system.	Privileged mode
debug ip tcp …	Turn on the debugging switch that the system sends and receives TCP packets.	Privileged mode
no debug ip tcp …	Turn off the debugging switch that the system sends and receives TCP packets.	Privileged mode
debug mstp …	Turn on the 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 function diagnosis.	Privileged mode
no debug igmp snooping …	Turn off the relevant debugging switch for IGMP SNOOPING function diagnosis.	Privileged mode
debug dhcp snooping …	Turn on the debugging switch for DHCP SNOOPIN protocol diagnosis	Privileged mode
no debug dhcp snooping …	Disable debugging related to DHCP SNOOPIN protocol diagnosis	Privileged mode
no debug all	Turn off all debugging switches in the system.	Privileged mode

25.2.4 View debugging information

The command to view debugging information is as follows:

command	description	CLI mode
show debugging [ip | mstp | igmp snooping | dhcp snooping]	Check the debugging switch configuration. If no parameters are entered, view the debugging switch configuration of all modules. If only one of the parameters is entered, only one module's debugging switch configuration is viewed. If the input parameter is ip, the debugging switch configuration of the IP, ICMP, ARP, UDP, and TCP modules will be checked.	Normal mode

25.3 Configuring SYSLOG

SYSLOG includes the following:

- SYSLOG introduction
- SYSLOG configuration
- SYSLOG configuration example

25.3.1 Introduction to SYSLOG

SYSLOG is a standard protocol for the management of device log information, and it has gained great application due to its concise design. In the SYSLOG system, it is divided into three parts. One is to define each sub-module in order to distinguish the log information generated by different modules; define different levels of log information in order to observe the operation status of the device. Various log information of the device is collected according to this agreement. The second is the configuration file, which defines how to process the collected log information, which can be saved locally, can be sent to a specified server on the network, can be distributed to the specified logged-in users, etc.; the configuration file determines how to save the device generated Log information. The third is to send SYSLOG protocol messages according to the message format defined by 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 functional sub-module in the switch, and sends each level of log information to the system log module. Four levels of log tables are maintained in the system log module. The second part of the SYSLOG protocol is the unified distribution of log information by the system log module. One is real-time or manual display on the serial terminal through the terminal display switch; the second is to save four levels of log tables in memory; the third is to save high-level on NVM Log information at the same level to avoid losing important log records in the event of a power failure; the fourth is to send the logs to a remote server for storage, collection, and sorting through SYSLOG messages. The SYSLOG submodule in the system log module only implements the third part of the function, and transmits the system log to the server.

25.3.2 SYSLOG configuration

SYSLOG configuration commands include:

- Open the syslog protocol
- Close the syslog protocol
- Set syslog send level
- Restore the syslog sending level to the default value

command	description	CLI mode
syslog open <server-ip> [udp-port]	Open the syslog protocol; the parameter server-ip is the server IP address, required; the parameter udp-port is the destination port number of the protocol packet, optional, if not set, the default value is 514; if the setting needs to be consistent with the server configuration.	Global configuration mode
syslog close	Close syslog protocol	Global configuration mode
syslog level <critical | warning | informational | debugging>	Set the sending level of logs. If it is set to debug level, all logs will be sent to the server.	Global configuration mode
no syslog level	Restore the sending level to the default value	Global configuration mode

25.3.3 SYSLOG configuration example

（1） Configuration

Configure the IP address of the syslog server as 192.168.2.201, and configure the server software to receive the UDP port of syslog packets as 200; connect the ge1/3 port to the server; the server only saves the highest two levels of log records.

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） Verification

```
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
```

This chapter mainly includes the following: :

- Introduction
- Protocol principle
- Configuration introduction

26.1 Introduction

When a loop occurs on a port of the switch, it will cause a broadcast storm on this port, and learn the source MAC addresses of all broadcast packets to this looped port, which will cause the device to fail to forward normally.

26.2 Protocol principle

The Ethernet Loopback Detection (ELD) protocol can detect loops through the interaction of data packets and block the ports where loops occur. The ELD protocol is a protocol based on port calculation, and can only detect the loop that occurs on this port.

26.2.1 Testing process

When the ELD protocol is enabled on a port, a timer will be enabled on this port periodically. When the timer expires, a loop detection packet will be sent. If the loop detection packet sent by itself is received within a timer period, then If there is a loop on this port, it will perform the operation of blocking the loop on this port and clear the FDB table of this port.

If a port belongs to a port member of multiple VLANs, then this port will automatically send loop detection packets to all VLANs. In other words, this port will automatically detect whether there is a loop in all VLANs to which it belongs.

26.2.2 Recovery Mode

As mentioned above, when a port loop occurs, the port will be blocked. The ELD protocol has two user-configurable recovery modes: automatic recovery and manual recovery.

Automatic recovery is that when a port is blocked by a loop, the ELD protocol enables a recovery timer. After the timer expires, it performs a reverse operation to block the loop and enables the loop detection timer again at this port.

Manual recovery is that after the port is blocked, the protocol no longer enables the timer to recover the port. The user must enter the command to perform the reverse operation of blocking the loop

26.2.3 Protocol Security

The ELD protocol is vulnerable to attacks in the network, which means that users can send ELD protocol packets to an ELD protocol-enabled port according to the ELD protocol packet format, resulting in this port being blocked and causing errors in the absence of loops. Decision.

The ELD protocol uses two strategies to prevent similar attacks and minimize errors.

Decision one, first of all, the ELD protocol is a non-interactive protocol, which means that it does not depend on other devices, then the data packet itself can be simply encrypted. Our operation here is to send an ELD protocol packet carrying a key, and the user cannot disguise this protocol packet without the key.

Decision two is mainly to prevent attackers from reflecting protocol packets through packet capture attacks. You can configure the format of the data packets received by the switch within a certain period to prevent attacks. This needs to be configured by the user.

26.3 Configuration introduction

The ELD protocol is implemented based on the port, and there is no uniformly enabled command.

26.3.1 Global configuration

Global configuration is the uniform property of the configuration protocol.

command	description	mode
loop-detection detection-time <1-65535>	Configure the loop detection time period. This time must be twice 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 greater than 2 times 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 check, which is off by default.	Global configuration mode
loop-detection respond-packets	Configure the number of packets that must be received within a certain period of time. If the protocol security check is enabled, this configuration will take effect. The default value is 10	Global configuration mode

26.3.2 Interface configuration

Interface configuration is the configuration of each port.

command	description	mode
Loop-detection enable	Enable ELD protocol on a port.	Interface configuration mode
Loop-detection resume	Manually recover and restart the loop check.	Interface configuration mode
loop-detection resume-mode {automation | manual}	Configure the recovery mode, select manual recovery or automatic recovery, the default is automatic recovery.	Interface configuration mode
loopback-detection shutdown-mode {no-shutdown | shutdown}	The command configures whether the port is shut down when a loop occurs.	Interface configuration mode

26.3.3 Display configuration

Show loop-detection [ifname]

Display all the configuration of the protocol and the configuration of an interface.

This chapter mainly includes the following：

- Introduction
- Configure SNTP
- Display SNTP

27.1 Introduction to SNTP

At present, the Internet generally uses a communication protocol to achieve network time synchronization, that is, NTP (Network Time Protocol), and another protocol is a simplified version of the NTP protocol, that is, SNTP (Simple Network Time Protocol). The NTP protocol can span various platforms and operating systems and uses very sophisticated algorithms, so it is almost not affected by the delay and jitter of the network, and can provide 1-50ms accuracy. NTP also provides an authentication mechanism with a high level of security. However, the NTP algorithm It is complicated and has high requirements on the system.

SNTP (Simple Network Time Protocol) is a simplified version of NTP. When it is implemented, a simple algorithm is used to calculate the time, and the performance is high. The accuracy can generally reach about 1 second, which can basically meet the needs of most occasions.

Since the SNTP message and the NTP message are completely the same, the SNTP Client implemented by this switch is fully compatible with the NTP Server

27.2 Configuring SNTP

27.2.1 Default SNTP settings

project	Default value
SNTP status	Disable disable SNTP service
NTP Server	There are three NTP servers by default. 211.115.194.21 203.109.252.5 192.43.244.18
SNTP synchronization time interval	1800 seconds
Local time zone	+8,Dongba District

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

Turn off SNTP

27.2.2 Configure SNTP Server address

Since the SNTP message and the NTP message are exactly the same, the SNTP Client is fully compatible with the NTP Server. There are many NTP Servers on the network, you can choose one with less network delay as the NTP on the switch Server.

The specific NTP server address can be obtained from http://www.time.edu.cn/ or http://www.ntp.org/.

Such as 192.43.244.18 (time.nist.gov)

The switch has three server addresses by default, which are 211.115.194.21, 203.1109.252.5 and 192.43.244.18. The switch uses the first server address to synchronize the time first. If the synchronization is not possible, the second server address is used. analogy. In general, users do not need to configure the Server address, just use the default Server address. If you need to configure the server address in special circumstances, you need to delete the default server address before adding a new server address.

The configuration for adding a server address is as follows:

Switch# configure terminal

Enter global configuration mode

Switch(config)# sntp server 210.72.145.44

Increase the SNTP server IP. If there are already three Server addresses on the switch, the increase will fail. You need to delete the address and add it

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 a server address

The configuration to set 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, addresses 211.115.194.21, 203.1109.252.5 and 192.43.244.18

27.2.3 Configure SNTP clock synchronization interval

The SNTP Client needs to synchronize the clock with the NTP Server at regular intervals in order to correct the clock at regular intervals.

The configuration is as follows:

Switch# configure terminal

Switch(config)# sntp interval 60

Set the interval of the timing synchronization clock, the unit is second, the range is 60 seconds-65535 seconds. The default value is 1800 seconds, here is set to 60 seconds

Switch(config)# no sntp interval

The interval of the timing synchronization clock is restored to the default of 1800 seconds

27.2.4 Configuring the Local Time Zone

The time obtained after communicating through the SNTP protocol is Greenwich Mean Time (GMT). In order to prepare for the hunting of local time, it is necessary to set up the local area to adjust the standard time. By default, the switch sets the local time zone to East Eight District, which is also the time zone where China is located.

The configuration is as follows:

Switch# configure terminal

Switch(config)# sntp time-zone -8

Set local time zone to west eight

Switch(config)# no sntp time-zone

The local time zone is restored to the East Eight District

27.3 SNTP information display

The configuration is as follows:

Switch# show sntp

Switch# show running-config

Chapter 28 OAM Configuration

This chapter mainly includes the following：

- OAM introduction
- Configure OAM
- OAM typical configuration example

28.1 OAM introduction

Ethernet OAM (Operations, Administration and Maintenance) is a tool for monitoring network problems. It works at the data link layer and utilizes regular interaction between OAMPDUs (OAM Protocol Data Units, OAM Protocol Data Units) to report the status of the network, enabling network administrators to manage the network more efficiently.

At present, Ethernet OAM mainly solves the common link problem in the "last mile" of Ethernet access. By enabling the Ethernet OAM function on two point-to-point connected devices, you can monitor the link status between the two devices.

This section mainly introduces the main functions of Ethernet OAM, including：

- Link performance monitoring: can detect link failures；
- Fault detection and alarm: can notify the network administrator in time when the link fails；
- Loop test: Link failure is detected by looping back non-OAMPDUs.

28.1.1 Link Performance Monitoring

Link monitoring is used to detect and discover link layer faults in various environments.

Ethernet OAM uses the interaction of Event Notification OAMPDU for link monitoring. When a link failure occurs, after the local link detects the failure, it will send an Event Notification OAMPDU to the peer Ethernet OAM entity to notify the general 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 within a unit of time
Errored Frame Event	Error frame event	Within a unit time, the number of error frames exceeds the threshold
Errored Frame Period Event	Error frame period event	Within the time of receiving the specified number of frames, the number of erroneous frames exceeds the threshold
Errored Frame Seconds Summary Event	Error frame seconds total events	The number of errored frame seconds exceeds the threshold within the specified time

28.1.2 Remote fault detection

Ethernet fault detection is very difficult, especially when the network physical communication is not interrupted and the network performance is slowly degraded.

OAMPDU defines a flag (Flag field) to allow the Ethernet OAM entity to transmit the fault information to the peer. 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	Signal loss from peer link	Send every second
Dying Gasp	Fatal failure	Unpredictable local failures, such as power outages	Non-stop sending
Critical Event	Emergencies	Unclear emergencies, such as single link	Non-stop sending

Information OAMPDUs are continuously sent during the Ethernet OAM connection. The local OAM entity can inform the remote OAM entity of the information about the emergency link event that occurred at the local end through the 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.

28.1.3 Remote loopback

The far-end loopback function means that when the OAM entity in active mode sends all other messages except the OAMPDU to the opposite end (remote end), the opposite end directly loops it back to the local end after receiving the message. It can be used to locate link faults and detect link quality: network administrators can evaluate link performance (including packet loss rate, delay, jitter, etc.) by observing the return of non-OAMPDU packets.

28.2 Configuring OAM

command	description	CLI mode
oam errored-frame period <1-60>	Configure the periodic value of the Ethernet port for error frame event detection. The default error frame event period is 1s.	Privileged mode
no oam errored-frame period	Reset the period value of the Ethernet port for error frame event detection. The default error frame event period is 1s.	Privileged mode
oam errored-frame threshold <0-4294967295>	Configure the threshold for error frame event detection. The default error frame event threshold is 1.	Privileged mode
no oam errored-frame threshold	Reset the threshold for error frame event detection. The default error frame event threshold is 1.	Privileged mode
oam errored-frame-period period <100-6000>	Configure the period value of the Ethernet port for error frame period event detection. The default error frame period event period is 1000 milliseconds.	Privileged mode
no oam errored-frame-period period	Reset the period value of the Ethernet port for error frame period event detection. The default error frame period event period is 1000 milliseconds.	Privileged mode
oam errored-frame-period threshold <0-4294967295>	Configure the threshold for error frame period event detection. The default error frame event threshold is 1.	Privileged mode
no oam errored-frame-period threshold	Reset the threshold for error frame period event detection. The default error frame event threshold is 1.	Privileged mode

oam errored-frame-seconds period <10-90>	Configure the period of the Ethernet port to detect the error frame seconds event. The default error frame event period is 60s.	Privileged mode
no oam errored-frame-seconds period	Reset the period value of the Ethernet port for error frame seconds event detection. The default error frame event period is 60s.	Privileged mode
oam errored-frame-seconds threshold <0-900>	Configure the threshold for detecting the error frame seconds event. The default error frame seconds event threshold is 1.	Privileged mode
no oam errored-frame-seconds threshold	Resets the threshold for detecting error frame seconds events. The default error frame seconds event threshold is 1.	Privileged mode
oam mode (active| passive)	Configure the working mode of Ethernet OAM. By default, the link mode of Ethernet OAM is active.	Interface configuration mode
oam enable	Turn on the Ethernet OAM function, and the default Ethernet OAM function is turned off.	Interface configuration mode
oam loopback	Enable the Ethernet OAM loopback function. By default, Ethernet OAM loopback is disabled.	Interface configuration mode
no oam loopback	Disable the Ethernet OAM loopback function. By default, Ethernet OAM loopback is disabled.	Interface configuration mode
show oam configuration	Window and threshold for displaying general link events.	Privileged mode
show oam local-state (IFNAME|)	View OAM local information	Privileged mode
show oam remote-state (IFNAME|)	View OAM peer information	Privileged mode
show oam link-event (IFNAME|)	View OAM link event information	Privileged mode
show oam-loopback IFNAME	Display loopback information for a port.	Privileged mode

28.3 OAM typical configuration example

1 Networking requirements
Configure the Ethernet OAM protocol on Device A and Device B to manage the data link layer; (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, configure the Ethernet OAM connection mode to passive mode and enable the Ethernet OAM function.
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
Configure the Ethernet OAM working mode of the port Ethernet1/0/1 as the default mode active, and enable the Ethernet OAM function.
Switch(config-fe1/1)#oam enable

(3) (On Device A) Check the configuration effect:
Switch>enable
Switch#show oam fe1/1

Chapter 29 CFM Configuration

The switch provides the CFM function, which is mainly used to detect link connectivity in the Layer 2 network, confirm the fault and determine the location of the fault, mainly including the following:

- Introduction to CFM
- Configure CFM basic settings
- CFM function configuration
- CFM display and maintenance
- CFM typical configuration example

29.1 Introduction to CFM

CFM is the abbreviation of Connectivity Fault Management. The CFM of this switch mainly refers to the detection of connectivity errors, following the CFM protocol defined by IEEE 802.1ag. It is a VLAN-based end-to-end OAM (Operations, Administration and Maintenance) mechanism on Layer 2 links. It is mainly used to detect link connectivity, confirm faults and determine faults in Layer 2 networks. Where it happened.

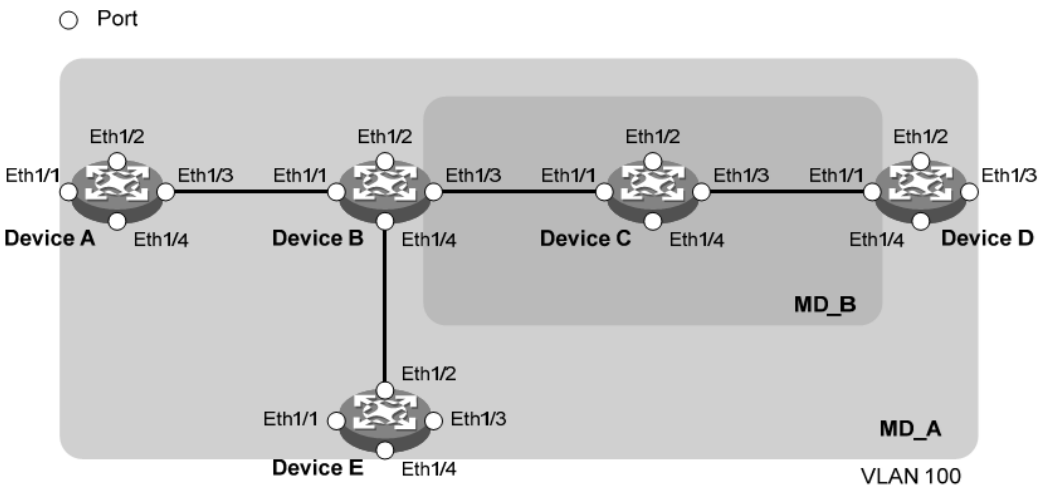
29.1.1 CFM basic concepts

1Maintenance domain

The maintenance domain (Maintenance Domain, MD) indicates the network covered by the connectivity error detection, and its boundary is defined by a series of maintenance endpoints configured on the port. The maintenance domain is identified by "maintenance domain name".

In order to locate the fault point accurately, the concept of level (level) was introduced in the maintenance domain. The maintenance domain is divided into eight levels, represented by integers from 0 to 7. The larger the number, the higher the level, and the greater the scope of the maintenance domain. Different maintenance domains can be adjacent or nested, but cannot intersect, and can only be nested from high-level maintenance domains to low-level maintenance domains during nesting, that is, low-level maintenance domains must be included within the high-level maintenance domains.

CFM PDUs in the low-level maintenance domain are discarded after entering the high-level maintenance domain; CFM PDUs in the high-level maintenance domain can traverse the low-level maintenance domain; CFM PDUs in the same-level maintenance domain cannot cross each other.



Picture 1-1

In practical applications, it is necessary to plan the maintenance domain reasonably: As shown in Figure 1-1, the maintenance domain MD_B is nested in the maintenance domain MD_A. To perform connectivity detection in MD_A, it is required that the CFM PDU of MD_A can traverse MD_B Therefore, the level of MD_A needs to be configured higher than MD_B. In this way, the CFM PDU of MD_A can traverse MD_B, thereby achieving connectivity fault management of the entire MD_A, and the CFM PDU of MD_B will not spread into MD_A.

The classification of the maintenance domain makes 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 found to be unreachable on the boundary of MD_A, it indicates that the devices in this domain have appeared. Failure, the failure may appear on the five devices Device A ~ Device E. At this time, if the link is not found on the boundary of MD_B, the fault scope is reduced to the three devices of Device B to Device D; conversely, if the devices in MD_B are working normally, at least Device C can be determined to be There is no malfunction.

2 Maintenance set

Multiple maintenance sets (Maintenance Association, MA) can be configured in the maintenance domain as required. Each maintenance set is a collection of maintenance points in the maintenance domain. The maintenance set is identified by "maintenance domain name + maintenance set name".

The maintenance set serves a VLAN, and the packets sent by the maintenance point in the maintenance set are tagged with the VLAN. At the same time, the maintenance point in the maintenance set can receive the packets sent by other maintenance points in the maintenance set.

3 Maintenance point

Maintenance points (Maintenance Point, MP) are configured on the port and belong to a certain maintenance set. They can be divided into maintenance endpoints (Maintenance Association End Point, MEP) and maintenance intermediate points (Maintenance Association Intermediate Point, MIP).

1) Maintain endpoint

The maintenance endpoint is identified by an integer called MEP ID, which determines the scope and boundary of the maintenance domain. The maintenance set and maintenance domain to which the maintenance endpoint belongs determine the VLAN attributes and level of the packets sent by the maintenance endpoint.

The level of the maintenance endpoint determines the level of packets it can process. The level of the packets sent by the maintenance endpoint is the level of the maintenance endpoint. When the maintenance endpoint receives a packet higher than its own level, it will not process it, but will forward it according to the original path; and when the maintenance endpoint receives a packet less than or equal to its own level, it will not forward it again, the maintenance endpoint Perform corresponding processing to ensure that packets in the low-level maintenance domain do not spread to the high-level maintenance domain.

The maintenance endpoints are directional, and are divided into outward MEPs and inward MEPs. The direction of the maintenance endpoint indicates the position of the maintenance domain relative to the port.

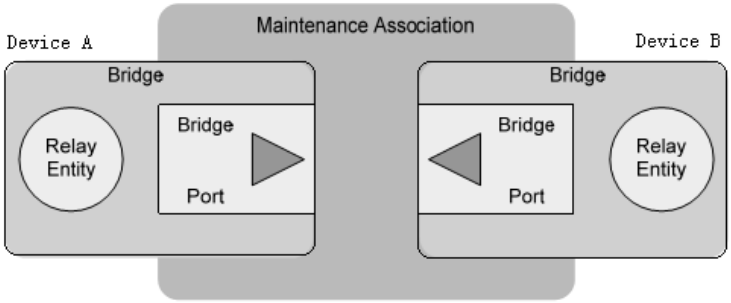


Figure 1-2 Schematic diagram of outward MEP

As shown in Figure 1-2, the outgoing maintenance endpoint sends out packets through its port,

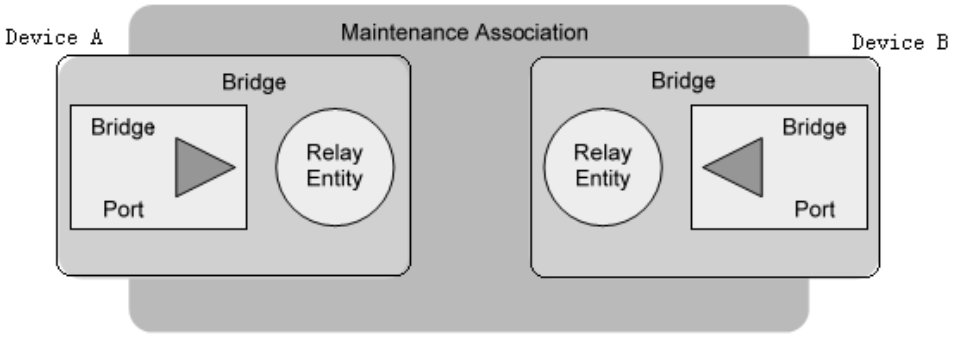


图 1-3

As shown in Figure 1-3, the inbound maintenance endpoint does not send packets out through its port, but sends out packets through other ports on the device.

2) Maintain the midpoint

The maintenance intermediate point is located inside the maintenance domain and cannot actively send out CFM protocol packets, but can process and respond to CFM protocol packets. The maintenance set and maintenance domain to which the maintenance intermediate point belongs determine the VLAN attributes and levels of the packets received by the maintenance intermediate point. The maintenance intermediate point can cooperate with the maintenance endpoint to complete functions similar to ping and tracert. Similar to the maintenance endpoint, when the maintenance intermediate point receives a packet higher than its own level, it will not process it, but will forward it according to the original path; when the maintenance intermediate point receives a packet less than or equal to its own level Will be processed.

As shown in Figure 1-4, it is a hierarchical configuration method of CFM. It is assumed that all six devices have only two ports, and maintenance endpoints and maintenance intermediate points are configured on some of the ports, such as port 1 of Device B. The configured maintenance points are as follows: a maintenance intermediate point at level 5, an inward maintenance endpoint at level 3, an inward maintenance endpoint at level 2, and an outward maintenance endpoint at level 0. There are four levels of maintenance domains in the figure. The maintenance domain with a larger identification number has a higher level and a wider control range; the maintenance domain with a smaller identification number has a lower level and a smaller control range.

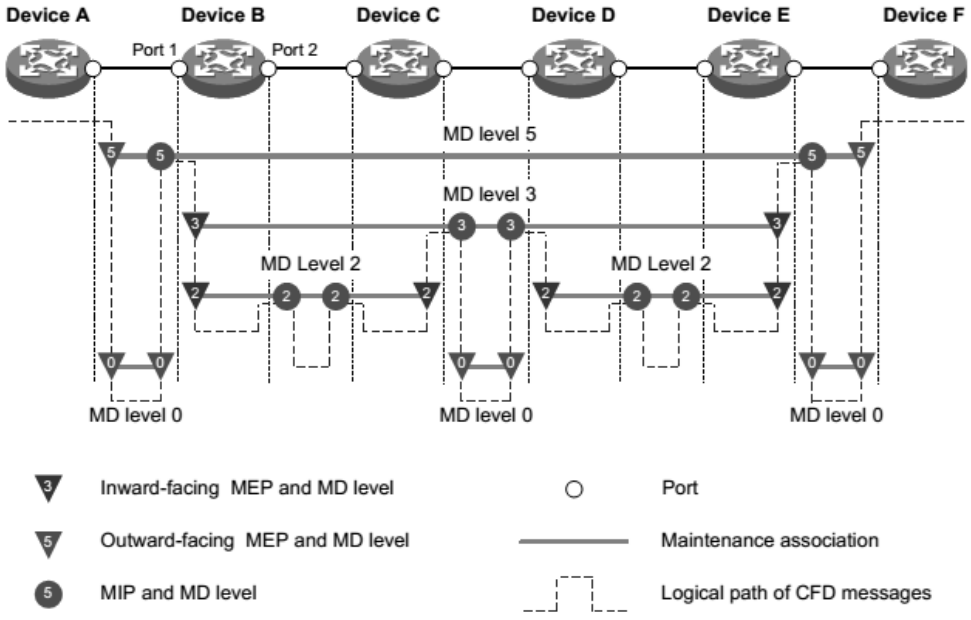


Figure 1-4 Hierarchical configuration of maintenance points

4 Maintain endpoint list

The maintenance endpoint list is a collection of local maintenance endpoints that can be configured in the same maintenance set and remote maintenance endpoints that need to be monitored. It limits the selection of maintenance endpoints in the maintenance set: all maintenance endpoints in the same maintenance set on different devices should be Included in this list, and the MEP IDs do not overlap each other. If the maintenance endpoint receives a CCM (Continuity Check Message) message from the remote device, the maintenance endpoint carried in the CCM (Continuity Check Message) message is not in the maintenance endpoint list of the same maintenance set, and the message is discarded.

5 Service instance

A service instance is represented by an integer, which represents a maintenance set in a maintenance domain. The maintenance domain and maintenance set determine the level attribute and VLAN attribute of the packets processed by the maintenance point in the service instance.

29.1.2 CFM functions

The effective application of connectivity error detection is based on reasonable network deployment and configuration. Its functions are implemented between the configured maintenance points, including:

- Continuity check function（Continuity Check， CC）
- Loopback function（Loopback， LB）
- Link tracking function（Linktrace， LT）

1. Continuity detection function

The continuity detection function is used to detect and maintain the connectivity between endpoints. Connectivity failure may be caused by equipment failure or configuration error. The implementation of this function is: the maintenance endpoint periodically sends a CCM message, which is a multicast message, and other maintenance endpoints in the same maintenance set receive the message and learn the remote state from it. If the maintenance endpoint does not receive the CCM message from the remote maintenance endpoint within 3.5 CCM message transmission cycles, it considers that there is a problem with the link and will output a log report. When multiple maintenance endpoints in the maintenance domain are sending CCM messages, multi-point to multi-point link detection is achieved.

2. Loopback function

The loopback function is similar to the ping function of the IP layer and is used to verify the connection status between the local device and the remote device. The implementation of this function is: the maintenance endpoint sends an LBM (Loopback Message, loopback message) to the remote maintenance point, and checks the chain according to whether it can receive the LBR (Loopback Reply, loopback reply message) fed back by the peer 路 status. Both LBM and LBR are unicast messages.

3. Link tracking function

The link tracking function is used to determine the path from the source end to the target maintenance endpoint. The implementation method is: the source end sends an LTM (Linktrace Message, link trace message) to the target maintenance endpoint, and the target maintenance endpoint and the maintenance performed by the LTM After receiving this message, the intermediate point will send an LTR (Linktrace Reply, link trace reply message) to the source, and the source will

determine the path to the target maintenance endpoint according to the received LTR. LTM is a multicast message, and LTR is a unicast message.

29.2 Introduction to CFM configuration tasks

Before configuring the CFM function, plan the network as follows:

- Classify the maintenance domains of the entire network and determine the boundaries of maintenance domains at all levels.
- Determine the name of each maintenance domain. The same maintenance domain has the same name on different devices.
- Determine the maintenance set in each maintenance domain according to the VLAN to be monitored.
- Determine the name of each maintenance set. The same maintenance set has the same name on different devices in the same maintenance domain.
- Maintenance endpoints should be planned on the boundary ports of the maintenance domain and maintenance set, and maintenance intermediate points can be planned on non-border devices or ports.
- Determine the remote maintenance endpoint list for the maintenance endpoint.

After completing the network planning, perform the following configuration.

Configuration tasks		Explanation	Detailed configuration
CFM basic configuration	Enable CFM function		29.3.1
	Configure service instance		29.3.2
	Configure maintenance endpoints		**Error! Reference source not found.**
	Configuration and maintenance intermediate point		29.3.4
Configure CFM functions	Configure continuity detection function		**Error! Reference source not found.**
	Configure the loopback function		**Error! Reference source not found.**
	Configure link tracking		**Error! Reference source not found.**

note:

- Ports blocked by the STP protocol cannot receive, send, and respond to CFM protocol packets; but if the port is configured as an outgoing MEP, even if the port is blocked by the STP protocol, it will still receive and send CCM packets.
- Only the Ethernet port supports CFM configuration.

29.3 CFM basic configuration

29.3.1 Enabling the CFM function

command	description	CLI mode
cfm enable	Enable the CFM function. Closed by default.	Configuration mode

29.3.2 Configuration Service Instance

Before configuring maintenance endpoints and maintenance intermediate points, you must first configure the service instance. A service instance is represented by an integer, which represents a maintenance set in a maintenance domain. The maintenance domain and maintenance set determine the level attribute and VLAN attribute of the packets processed by the maintenance point in the service instance.
Please strictly follow the following order to create a maintenance domain, maintenance set and service instance.

command	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. No maintenance set is created by default	Configuration mode
cfm service-instance <instance-id> md <md-name> ma <ma-name>	Create a service instance. No service instance is created by default	Configuration mode

29.3.3 Configure maintenance endpoints

The maintenance endpoint is a functional entity in the service instance. The CFM function is mainly reflected in the operation of the maintenance endpoint. It implements the CC, LB, and LT functions, and alerts the wrong CCM message and cross-connect. Since the maintenance endpoint is configured on the service instance, the level and VLAN attributes of the maintenance domain represented by the service instance naturally become the attributes of the maintenance endpoint.
After creating a maintenance endpoint, you need to configure a remote maintenance endpoint list that specifies the maintenance endpoint. The remote maintenance endpoint list is a collection of remote maintenance endpoints that need to be monitored in the same maintenance set.

command	description	CLI mode
cfm mep <mep-id> service-instance <instance-id> {inbound | outbound}	Create maintenance endpoints. There is no maintenance endpoint on	Interface mode

	the default port.	
cfm remote-meplist <mep-list> service-instance <instance-id> mep <mep-id>	Configure the remote maintenance endpoint list for the specified maintenance endpoint. There is no maintenance endpoint list for the default port.	Interface mode
cfm mep service-instance <instance-id> mep <mep-id> enable	Enable maintenance endpoints. The maintenance endpoint is turned off by default.	Interface mode

note:

- After the maintenance endpoint is enabled, the maintenance endpoint will process the received CCM message.

29.3.4 Configuration and Maintenance Intermediate Point

The maintenance intermediate point is a functional entity in the service instance that is used to respond to LBM and LTM messages.
The maintenance intermediate point is automatically created by the system on each port according to the rules. The creation rules are as follows: If there is no maintenance intermediate point on the port, then the maintenance set in each maintenance domain is checked in order from low to high, and as shown in the figure The process shown in 1-5 is to decide whether to create a maintenance intermediate point (in the same VLAN).

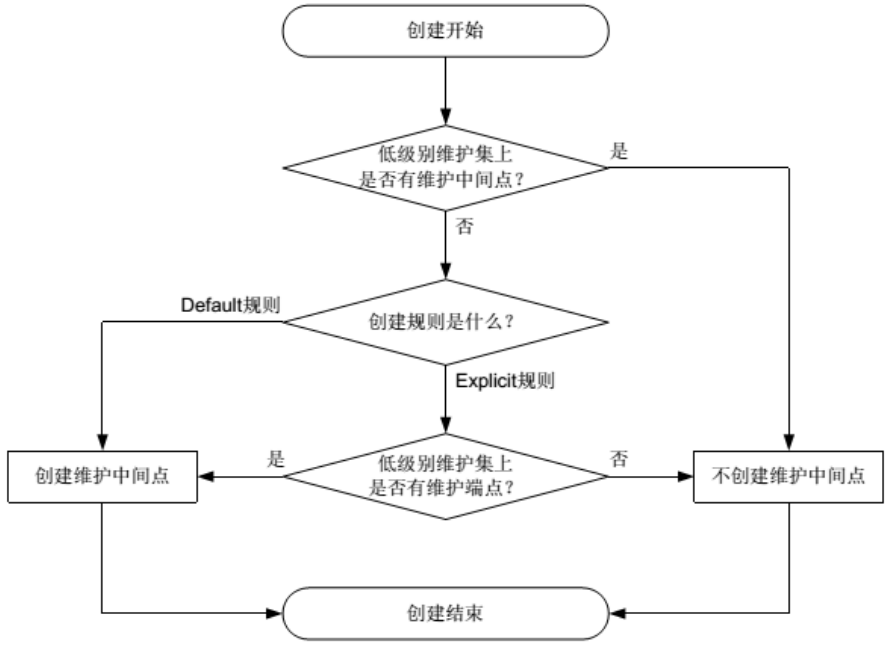


Figure 1-5 Maintaining the creation process of intermediate points

Please configure and maintain the rules for creating intermediate points according to the network plan.

command	description	CLI Mode
cfm mip-rule {explicit | default} service-instance <instance-id>	Configure rules for creating and maintaining intermediate points. By default, there are no rules for creating and maintaining intermediate points, and there are no rules for creating and maintaining intermediate points.	Configuration mode

note:
After configuring the maintenance intermediate point creation rule, any of the following conditions can trigger the creation or deletion of the maintenance intermediate point:

- Enable the CFM function.
- Create or delete a maintenance endpoint on the port.
- The VLAN attributes of the port have changed.
- The creation rules for maintenance intermediate points have changed.

29.4 Configure CFM functions

Before configuring CFM functions, you need to complete the basic configuration of CFM.

29.4.1 Configure continuity detection function

By configuring the continuity detection function, you can enable maintenance endpoints to send CCM messages to each other to detect the connectivity status between these maintenance endpoints, thereby realizing link connectivity management.

command	description	CLI mode
cfm cc interval <interval-value> service-instance <instance-id>	Configure the value of the time interval field in the CCM messages 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.	Configuration mode
cfm cc service-instance <instance-id> mep <mep-id> enable	Enables the maintenance endpoint to send CCM messages. By default, the CCM message sending function of the maintenance endpoint is turned off.	Interface mode

The relationship between the value of the Interval field (Interval field) in the CCM message sent by the maintenance endpoint, the CCM transmission interval, and the remote MEP timeout time is shown in Table 26-1.

时间间隔域的值	CCM 发送时间间隔	远端 MEP 超时时间
3	100 毫秒	350 毫秒
4	1 秒	3.5 秒
5	10 秒	35 秒
6	60 秒	210 秒
7	600 秒	2100 秒

Table 26-1 Relationship between the value of the time interval field, the CCM transmission interval, and the remote MEP timeout

note:

- Maintenance endpoints on the same maintenance domain and maintenance set on different devices must have the same interval for sending CCM messages.
- If the time interval of the CCM message sent by the maintenance endpoint is set to 3, it is recommended not to configure too many maintenance endpoints in the same maintenance domain and maintenance set, otherwise it will affect the performance of the whole machine.

29.4.2 Configuring Loopback

By configuring the loopback function, you can check the link status to verify link connectivity.

command	description	CLI mode
cfm loopback service-instance <instance-id> mep <mep-id> { target-mep <target-mep-id> | target-mac <mac-address> } [number <number>]	Enable the loopback function to check the link status.	Privileged mode

29.4.3 Configure link tracking

By configuring the link tracking function, you can find the path from the designated maintenance endpoint to the destination maintenance endpoint, thereby realizing the link fault location. It includes the following two functions:

- Find the path from the designated maintenance endpoint to the destination maintenance endpoint: determine the path between the devices by sending an LTM message from the designated maintenance endpoint to the destination maintenance endpoint, and detecting the response LTR message.
- Automatically send link tracking message: After this function is enabled, when the maintenance endpoint does not receive the CCM message from the remote maintenance endpoint within 3.5 CCM message transmission cycles, it is determined that the connection with the remote maintenance endpoint is wrong At this time, an 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 a maximum of 255), and the fault will be located by detecting the response LTR message.

command	description	CLI mode
cfm linktrace service-instance <instance-id> mep <mep-id> {target-mep <target-mep-id> |	Find the path from the specified maintenance endpoint to the	Privileged mode

target-mac <mac-address> } [ttl <ttl-value>] [hw-only]	destination maintenance endpoint.	
cfm linktrace auto-detection [size <size-value>]	Enable the function of automatically sending link tracking messages. By default, the function of automatically sending link trace messages is turned off.	Configuration mode

29.5 CFM display and maintenance

After completing the above configuration, execute the show command in any view to display the running status of the configured CFM, and verify the effect of the configuration by viewing the displayed information.

command	description	CLI mode
show cfm status	Displays the enabled state of CFM.	Privileged mode
show cfm md	Display the configuration information of the maintenance domain	Privileged mode
show cfm ma [[<ma-name>] md <md-name>]	Display the configuration information of the maintenance set	Privileged mode
show cfm service-instance [<instance-id>]	Display configuration information of service instance	Privileged mode
show cfm mp [interface <interface-name>]	Display maintenance point information	Privileged mode
show cfm mep <mep-id> service-instance <instance-id>	Display maintenance endpoint properties and operation information	Privileged mode
show cfm linktrace-reply [service-instance <instance-id> [mep <mep-id>]]	Display LTR message information obtained on the maintenance endpoint	Privileged mode
show cfm remote-mep service-instance <instance-id> mep <mep-id>	Display information about the remote maintenance endpoint	Privileged mode
show cfm linktrace-reply auto-detection [size <size-value>]	Display the contents of the LTR message received by automatically sending the LTM message	Privileged mode

29.6 Typical Configuration Examples

Networking requirements：

The network composed of five devices is divided into two maintenance domains MD_A and MD_B, the levels of which are 5 and 3 respectively. Each device's respective ports Ethernet1/0/1～Ethernet1/0/4 belong to VLAN 100, and each The maintenance sets in the maintenance domain all serve this VLAN.

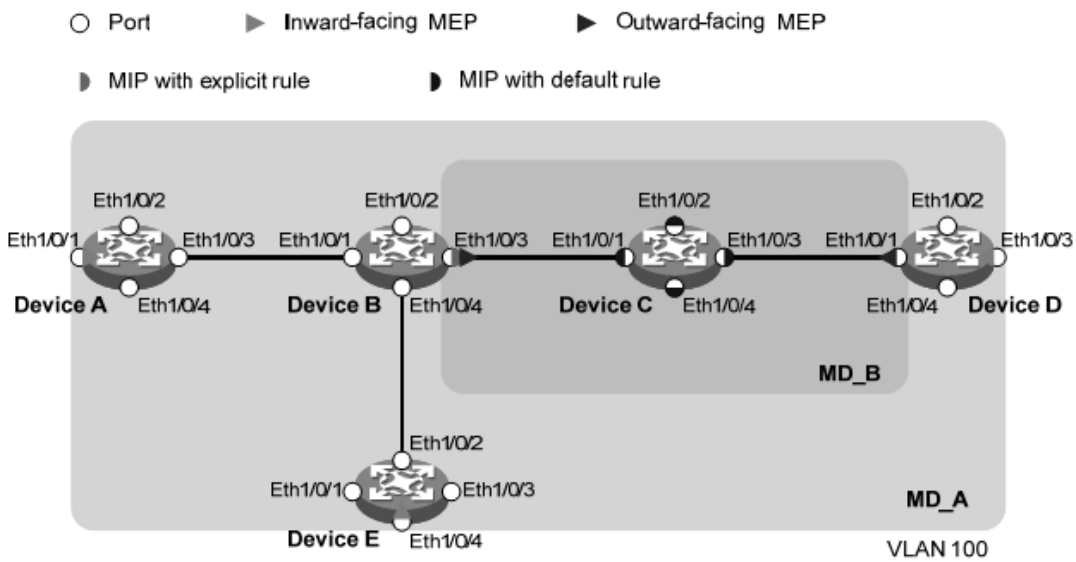
The boundary port of MD_A is Ethernet 1/0/1 of Device A, Ethernet 1/0/3 of Device D and Ethernet 1/0/4 of Device E, and inward maintenance endpoints are configured on these ports; the boundary port of MD_B is Device B Ethernet 1/0/3 and Device D's Ethernet 1/0/1, and configure outgoing maintenance endpoints on these ports.

It is required to plan the maintenance intermediate point of MD_A on Device B and configure it only when there are low-level maintenance endpoints on the port. According to this plan, since the maintenance endpoint of MD_B is configured on Ethernet 1/0/3 of Device B, the maintenance intermediate point of MD_A needs to be configured on Device B, and its creation rule is the Explicit rule.

It is required to plan the maintenance intermediate point of MD_B on Device C and configure it on all its ports. According to this plan, configure the maintenance intermediate point of MD_B on Device C, and its creation rule is the Default rule.

It is required to use the continuity detection function to detect the connection status between all maintenance endpoints in MD_A and MD_B. When a link failure is detected, use the loopback function to locate the fault; or after obtaining the status of the entire network, use The link tracking function performs path search or fault location.

Network diagram:



Configuration steps：

Configure VLANs and ports

Create VLAN 100 on each device and configure ports Ethernet 1/0/1 to Ethernet 1/0/4 to belong to VLAN 100.

2) Enable CFM function

Enable CFM on Device A.

DeviceA> config t

[DeviceA] cfm enable

The configuration of Device B to Device E is similar to Device A, and the configuration process is omitted.

3) Configure service instance

Create a maintenance domain MD_A of level 5 on Device A, create a maintenance set MA_A serving 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 at level 5 on Device B, create a maintenance set MA_A serving VLAN 100 in MD_A, and create service instance 1 for MD_A and MA_A; then create a maintenance domain MD_B at level 3, and set it at MD_B Create a maintenance set MA_B that serves VLAN 100 and create service instance 2 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 Device B, and the configuration process is omitted.

Create a maintenance domain MD_B of level 3 on Device C, create a maintenance set MA_B serving VLAN 100 in MD_B, and create service instance 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 maintenance endpoints
Create an inbound maintenance endpoint 1001 in service instance 1 on DeviceA port Ethernet1/0/1, configure the remote maintenance endpoint list corresponding to maintenance endpoint 1001, and then enable maintenance endpoint 1001.
[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 an outgoing maintenance endpoint 2001 in service instance 2 on DeviceB port Ethernet1/0/3, configure a list of remote maintenance endpoints corresponding to maintenance endpoint 2001, and then enable 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 an outgoing maintenance endpoint 4001 in service instance 2 on port Ethernet 1/0/1 of Device D, configure the remote maintenance endpoint list corresponding to maintenance endpoint 4001, and then enable maintenance endpoint 4001.
Create and enable the inbound maintenance endpoint 4002 in service instance 1 on port Ethernet1/0/3, and create a list of 4002 remote maintenance endpoints.
[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
#Create and enable the inbound maintenance endpoint 5001 in service instance 1 on the port Ethernet1/0/4 of Device E, 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) Configuration and maintenance intermediate point
In Service instance 1 of Device B, configure the creation rule of the maintenance intermediate point to be the Explicit rule.
[DeviceB] cfm mip-rule explicit service-instance 1
Configure the creation rule of the maintenance intermediate point as the Default rule in Service Instance 2 of Device C.
[DeviceC] cfm mip-rule default service-instance 2

Configure continuity detection function
Enable the function of sending CCM messages of the maintenance endpoint 1001 in service instance 1 on Ethernet 1/0/1 of Device A.
[DeviceA] interface ethernet 1/0/1
[DeviceA-Ethernet1/0/1] cfm cc service-instance 1 mep 1001 enable
[DeviceA-Ethernet1/0/1] quit
Enable the CCM message sending function of the maintenance endpoint 2001 in service instance 2 on the Ethernet 1/0/3 port of 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
Enable the CCM message sending function of the maintenance endpoint 4001 in the service instance 2 on the port Ethernet1/0/1 of Device D, and enable the CCM message sending of the maintenance endpoint 4002 in the service instance 1 on the port Ethernet1/0/3 Features.
[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
Enable the CCM message sending function of the maintenance endpoint 5001 in service instance 1 on the Ethernet 1/0/4 port 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
6) Check the configuration effect
When a link fault is detected by the continuity detection function, you can use the loopback function to locate the fault. for example:
Enable the loopback function on Device A and check the link status of maintenance endpoints 1001 to 5001 in 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 entire network through the continuity detection function, you can use the link tracking function to perform path search or fault location. for example:
Find the path of maintenance endpoints 1001 to 5001 in Device A's service instance 1.
[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 30 Basic IPv6 Configuration

The switch supports basic IPv6 functions, including IPv6 Layer 2 forwarding and IPv6 ND functions. This chapter describes how to configure IPv6, mainly including the following：

- Introduction to IPv6
- Configure basic IPv6 functions
- Configure IPv6 Neighbor Discovery Protocol
- IPv6 display and maintenance

30.1 Introduction to IPv6

IPv6 (Internet Protocol Version 6, Internet Protocol Version 6) is the second generation standard protocol of the network layer protocol, also known as IPng (IP Next Generation, next-generation Internet), it is IETF (Internet Engineering Task Force, Internet engineering task Group) A set of specifications designed to be an upgraded version of IPv4. The most significant difference between IPv6 and IPv4 is: the length of the IP address is increased from 32 bits to 128 bits.

30.1.1 IPv6 protocol features

1 Simplified message header format

By reducing or moving certain fields in the IPv4 header to the extended header, the length of the basic IPv6 header is reduced. IPv6 uses a fixed-length basic packet header, which simplifies the processing of IPv6 packets 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 basic header is only 40 bytes, which is twice the length of the IPv4 header (excluding the option field).

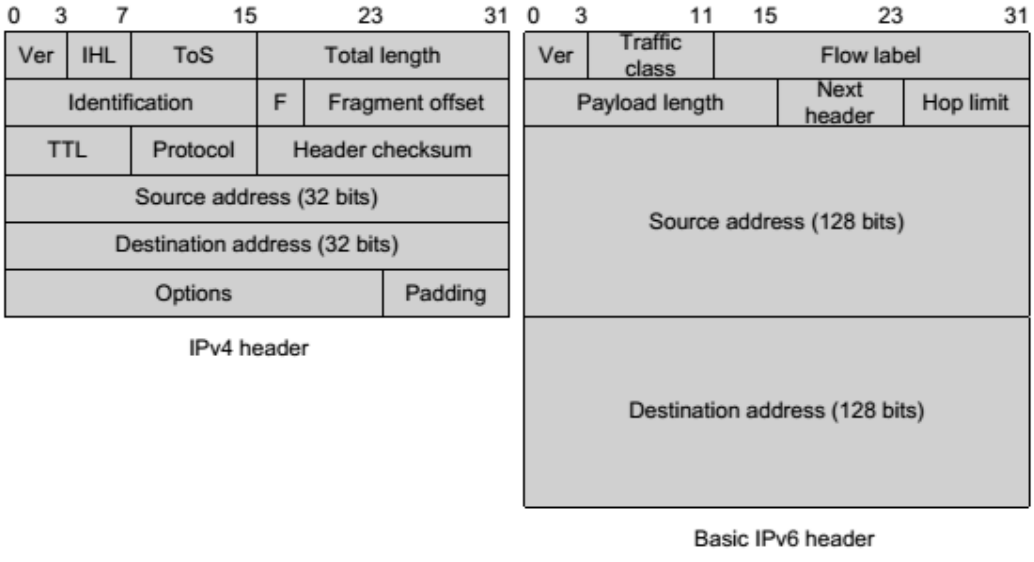


Figure 1-1 Comparison of IPv4 header and IPv6 basic header format

2 Ample address space

Both IPv6 source and destination addresses are 128 bits (16 bytes) in length. It can provide more than 3.4×1038 possible address spaces, which can fully meet the needs of multi-level address division and address allocation for public networks and private networks within organizations.

3 Hierarchical address structure

The address space of IPv6 adopts a hierarchical address structure, which is conducive to fast route search, and at the same time, it can effectively reduce the system resources occupied by the IPv6 routing table by means of route aggregation.

4 Address auto configuration

To simplify host configuration, IPv6 supports stateful address configuration and stateless address configuration:

1) Stateful address configuration refers to obtaining IPv6 addresses and related information from a server (such as a DHCP server)；

2) Stateless address configuration means that the host automatically configures the IPv6 address and related information based on its link layer address and the prefix information issued by the router.

At the same time, the host can also form a link-local address based on its own link-layer address and default prefix (FE80::/10) to communicate with other hosts on this link.

5 Built-in security

IPv6 uses IPSec as its standard extension header and can provide end-to-end security features. This feature also provides a standard for solving network security problems and improves interoperability between different IPv6 applications.

6 Support QoS

The Flow Label field in the IPv6 packet header identifies the flow, allowing the device to identify the packets in a flow and provide special processing.

7 Enhanced neighbor discovery mechanism

IPv6 Neighbor Discovery Protocol is implemented through a set of ICMPv6 (Internet Control Message Protocol for IPv6, IPv6 Internet Control Message Protocol) messages, and manages the exchange of information between neighbor nodes (that is, nodes on the same link). It replaces ARP (Address Resolution Protocol), ICMPv4 router discovery and ICMPv4 redirect messages, and provides a series of other functions.

8 Flexible header extension

IPv6 cancels the option field in the IPv4 header and introduces a variety of extended headers. While improving processing efficiency, it also greatly enhances the flexibility of IPv6 and provides good expansion capabilities for the IP protocol. The option field in the IPv4 header is only 40 bytes at most, while the size of the IPv6 extended header is only limited by the size of the IPv6 packet.

30.1.2 Introduction to IPv6 Address

1. IPv6 address representation

2. IPv6 addresses are represented as a series of 16-bit hexadecimal numbers separated by colons (:). Each IPv6 address is divided into 8 groups, each group of 16 bits is represented by 4 hexadecimal numbers, and the groups are separated by colons, for example: 2001:0000:130F:0000:0000:09C0:876A:130B.

In order to simplify the representation of IPv6 addresses, the "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 2001:0:130F:0:0:9C0:876A:130B.

2)If the address contains two or more consecutive groups that are all 0, you can use a double colon "::" instead, that is, the above address can be written as 2001:0:130F::9C0:876A:130B.

note:

You can only use the double colon "::" once in an IPv6 address. Otherwise, when the device converts "::" to 0 to restore the 128-bit address, it will be impossible to determine the number of 0s represented by "::".

An IPv6 address consists of two parts: address prefix and interface identification. Among them, the address prefix is equivalent to the network number field part in the IPv4 address, and the interface identifier is equivalent to the host number part in the IPv4 address.

The address prefix is expressed as: IPv6 address/prefix length. Among them, the IPv6 address is any of the forms listed above, and the prefix length is a decimal number, indicating how many left-most bits of the IPv6 address are the address prefix.

2 IPv6 address classification

There are three main types of IPv6 addresses: unicast addresses, multicast addresses, and anycast addresses.

1）Unicast address: used to uniquely identify an interface, similar to the IPv4 unicast address. The data packet sent to the unicast address will be transmitted to the interface identified by this address.

2）Multicast address: used to identify a group of interfaces (usually this group of interfaces belong to different nodes), similar to IPv4 multicast addresses. Data packets sent to the multicast address are transmitted to all interfaces identified by this address.

3）Anycast address: used to identify a group of interfaces (usually this group of interfaces belongs to different nodes). The data packet sent to the anycast address is transferred to the one of the set of interfaces identified by this address that is closest to the source node (measured according to the routing protocol used).

There is no broadcast address in IPv6, and the function of the broadcast address is realized by the multicast address.

IPv6 address types are specified by the first few bits of the address (called format prefixes).

3 Types of unicast addresses

There are many types of IPv6 unicast addresses, including global unicast addresses, link-local addresses, and site-local addresses.

1）Global unicast addresses are equivalent to IPv4 public network addresses and are provided to network service providers. This type of address allows the aggregation of routing prefixes, thereby limiting the number of global routing entries.

2) Link-local addresses are used for communication between nodes on the link-local in the neighbor discovery protocol and stateless autoconfiguration. Data packets that use link-local addresses as source or destination addresses will not be forwarded to other links.

3) Site-local addresses are similar to private addresses in IPv4. Data packets that use the site's local address as the source or destination address will not be forwarded to other sites outside this site (equivalent to a private network).

4) Loopback address: Unicast address 0:0:0:0:0:0:0:1 (simplified as ::1) is called the 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 IPv6 packets to itself.

5) Unspecified address: The address "::" is called an unspecified address and cannot be assigned to any node. Before the node obtains a valid IPv6 address, it can be filled in the source address field of the sent IPv6 packet, but it cannot be used as the destination address in the IPv6 packet.

4 Multicast address

In addition, there is a type of multicast address: the requested node (Solicited-Node) address. This address is mainly used to obtain the link layer address of neighboring nodes on the same link and implement 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

Among them, FF02:0:0:0:0:1:FF is a 104-bit fixed format; XX:XXXX is the last 24 bits of a unicast or anycast IPv6 address.

5 Interface identifier in IEEE EUI-64 format

The interface identifier in the IPv6 unicast address is used to identify a unique interface on the link. Currently, IPv6 unicast addresses basically require 64-bit interface identifiers. The interface identifier in IEEE EUI-64 format is derived from the link layer address (MAC address) of the interface. The interface identifier in the IPv6 address is 64 bits, and the MAC address is 48 bits, so you need to insert the hexadecimal number FFFE (1111111111111110) in the middle of the MAC address (after the 24th bit from the high bit). In order to ensure that the interface identifier obtained from the MAC address is unique, the Universal/Local (U/L) bit (the seventh bit from the upper bit) is also set to "1". The final set of numbers is used as the interface identifier in EUI-64 format.

30.1.3 Introduction to IPv6 Neighbor Discovery Protocol

The IPv6 neighbor discovery protocol uses five types of ICMPv6 messages to implement the following functions: address resolution, verifying neighbor reachability, duplicate address detection, router discovery/prefix discovery, address auto-configuration, and redirection.

The types and functions of ICMPv6 messages used by the neighbor discovery protocol are shown in Table 1-3.

ICMPv6 Message	Type Number	Function
Neighbor Solicitation (NS)	135	- Obtain the link-layer address of a neighbor - Verify neighbor reachability - Perform duplicate address detection
Neighbor Advertisement (NA)	136	- Response to NS messages - When the node's link-layer address changes, it actively sends NA messages to notify neighbors of the change
Router Solicitation (RS)	133	- Sent by a node to request routers to send RA messages immediately - Used for address configuration and node bootstrapping
Router Advertisement (RA)	134	- Response to RS messages - Periodically sent by routers under certain conditions to announce their presence and provide some configuration information
Redirect	137	- Sent by routers when better forwarding paths are available - Informs hosts to update their routing for specific destinations (redirect traffic to a better next-hop)

Table 1-3 ICMPv6 message types and functions used by the neighbor discovery protocol

The main functions provided by the neighbor discovery protocol are as follows:

1 Address resolution

Obtain the link layer address of the neighbor node on the same link (same as the ARP function of IPv4), through the neighbor request message NS and neighbor announcement message NA. As shown in Figure 1-3, node A needs to obtain the link layer address of node B.

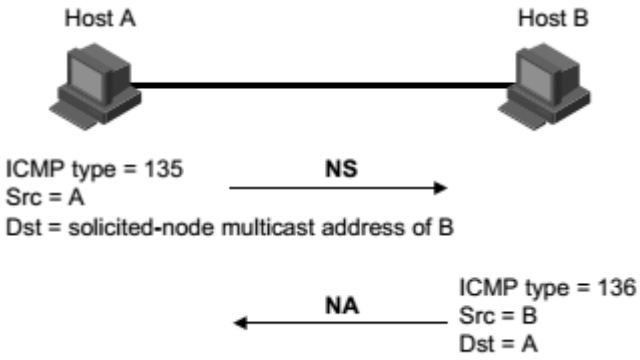


图 1-3 地址解析示意图

(1) Node A sends NS messages in multicast mode. The source address of the NS message is the interface IPv6 address of node A, and the destination address is the multicast address of the requested node of node B. The message content contains the link layer address of node A.

(2) After receiving the NS message, Node B determines whether the destination address of the packet is the multicast address of the requested node corresponding to its IPv6 address. If yes, Node B can learn the link layer address of Node A and return the NA message in unicast, which contains its own link layer address.

(3) Node A can obtain the link layer address of Node B from the received NA message.

2 Verify that the neighbor is reachable

After obtaining the link layer address of the neighbor node, the neighbor request message NS and the neighbor advertisement message NA can verify whether the neighbor node is reachable.

(1) The node sends an NS message, where the destination address is the IPv6 address of the neighbor node.

(2) If it receives the acknowledgment message from the neighbor node, the neighbor is considered reachable; otherwise, the neighbor is considered unreachable.

3 Duplicate address detection

When a node obtains an IPv6 address, it needs to use the duplicate address detection function to determine whether the address has been used by other nodes (similar to the free ARP function of IPv4). Duplicate address detection can be achieved through NS and NA, as shown in Figure 1-4.

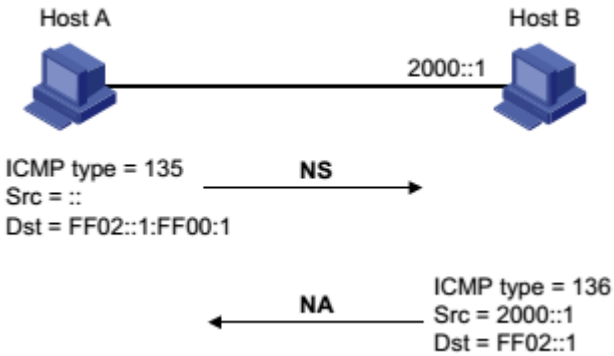


Figure 1-4 Schematic diagram of duplicate address detection

(1) Node A sends an NS message. The source address of the NS message is an unspecified address ::, and the destination address is the multicast address of the requested node corresponding to the IPv6 address to be detected. The message content contains the IPv6 address to be detected.

(2) If Node B has already used this IPv6 address, it will return NA message. 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. Otherwise, it means that the address is not used, and node A can use this IPv6 address.

4 Router discovery/prefix discovery and address auto-configuration

Router discovery/prefix discovery means that the node obtains the prefix of the neighbor router and the network where it is located from the received RA message, and other configuration parameters.

Stateless auto-configuration of addresses means that nodes automatically configure IPv6 addresses based on information obtained by router discovery/prefix discovery. Router discovery/prefix discovery is implemented by router request message RS and router advertisement message RA. The specific process is as follows:

(1) When the node starts, it sends a request to the router through the RS message, requesting the prefix and other configuration information, so as to be used for the configuration of the node.

(2) The router returns the RA message, which includes the prefix information option (the router also periodically publishes the RA message).

(3) The node uses the address prefix and other configuration parameters in the RA message returned by the router to automatically configure the IPv6 address and other information of the interface.

- The prefix information option includes not only the information of the address prefix, but also the preferred lifetime and valid lifetime of the address prefix. After receiving the RA message sent periodically, the node will update the preferred lifetime and valid lifetime of the prefix according to the message.
- In the effective life period, the automatically generated address can be used normally; after the effective life period expires, the automatically generated address will be deleted.

5Redirect function

When the host starts, it may have only one default route to the default gateway in its routing table. When certain conditions are met, the default gateway will send an ICMPv6 redirect message to the source host, informing the host to choose a better next hop for subsequent packet transmission (the same function as the IPv4 ICMP redirect message).

- The device will send an ICMPv6 redirect message to the host when the following conditions are met:
- The interface for receiving and forwarding data packets is the same interface;
- The selected route itself has not been created or modified by ICMPv6 redirect messages；
- The selected route is not the default route;
- The forwarded IPv6 data packet does not contain the routing extension header.

30.1.4 IPv6 PMTU discovery

The transmission path of the packet from the source to the destination may have different MTUs. In IPv6, when the length of the packet is greater than the MTU of the link, the fragmentation of the packet will be performed at the source end, thereby reducing the processing pressure of the intermediate forwarding device and making reasonable use of network resources.

The purpose of the PMTU (Path MTU) discovery mechanism is to find the smallest MTU on the path from the source to the destination. The working process of PMTU is shown in Figure 1-5.

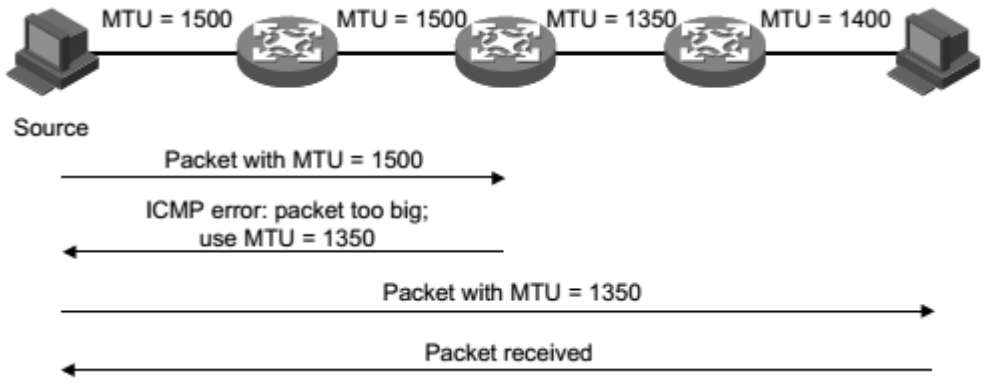


Figure 1-5 PMTU discovery process

(1) The source host uses its own MTU to fragment the packet, and then sends the packet to the destination host.
(2) When the intermediate forwarding device receives the message and forwards it, if it finds that the MTU value supported by the interface that forwards the message is less than the length of the message, it will discard the message and return an ICMPv6 error message to the source, which contains the forwarding failure MTU of the interface.
(3) After receiving the erroneous message, the source host will use the MTU carried in the message to fragment and send the message again.
(4) This is repeated until the destination host receives the message, thereby determining the minimum MTU in the path of the message from the source to the destination.

30.1.5 Protocol specification

The protocol specifications related to the IPv6 foundation 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

30.2 Introduction to IPv6 basic configuration tasks

Configure basic IPv6 functions
Configure IPv6 Neighbor Discovery Protocol
Configure PMTU Discovery
Configure ICMPv6 message sending

30.3 Configure basic IPv6 functions

30.3.1 Configure IPv6 unicast address

The IPv6 global unicast address is obtained by manual designation.

The IPv6 link local address is obtained in the following two ways:

- Automatic generation: When the VLAN port is up, the device automatically generates a link-local address for the interface based on the link-local address prefix (FE80::/10) and the link-layer address of the interface
- Manually specify: The user manually configures the IPv6 link local address.

command	description	CLI mode
ipv6 address <ipv6-address>/<prefix-length>	Specify the IPv6 address manually. By default, the link-local address is automatically generated based on the VLAN interface MAC address under the Layer 3 interface.	Configuration mode

30.4 Configuring IPv6 Neighbor Discovery Protocol

30.4.1 Configure the parameters of RA messages

Users can configure whether the interface sends RA messages and the time interval for sending RA messages according to the actual situation. At the same time, they can configure the relevant parameters in the RA messages to notify the host. When the host receives the RA message, it can use these parameters to perform corresponding operations. The parameters and meanings in the RA messages that can be configured are shown in Table 1-4.

Table 1-4 Parameters and description in RA message

parameter	description
Hop limit（Cur Hop Limit）	When the host sends an IPv6 packet, it will use this parameter value to fill the Hop Limit field in the IPv6 packet header. At the same time, the value of this parameter is also used as the value of the Hop Limit field in the response message of the device.
Prefix information（Prefix Information）	After receiving the prefix information issued by the device, the hosts on the same link can perform stateless automatic configuration and other operations.
Managed address configuration flag（M flag）	Used to determine whether the host uses stateful automatic configuration to obtain an IPv6 address. If this flag is set to 1, the host will obtain IPv6 addresses through stateful automatic configuration (such as a DHCP server); otherwise, it will obtain IPv6 addresses through stateless automatic configuration, which is based on its own link layer address and the prefix issued by the router The information generates an IPv6 address.
Other configuration flags（O flag）	It is used to determine whether the host adopts stateful automatic configuration to obtain other information except IPv6 address. If the other configuration flag is set to 1, the host will obtain other information besides the IPv6 address through stateful automatic configuration (such as a DHCP server); otherwise, it will obtain other information through stateless automatic configuration.
Router lifetime（Router Lifetime）	Used to set the time when the router that publishes RA messages serves as the default router of the host. Based on the value of the router survival time parameter in the received RA message, the host can determine whether to use the router that issued the RA message as the default router.

Neighbor request message retransmission interval（ Retrans Timer）	After the device sends an NS message, if it does not receive a response within the specified time interval, it will resend the NS message.
Time to keep neighbor reachable（Reachable Time ）	After the neighbor reachability check confirms that the neighbor is reachable, the device considers that the neighbor is reachable within the set reachable time; after the set time, if a packet needs to be sent to the neighbor, the neighbor is re-confirmed whether it is reachable.
Link maximum transmission unit(Link MTU)	The MTU option is used in the RA message to ensure that all nodes on the link use the same MTU value. It is mainly used when the node may not know 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 advertised by the router is limited to 64

Cancel the suppression of RA messages

Command：**ipv6 nd send-ra**

View mode：VLAN interface mode

Default configuration: By default, RA messages are suppressed

Configure the maximum and minimum time intervals for RA message publication

Command: ipv6 nd max-ra-interval value

View mode: VLAN interface mode

Default configuration: By default, the maximum interval for RA message publication is 600 seconds

Command: ipv6 nd min-ra-interval value

View mode: VLAN interface mode

Default configuration: By default, the minimum interval for RA message publication is 198 seconds

note：

- When RA messages are periodically released, the two adjacent time intervals are a value randomly selected between the maximum time interval and the minimum time interval as the time interval for periodically publishing RA messages.
- The configured minimum time interval should be less than or equal to 0.75 times the maximum time interval.

Configure prefix information in RA messages

Command：**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. In this case, the IPv6 address of the interface sending the RA message will be used as the prefix information in the RA message.

Set the managed address configuration flag

Command：**ipv6 nd managed-config-flag**

View mode: VLAN interface mode

Default configuration: By default, the managed address flag is 0, that is, the host obtains an IPv6 address through stateless automatic configuration.

Set other configuration flags

Command：**ipv6 nd other-config-flag**

View mode: VLAN interface mode
Default configuration: By default, the other configuration flag is 0, that is, the host obtains other information through stateless automatic configuration.

Configure the router lifetime in RA messages

Command：**ipv6 nd ra-lifetime** *value*

View mode: VLAN interface mode

Default configuration: By default, the router lifetime in RA messages is 1800 seconds.

Configure the neighbor request message retransmission interval

Command：**ipv6 nd base retrans-timer** *value*

View mode: configuration mode

Default configuration: By default, the interval for sending NS messages on an interface is 1000 ms.

Configure the retransmission interval of the router in RA messages

Command：**ipv6 nd retrans-timer** *value*

View mode: VLAN interface mode

Default configuration: By default, the value of the Retrans Timer field in RA messages issued by the interface is 0

Configure the time to keep the neighbor reachable

Command：**ipv6 nd base reachable-time** *value*

View mode: configuration mode

Default configuration: By default, the interface keeps the neighbor reachable for 30000 milliseconds.

Configure the time to keep the neighbor reachable
Command: ipv6 nd reachable-time value
View mode: VLAN interface mode
Default configuration: By default, the value of the Reachable Timer field in RA messages posted by the interface is 0.

Configure the link MTU size
Command: ipv6 nd link-mtu value
View mode: VLAN interface configuration mode
Default configuration: By default, the value of the link mtu field in RA messages published by the interface is 0.

When the source host sends a message from the interface, it will compare the MTU and Link MTU of the interface. If the length of the message is greater than the minimum value of the two, the minimum value will be used to fragment the message.

30.4.2 Configuring the Number of Times to Send Neighbor Solicitation Messages for Duplicate Address Detection

After the interface obtains the IPv6 address, it will send a neighbor request message for duplicate address detection. If it does not receive a response within the specified time (configured by the ipv6 nd retrans-timer command), it will continue to send the neighbor request message. After the set number of times, if no response is received, the address is considered available.

command	description	CLI Mode
ipv6 nd dad attempts <value>	By default, the number of neighbor request messages sent during duplicate address detection is 1. When the value is 0, it means that	Configuration mode

	duplicate address detection is prohibited.	

30.5 IPv6 static routing configuration

Command	description	CLI mode
ipv6 route <X:X::X:X/M> (<X:X::X:X> | <ifName>) <distance>	Configure IPv6 static routing.	Configuration mode

30.6 IPv6 display and maintenance

After completing the above configuration, execute the show command in the privilege view to display the running status of IPv6 after the configuration, and verify the effect of the configuration by viewing the displayed information.

Command	description	CLI mode
show ipv6 ndp nc	Display neighbor information.	Privileged mode
show ipv6 interface (<ifName>) brief	Display IPv6 information of interfaces that can be configured with IPv6 addresses	Privileged mode
show ipv6 route (database)	Show IPv6 routing	Privileged mode

Chapter 31 POE Configuration

The switch supports the POE function, mainly including the following content：

- POE introduction
- Configure POE

31.1 Introduction to POE

PoE (Power over Ethernet, also known as remote power supply) means that the device uses a twisted pair to connect to an external PD (Powered Device) device (such as an IP phone, wireless AP, network camera, etc.) through an Ethernet interface) Remote power supply.

1、Advantages of PoE

- ✧ Reliable: centralized power supply, convenient backup
- ✧ Network terminal does not need external power supply, only one network cable
- ✧ Standards: Complies with IEEE 802.3af and 802.3at standards and uses a globally uniform power interface
- ✧ Wide application prospects: can be used for IP phones, wireless AP (Access Point,

access point), portable device chargers, credit card machines, network cameras, data collection, etc.

2、POE system composition

- ✧ PoE system includes PoE power, PSE and PD
- ✧ PoE power supply
- ✧ PoE power supply for the entire PoE system, divided into two types of external power supply and internal power supply
- ✧ PSE
- ✧ PSE (Power Sourcing Equipment) is a single board (daughter card). Each PSE independently manages the PoE interface in the board (subcard). The PSE finds and detects PD on the line of the PoE interface, classifies the PD, and supplies power to it. When the PD is detected to be unplugged, the PSE stops supplying power. The Ethernet interface with PoE power supply capability is called PoE interface, including FE and GE.
- ✧ PD
- ✧ PD is a device that receives power from PSE. Divided into standard PD and non-standard PD, standard PD refers to the PD equipment that complies with IEEE 802.3af and 802.3at standards. While receiving power from the PoE power supply, PD devices are allowed to connect to other power supplies for power redundancy backup.

31.2 Configuring POE

The POE configuration content includes the following three parts:

- Manual POE configuration
- POE policy configuration
- PD query configuration

31.2.1 Manual POE Configuration

The commands for manual POE configuration are as follows：

- Turn on or turn off the interface power supply
- Display POE information

command	description	CLI mode
[no] poe enable	Turn on or turn off the power supply of the interface POE. By default, the power supply state of the interface is on.	Interface configuration mode
show poe	Display POE information of all interfaces.	User mode or privileged user mode

31.2.2 POE policy configuration

The commands for POE policy configuration are as follows：

- Open or close the POE policy of the interface

- Set the POE policy entry for the interface
- Display POE strategy information

Command	description	CLI Mode
[no] poe policy enable	Open or close the interface POE strategy, the default interface POE strategy is closed.	Interface configuration 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. By default, no POE policy entry is set. clock-value is time or time range, 24-hour system, if the value is 1, it means 1 o'clock (that is, between 1 o'clock and 2 o'clock), 20-23 means 20 o'clock to 23 o'clock (that is, between 20 o'clock and 0 o'clock) . The day-value is the day of the week, which means a certain day or a certain number of consecutive days, such as 3 means Wednesday, and 1-7 means Monday to Sunday. The POE strategy can only take effect if the interface's POE strategy is enabled.	Interface configuration mode
show poe policy <if-name>	Display POE policy information of an interface	User mode or privileged user mode

31.2.3 PD query configuration

The PD query configuration commands are as follows:

- Set the IP address of the PD
- Set the time interval for querying PD
- Set the timeout for querying PD
- Set PD start time
- Display PD information

Command	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 the PD	Interface configuration mode

	is configured, the system will periodically query the IP address. If the PD does not respond within a given number of times, it will restart the PD through POE control.	
poe pd-query-interval <interval> no poe pd-query-interval	Set the interval for querying PD. The default interval for querying PD is 5 seconds.	Interface configuration mode
poe pd-timeout-number <number> no poe pd-timeout-number	Set the timeout times for querying PD. The default timeout times for querying PD is 3 times.	Interface configuration mode
poe pd-boot-time <time> no poe pd-boot-time	Set the PD startup time. The default PD startup time is set to 120 seconds.	Interface configuration mode
show poe pd-information	Display information about all configured PDs	User mode or privileged user mode