
ovolink

User Manual

OL- S3000 series

Version1.0

ovolink

Content

Chapter1 Introduction	8
Chapter2 Product Overview	9
Chapter3 Configuration Preparation	10
3.1 Web Interface Access	10
3.2 WEB configuration interface	11
3.2.1 System Management Interface	11
3.2.2 Common Icon	13
3.2.3 Save Configuration	13
3.2.4 Logout Web configuration interface	14
3.2.5 Web Timeout	14
Chapter4 System Management	14
4.1.1 Overview	14
4.1.2 Check system information	15
4.1.3 Configure system name	15
4.2 Device reboot	15
4.2.1 Overview	15
4.2.2 Reboot device	16
4.3 Software Upgrade	17
4.4 Date and Time	19
4.4.1 Overview	19
4.4.2 Manage System Time	19
4.5 SNMP	21
4.5.1 Overview	21
4.5.2 SNMP Settings	21
4.5.3 SNMP Group Settings	23
4.5.4 SNMP User Settings	24
4.5.5 TRAP settings	25
Chapter 5 Device Management	26

5.1 User management.....	26
5.1.1 Overview	26
5.1.2 User Accounts	27
5.1.3 User verify.....	28
5.1.4 Login Time.....	29
5.2 Configuration Management.....	29
5.2.1 Overview	29
5.2.2 Restore factory settings.....	30
5.2.3 Export configuration	31
5.2.4 Configuration import.....	31
5.2.5 Save configuration	32
Chapter6 Switch Management.....	33
6.1 Port Management	33
6.1.1 Port settings.....	33
6.1.2 Port Mac Limit.....	35
6.1.3 Port Statistic	37
6.2 VLAN	38
6.2.1 Overview	38
6.2.2 Create VLAN	39
6.2.3 Access VLANs.....	40
6.2.4 Trunk VLANs	41
6.2.5 Hybrid VLANs.....	42
6.3 MAC setting	43
6.3.1 Overview	43
6.3.2 Dynamic Address	44
6.3.3 Static Address.....	45
6.3.4 Blackhole Address	45
6.3.5 Dynamic Address Aging Time	46
6.4 Quality of service.....	47
6.4.1 Overview	47
6.4.2 QOS.....	47
6.4.3 Port Line rate.....	48

6.5 Multicast IGMP snooping	49
6.5.1 Overview	49
6.5.2 Global Settings	50
6.5.3 VLAN setting	50
6.5.4 Interface Setting	52
6.5.6 IGMP Router Port Table	54
6.6 Link Aggregation	54
6.6.1 Overview	54
3.6.1 LAG management	55
6.6.3 LAG setting	57
6.6.4 LACP	58
6.7 Spanning Tree	59
6.7.1 STP Status and Global Settings	59
6.7.2 STP Status and Global Settings	61
6.7.3 STP interface Settings	62
6.7.4 RSTP interface Settings	64
6.7.5 MSTP properties	66
6.7.6 VLAN to MSTP	67
6.7.7 MSTP Instance Settings	68
6.7.8 MSTP Interface Settings	69
6.8 ERPS	72
6.8.2 ERPS Global Settings	73
6.8.2 Ring Setting	74
Chapter 7 Route Management	76
7.1 Virtual port	77
7.1.1 overview	77
7.1.2 Virtual Interface Settings	77
7.2 ARP Management	78
7.2.1 Overview	78
7.2.2 ARP properties	79
7.2.3 Dynamic ARP	79
7.2.3 Static ARP	80

7.3Route Table Management.....	81
7.3.1 Overview	81
7.3.2Direct Table.....	82
7.3.3 Dynamic Table.....	82
7.3.4 Static Route Table	83
7.3.5 Blackhole Table	84
7.3.6 Reject Table	85
7.4 OSPF Management	86
7.4.1 Overview	86
7.4.2 OSPF setting.....	87
7.4.3 OSPF Setting	88
7.4.4 OSPF area	88
7.4.5 OSPF status	89
7.4.6 OSPF Neighbor	90
7.5 RIP Management.....	91
7.5.1 Overview	91
7.5.2 RIP Status setting.....	91
7.5.3 RIP Settings.....	92
7.5.4 RIP neighbor	92
Chapter 8 Network Security.....	93
8.1 Broadcast Storm Suppression	93
8.1.1 Overview	93
8.1.2 Storm Control.....	93
8.2 IP Source Guard	94
8.2.1 Overview	94
8.2.2 Interface Setting	95
8.2.3 Binding Database.....	95
8.3 DHCP Snooping	97
8.3.1 Overview	97
8.3.2 Global settings	98
8.3.3 Interface setting	99
8.3.4 Snooping Bind Table	100

8.4 DHCP RELAY	102
8.4.1 Overview	102
8.4.2 Global setting	102
8.4.3 DHCP Relay Vlanif set	103
8.4.4 Snooping Bind Table	105
8.5 DHCP SERVER	105
8.5.1 Overview	105
8.5.2 Global setting	106
8.5.3 IP Resource Pool	107
8.5.4 Static binding configuration.....	109
8.5.5 Snooping Bind Table	110
8.6 ACL	111
8.6.1 Traffic Setting	111
8.6.2 MAC-Based ACL	114
8.6.3 MAC based RULE	115
8.6.4 IPv4-Based ACL.....	118
8.6.5 IPv4 Based RULE	119
8.6.6 IPv6 Based	121
8.6.7 IPv6 Based Rule.....	122
8.7 POE	125
8.7.1 Overview	125
8.7.2 PoE configuration	126
8.7.3 POE status	129
Chrpter9 Maintenance diagnosis.....	130
9.1 System log	130
9.1.2 Log Setting	131
9.1.3 Check log	132
9.2 Port Maintain	133
9.2.1 Overview	133
9.2.2 Mirror	133
9.3 LLDP	135
9.3.2 Global setting	136

9.3.3 Port Settings	137
9.3.4 LLDP Local information	139
9.3.5 LLDP Neighbor.....	140

oVolink

Chapter1 Introduction

Thanks for purchasing OL-S3000 series full gigabit management switch. This series of switches could provide visualized security configuration system with superior performance. It is web management interface easily, supports IEEE802.3AF/AT self-adaptive standard POE power supply and mandatory power supply for non-standard POE device. Multiple ports are suitable for all scenarios and semi-industrial network application. It's an ideal choice for built security and efficiency network.

This manual aims to help you use the switch correctly. It will guide you to manage OL-S3000 series ethernet switch on web interface.

The information in this document is subject to change due to product upgrading or other reason without notice. Our company reserve the right to modify and explain the manual's content. The manual is only used as guide. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information and recommendations in this document do not constitute the warranty of any kind, express or implied.

Chapter2 Product Overview

OL-S3000 series full Gigabit management ethernet switch, which provides higher, reliable and easy install network environment. Multiple ports are suitable for various scenarios and large-scale industrial network application. The switch adopts new energy-saving chipset and initiative structure design, realize connect gigabit switch's lowest energy consume, provide user a green, environment-friendly, energy-efficient new network access facility

OL-S3000 series support multiple routing management modes, such as multi-IP interface management, DHCP SNOOPING, DHCP server, OSPF, RIP, static routing, etc. The Layer2 series supports ERPS redundant ring network protocol (self-healing time < 20ms, ITU-based G.8032), MSTP, RSTP, STP, port broadcast storm suppression, multicast filtering, IGMP SNOOPING, IGMP SNOOPING. IEEE802.1Q VLAN, port priority, port mirror, quality of service, rate control, fault alarm and firmware online upgrade functions.

Chapter3 Configuration Preparation

This chapter including following content:

- Login WEB
- WEB configure interface
- Current configure information

Accessing the switch

3.1 Web Interface Access

The web interface is accessible through the web-based authentication.

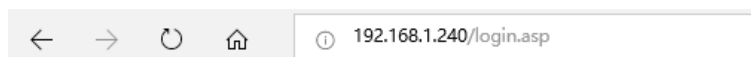
Login Web

Default IP address is **192.168.1.240**. Before login, please make sure the following points:

- (1) Management PC's IP address could ping switch's IP address;
- (2) Make sure that the route between the host PC and the switch is available. Neither aggregate port nor ERPS port/other blocking ports;
- (3) Web browser should be IE8 or above.

Login steps

- (1) Launch a web browser
- (2) Enter the switch's IP address in the web browser's address bar. The switch's default IP address is **192.168.1.240**.



(3) Enter the username and password in the pop-up login window. Use **admin** for both username and password in lower case letters.

- (4) Click <login> to enter Web configuration interface

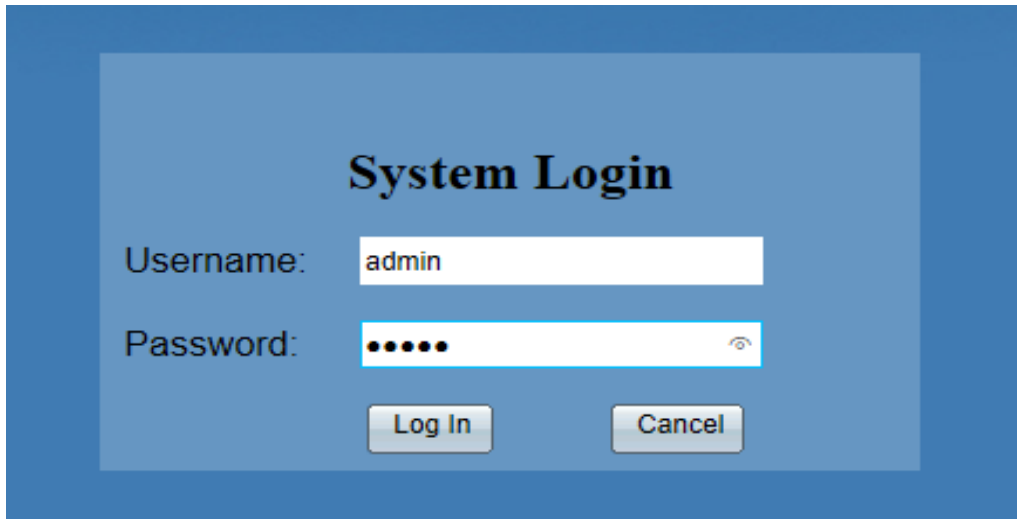


Figure3-1 of Web Login interface's config description

Table3-1 Web login interface description.

Title	Description
username	Login by enter username. By default, username is admin
password	Enter login password. By default, username is admin
Language	Interface display in English Note: current support English only

5) The typical web interface displays below. You can view the switch's running status and configure the switch on this interface

3.2 WEB configuration interface

3.2.1 System Management Interface

Refer to figure 3-2.

System Information

Version Information

Software Version: OL-GS3428CP-4CV1.0.2

Hardware Version: VER.A

Bootrom Version: GS3428CP-4C_UBOOTV1.3

System Name: SWITCH (1~32 Characters)

Serial Number: 01010120N00B300108

MAC Type Address: 00:17:73:A0:09:D5

System Runtime: 0 day 0 hour 20 minutes 20 sec

Apply Cancel

Figure 3-2 System Information Interface

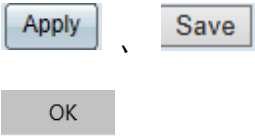


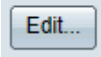
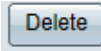
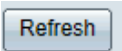
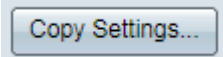




Table 3-2 WEB configuration interface description

No.	Name	Description
1	Navigation bar	Menu bar could direct to any of created configured interface.
2	Selected page	Current location of config interface in the navigation bar
3	Config interface	Main interface needs to configure
4	Interface management function	<ul style="list-style-type: none"> ➤ Current user: Display current username ➤ Save: Save current configuration to config files. Remain same color display no configuration need to be saved. Configuration need to be saved for color flashing display. ➤ Logout: Single click to logout web management interface


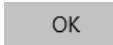

3.2.2 Common Icon

Common icon description, see table3-3 below:

Table 3-3 Common icon description

Button	Description
	Click to take effect.
	Click to cancel current config content, make page jump to corresponding list display page
	Click to go create pages
	Click to edit page
	Click to delete selected items in the list
	Click to refresh current page information
	Click to go copy config page
	Click to jump to Home page
	Click to jump to the previous pages
	Click to jump to the next page
	Click to jump to the last page

3.2.3 Save Configuration

- (1) When current configuration completed, click  to enter system. Save in memory but not save to config files. Before device power off or reboot, click  to save new operations.
- (2) Click  when current config completed.

3.2.4 Logout Web configuration interface

Save changes when configuration completed to avoid config lost. Then logout Web config interface.

Close browser directly can't logout Web interface. User could login Web interface directly if not timeout.

3.2.5 Web Timeout

The system will logout automatically if users do nothing on Web during session timeout. After time out, if user want to do any operation for Web config interface, system will remind and return login window. To continue operation, it must login again.

Note: By default, Web time out session is set as 10 minutes. Support configure timeout time. Details refer to Chapter5.1.4.

Chapter4 System Management

In System management module, the system information can be viewed, and the system parameters and features of the switch can be configured.

4.1.1 Overview

System module shows the current system software and hardware version, bootrom version, system name, device serial number, MAC address, and system operation time.

Besides, could config system name

Version Information	
Software Version:	ES2428C-4CV1.0.2
Hardware Version:	VER.A
Bootrom Version:	ES2428C-4C_UBOOTV1.3
System Name:	<input type="text" value="SWITCH"/> (1-32 Characters)
Serial Number:	01010115N00B300084
MAC Type Address:	00:17:73:A0:08:EB
System Runtime: 0 day 0 hour 13 minutes 21 sec	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Figure 4-1 Supported Features System Info

Port status, system information, device description configuration, system time and daylight-saving time showed in this window.

User account can be managed for login the switch. Multiple access levels are ready to create different user accounts per needed.

To configure the boot file of the switch, backup and restore the configurations, update the firmware, reset the switch and reboot the switch can be operated on System Management page.

4.1.2 Check system information

Select 'System Management > System information' in the navigation bar to enter the interface showed on Table 4-1.

Table4-1 System information description

Title	Description
Software version	Displays the current Software version of the device.
Hardware version	Displays the current hardware version of the device
Bootrom version	Device software's Bootrom version
System name	System name
Serial Number	Serial number of the device
MAC address	MAC address of the device
System run time	Elapsed time since last reboot

4.1.3 Configure system name

Select 'System management >System information' in the navigation bar to enter the page.

'System name' configure parameter:

Length:1-32 characters

Parameter requirement: A~Z, a~z, _, -,

4.2 Device reboot

4.2.1 Overview

Device can be rebooted by Web access. Login after reboot the device. Some modified configuration will take effect only after device reboot. Reboot the switch could delete operation config therefore it's very important to SAVE operation modifications before reboot. Click '**Apply**' will NOT save operation config before reboot.

4.2.2 Reboot device

1. In the navigation bar, Select 'System management' > 'Device Reboot', open 'Reboot' page.

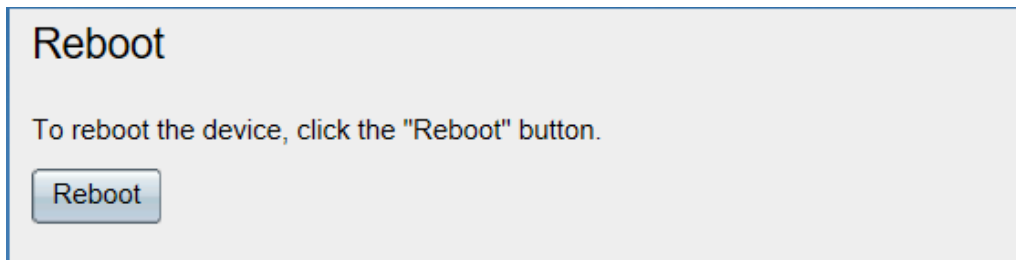


Figure 4-2 System reboot page

Click '**Reboot**', the dialog box 'Are you sure to reboot the device' will pop-up.

Click '**OK**' to confirm reboot the device, then jump to reboot progress page.

Click '**Cancel**' to not to reboot the device. Reboot progress as shown in figure4-4

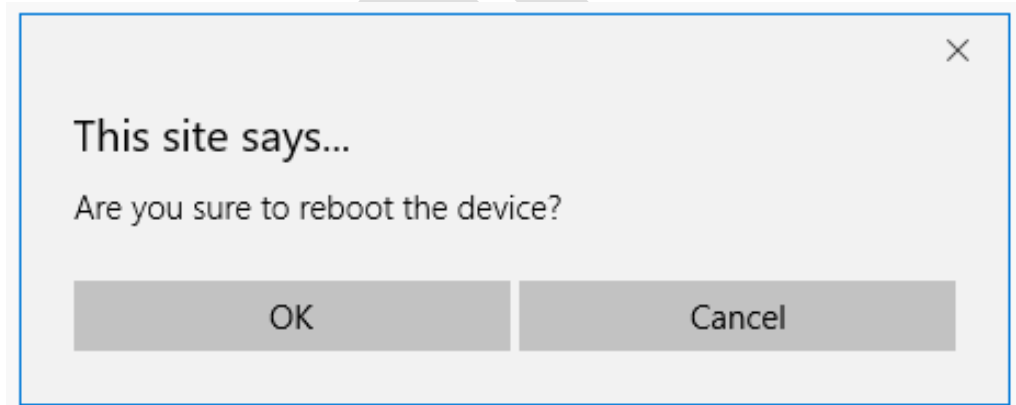


Figure4-3 'Are you sure to reboot the device' dialog box'

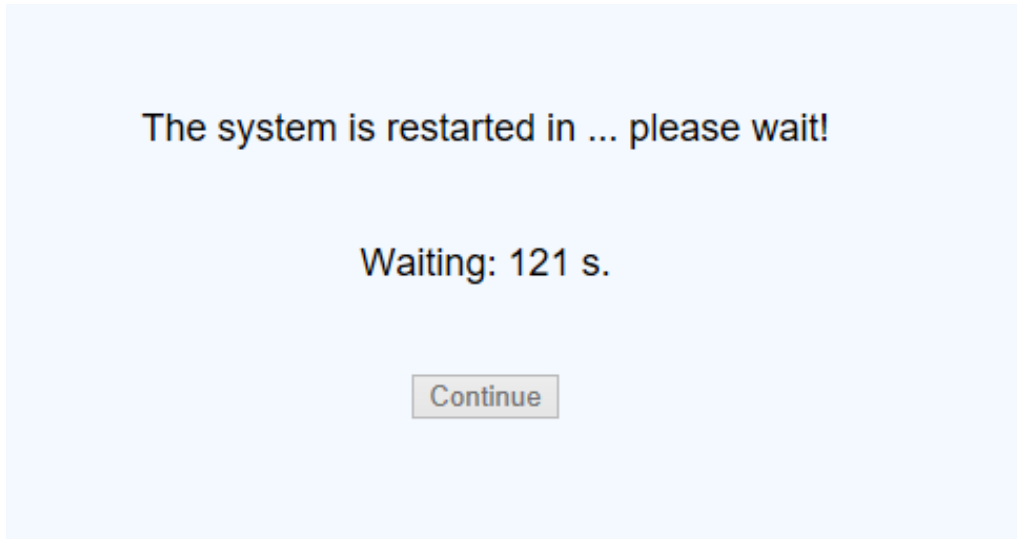


Figure 4-4 Reboot Progress

4.3 Software Upgrade

Web management has the function to upgrade device software on-line easily.

Follow these steps to upgrade the Software of the switch:

Select 'System management' > 'Software Upgrade' in the navigation bar to enter 'Software upgrade' page. As shown in figure 4-5.

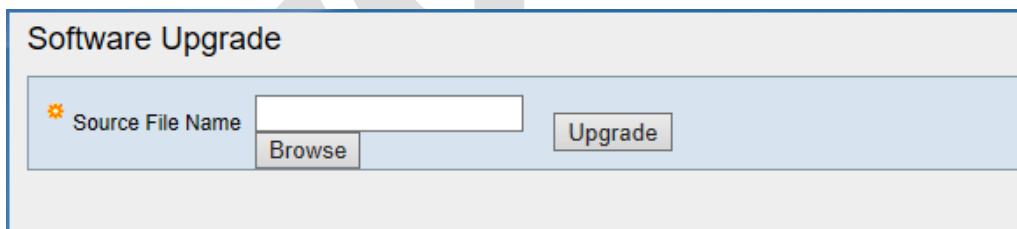


Figure 4-5 'Software Upgrade'

Click '**Browser**' in 'software upgrade' interface. Select the software need to import (format at **.bin**). Click '**upgrade**' to pop up the dialog box to confirm the restart of the device. As shown in figure 4-6.

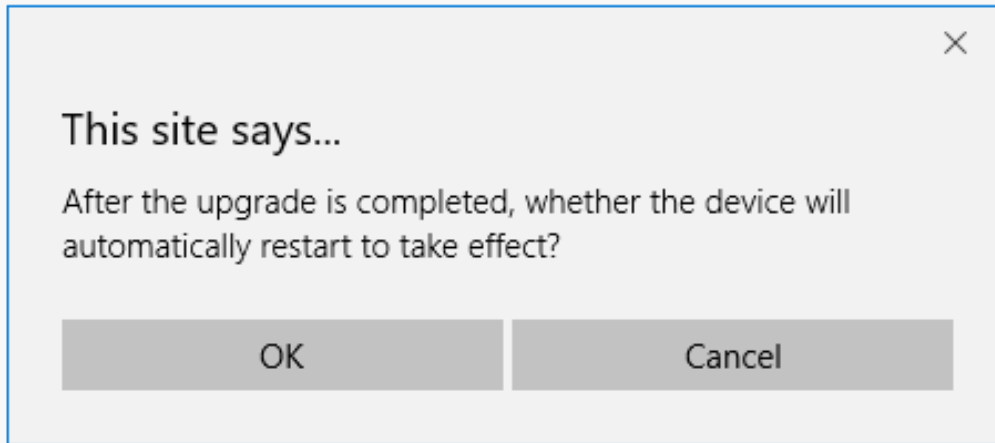


Figure 4-6 Whether reboot dialog box

Select '**OK**' to reboot automatically after the upgrade is completed and system will upgrade to new software.

Select '**Cancel**' to cancel the reboot automatically. Existing operating software is at its old version. Reboot the device to make sure to upgrade to new software version.

Click '**OK**' on dialog box. A notice will pop up to remind user do not turn off power and wait patiently. As shown in figure4-7.

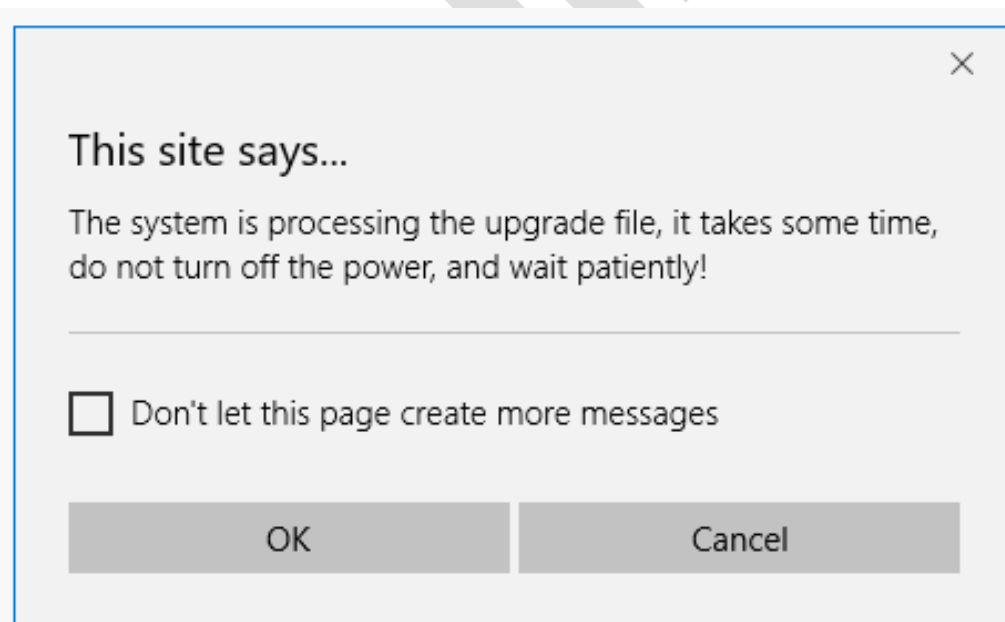


Figure 4-7 Upgrading notice

Note: If Select '**Yes**', it will start upgrade. If Select '**Cancel**', upgrade will be canceled.

Click '**Yes**' start to upgrade and jump to progressing page, as shown in figure4-8.

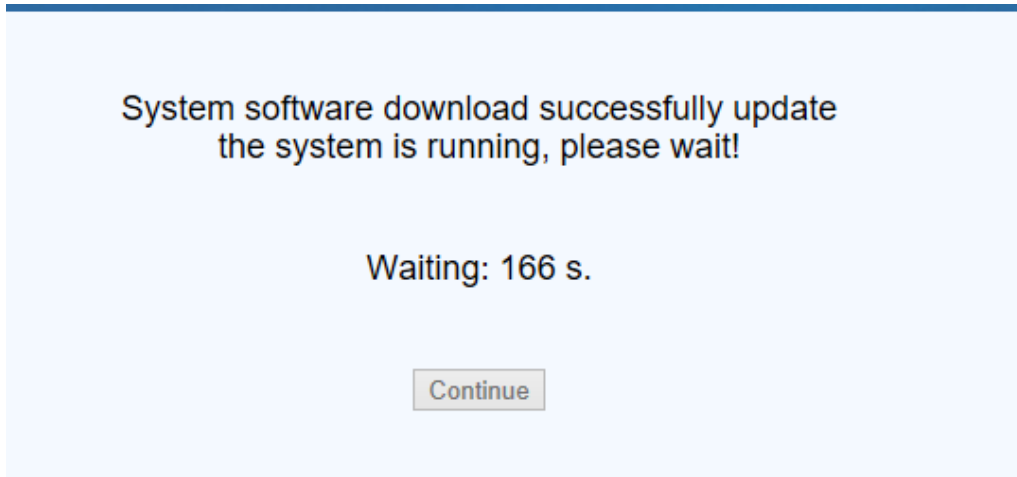


Figure 4-8 Software upgrade progress page

Device will reboot once upgrade complete.

Note:

- *It will take some time to upgrade the switch. Please wait without any operation.*
- *It is recommended to back up your configuration before upgrading.*

4.4 Date and Time

4.4.1 Overview

In order to ensure the device coordinate with the other devices, system date and time need to configure. System date and time module could configure system date, time and time zone...etc. System support configuration manually and NTP (Network Time Protocol) server's time.

Specific to the situation that there are many devices in the networks, it's impossible to configure each device's system time manually to ensure the consistency and accuracy. Use NTP could synchronous time of server and client, keep the time of all the devices in the network consistent and accurate, enable device to provide a variety of applications based at same time.

4.4.2 Manage System Time

Choose 'System Management' > 'System Time' in the navigation bar to enter System Time config interface, as shown in figure4-9.

Figure 4-9 System time support manual configuration and NTP synchronous.

(1) Manual set time:

- Do not check the box in front of 'NTP Synchronous'. In 'Time setting' session select correct date (Year/Month/Day) and time (Hour/Minutes/Second).
- 'Local time' could set local time.
- Click 'Apply'.

(2) NTP synchronous :

- Check the box in front of 'NTP synchronous'.
- Configure NTP server's IP address.
- Click 'Renew Now' button. In 'Local Time' session, you can view synchronous success and show the system time after synchronizations.

Table4-2 System time management description

Title	Description
Local time	Display real system time
Synch State	Display whether system time synchronous with NT. If manual time configuration failed or NTP synchronous failed, it will show 'Synchronous fail'
Time Zone	Set system time zone. Select any one of time zone from drop-down list
NTP synchronous	Set system time by SNTP Server synchronous
NTP server address	Set NTP server IP address
Update cycle	Synchronizing Cycle from system to SNTP server
Time setting	To set time manually, Year range at 1970~2037.

4.5 SNMP

4.5.1 Overview

SNMP (*Simple Network Management Protocol*) is a standard network management protocol, widely used on realize access and manage devices by programed device.

1.SNMP working mechanism

SNMP system consists of NMS (Network Management System) and Agent factors.

NMS is SNMP system's manager with user friendly design. To facilitate network administrators to complete most of the network management work.

Agent is a subordinate of SNMP network, responsible for receiving, progressing requests from NMS. Agent will actively send alert information to NMS in certain situations, such as port state changed.

Attention is needed to some parameters when NMS manage device, such as port state, CPU usage rate. These parameters are called MIB (Management information Base). Each Agent has its own MIB. Managed device has its own MIB file. Compile these MIB files will generate the device's MIB. NMS read/write MIB code according to visit its limit in order to realize Agent's management.

2.SNMP Version

Right now, Agent supports three versions: SNMPv1、SNMPv2c and SNMPv3.

SNMPv1 adopts Community Name authentication mechanism. Community Name can be used as password to limit communication between NMS and Agent. If Community Name set by NMS are different with the name of the managed device, NMS and Agent is not able to set up SNMP communication.

SNMPv2c adopts Community Name authentication mechanism. SNMPv2c expand SNMPv1's function: provide more operating types, support more data types, provide error codes to distinguish errors particularly.

SNMPv3 adopts USM (User-Based Security Model) authentication mechanism. Network administer could set authentication and encryption. Authentication use to verify legacy of the message sender to avoid illegal user visit. Encryption specific to the message between NMS and Agent communication.

4.5.2 SNMP Settings

Select 'System management>SNMP>SNMP Settings' in the navigation bar to enter 'SNMP setting interface. As shown in figure 4-10

The image shows the 'SNMP Settings' configuration interface. It includes the following fields and options:

- SNMP Status:** A dropdown menu currently set to 'close'.
- Engine ID:** A text input field containing '80001f88803cd4279a386d4384' with a note '(10-31 Characters)'.
- Max Message:** A text input field containing '1500' with a note '(1500-64000 Bytes)'.
- Location Information:** A text input field containing 'China' with a note '(1~80 Characters)'.
- Contact Information:** A text input field containing 'RD' with a note '(1~80 Characters)'.
- SNMP Version:** Radio buttons for 'v1', 'v2c' (which is selected), and 'v3'.
- Trust Host:** A text input field containing 'default' with a note '(For example: 192.168.0.100, or "default" mean every host)'.
- New Communities:** An unchecked checkbox.
- Communities:** Two radio buttons: 'Standard Communities' (selected) with a dropdown menu showing 'public', and 'User Defined' with a text input field and a note '(1~32Characters)'.
- Access Mode:** A dropdown menu currently set to 'Read Only'.

Figure 4-10 SNMP Setting interface

- (1) SNMP setting interface displays current SNMP setting situation.
- (2) Modify setting parameter. Click <Apply> to complete modification. Details show in following table.
- (3) Click 'Delete' to delete corresponding Community Name

Table 4-3 SNMP setting config description

Title	Description
SNMP Status	Enables SNMP on the switch. (Default: Close) > Open: Open SNMP function > Close: close SNMP function
SNMP Engine ID	Set SNMP engine ID SNMP Engine ID is the unique identifier for managing SNMP modules. It uniquely identifies an SNMP entity in an administrative domain. By default, device generate an SNMP engine ID automatically by using internal algorithm.
Maximum Packet Message	Set SNMP packet's maximum length
Location Information	Display location information
Contact Information	Display maintenance information
SNMP version	Select SNMP versions, support v1、v2c and v3

Trusted Host	<p>Configure Trusted Host.</p> <p>Host IP address: Authorized the host access and manage the device only.</p> <ul style="list-style-type: none"> ➤ Default : Authorized all hosts access and manage device
New Communities	Create new community
Communities Group	<p>Configure new community name</p> <ul style="list-style-type: none"> ➤ Standard communities: Public or private Default strings optional: 'public' (Read-Only), 'private' (Read/Write) ➤ User defined : Support user defined communities, request 1-32 byte. <p>Communities group device (SNMPv1 and SNMPv2 support), it is a kind of interface used for managing multiple devices in reading and writing. This parameter should be the same as network management configuration.</p>
Access Mode	<p>Config new community's access mode.</p> <ul style="list-style-type: none"> ➤ Read only ➤ Read and Write

4.5.3 SNMP Group Settings

Click 'System Management > SNMP > SNMP Group Settings' to enter 'SNMP Group settings' Interface. As shown in figure 4-11.

Group Name	Security Level	Access Mode	Delete
group0	No Authentication No Privacy	Read Write	Delete

Figure 4-11

- 'SNMP group setting' displays current created SNMP groups.
Create SNMP group on 'SNMP group setting' interface
- Configure SNMP group parameter to detail parameter show in below table.
Click <Apply> complete creating SNMP group
- Delete SNMP group on 'SNMP group setting' interface.
Click <delete> to delete corresponding SNMP group.

Table 4-4 SNMP Group Configuration

Title	Description
Group Name	Configure the name of the SNMPv3 group to which the user is assigned. (Range: 1-32 characters)
Security Level	Select SNMPv3 security level in three ways: <ul style="list-style-type: none"> No Authentication No Privacy : no authentication or encryption used in SNMP communications. (This is the default security level.) Authentication No Privacy: use authentication, but the data is not encrypted Authentication Privacy: use both authentication and encryption
Access mode	Configure the access mode for the group <ul style="list-style-type: none"> ➤ Read only ➤ Read and Write

4.5.4 SNMP User Settings

Select 'System Management > SNMP > SNMP User Settings' to enter 'SNMP user' interface, as shown in figure 4-12.

Figure 4-12

- 'SNMP user' interface displays all the user's information:
- To create user
 - Set SNMP user's parameter, details configuration show in following table.
 - Click <Apply> to complete the operation of creating SNMP user.
- In 'SNMP user' interface delete SNMP user
 - Click <Delete> button to delete SNMP user

Table 4-5 SNMP config description

Title	Description
SNMP Username	Config the username of SNMP
Security Level	Select user security level
Group Name	Select binding user group (for groups at the same security level can be selected)
Authentication Mode	Default: MD5
Authentication Password	Set authorization password when security level supports.
Confirm Authentication Password	Enter same password again to confirm authentication password.
Privacy Mode	Default: DES encryption mode
Privacy Password	Set privacy password when security level supports.
Confirm Privacy Password	Enter same password again to confirm privacy password.

4.5.5 TRAP settings

Select 'system management >SNMP>TRAP setting' to enter 'TRAP setting' interface. As shown in figure4-13.

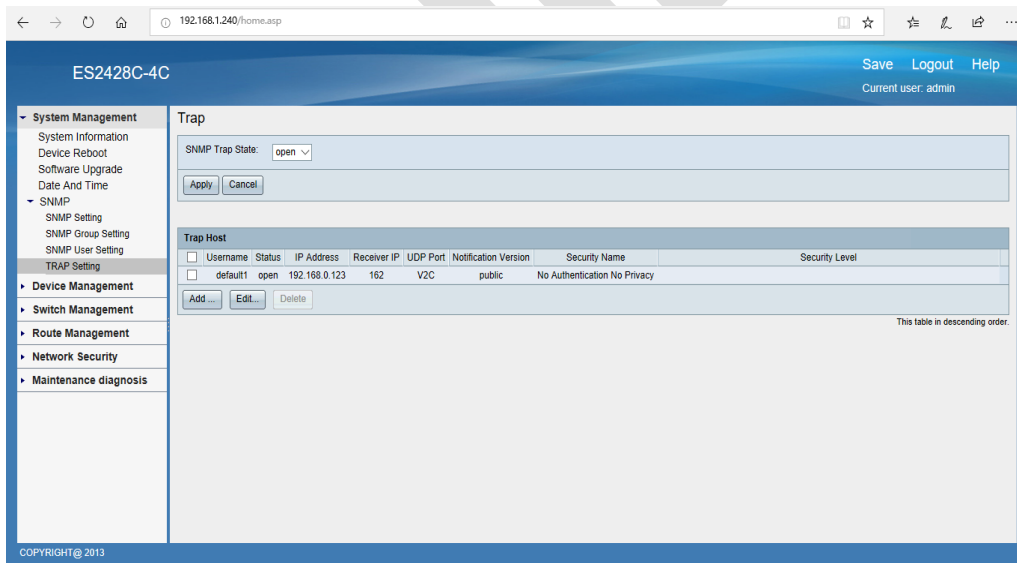


Figure4-13

- View and set SNMP TRAP global status on 'TRAP setting' interface. Select 'Open' or 'Close' in drop-down list, click <Apply> to complete operation.
- Add TRAP host on 'TRAP setting' interface. In 'Trap host' list, click <Add> to enter TRAP host interface, as shown in figure 4-14.
- Configure Trap host parameter, details shown in following table4-6. Click <Apply> to complete operation

- Support modify trap host on 'Trap setting' interface.
Select the trap that needs to modify in the 'Trap host 'list. Click< **Edit**> to enter host interface. As shown in figure4-14.
- Modify trap host's parameter. Details as show in following table.
Click <**Apply**> to complete operation
- Support delete trap host on 'Trap setting' interface.
Select the trap that needs to delete in the trap host list. Click< **Delete**> to complete operation

Figure 4-14

Table4-6

Title	Description
Username	Set Trap username
SNMP Trap State	Set SNMP trap state
Receiver IP	Set TRAP server's IP address.
UDP Port	Set the UDP port number
Notification Version	Notification version Default: v2
Security Name	Select community Name from created community names by drop-down list. The information of all created communities name can view in 'SNMP setting'.
Security Level	Default at no Authentication No Privacy.

Chapter 5 Device Management

5.1 User management

5.1.1 Overview

In order to maintain customer's information. Web manager provides the function of add user, change password and delete users.

5.1.2 User Accounts

With User Management, you can create and manage the user accounts for login to the switch.

Select 'system management >device management>user management' on the left of the interface to enter the page as show in figure 5-1. On the page, it displays all the user list.

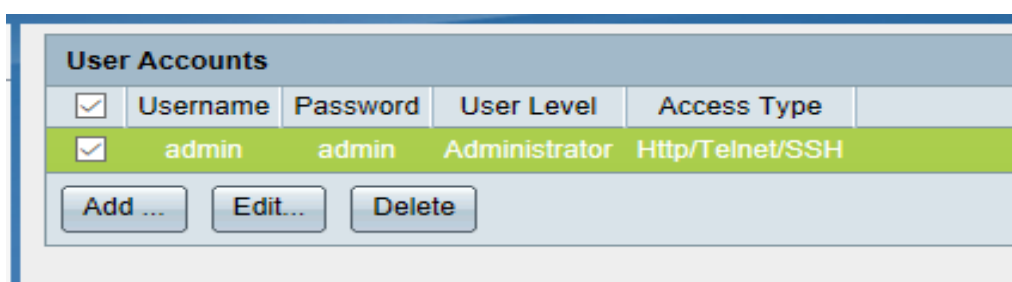


Figure 5-1 User Accounts

Click<Add> to enter the config page to create new user account.

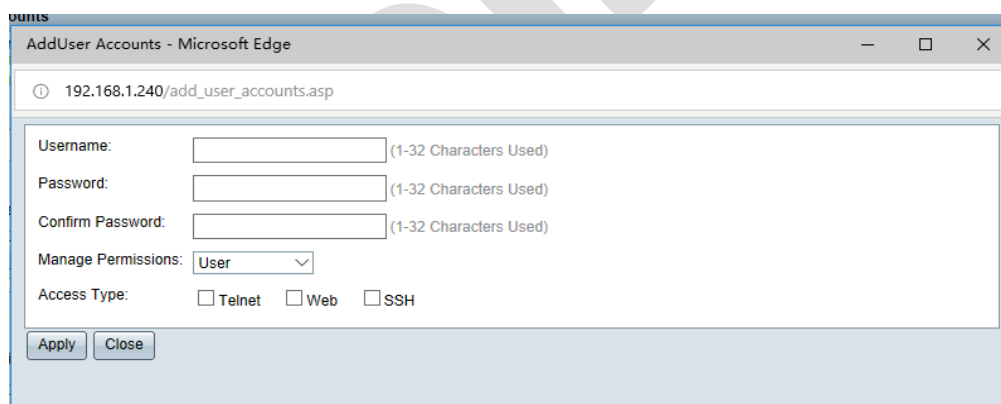


Figure 5-2 Add user accounts

Check the check box in front of username, click<Edit> to enter the page of edit user account.

Users' information including user password, manage permission and access type can be modified on Edit user account page as shown in figure5-3.

The screenshot shows a web browser window titled "AddUser Accounts - Microsoft Edge" with the address bar displaying "192.168.1.240/edit_user_accounts.asp". The main content area contains a form with the following fields:

- Username:** Input field containing "admin" with a note "(1-32 Characters Used)".
- Password:** Input field containing "admin" with a note "(1-32 Characters Used)".
- Confirm Password:** Input field containing "admin" with a note "(1-32 Characters Used)".
- Manage Permissions:** A dropdown menu currently set to "Administrator".
- Access Type:** Three checkboxes: Telnet, Web, and SSH.

At the bottom of the form, there are two buttons: "Apply" and "Close".

Figure 5-3 Edit user accounts

- Check the check box in front of user list, click <delete> to delete user.
- Admin account in the table by default. It can be edited but not deleted.
- Real-time login user cannot be deleted. Details config description show in table 5-1

Table5-1 Config User account

Title	Description
Username	Username
Password	User's login password
Confirm password	Specify a password for the account which contains 1-32 alphanumeric characters or symbols, compose of digits, English letters (case sensitive). Configured password and confirmed password must be same.
Manage Authentication	To configure user authorization, select admin or common user by drop-down list Admin: High level, implements all operations, including edit, modification and view all the settings of different functions. Common user: Low level, view the settings without the right to edit.
Access Type	Configure the type that user could access device. Telnet、WEB、SSH Optional.

5.1.3 User verify

Select 'Device management>user management' on the left side in the navigation bar to enter user management interface. Enable or disable the Telnet user verify and Web user verify as shown in figure 5-4.

Click <Apply> to send user verification configuration. Click <Cancel> to cancel user modification.

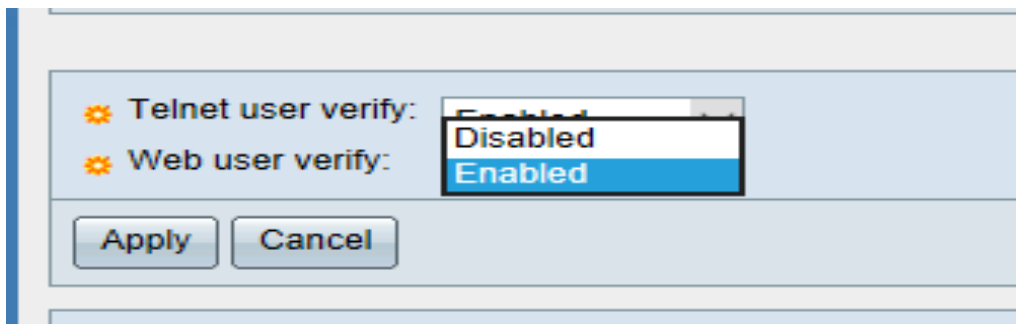


Figure 5-4 User verify interface

5.1.4 Login Time

Select 'Device management>user management' on the left of the navigation bar to enter user management interface. As shown in figure5-5.

Telnet and web login timeout showed in the user management interface.

Click<Apply> to send user verify configuration. Click<Cancel> cancel user configuration.

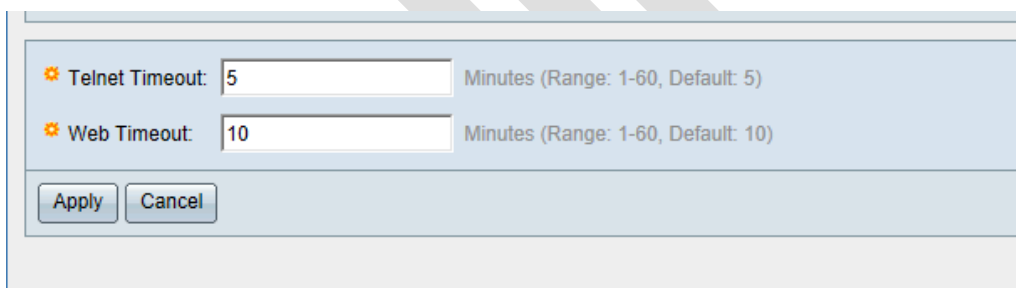


Figure 5-5 login timeout interface

5.2 Configuration Management

5.2.1 Overview

The Configuration Management module provides following functions.

- Save current configuration
- Configure files management
- Reset factory setting

1. Save configuration

Use 'Save configuration' to save user current configuration to disk.

- Improve access speed and reduce read/write time of disk in order to expand its lifetime. Some devices

save data to memory database instead of to disk directly. Save configuration to disk needs to be done manually or else the configuration that did not save in the disk may lost after device reboot.

2. Configure file management

Configure file module could realize following functions:

➤ Import file:

Import the designated config file from local host to device disk and reboot device to make configuration take effect.

➤ Export config file:

Download current configuration to local host and save as config files. It can be applied to group devices in the network with similar configurations.

- Complete configuration on one device first and export the configuration to local host.
- Import the config file to other devices to avoid repeat job.

3. Restore factory setting

Clear all current configuration and restore factory setting.

5.2.2 Restore factory settings

Select 'Device management>configuration management' to enter configuration management interface. Click <Restore factory setting>.

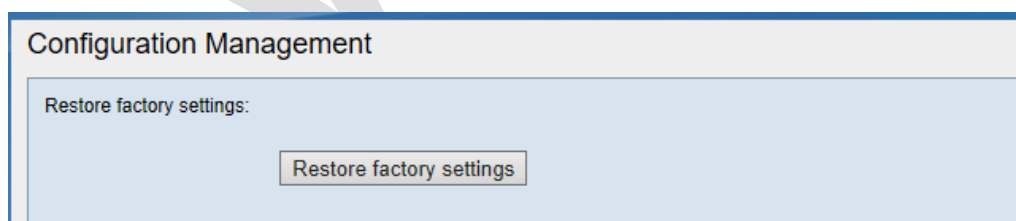


Figure 5-6 Restore factory setting

Click<Apply> restore factory setting in the pop-up page. Click <Cancel> to cancel restore factory setting. Factory setting will take effect after system reboot.

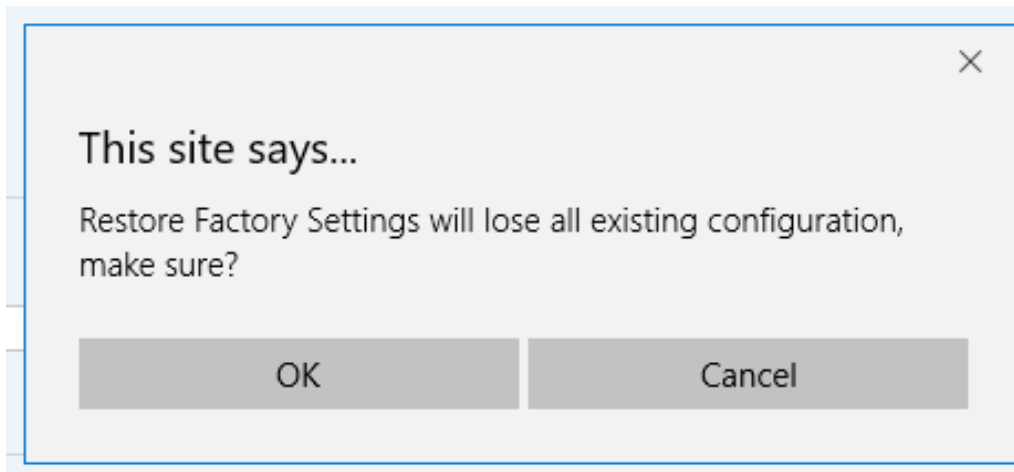


Figure 5-7 restore factory setting dialog box

5.2.3 Export configuration

Select 'Device management>configuration management' to enter management interface. Click<Export> as shown in figure5-8.

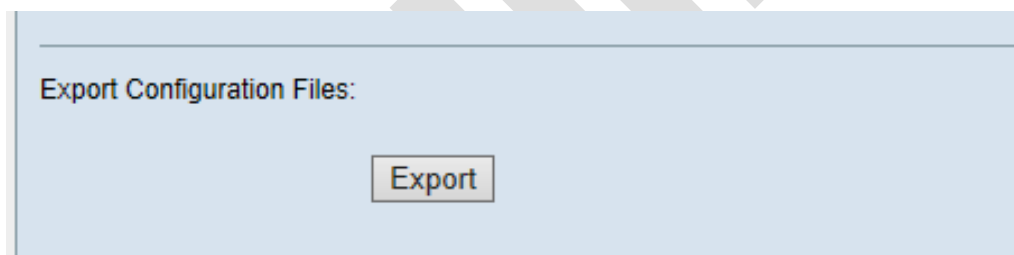


Figure 5-8 Export Configuration Files Interface

Select the file that need to save and designated directory path in the pop-up dialog box as shown in figure 5-9. Click< Save > to export configuration file. Click<Cancel> to cancel export configuration file.

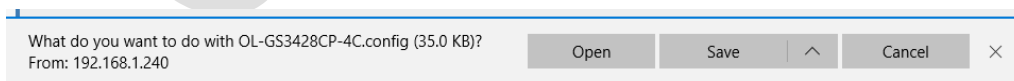


Figure 5-9 dialog box of confirm to export configuration

5.2.4 Configuration import

Select 'Device management>configuration management' to enter configuration interface. Click<Browse> and select the file that needs to import. As shown in figure 5-10.

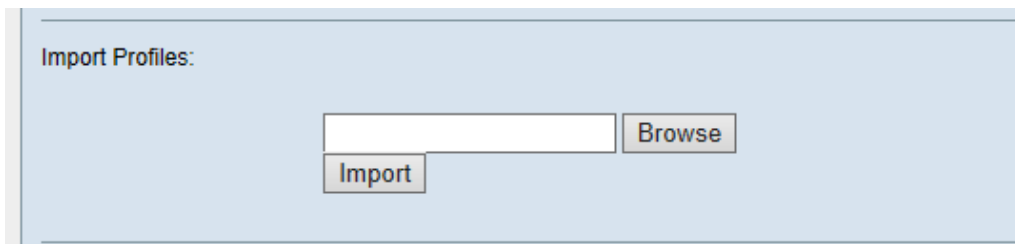


Figure 5-10 Configuration import Interface

- Click **<Import>** in the pop-up window and select **<Apply>** to start to import configuration file. Select **<Cancel>** to cancel import configuration file.
- After import the confirmation file, system will reboot to take effect.

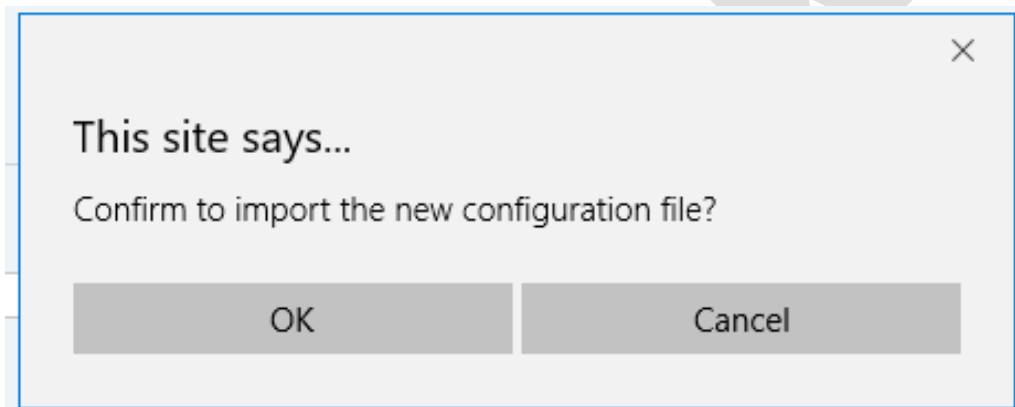


Figure 5-11 Dialog box of confirm to import

5.2.5 Save configuration

Select 'Device management> configuration management' to enter configuration interface and save current configuration to enter device. As shown in figure 5-12.

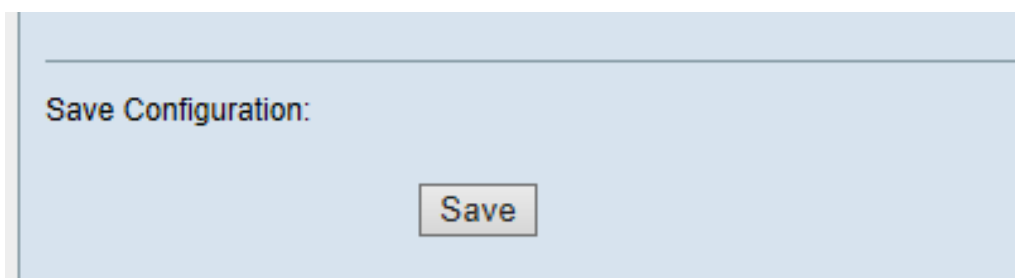


Figure 5-12 Save Updated Configuration

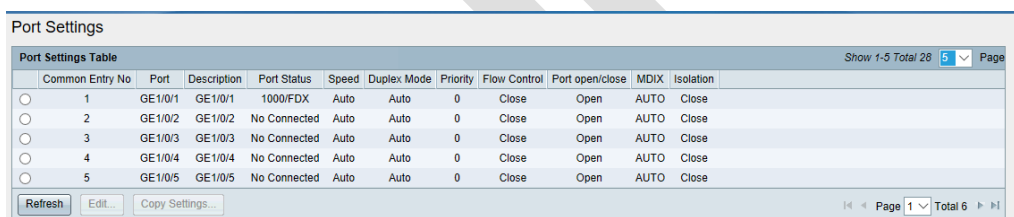
Chapter6 Switch Management

6.1 Port Management

6.1.1 Port settings

Select 'Switch management>Port management >Port setting' to enter 'port settings' interface. As shown in figure6-1.

- Check each port operation status and configuration information in the 'Port settings Table' interface.
- Set the number of columns to display per page.
- Click arrow button to turn page.
- Click<**Refresh**> to refresh port settings and status.



Common Entry No	Port	Description	Port Status	Speed	Duplex Mode	Priority	Flow Control	Port open/close	MDIX	Isolation
1	GE1/0/1	GE1/0/1	1000/FDX	Auto	Auto	0	Close	Open	AUTO	Close
2	GE1/0/2	GE1/0/2	No Connected	Auto	Auto	0	Close	Open	AUTO	Close
3	GE1/0/3	GE1/0/3	No Connected	Auto	Auto	0	Close	Open	AUTO	Close
4	GE1/0/4	GE1/0/4	No Connected	Auto	Auto	0	Close	Open	AUTO	Close
5	GE1/0/5	GE1/0/5	No Connected	Auto	Auto	0	Close	Open	AUTO	Close

Figure 6-1 'Port Settings table'

- Change port's configuration
Select corresponding port and click <**Edit**> to enter the interface as shown in figure6-2
- Change corresponding configuration.
Relevant parameters description as shown in Table 6-1.
- Click <**Apply**> to complete modification.
- Click <**Cancel**> to cancel modification.

The screenshot shows a configuration window for a network port. The fields are as follows:

- Port: GE1/0/1
- Description: GE1/0/1 (1~64 Characters)
- Speed: Auto Negotiati
- Duplex Mode: Auto Negotiati
- Priority: 0
- Port open/close: Open
- Flow Control: Close
- MDIX: AUTO
- Isolation: Close

Buttons: Apply, Close

Figure 6-2 Edit Port Settings Interface

Table6-1 Port Settings Information

Title	Description
Port	Current configured port name
Description	By default shows port number.
Speed	<p>Set port speed.Optional:</p> <p>GE1/0/1~GE1/0/24 is ethernet electrical port</p> <ul style="list-style-type: none"> ➤ Electrical port: Auto-negotiation、10Mbps、100Mbps、1000Mbps, Default: Auto-negotiation <p>GE1/0/25~GE1/0/28 is Combo port</p> <ul style="list-style-type: none"> ➤ Optical port: Support 100Mbps、1000Mbps
Duplex Mode	<p>Configure port duplex mode</p> <ul style="list-style-type: none"> ➤ Electrical port: Auto-negotiation, full duplex, half duplex three mode optional. Default: auto-negotiation

	➤ Fiber port: Support Full duplex only
Priority	Configure port priority range at 0~7. Default:0.
Port Open/Close	Configure port forward data status. When port configured as close it cannot forward data. All ports are open by default.
Flow Control	Select if doing transmit flow control.
MDIX	Select the type of MDIX, ACROSS, AUTO, NORMAL by optional <ul style="list-style-type: none"> ➤ Set as AUTO: through line or cross wire connect randomly. ➤ When one end is set as ACROSS and another end is NORMAL: only use through line to connect. ➤ When both ends have same configuration (either ACROSS or NORMAL): only use cross line to connect
Isolation	Configure isolation function: No communication between isolated ports. Communications take place between isolated port and non-isolate port. Communications take place between non-isolated ports.

- Bulk copy configuration:
Select copied port, click< **Copy configuration**>
Enter port number that needs to copy in pop-up page.
- Click<**Apply**> to complete operation.

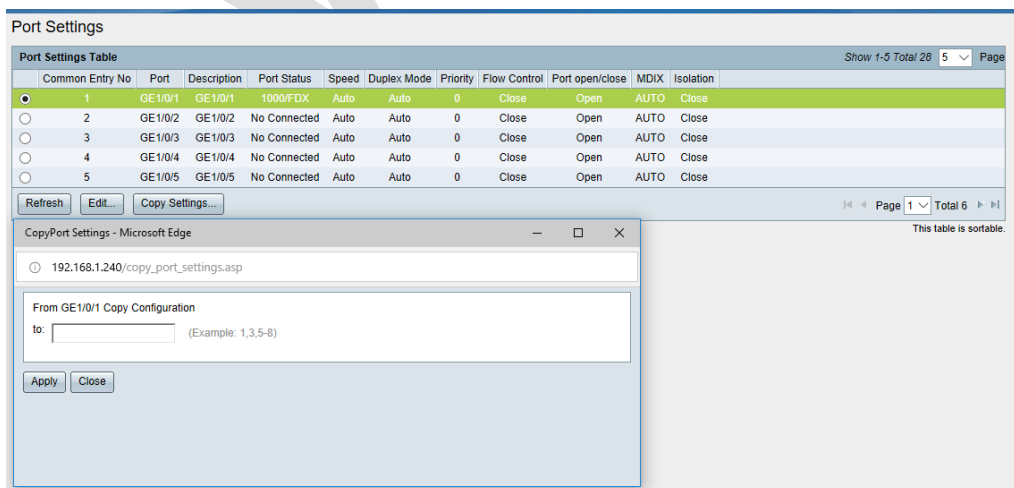


Figure 6-3 Port Settings

6.1.2 Port Mac Limit

Ethernet switch could use MAC address learning function to acquire the MAC addresses of the devices at the network segments that connect with one of the ports. Ethernet switch forwards directly by viewed MAC address forwarding table to improve transmission rate. In the case of the large MAC address forwarding table, it may take longer time to search and cause the decrease of forwarding performance of the switch.

Administrators can restrain the maximum number of Mac addresses that ethernet port can learn and control the number of entries in Mac address forwarding table maintained by the switch.

When the number of MAC addresses bar learned by the port reaches the limit that set by the user, port will no longer learn MAC address.

Configure Port Mac limit

1. Select 'Switch management>Port management>Port mac limit' to enter 'Port MAC limit' interface. As shown in figure 6-4.

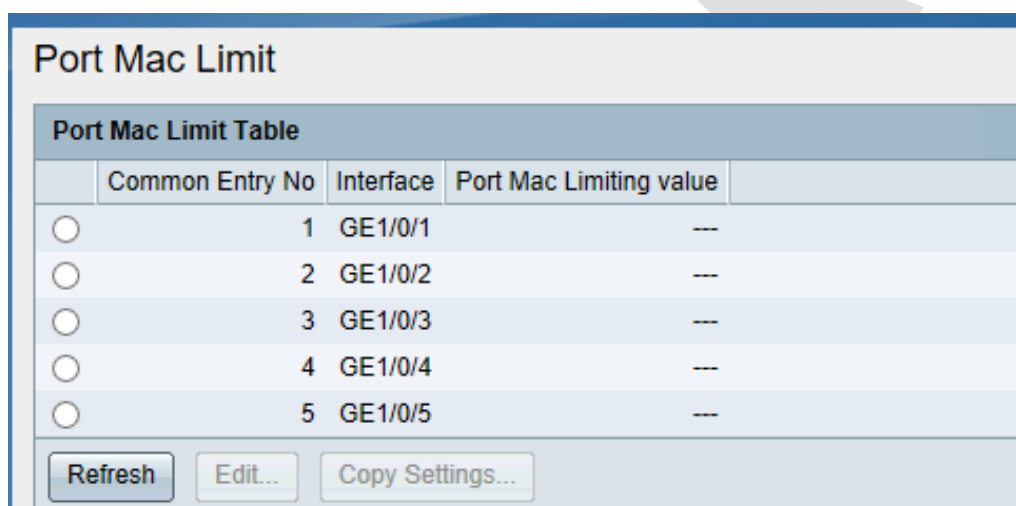


Figure 6-4 'Port Mac Limit' interface

2. View relevant configuration information related to port learning ability in 'Port MAC limit' interface.
3. Select corresponding port, click <Edit> to enter port configuration interface to change port MAC limit.

As shown in figure 6-5

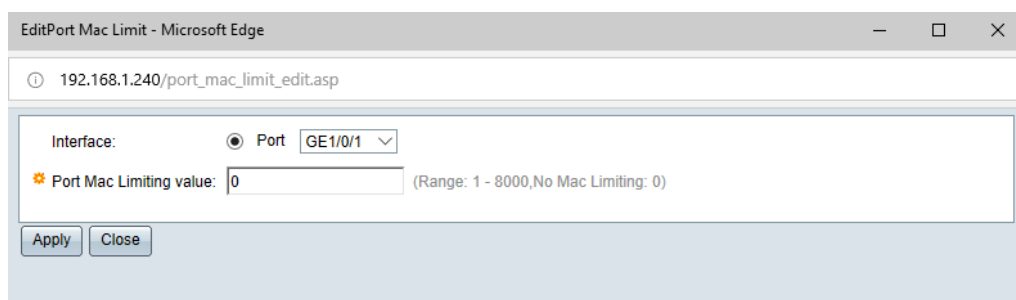


Figure 6-5

Use <Copy configuration> to copy one port configuration to another port.

6.1.3 Port Statistic

Port statistic function is used to count the number of packets and data transmitted by each port. Port traffic and data packet types to facilitate the location of network problems can be viewed.

- Select 'Switch management> Port management> Port statistics' to enter 'port statistic' interface. As shown in figure 6-6.
- It displays the statistical information of a port to view statistics of other ports by selecting the drop-down list on the left side of the port.
- Click<Clear Interface Counters> to clear current port's counter
- Click<Clear All Interface Counters> to clear all interface counters.
- Click<Refresh> to update the current port statistic.

Port Statistics

Port: ▾

Total number of packets received:	0
Total number of packets sent:	0
The total number of bytes received:	0
The total number of bytes sent:	0
Unicast packets received:	0
Unicast packets sent:	0
Broadcast packets received:	0
Broadcast packets sent:	0
Multicast packets received:	0
Multicast packets sent:	0
Flow control frames received:	0
Flow control frames sent:	0
Error packets received:	0
Error packets sent:	0

Figure 6-6 Port Statistics Information

6.2 VLAN

6.2.1 Overview

Vlan (Virtual Local Area Network) is the data transmission technology that logically partitioned LAN to enter several networks and to realize data exchange technology of dividing a large physical network to enter several virtual workgroups. Devices and users are not limited by physical location. Devices can be set as a group according to function, departments and applications, communicate with each other as in the same physical segment.

Web interface supports port based VLAN configuration. Only port based VLAN is introduced in this chapter.

1. Port link type

Ports deal with VLAN Tag when forwarding messages in different ways. Link connection of ports can be divided into three types.

- Access Link:

Port send message without VLAN Tag. Usually used to connect with terminal devices that cannot recognize VLAN Tag or when there is no need to distinguish different VLAN members.

- Trunk Link:

Message send out from the ports, packet in port default VLAN do not carry Tag. Other VLAN messages must carry Tag. Usually used for interconnection between network transmission devices.

- Hybrid Link:

Message sent by ports can be set with Tag in some VLANs as needed or may need to configure message in some VLAN with or without Tag. Hybrid ports can be used not only for interconnection between network transmission devices, but also for direct connection to terminal device.

Port-based VLAN partitioning is the simplest and most effective VLAN partitioning method. It defines VLAN members according to device ports. The port can forward the message of the specified VLAN after adding the specified ports to the specified VLAN.

2. PVID

The PVID is Port-Base VLAN ID, which is the virtual LAN ID of the port. VLAN Tag Marking Related to Port Receiving and Sending Data Frames. PVID is the property of each port when dividing VLAN.

3. Port-to-Packet Processing

After configuring the port connection type and the default VLAN, there are several different situations in which the port receives and sends messages, as shown in Table 6-2.

Table 6-2 Port-to-Packet Signal Processing

Port Type	Processing of Receiving messages		Processing of sending messages
	Tag-free when receiving	Tag when receiving	
Access	Add PVID's Tag to the message	When the VLAN is same as PVID. Receive the message. When the VLAN is different from PVID, drop the message.	Remove the Tag and send the message
Trunk	When the PVID in the list of VLANs allowed to pass through the port, receive the message, add default VLAN's Tag to the message;	When the VLAN is in the list and allowed to pass through the port, receive the message. When the VLAN is NOT in the list allowed to pass through the port, drop the message.	When VLAN is same as PVID and the port allowed to pass through the VLAN list, remove Tag, send the message; When VLAN is different from PVID and the port allowed to pass through the VLAN list, keep the tag, send the message.
Hybrid	When the PVID is not in the list of VLANs allowed to pass through the port, drop the message		When VLAN is in the list of VLAN ports allowed to pass through, send the message; Whether to remove Tag can be configured by user manually.

6.2.2 Create VLAN

1. Select 'Switch Management> VLAN management>Creating VLAN' to enter the page as shown in figure 6-7.

Create Vlan

Create / DeleteVLAN:
 Create
 Delete

VLAN ID: Range:1-4094, Use "-" or "," to add vlans

VLAN list	
<input type="checkbox"/> VLAN ID	Port member
<input type="checkbox"/> 1	FE1/0/1,FE1/0/2,FE1/0/3,FE1/0/4,FE1/0/5,FE1/0/6,FE1/0/7,FE1/0/8,FE1/0/9,FE1/0/10,FE1/0/11,FE1/0/12,FE1/0/13,FE1/0/14,FE1/0/15,FE1/0/16,FE1/0/17,FE1/0/18,FE1/0/19,FE1/0/20,FE1/0/21,FE1/0/22,FE1/0/23,FE1/0/24,GE1/0/25,GE1/0/26,GE1/0/27,GE1/0/28.LAG1,LAG2,LAG3,LAG4,LAG5,LAG6,LAG7,LAG8

Figure 6-7 Create VLAN interface

Allow to Create/Delete VLAN2~4094, select 'Create' or 'Delete', enter VLAN ID, click<Apply>, complete operation.

'VLAN list' displays current VLAN ID and corresponding port members. According to VLAN ID expand from small to large, VLANs with identical port members are merged to enter a group.

Select one or a group of VLAN from 'VLAN list', click <Delete>could complete operation.



Note: It is not allowed to delete default VLAN1. After VLAN ID is created, no port member is defaulted, port configuration needs to be modified.

6.2.3 Access VLANs

Select 'Switch management>VLAN management>Access VLAN' to enter the page as shown in figure 6-8.

Select corresponding port in the 'Port' s drop down list, any VLAN that has been created in the PVID can be configured on this port. Click<Apply> complete operation.

In 'Access VLAN list', you can view all Access port's PVID. Set the items displayed on each page and view by turning the page through the arrow button at the bottom right corner of the interface.

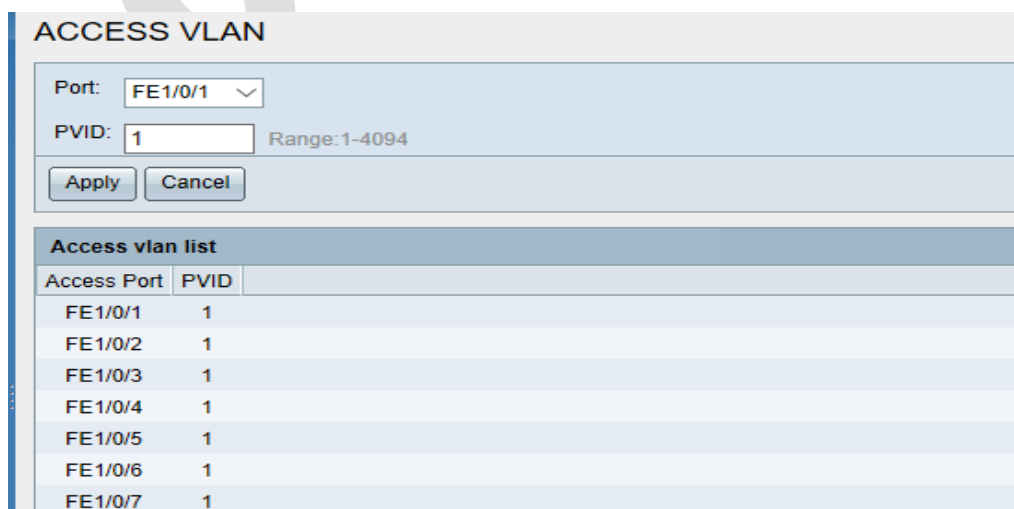


Figure 6-8 Access VLAN

3.2.2 Trunk VLANs

In the navigation bar, select 'Switch management>VLAN management>Trunk VLAN' to enter Trunk VLAN's configuration and display interface. As shown in figure 6-9

(1) Display Trunk ports

In 'Trunk VLAN list', you can view all Trunk ports' PVID and Permit VLANs.

(2) Create Trunk port.

Select the port need to be created through the drop-down list of VLAN PORT', configure PVID, select '**Create**' and set the list of VLANs allowed to pass. Click<**Apply**> complete operation.

(3) Modify Trunk port's configuration.

Select the port need to be modified through the drop-down list of VLAN PORT. Modify PVID, select '**Create**' or '**Delete**' VLAN to allow pass through. Click<**Apply**>.Complete configuration.

*Note: When modify configuration, '**Create**' and configure '**Permit Vlan**' are to perform add operation. Add VLAN to enter '**Permit VLAN**', won't cover original VLAN. '**Delete**' will delete the VLAN from the list.*

(4) Delete Trunk port.

In 'Trunk VLAN list', Select one or several Trunk ports. Click<**Delete**> complete delete operation.

Note: When Trunk port is deleted, it becomes Access port. As shown in figure 6-8 'Access Vlan list'.

The below table describes the meaning of the parameters:

Table 6-3 Trunk VLAN configuration description

Title	Description
VLAN_PORT	Select the name of the port configured, including the ethernet port and LAG port.
PVID	Configure port's PVID, range is1-4094. Configuration requires VLAN must be created.
Create	Add VLAN to permitted VLAN
Delete	Delete VLAN from permit VLANs

Permitted VLAN	Configure permitted VLAN list. it can't be blank All VLAN: Range is 1-4094. Appointed VLAN: Appointed one/ several VLANs.
----------------	---

6.2.5 Hybrid VLANs

Select 'Switch management>VLAN management> Hybrid VLAN' to enter Hybrid VLAN's configuration and display interface. As shown in figure 6-10

(1) Display Hybrid port

All Hybrid port's PVID, Tag VLAN list and Un- Tag list can be viewed in 'Hybrid VLAN list'

(2) Create Hybrid port

Select the port need to be created through the drop-down list of 'VLAN port', set PVID, Select '**Create**' and set Tag VLAN list and Un-Tag list. Click<**Apply**> complete configuration.

(3) Modify hybrid port configuration

Select the port need to be modified through the drop-down list of 'VLAN PORT', modify PVID. Select '**Create**' or '**Delete**' Tag VLAN list and Untag list. Click<**Apply**> complete operation.

Note: When modify configuration, 'Create' is perform add operation. Add VLAN to Tag VLAN list and UnTag list, original VLAN won't be covered. 'Delete' is delete VLAN from list.

(5) Delete Hybrid port

In' Hybrid VLAN list' select one or several Hybrid ports. Click<**Delete**> complete delete operation.

Note: When delete Hybrid port, it becomes Access port. As shown in figure 6-8 'Access vlan list'

Table6-4 Hybrid VLAN configuration parameter description

Title	Description
VLAN_PORT	Select the name of configured ports, including Ethernet port and aggregate logical port.
PVID	Configure Port's PVID, range is 1-4094. Configuration requires VLAN must be created.
Create	Add VLAN to permitted VLAN
Delete	Delete VLAN from allowed VLAN.
Tagged VLAN	Configure Tagged and Untagged list, range is 1-4094, configuration requires must be created VLAN.
Untagged VLAN	Note: Tagged VLAN and Untagged VLAN can't be empty at the same time; There can't be same VLA

Figure 6-10 Hybrid port

6.3 MAC setting

6.3.1 Overview

The MAC address table records the destination MAC address, the interface corresponding to the MAC address and the VLAN ID to which the MAC address belongs. When forwarding packets, the device queries the MAC address table according to the destination MAC address of the message locates in the interface quickly, thus reducing broadcasting.

(1) MAC address table generation method

There are two ways to generate MAC address table entries: automatically, manually configuration.

(2) Classification of MAC address table items

MAC address table items are divided to enter static MAC address table items, dynamic MAC address table items, blackhole MAC address table items and multiport unicast MAC address table items.

Static MAC address table entries are manually configured by users to forward messages from corresponding port for a MAC address without ageing.

Dynamic address table items contain user configured MAC address and learned by switch automatically from source MAC addresses. Messages intended for a MAC address are forwarded from the corresponding port, and the table items have aging time.

Black hole MAC address table entries are used to drop the messages containing specific source MAC address or destination MAC address (For example, for security reasons, a user can be shielded from receiving

message), which are manually configured by the user, and the entries are not ageing.

6.3.2 Dynamic Address

Select 'Switch Management> MAC setting>Dynamic address' to enter 'Dynamic address table' interface, as shown in figure 6-10.

'Dynamic address table' interface display address items learned by device.

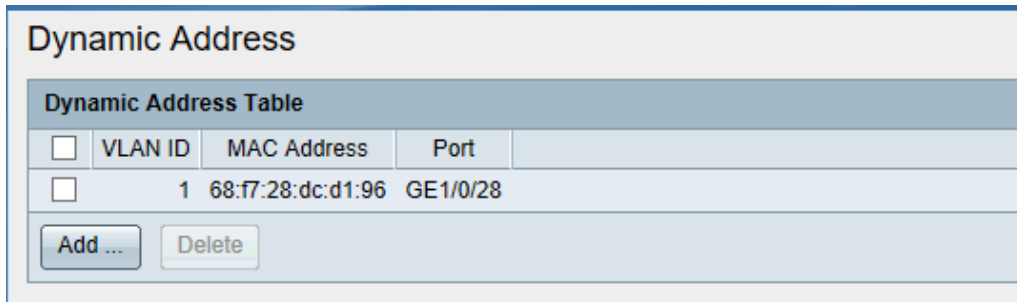


Figure 6-10

(2) Add dynamic address

—Click<Add> enter add dynamic address interface, as shown in figure6-11

—Enter configuration parameter.

—Click<Apply> to complete operation. Added dynamic address could be checked in 'Dynamic address table' as shown in figure 6-10.

Note: Added dynamic address support aging

When added, the VLAN is required to exit and the interface exists in the VLAN

(3) Delete dynamic address

Dynamic address supports manual deletion. Select one or more address entries that need to be deleted in the 'Dynamic Address Table' interface and click the < Delete > button to complete the deletion operation.

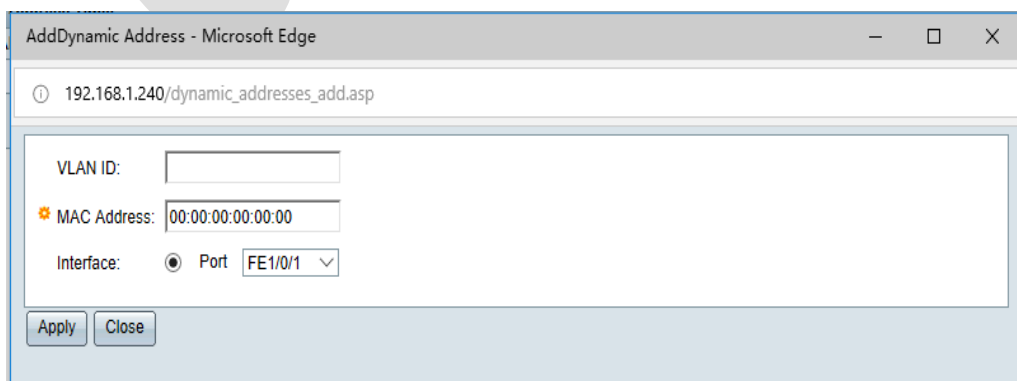


Figure6-11

6.3.3 Static Address

In the navigation bar, select 'Switch Management>Mac Setting>Static Address' to enter 'Static address' interface, as shown in figure 6-12.

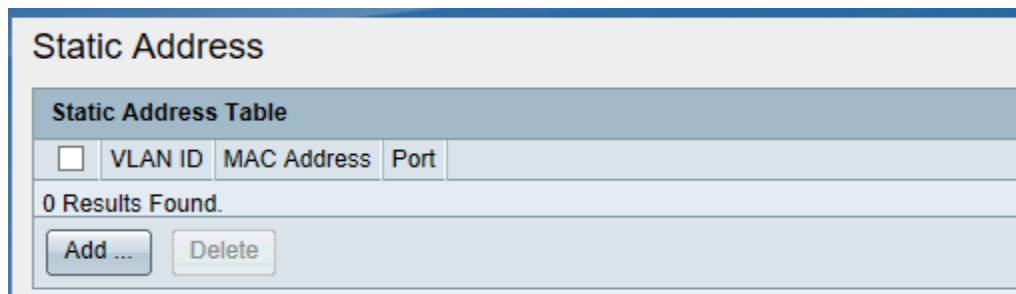


Figure 6-12 'Static Address Table' interface

(4) Add static address

- Click<**Add**> to enter 'Add static address' interface. As shown in figure6-13
- Enter configuration parameter.
- Click<**Apply**> to complete operation. Added static address could be viewed in 'Static address table'.

Note: When adding static address, VLAN is required to exist and the interface exists in VLAN

Delete static address

Select one or several addresses in 'Static address table' interface, click<**Delete**> to complete delete operation.

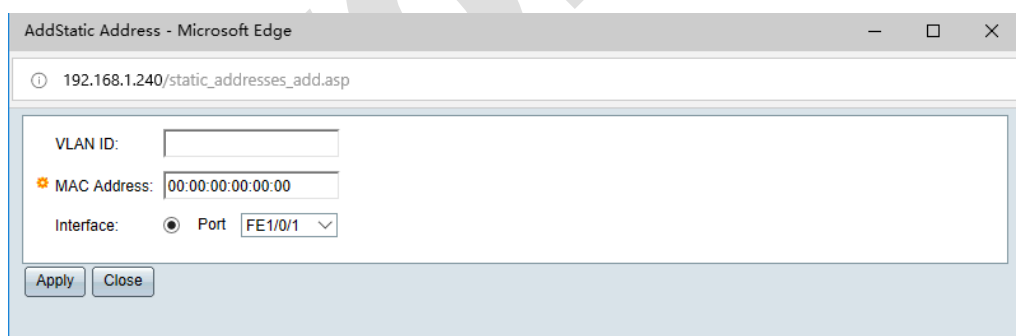


Figure 6-13 Add Static Address

Note:

- Multicast or broadcast addresses cannot be set as static addresses.
- Ports in LAGs (Link Aggregation Group) are not supported for static address configuration

6.3.4 Blackhole Address

(1) Select 'Switch management>MAC setting>Blackhole address' to enter 'Blackhole MAC address' interface, as shown in figure 6-14

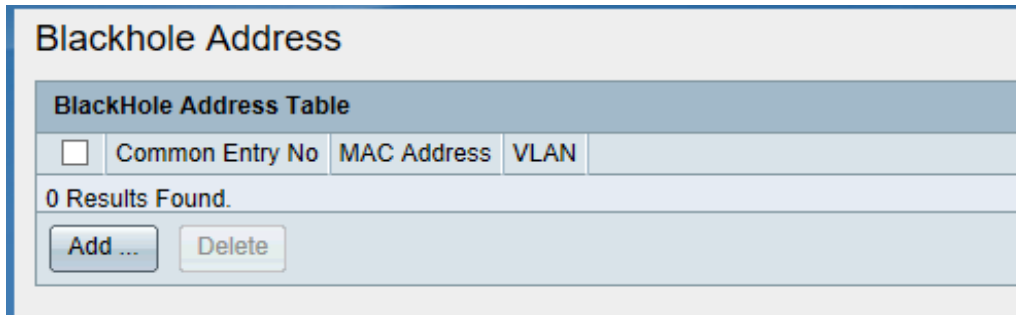


Figure 6-14 'Blackhole Address Table' interface

(2) Add blackhole address.

- Click<**Add**> to enter 'Add blackhole address' interface, as shown in figure6-15
- Enter configuration parameter.
- Click<**Apply**> to complete operation. Added blackhole address could be viewed in 'blackhole address table'.

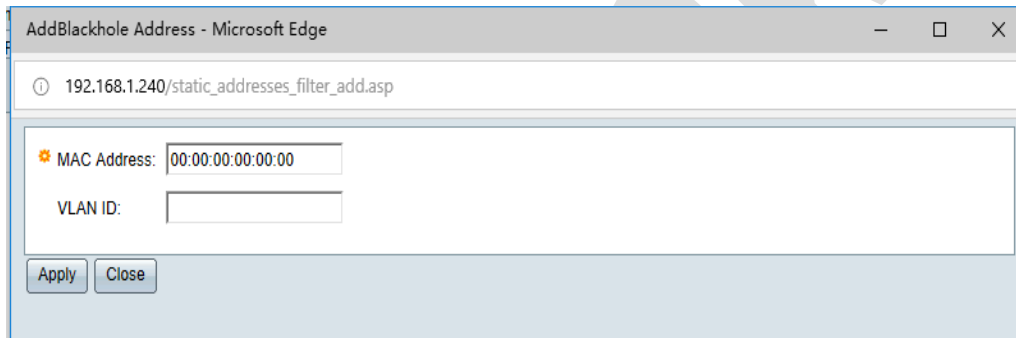


Figure 6-15 Add blackhole address

6.3.5 Dynamic Address Aging Time

- (1) In the navigation bar, select 'Switch management> Mac setting> Dynamic address aging Time' to enter interface, as shown in figure6-16.
- (2) Configure aging time (Range is 10-1000000, 0 means that MAC address will not age.)
- (3) Click<**Apply**> to complete operation.

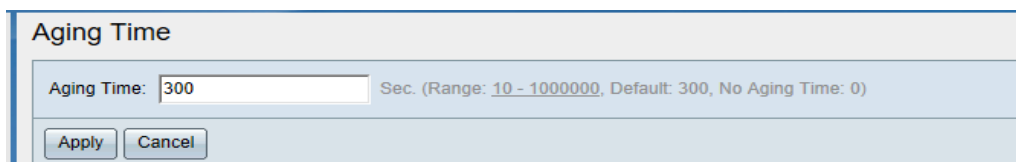


Figure 6-16 Dynamic MAC Aging Time

6.4 Quality of service

6.4.1 Overview

By setting the priority of ports, when network congestion occurs, the system will drop the message on low priority port first to ensure the transmission of high priority ports.

Switches support two priority mode: COS and DSCP; Support WRR and HQ-WRR priority queue schedule mode; There are 4 priority queues: queue 1 is the lowest priority, and queue4 is the highest priority.

(1) Priority type

- **COS**
- **DSCP**

(2) Schedule mode

When network congestion occurs, it is necessary to solve the problem of multiple messages competing to use resources at the same time, which is usually solved by queue scheduling.

➤ **WRR**

WRR queue scheduling algorithm schedules the queues in turn to ensure that each queue has a certain service time. WRR can configure a weighted value for each queue (w_3, w_2, w_1, w_0 corresponding to queue4-queue1) with four output queues as an example. The weighted value represents the proportion of resources obtained.

For a 100M port, the weighted values of WRR queue scheduling algorithm are 5, 3, 1, 1 (corresponding to w_3, w_2, w_1, w_0 in turn). This ensures that the lowest priority queue can obtain at least 10Mbit/s ($100\text{Mbps} * 1 / (5+3+1+1)$) bandwidth, avoiding the possibility that messages in low priority queues may not be available for a long time when SP scheduling is adopted. Disadvantages of services

➤ **HQ-WRR**

Based on WRR, HQ-WRR queue scheduling algorithm Clicks queue 4 as high priority queue in four output queues. If the bandwidth occupied by four queues exceeds the capacity of the port, the switch first guarantees that the message of queue 4 is sent out first, and then schedules the remaining three queues with WRR.

6.4.2 QOS

Select 'Switch Management>QOS service>QOS' to enter QOS interface. As shown in figure 6-16.

QoS

Priority Type: COS

Schedule Type: HQ-WRR WRR

Priority	0	1	2	3	4	5	6	7	Weight
Queue1(lowest)	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	1
Queue2(general)	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	2
Queue3(higher)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	4
Queue4(highest)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	8

Description:
 1. There are 64 priority of COS being divided into four groups, each group of 16 and corresponds to a scheduling priority queue; 1-2 corresponds queue priority 1, 0-3 corresponds queue priority 3, 6-7 corresponds queue priority 4.
 2. Four scheduling queues in switches are available with the weight value, the value is divided into 31 levels.

Apply Cancel

Figure 6-16

Config procedure:

- (1) In 'Priority type' drop down list, select priority COS or DSCP. Select priority type COS or DSCP in the 'Priority Type' drop-down list.
- (2) Select schedule type HW-WRR or WRR.
- (3) Select the weight ratio for each queue. As shown in Figure 6-16, the weight ratio of queue 1, queue 2, queue 3 and queue 4 is 1:2:4:8. If the queue scheduling mode is WRR, the data packets of queue 1, 2, 3 and 4 will be sent at a 1:2:4:8 traffic ratio when congestion occurs at a certain port. If the scheduling mode chooses HQ-WRR, the switching opportunity first ensures that the messages in queue 4 are sent out first, and then WRR scheduling is applied to the other three queues
- (4) Click <Apply> to complete QOS configuration.

6.4.3 Port Line rate

After setting the port speed limit, the rate of outgoing or inbound messages can be limited to maintain the normal and orderly operation of the network.

- (1) In the navigation bar, select 'Switch management>QOS service>Port line rate' to enter the page as shown in figure6-17.
- (2) The 'Port line rate table' shown in the figure display the situation of each port in and out speed limit. The '-' indicates that the speed limit is not carried out.

Port Linerate

Port Linerate Table Show 1-5 Total 28 5 Page

Common Entry No	Interface	IN Port Linerate Limit(kbps)	Out Port Linerate Limit(kbps)
<input type="radio"/> 1	GE1/0/1	---	---
<input type="radio"/> 2	GE1/0/2	---	---
<input type="radio"/> 3	GE1/0/3	---	---
<input type="radio"/> 4	GE1/0/4	---	---
<input type="radio"/> 5	GE1/0/5	---	---

Refresh Edit... Copy Settings...

Page 1 Total 6

Figure 6-17 'Port line rate table'

Select port in the 'Port limit rate table', click<Edit> to enter the interface as shown in figure 6-18. Enter speed limit, click<Apply> to complete limit configuration.

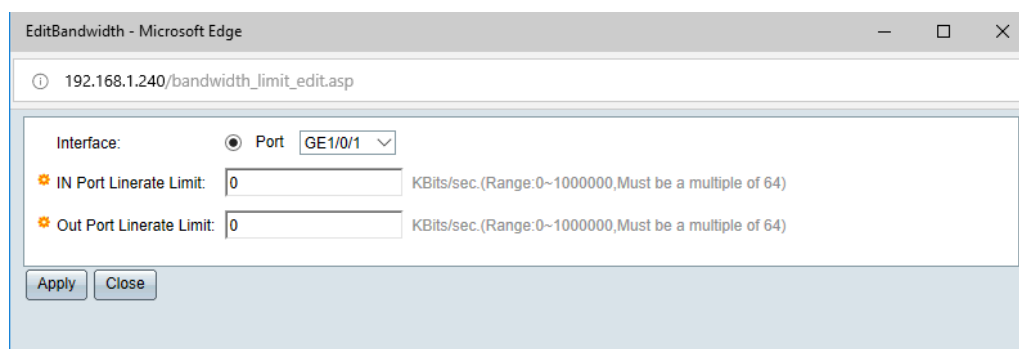


Figure 6-18 Port Line rate Limit configuration

In the 'Port limit rate table' interface, the speed limit configuration can be copied to other ports by copying settings. For example:

- Check the circle in front of serial number '1'
- Click <Copy> to enter the interface as shown in figure6-19
- In the pop-up interface, copy configuration to '2-4'.
- Click <Apply> complete configuration. Can see that the speed limit configuration of GE1/0/1 has been copied to GE1/0/2~GE1/0/4.

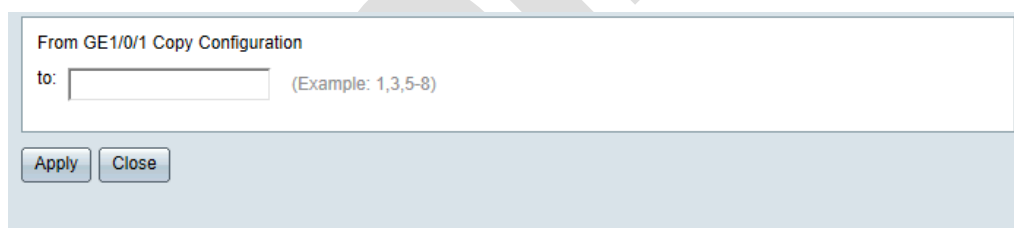


Figure6-19 Copy 'Port Line Rate' configuration

In the top right corner of the 'Port line Rate' interface (Figure 6-17), can set the number of entries displayed on each page. Can choose to turn the page through the arrow button in the lower right corner.

6.5 Multicast IGMP snooping

6.5.1 Overview

IGMP Snooping is abbreviated name of Internet Group Management Protocol Snooping. It's a multicast constrain mechanism running on Layer2 devices, use to manage and control multicast group.

(1) Theory

The Layer 2 device running IGMP Snooping establishes a mapping relationship between port and MAC multicast address by analyzing the received IGMP message, and forwards multicast data according to the mapping

relationship.

When IGMP Snooping is not run by the Layer2 device, multicast data is broadcast in the Layer2 network; When IGMP Snooping is run by the Layer2 device, multicast data of known multicast group will not be broadcast in the Layer2 network but will be multicast to the designated receiver.

Basic concept:

Router Port: The port on the switch toward Layer3 multicast device (DR or IGMP query). The switch records all router ports on the device in the list of router ports.

Member Port: Also known as the member port of multicast group, which means the port toward multicast group on the switch. The switch records all member ports on the device in the IGMP Snooping forwarding table

6.5.2 Global Settings

(1) In the navigation bar, Select 'Switch management>multicast>global setting' to enter multicast global setting interface. As shown in figure 6-20.

Enable /Disable IGMP Snooping in the session of global settings. Click<Apply>button to complete operation.

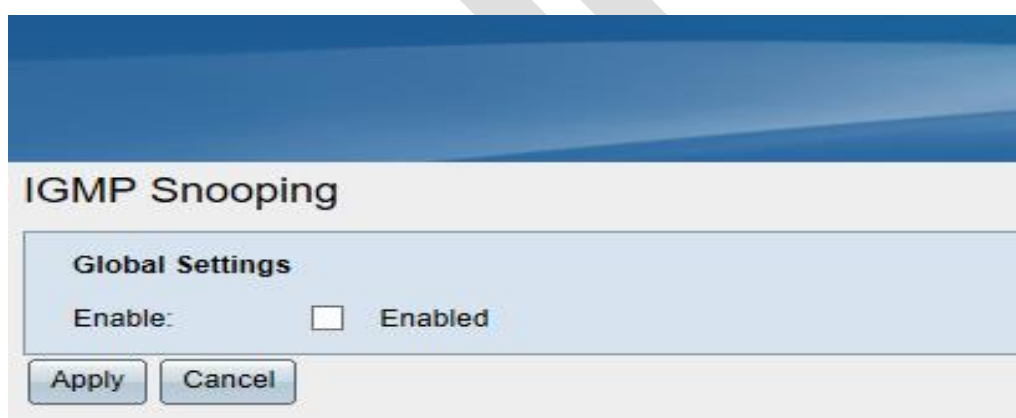


Figure 6-20

6.5.3 VLAN setting

(1) Select 'Switch management>Multicast>VLAN setting ' in to VLAN setting interface. As shown in figure6-21.

(2) In VLAN configure interface, configure the information of IGMP Snooping function in VLAN. Detailed configuration is shown in Table6-5.

(3) Click<Apply> to complete operation.

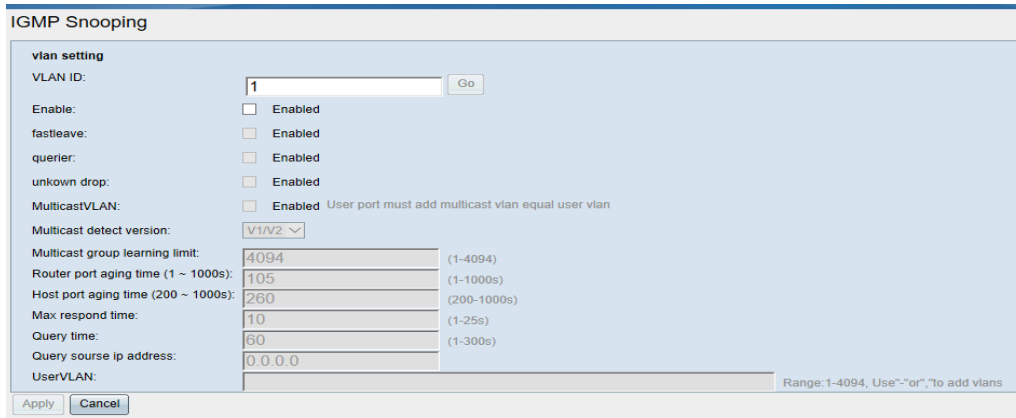


Figure 6-21 Multicast VLAN setting interface

Table 6-5 VLAN, IGMP Snooping detailed configuration

Title	Description
VLAN ID	VLAN ID currently to be configured.
Enable	Set the enable/disable IGMP Snooping in the VLAN. Only when this check is enabled can the following configuration items be set up
Fast leave	Enable/Disable Fast leave feature on this VLAN. <ul style="list-style-type: none"> ➤ Disable ➤ Enable: After enabling multicast group members to leave the multicast group quickly, when a multicast member initiates to leave, don't wait for the aging time to come, leave quickly
Querier	Set to enable or disable query function on the VLAN <ul style="list-style-type: none"> ➤ Disable ➤ Enable: If the query is enabled, the corresponding query interval and the source IP need to be set
Unknown Multicast drop	Set to enable or disable drop unknown multicast data messages on the VLAN. Unknown multicast data packets refer to those multicast data messages that do not have corresponding forwarding table entries in IGMP Snooping forwarding table (Unknow multicast data packets refer to those multicast messages that do not have corresponding forwarding table entries in IGMP Snooping forwarding table): <ul style="list-style-type: none"> ➤ Enable: Switch will drop all the received unknow multicast data packets. ➤ Disable: The Switch will broadcast the message in the VLAN to which the unknown multicast data belongs.
Multicast VLAN	Enable multicast VLAN
Multicast detect version	Set the version of IGMP Snooping, the version of IGMP message that IGMP Snooping could handle. <ul style="list-style-type: none"> ➤ V1/V2:

	<p>IGMP Snooping can process the messages of IGMPv1 and IGMPv2, while the messages of IGMPv3 are not processed, but broadcast in VLAN.</p> <p>➤ V3: IGMP Snooping can process Upon V3 messages of IGMPv1\IGMPv2 and IGMPv3</p>
IGMP Multicast group learning limit	Set the maximum number of multicast groups that allow ports to join.
Router port-aging-time	Config Router port's aging time
Host-aging-time	Config aging time of host
Max response time	<p>config maximum response time.</p> <p>If the IGMP member message that the host responds to a particular group query is not received from the port in the maximum response time, it is deleted from the output port column table of the table item forwarded by the multicast group.</p>
Query time	Set the time interval for sending IGMP universal group query messages
IP Query source IP	Set the source IP address of query packet sent by the querier, and the valid unicast address
User VLAN	Config binding user VLAN. Multicast VLAN needs to join user interface in the same way as user VLAN when configuring.

6.5.4 Interface Setting

In the navigation bar, select 'Switch management>IGMP snooping>interface setting' to enter 'Interface setting' as shown in figure 6-22.

In the interface, you can view all the ports' configuration. In the upper right corner of the interface display the number display each page, in the bottom right corner can turn the page through arrow button.

Interface Settings Table			Show 1-5 Total 28	5	Page
Filter: Interface Type equals to Port <input type="button" value="Go"/>					
Sequence	Interface	fastleave			
<input type="radio"/>	1	GE1/0/1	No		
<input type="radio"/>	2	GE1/0/2	No		
<input type="radio"/>	3	GE1/0/3	No		
<input type="radio"/>	4	GE1/0/4	No		
<input type="radio"/>	5	GE1/0/5	No		
<input type="button" value="Edit ..."/>			Page 1 Total 6		

Figure 6-22

Click<**Edit**> to enter edit interface. As shown in figure 6-23

(2) Set whether open 'Fast leave' function on the port.

Click<**Apply**> to complete operation.

Table 6-6 Multicast interface configuration description

Title	Description
Interface	Config the port that need to configure, including ethernet port and Layer2 aggregate port.
Fast Leave	<p>Enable or Disable Fast Leave feature for the desired port.</p> <p>Port fast leave specify that when a switch receives IGMP message from a host that leaves a multicast group from a certain port, it deletes the port directly from the table column of the outgoing port corresponding to the forwarding items.</p> <p>Thereafter, when the switch receives the IGMP specific group query message for the multicast group, the switch will no longer forward to the port.</p> <p>On switch ports, bandwidth and resources can be saved by enabling port quick departure</p>

6.5.5 IGMP Forward table

Select 'Switch management>IGMP Snooping>IGMP Forward table' to enter IGMP forward interface as shown in figure 6-24.

In the interface, all multicast forwarding entries including static and dynamic can be queried in the interface.

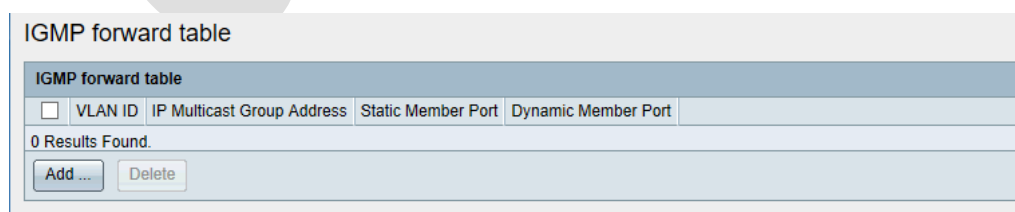


Figure 6-24 IGMP forward table

Table6-7 IGMP forward table detail description

Title	Description
-------	-------------

VLAN ID	VLAN ID to which the IGMP belongs.
IP IGMP address	Specify IGMP address
Type	IGMP type ➤ Dynamic, learning IGMP ➤ add IGMP manually
Member port	Specify all member ports

(2) Add static IGMP

- Click<Add> to enter add static IGMP interface as shown in figure 6-25.
- Edit, enter configure parameter. Parameter description refer to table6-7.
- Click<Apply> to complete operation

6.5.6 IGMP Router Port Table

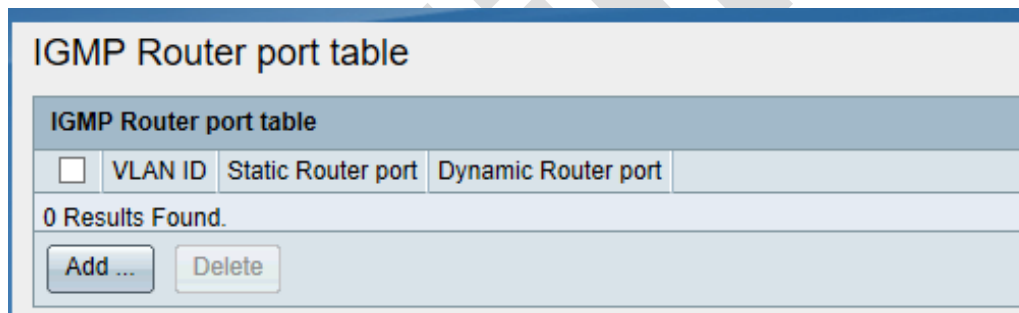


Figure 6-25 IGMP Router port table

6.6 Link Aggregation

6.6.1 Overview

Link aggregation is the aggregation of multiple physical Ethernet ports to form a logical aggregation group. The upper entities of link aggregation service regard multiple physical links in the same aggregation group as a logical link.

Link aggregation achieves load sharing among member ports in aggregation group to increase bandwidth. At the same time, each member port of the same aggregation group backs up dynamically with each other, which improves the reliability of the connection.

(1) Link Aggregation

According to different aggregate mode, Link aggregation can be divided to enter two modes: Static aggregation and dynamic aggregation.

➤ Static aggregation

In static aggregation mode, the LACP protocol of member ports is closed.

➤ Dynamic aggregation

When the aggregation group is configured as a dynamic aggregation mode, the LACP protocol of the member ports in the aggregation group is automatically enabled.

3.6.1 LAG management

Select 'Switch management > link Aggregation > LAG management' to enter LAG management interface as shown in figure 6-26

On the aggregation group interface, you can set up aggregation group load balancing algorithm, create and edit aggregation groups, and view the information of aggregation groups that have been created.

Setting up load balancing algorithm. On the aggregate group management interface, select the load balancing algorithm and click the < **Apply** > button to complete the operation

View the created aggregation group. The 'Aggregate Group Management Table' displays the created aggregate group and the information about the aggregate group (type, active member, standby member).

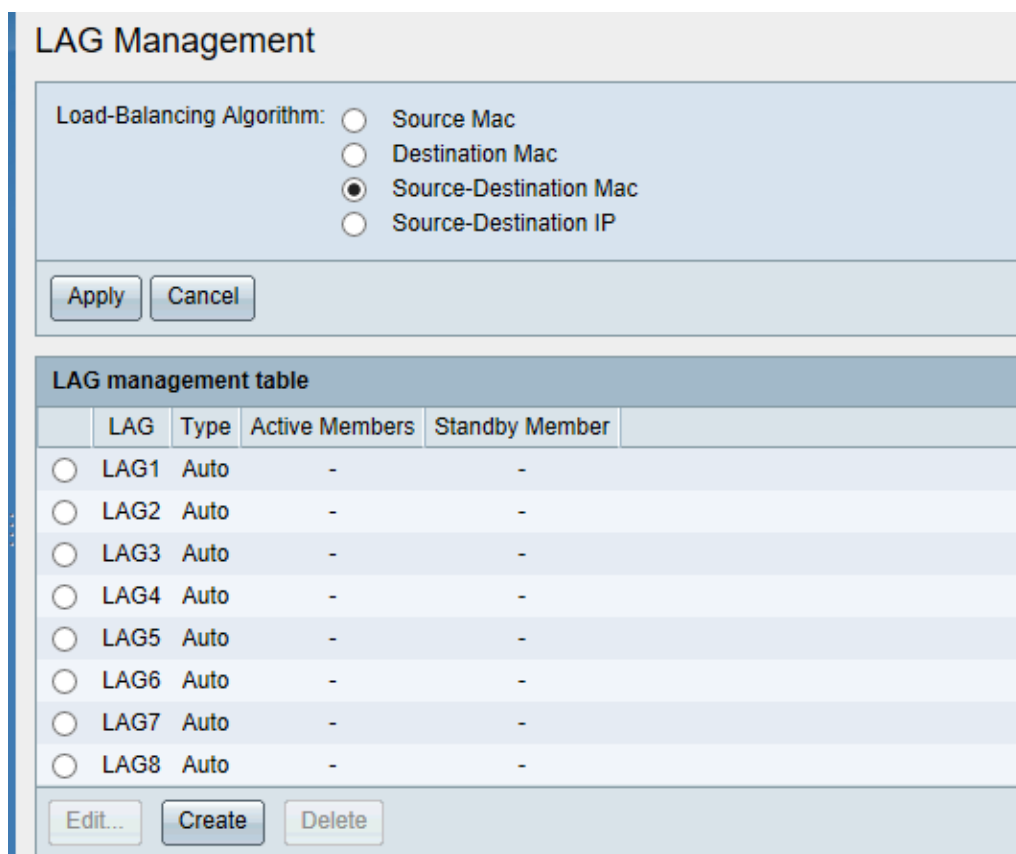


Figure 6-26 LAG management table interface

(1) Create Link Aggregation group

- On 'Aggregate Group Management Table' click <Create> to enter the create aggregation interface, as shown in figure 6-27.
- Configure aggregation group information, as shown in table 6-8
- Click <Apply> to complete operation

(2) Modify membership ports

- Select the aggregation group that needs to be modified on the 'aggregation group management table' and click the < Edit > button to enter the edit aggregation group interface
- Modify the member ports of the aggregation group, add the ports from the 'Port column table' to the 'Aggregation group member' or remove the ports from the 'Aggregation group member'.
- Click <Apply> to complete operation.

(3) Delete LAG

Select the group you want to delete from the 'Aggregate Group Management Table' and click the < Delete > button to complete the operation.

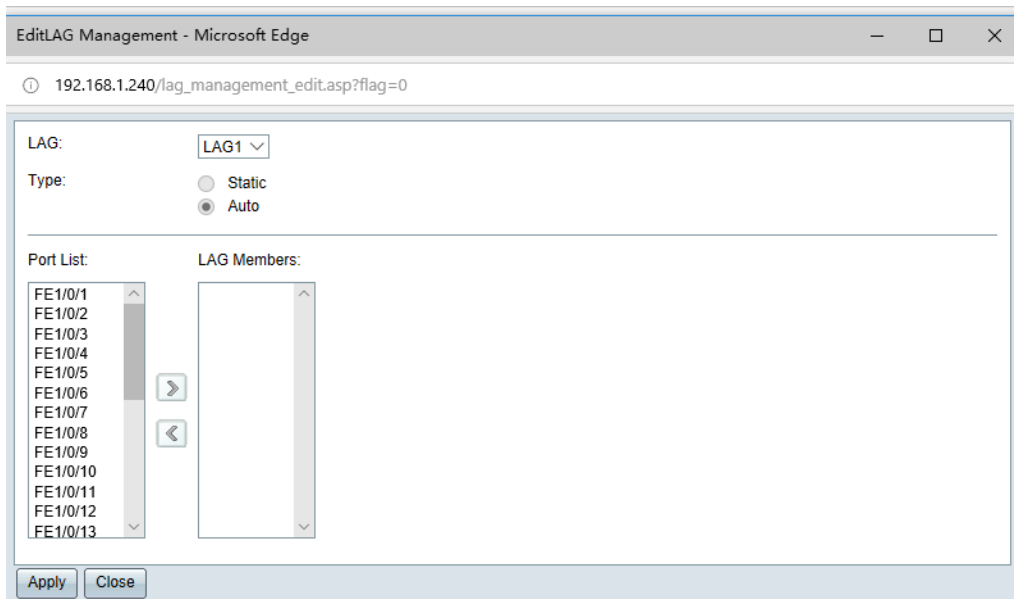


Figure 6-27 Create LAG interface

Table 6-8 Detailed configuration description for creating Aggregation Group

Title	Description
Link Aggregation group	Select LAG ID that need to be created. LAG1~LAG8 optional. By default, the system has created eight groups
Type	Select LAG type <ul style="list-style-type: none"> ➤ Static(LACP disable) ➤ Dynamic (LACP enable automatic)
Port Column Table	Port column tables that can be selected as aggregate group ports, usually ports that do not join aggregate groups
Member ports of Link aggregation group	Configure LAG's member ports. Move the ports to be assigned to LAG from the 'Port Column Table' to the 'LAG Member Column Table'. Each static LAG can be allocated up to 8 ports and dynamic LAG can be allocated up to 16 ports.

6.6.3 LAG setting

Select 'Switch management> LAG management>LAG setting' to enter 'LAG setting table', as shown in figure 6-28
In the 'LAG configuration table, you can view all the port information of the created aggregation group.

Modify aggregation/port's information

- Select the aggregate group that needs to be modified on the 'aggregate group settable' and click the <Edit> button to enter the interface of the edit aggregate group port.
- Modify LAG port information, detailed configuration as shown in Table 6-9.
- Click <Apply> to complete operation

Table6-9 LAG port configuration description

Title	Description
Link Aggregation group	Select the LAG to modify. LAG1~LAG8 is optional, requiring that it has been created.
Description	Configure LAG description, range is 0-64 byte
Management status	Set the selected LAG to run (connect) or non-run (disconnect)
Management Auto Negotiation	Sets whether the aggregation group port is enabled in self-negotiation mode (Post-enabled ,management speed is not optional)
Management Speed	Set the port management rate for the aggregation group (Require auto-negotiation must be disable)
Flow control	configure whether enable/disable flow control.

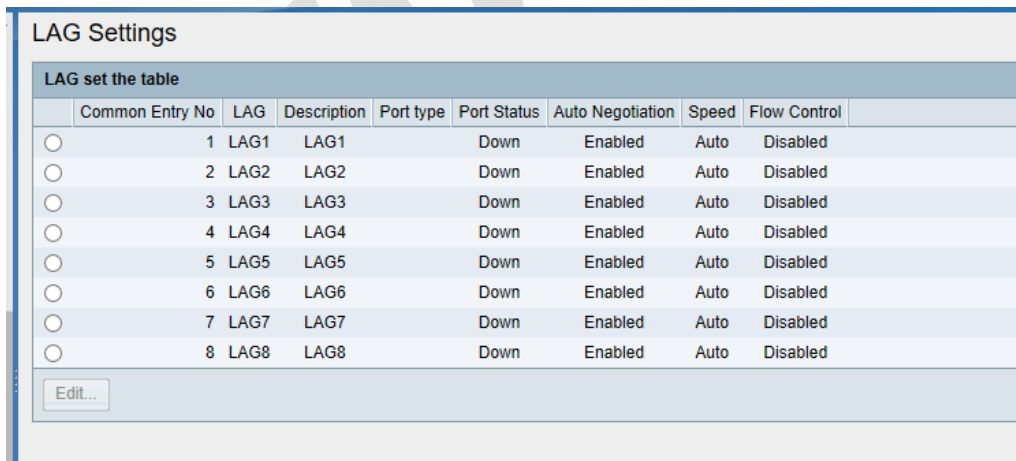


Figure 6-30 LACP interface settings

6.6.4 LACP

Select 'Switch management> LAG> LACP setting' to enter LACP setting interface, as shown in figure 6-30

- System priority and member port priority can be viewed and set in LACP setting interface. Detailed configuration instructions are shown in table6-10.

- Enter system priority directly in the interface, click the < **Apply** > button to complete the operation of modifying system priority configuration.
 - On the interface, select the interface that needs to modify the port priority, click the < **Edit** > button, enter the edit interface, and modify the port priority.
2. Priority configuration of one port can be copied to other ports through the < **Copy** > button
 - Select the port to be copied and click < **Copy** > to enter the Copy Settings Interface
 - In the copy interface, enter the port's number that need to be copied to.
 - Click < **Apply** > to complete operation.

LACP			
LACP System Priority:		<input type="text" value="32768"/>	(Range: 1 - 65535, Default: 32768)
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>			
LACP Interface Table			
	Common Entry No	Port	Port Priority
<input type="radio"/>	1	FE1/0/1	32768
<input type="radio"/>	2	FE1/0/2	32768
<input type="radio"/>	3	FE1/0/3	32768
<input type="radio"/>	4	FE1/0/4	32768
<input type="radio"/>	5	FE1/0/5	32768

Figure 6-30 LACP interface table

Table6-10 Detailed configuration description of LACP

Title	Description
LACP system priority	Set the priority of LACP system, range is1-65535, default value is 32768. The smaller the priority value, the better.
Port	Ethernet physical port
Port priority	Set the priority of the port, ranging is1 - 65535, default value is 32768. The smaller the priority value, the better,

6.7 Spanning Tree

6.7.1 STP Status and Global Settings

In order to solve the loop problem in switching networks, a spanning tree protocol (STP) is proposed. If there are

loops in the network, the spanning tree protocol can through topological calculation to realize:
 Eliminate loops: Eliminate possible network communication loops in a network by blocking redundant links.

Link backup: Activate redundant backup links to restore network connectivity when the current active path fails.

Spanning tree protocol is constantly updated with the development of network. At present, there are three protocols STP, RSTP and MSTP.

MSTP is compatible with RSTP, STP and RSTP is compatible with STP.

The comparison of the three spanning tree protocols is shown in table below

Table6-11 The 3 Tree protocol comparison

Spanning Tree protocol	Attribute	Application
STP	<p>Form a tree without loop to solve broadcast storm and realize redundant backup</p> <ul style="list-style-type: none"> ➤ Slow convergence rate 	
RSTP	<p>Form a tree without loop to solve broadcast storm and realize redundant backup</p> <ul style="list-style-type: none"> ➤ convergence rate 	Without distinguishing between user and traffic, all VLANs share one tree
MSTP	<p>Form a number of non-loop trees to solve the broadcast storm and achieve redundant backup</p> <ul style="list-style-type: none"> ➤ Fast convergence rate <p>Multiple spanning trees achieve load balancing among VLANs, and the traffic of different VLANs changes according to different paths.</p>	It is necessary to differentiate user or business traffic and realize load sharing. Different VLAN forwards traffic through different spanning trees, and each spanning tree is independent of each other

6.7.2 STP Status and Global Settings

Select 'Switch management > Spanning Tree > STP status and Global setting' to enter 'STP status and Global setting' interface, as shown in figure 6-31.

- In the interface, you can view STP global setting, bridge settings and status. Details configuration show as table 6-12
- Entering the interface to view the global settings, bridge settings and status of STP. Detailed configuration instructions as shown in table6-12
- Modify the configuration information directly on the interface and click the < **Apply** > button to complete the modification of STP configuration operation

STP Status and Global Settings

Global Settings

Spanning Tree State: Enabled

STP Operation Mode: STP
 RSTP
 MSTP

BPDU transparent: Disabled
 Enabled

Path Cost Default Values: dot1t
 dot1d-1998

Bridge Settings

Priority: (Range: 0-81440, Default: 32768)

Hello Time: sec. (Range: 1 - 10, Default: 2)

Max Age: sec. (Range: 6 - 40, Default: 20)

Forward Delay: sec. (Range: 4 - 30, Default: 15)

Status

Bridge ID: 32768/ 00: 17: 73: a0: 09: d5

Root Bridge ID: 32768/ 00: 17: 73: a0: 09: d5

Root Port: 0: 0

Root Path Cost: 0

Topology Changes Counts: 0

Last Topology Change: 0

Figure 6-31 'STP status and global settings'

table6-12 'STP status and global settings' configuration description

		Description
Global setting	Spanning tree status	Enable or Disable STP on switch
	STP operation mode	Select one of STP mode
	BPDU data transfer	Set whether BPDU transmission is allowed when STP is prohibited on switches: ➤ Disable: Filter BPDU data packet

		➤ Enable: forward BPDU data packet
	Path cost	Choosing a Method to Calculate Path Cost ➤ do1t ➤ Do1d-1998
Bridge settings	Priority	Set the bridge priority value. After switching BPDU, the device with the lowest priority will become the root bridge. If all bridges have the same priority, their MAC addresses will be used to determine the root bridge. The increment of bridge priority value is 4096
	Hello Time	Set the time interval for the root bridge to wait between configuration messages in seconds
	Aging Time	Set the time interval in seconds that a switch can wait to receive configuration messages before attempting to redefine its own configuration.
	Forward delay	Set the time interval for the bridge to remain in the acquired state before forwarding the packet, in seconds
Status	ID Bridge	It consists of bridge priority and MAC address of switch
	Root bridge ID	It consists of root bridge priority and root bridge MAC address.
	Root bridge port	Ports that provide the lowest cost path from the bridge to the root bridge
	Root bride cost	Path Cost from the Bridge to the Root Bridge
	Total number of topology changes	Total number of STP topology changes that have occurred
	Latest topology change	Total number of STP topology changes that have occurred

6.7.3 STP interface Settings

- Select 'Switch management> Spanning tree> STP interface' to enter STP interface setting, as shown in figure 6-32.
- Click on the 'STP Interface Settings' interface to view the STP settings of all interfaces. Use filters to select an interface type of 'Port' or 'Aggregation group'
- The top right corner of the interface can set the number of items displayed on each page, and turn the page back and forth through the arrow button in the bottom right corner
- In 'STP port setting' interface, could edit STP interface setting.
- Click<Edit> to enter modify STP interface, as shown in figure 6-33.

- Modify configuration parameter. Detailed configuration, as shown in figure 6-13.
- Click<Apply> to complete operation.

The screenshot shows the 'STP Interface Settings' interface. At the top, there is a title 'STP Interface Settings' and a sub-header 'STP Interface Settings Table'. Below this, there is a filter section: 'Filter: Interface Type equals to Port' with a dropdown menu and a 'Go' button. The main part of the interface is a table with the following columns: Entry No., Interface, STP State, Edge Port, BPDU Guard, BPDU Filtering, Port Role, Path Cost, Priority, Port State, Designated Bridge ID, and Designated Port ID. The table contains five rows of data, each with a radio button in the first column. The data is as follows:

Entry No.	Interface	STP State	Edge Port	BPDU Guard	BPDU Filtering	Port Role	Path Cost	Priority	Port State	Designated Bridge ID	Designated Port ID
<input type="radio"/>	1 GE1/0/1	Yes	No	No	No	Disabled	20000	128	Forwarding	0/00:00:00:00:00:00	0/0
<input type="radio"/>	2 GE1/0/2	Yes	No	No	No	Disabled	20000	128	Disabled	0/00:00:00:00:00:00	0/0
<input type="radio"/>	3 GE1/0/3	Yes	No	No	No	Disabled	20000	128	Disabled	0/00:00:00:00:00:00	0/0
<input type="radio"/>	4 GE1/0/4	Yes	No	No	No	Disabled	20000	128	Disabled	0/00:00:00:00:00:00	0/0
<input type="radio"/>	5 GE1/0/5	Yes	No	No	No	Disabled	20000	128	Disabled	0/00:00:00:00:00:00	0/0

At the bottom of the table, there is an 'Edit...' button and a pagination control showing 'Page 1 Total 6'.

Figure 6-32 'STP interface Settings' interface

Table6-13 'STP interface settings' config description

Title	Description
interface	Select the port or LAG on which you want to configure STP
STP Enable	STP Enable or disable STP on the port
Edge port	Enable or Disable fast link on the interface Enable fast link --- Enable Fast Link Immediately Disable- disable fast link Note: If fast link mode is enabled for ports, the system will automatically put the port state in forwarding state when the port link is connected. Fast Link Optimizes STP Protocol Aggregation.
BPDU Guard	Enabling this option automatically restores ports when they enter the err-disable state due to BPDU protection
BPDU Filter	Enable this option to filter BPDU packets when STP is enabled
Path cost	Select 'User define' to manually set the root path cost generated by the port, or 'User default settings' to use the default path cost generated by the system.
Priority	Config port's priority value Note: If the bridge connects two ports in a loop, the priority value will affect port selection. Priority is from 0 to 240 with an increment of 16

Port status	<p>Display the current STP status of the port</p> <ul style="list-style-type: none"> ➤ Disable— STP is currently disabled on ports. Port forwards traffic while acquiring MAC address ➤ Blocking—Ports are currently blocked and cannot forward traffic (except BPDU data) or obtain MAC addresses ➤ Monitoring— The port is in monitoring mode. Ports cannot forward traffic, nor can they get MAC addresses. ➤ Learning— Ports are in learning mode. Ports cannot forward traffic, but can get new MAC addresses ➤ forwarding —The port is in forwarding mode. Ports can forward traffic and get new MAC addresses
Designated Bridge ID	Display bridge priority and MAC address of specified bridge
Designated Port ID	Display the priority and interface of the selected port
Designated Cost	Show the cost of adding ports to STP topology. If STP detects loops, the less expensive ports are, the less possibility they are to be blocked

6.7.4 RSTP interface Settings

Select 'Switch Management> Spanning Tree> RSTP interface settings' to enter 'RSTP interface setting'. As shown in figure 6-34

The screenshot shows the 'RSTP Interface Settings' window. At the top, it says 'RSTP Interface Settings Table' and 'Show 1-5 Total 28'. Below this is a filter bar: 'Filter: Interface Type equals to Port' with a dropdown arrow and a 'Go' button. The main part of the window is a table with the following columns: Entry No., Interface, Link TYPE, Port Role, Edge Port Operational Status, and Port Status. There are five rows of data, each with a radio button in the first column.

Entry No.	Interface	Link TYPE	Port Role	Edge Port Operational Status	Port Status
<input type="radio"/>	1 GE1/0/1	Point to Point	Disabled	No	Enabled
<input type="radio"/>	2 GE1/0/2	Point to Point	Disabled	No	Disabled
<input type="radio"/>	3 GE1/0/3	Point to Point	Disabled	No	Disabled
<input type="radio"/>	4 GE1/0/4	Point to Point	Disabled	No	Disabled
<input type="radio"/>	5 GE1/0/5	Point to Point	Disabled	No	Disabled

At the bottom left, there is an 'Edit...' button and a 'Active Protocol' button. At the bottom right, there is a pagination control: 'Page 1 Total 6' with navigation arrows.

Figure 6-34 'RSTP interface settings'

On the 'RSTP Interface Settings' interface, you can view the RSTP settings of all interfaces. Through filters, you can filter and select the interface type as 'Port' or 'Aggregation group'.

The top right corner of the interface can set the number of items displayed on each page and turn the page back

and forth through the arrow button in the bottom right corner.

- On the 'RSTP Interface Settings' interface, you can edit and modify RSTP interface settings.
- Select the interface that needs to be modified, click < **Edit** > button, and enter the interface of modifying RSTP interface settings, as shown in Figure 6-35
- Modify config parameter. Detailed configuration as shown in table 6-14,
- Click<**Apply**> to complete operation.

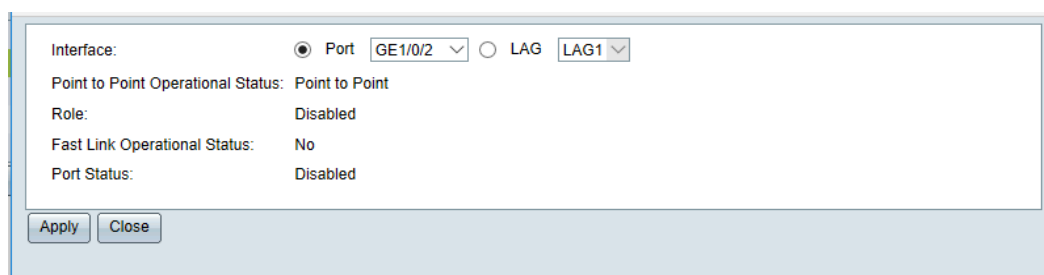


Figure 6-35 Modify 'RSTP interface setting'

Table6-14 'RSTP interface settings' configuration description

Title	Description
Interface	Select the port or LAG to configure RSTP
Link type management status	<p>Management status for selecting link type</p> <ul style="list-style-type: none"> ➤ Point to Point— Define the link state from point to point. Ports defined as full duplex are considered point-to-point port links. If this feature is enabled, the port is an RSTP edge port that can quickly enter forwarding mode (usually within 2 seconds) ➤ Sharing—The port link type is sharing. Ports defined as half-duplex are considered shared links ➤ Auto—Automatically determine switch status using RSTP BPDU
Link operation status	Display current Link type operation status.
Role	<p>Displays port roles specified by RSTP to provide STP paths. Possible roles are</p> <ul style="list-style-type: none"> ➤ Root—Minimum Cost Path for Forwarding Packets to Root Bridge ➤ Designated— Bridge provides the lowest cost path from LAN to root bridge through its interface to LAN ➤ Replace— Provide alternate paths from root interface to root bridge ➤ Backup—

	<p>Provides a backup path to the specified port path of the generated leaf node.</p> <p>If two ports in a loop are connected through a point-to-point link, a backup port will appear. If a LAN has two or more connections to a shared segment, a backup port will also appear</p> <ul style="list-style-type: none"> ➤ Disable—Ports do not add spanning Tree.
Edge port operation status	<p>Display the Edge Port Mode State on the Interface</p> <ul style="list-style-type: none"> ➤ Enable —Enable fast link ➤ Disable—Disable fast link ➤ Auto— Enable Fast Link Mode within seconds after the interface starts to be active
Port status	<p>Display RSTP status on a specific port :</p> <ul style="list-style-type: none"> ➤ Disable —STP is currently disabled on ports ➤ Blocking— Ports are currently blocked and cannot forward traffic or obtain MAC addresses ➤ Learning— Ports are in learning mode. Ports cannot forward traffic, but can get new MAC addresses ➤ Forwarding— The port is in forwarding mode. Ports can forward traffic and get new MAC addresses

6.7.5 MSTP properties

Select 'Switch management>Spanning Tree>MSTP', to enter 'MSTP properties' interface as shown in figure6-36.

Figure 6-36 MSTP properties

On the interface, you can view the current MSTP attributes or modify the configuration information directly, and then click < **Apply** > button to complete the configuration operation of modifying MSTP attributes. The detailed configuration is shown in table below.

Table 6-15 'MSTP properties' config description

Title	Description
Region Name	Setting Domain Name of MSTP Domain
Revision	Set up a modified version to identify the current MSTP configuration
MAX hops	The maximum number of hops in MST domain is set, which determines the size of MST domain. Only the parameter configured on the domain root will be valid in the domain, and the configuration on the non-domain root will not be valid.

6.7.6 VLAN to MSTP

Select 'Switch management> Spanning Tree> VLAN to MSTP instance' to enter VLAN to MSTP instance, as shown in figure 6-37.

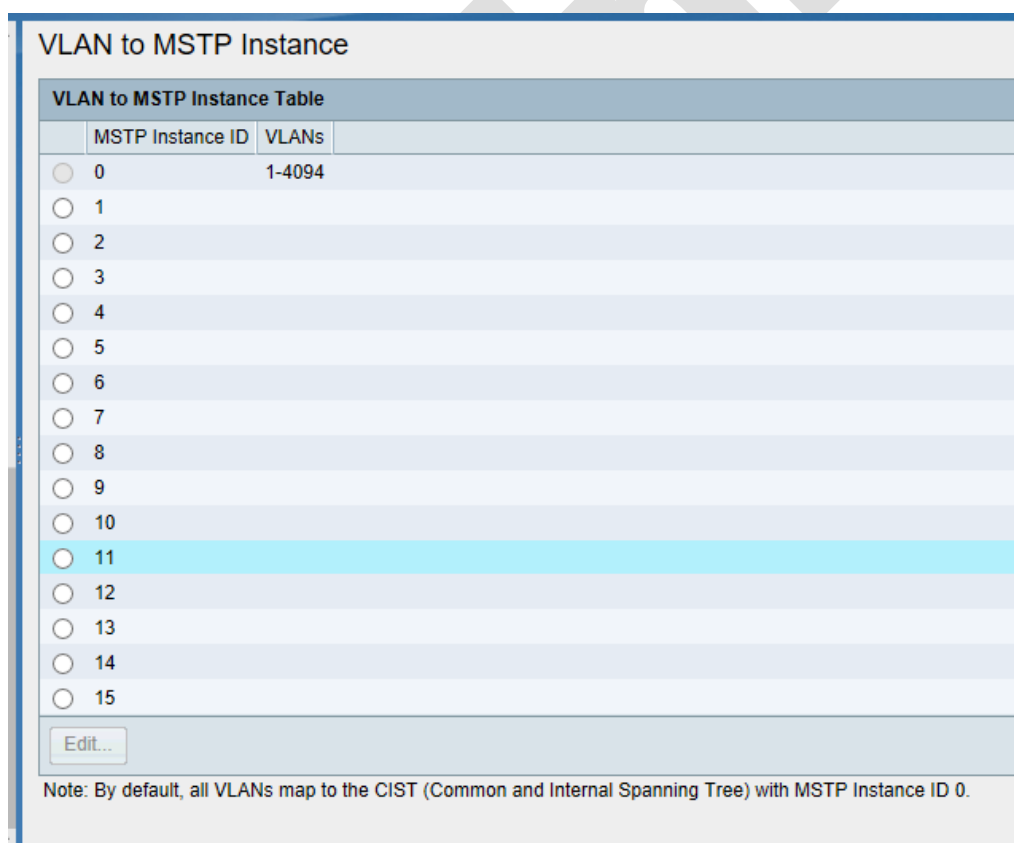


Figure 6-37 VLANs map to MSTP

On the 'VLAN Mapping to MSTP Instances' interface to view the VLAN mapping of each current instance.

(1) Modify the VLAN mapping of the instance

- Select the instance that needs to modify the VLAN mapping, click < Edit > and enter the modification

interface, as shown in Figure 6-38

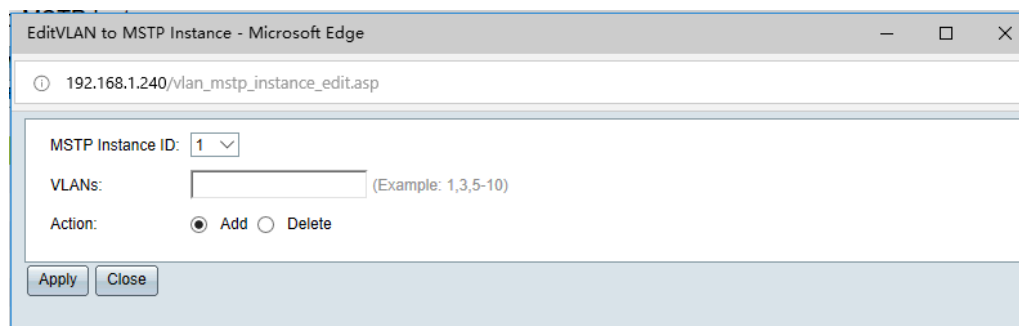


Figure 6-38 modify VLAN instance

- Modify the VLAN mapping corresponding to the instance, and configure it in detail as shown in table6-16
- Click<**Apply**> to complete operation.

Table 6-16 Description of VLAN Mapping Configuration for Instances

Title	Description
MSTP instance ID	Select the instance ID of the settings 1-15 is optional
VLANs	Set instance protection VLAN
Operation	<ul style="list-style-type: none"> ➤ Add: Add the input VLAN value to the protected VLAN of the instance ➤ Delete: Delete the input VLAN value from the protected VLAN of the instance

6.7.7 MSTP Instance Settings

Select 'Switch management> Spanning Tree > MSTP instance settings.' To enter 'MSTP instance settings' as shown in figure 6-39

Figure 6-39 MSTP instance settings

In the ‘MSTP instance settings’ interface, you can view the settings of the instance, or directly modify the configuration information, and then click the < **Apply** > button to complete the modification of the MSTP instance settings. The detailed configuration is shown in table below.

Table 6-17 Description of MSTP instance settings MSTP

Title	Description
Instance	Select the MSTP instance to set, range is 0-15
Bridge priority	Set the priority of the bridge in the instance
Designated Root Bridge ID	Display the priority and MAC address of the root bridge of the MSTP instance
Root port	Display the root port of the selected instance
Root path cost	Display the root path cost of the selected instance
Bridge ID	Displays the bridge priority and MAC address of this switch for the selected instance
Remaining Hops	Display the number of hops reserved for the next target

6.7.8 MSTP Interface Settings

Select ‘Switch management>Spanning Tree > MSTP interface setting’ to enter ‘MSTP interface setting. As shown in figure 6-40.

MSTP Interface Settings														
MSTP Interface Settings Table													Show 1-5 Total 28	
Entry No.	Interface	Interface Priority	Path Costs	Port Status	Port Role	Mode	Type	Designated Bridge ID	Designated Port ID	Designated Cost	Remaining Hops			
<input type="radio"/>	1	GE1/0/1	128	0	Forwarding	Disabled	MSTP	Point to Point	0/00:00:00:00:00:00	0/0	0	20		
<input type="radio"/>	2	GE1/0/2	128	0	Disabled	Disabled	MSTP	Point to Point	0/00:00:00:00:00:00	0/0	0	20		
<input type="radio"/>	3	GE1/0/3	128	0	Disabled	Disabled	MSTP	Point to Point	0/00:00:00:00:00:00	0/0	0	20		
<input type="radio"/>	4	GE1/0/4	128	0	Disabled	Disabled	MSTP	Point to Point	0/00:00:00:00:00:00	0/0	0	20		
<input type="radio"/>	5	GE1/0/5	128	0	Disabled	Disabled	MSTP	Point to Point	0/00:00:00:00:00:00	0/0	0	20		

Figure 6-40 'MSTP Interface Settings'

On the 'MSTP Interface Settings' interface to view the MSTP settings of all interfaces. Through filters, you can filter the selection of instances and interface types ('ports' or 'aggregation groups').

The top right corner of the interface can set the number of items displayed on each page, turn the page back and forth through the arrow button in the bottom right corner.

- On the MSTP Interface Settings interface, you can edit and modify the MSTP interface settings.
- Select the port need to be modified, click <Edit> to enter 'MSTP interface settings. As shown in figure 6-41.
- Select the interface that needs to be modified, click the < Edit > button, and enter the interface of modifying MSTP interface settings, as shown in figure 6-41.
- Modify the configuration parameters and configure them in detail as shown in table6-18
- Click <Apply> to complete operation

Interface:	<input checked="" type="radio"/> Port <input type="radio"/> LAG	<input type="text" value="GE1/0/1"/> <input type="text" value="LAG1"/>
Interface Priority:	<input type="text" value="128"/>	
Path Cost:	<input checked="" type="radio"/> Use Default Settings <input type="radio"/> User Defined <input type="text" value="0"/> (Range: 0-65535, Default: 19)	
Port State:	Forwarding	
Port Role:	Disabled	
Mode:	MSTP	
Type:	Point to Point	
Designated Bridge ID:	0/00:00:00:00:00:00	
Designated Port ID:	0/0	
Remaining Hops:	20	
<input type="button" value="Apply"/> <input type="button" value="Close"/>		

Figure 6-41

Table6-18 Configuration description for 'MSTP Interface Settings'

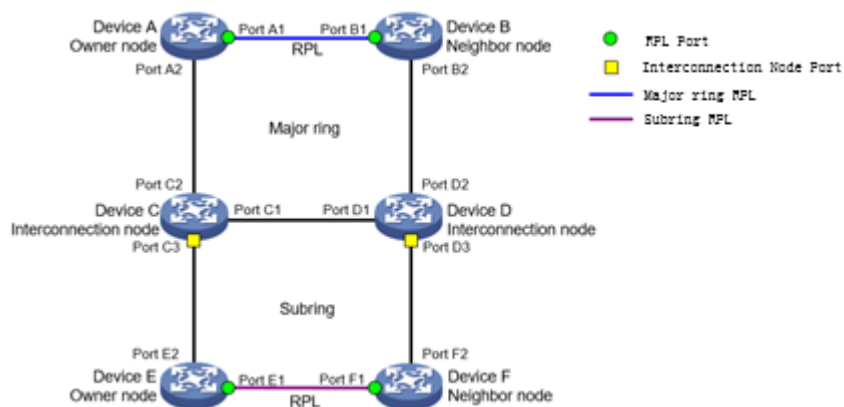
Title	Description
-------	-------------

Interface	Select the interface type and port for which you want to define the MSTP instance
Port priority	Select the priority of the MSTP instance for the specified port
Path cost	<p>Root path cost generated by setting ports.</p> <p>Select Use Default Settings to enter the root path cost manually using default values or select User Definition. Root path cost is the cost of the root bridge from the switch to the specified MSTP instance.</p>
Port status	<p>Display MSTP status of specific ports on specific MSTP instances</p> <ul style="list-style-type: none"> ➤ Disable – STP is currently banned ➤ Blocking— The port on this instance is currently blocked and cannot forward traffic (except BPDU data) or obtain a MAC address ➤ Monitoring — The port on this instance is in listening mode. Ports cannot forward traffic, nor can they get MAC addresses. ➤ Acquisition —The port on this instance is in acquisition mode. Ports cannot forward traffic, but can get new MAC addresses. ➤ Forwarding—The port on this instance is in forwarding mode. Ports can forward traffic and get new MAC addresses
Port role	<p>Display each port or LAG role of each instance (specified by the MSTP algorithm to provide STP paths):</p> <ul style="list-style-type: none"> ➤ Master — Master port refers to the port connected to the MST domain to the total root, which is located on the shortest path from the whole domain to the total root. ➤ Root— Forwarding data packets through this interface provides the lowest cost path for forwarding data packets to the root device ➤ Designated— Bridges provide the lowest root path cost of root bridges from LAN to MSTP instances through their interfaces to LAN. Replace—This interface provides alternate paths from the root interface to the root device ➤ Backup— This interface provides a backup path to the specified port path of the generated leaf node. If two ports in a loop are connected through a point-to-point link, a backup port will appear. If a LAN has two or more connections to a shared segment, a backup port will also appear ➤ Disable —Interfaces do not add spanning trees
Mode	<p>Display current spanning tree's mode</p> <ul style="list-style-type: none"> ➤ STP —Enable Classic STP on port.

	<ul style="list-style-type: none"> ➤ RSTP —Enable RSTP on port ➤ MSTP —Enable MSTP on port
Type	<p>Display MSTP type of the port</p> <ul style="list-style-type: none"> ➤ Boundary — The edge port can connect the MSTP bridge to the LAN in the edge area. If the port is an edge port, it also indicates whether the device at the other end of the link works in RSTP or STP mode. ➤ Internal —Ports are internal ports.
Designated Bridge ID	Display the bridge ID number that connects the link or shared LAN to the root
Designate Port ID	Displays the port ID number of the link or shared LAN connected to the root on the specified bridge
Remaining Hops	<p>Display remaining Hops</p> <p>Display hops reserved for the next target</p>

6.8 ERPS

ERPS (Ethernet Ring Protection Switching) is a link layer technology with high reliability and stability. It prevents broadcast storms caused by data loops when the Ethernet ring is complete. When the link failure occurs, it quickly restores the communication pathway between the nodes in the ring network and has a high convergence speed.



Picture 6-42 ERPS basic network forming

(1) ERPS ring

ERPS rings are divided to enter main rings and sub-rings. ERPS can be composed of a single main ring or multiple main rings and sub-rings as shown in Figure 6-42. The main ring is a closed ring, and the sub-ring is attached to the main ring and is not closed.

(2) Node role

Each device on the ERPS ring is called a node. Node roles are determined by the user's configuration and are divided to enter the following categories:

Owner node: The primary node is responsible for blocking and releasing the ports on the RPL of the node to prevent the formation of loops and link reversal.

Neighbor node. Node on RPL and Owner node. Coordinate Owner node to block and release port on RPL at this node.

Neighbor Node: Neighbor node, the node connected with Owner node on RPL, cooperate with Owner node to block and open the port on RPL on this node, and perform link inversion

Normal Node: A common node responsible for receiving and forwarding protocol and data messages in the link

(3) Port role

RPL Port: The port at both ends of the RPL link, only the primary node and the neighbor node exist

Ordinary Port: Ring Port of Non-RPL Port

(4) ERPS ring status

Idle state: After the ring initialization, it enters the stable state. When Owner node enters the Idle state, other nodes enter the Idle state accordingly. Among them, the RPL ports of Owner node and Neighbor node are blocked, i.e. PRL is not accessible; Owner node sends (NR, RB) messages regularly

Protection state: When a link in the loop network fails, the loop is protected and replaced, and finally stabilizes to the state. The RPL port of Owner node and Neighbor node is opened, that is, PRL is opened to ensure that the whole ring network is still open. When one node in the link enters the Protection state, the other nodes then enter the Protection state.

MS status: In MS status, traffic forwarding paths can be manually reversed. When MS operation is performed on one node in the link, other nodes enter the MS state accordingly

FS state: FS state can forcibly reverse traffic forwarding path. When FS operations are performed on one node in the link, the other nodes then enter the FS state.

Pending state: Pending state is an unstable state, a transitional state of states during jumping

When the loop is normal, it is in the Idle state; when the link fails, it is in the Protection state.

6.8.2 ERPS Global Settings

Select 'Switch management>ERPS> Global setting' to enter ERPS global setting interface. As shown in figure6-43

- In ERPS global setting interface, could enable/disable ERPS global.
- Check 'Enable', click <Apply>, enable ERPS.

- Do not check 'Enable', click the 'Apply' button and disable ERPS

Figure 6-43 ERPS Global setting

Note: The global configuration page is also a display page, if you open the page. 'Enable' is a check state, table indicates that ERPS is currently globally enabled, and table indicates that ERPS is currently globally disabled if the state is to be checked.

ERPS global enablement is required before ERPS ring or editing ring information can be created

6.8.2 Ring Setting

Select 'Switch management >ERPS> ERPS ring setting' to enter ERPS ring setting interface.

ERPS ring settings page can create ERPS ring and edit setting ring information

(1) Create ERPS ring

- Enter the ERPS ID number in 'Create ERPS Ring' and click <Create> to create the corresponding ERPS Ring and display the ring information in 'Ring Table', as shown in Figure 6-44.
- 'Ring table' displays information about all rings currently created
- After the ring is created, all information is in the default state and needs editing and modification

Ring ID	ERPS Type	Belong Major	Node Mode	Control Vlan	Instance	Revertive Mode	Ring State	Ring Port	Ring Port
0 Results Found.									

Figure 6-44 ERPS ring config interface

(2) Delete ERPS ring.

In the 'ring table', select the ERPS ring that needs to be deleted and click the < **Delete** > button

(3) Edit ERPS ring

Select the ERPS ring (check box) in the 'Ring Table' to modify the information, click the < **Edit** > button, and pop up the edit dialog box in Figure 6-45 below.

The WEB interface can modify ERPS type, node mode, protocol VLAN, protection instance, revertive mode and Ring Port. Detailed configuration is shown in table6-19.

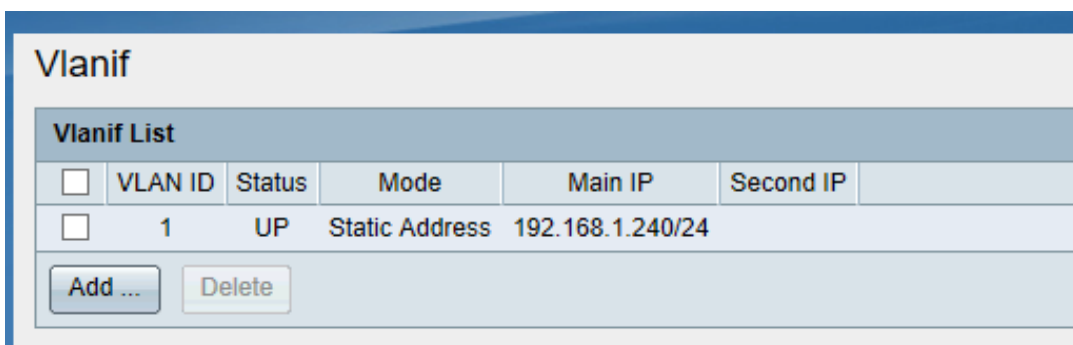


Figure 6-45 ERPS ring edit interface

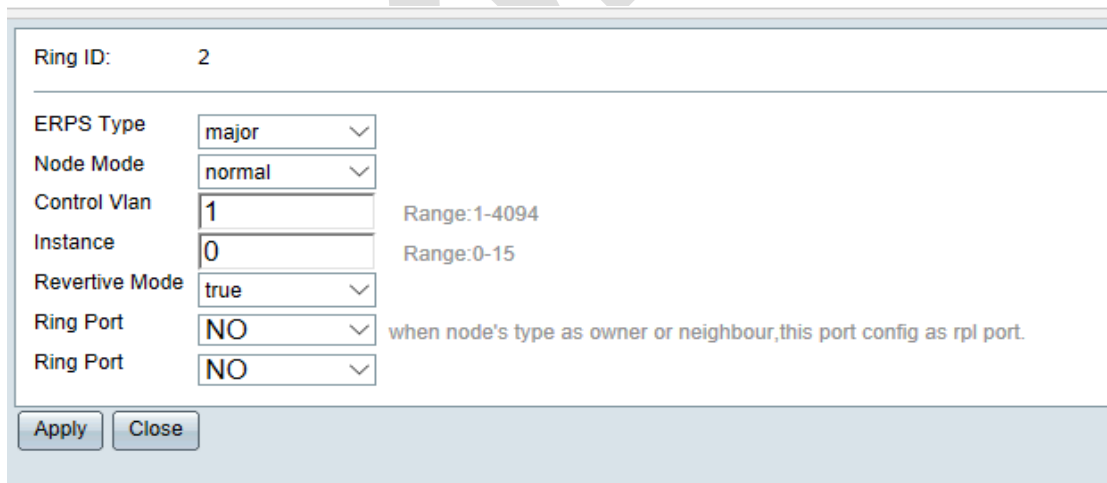


Table6-19 Description of ERPS configuration parameter

Title	Description
ERPS ring type	Select the type of ring you want to create, Major or sub

Major ring Mark	<p>That is, the main ring identifier of the sub-ring belongs to. When the ring type is Sub, the main ring identifier needs to be input</p> <p>Note: Subrings at intersecting nodes need to be configured as Sub and the identity of the primary ring to which they belong. Subrings of non-intersecting nodes, because they do not belong to a main ring, do not need to configure the ring type to be Sub</p>
Node type	<p>The role of the node in the ring. The node types include normal, owner, neighbors</p>
Protocol VLAN	<p>Created ring's ERPS protocol VLAN, range 1-4094. And created VLAN</p> <p>The ERPS protocol VLAN of the created ring ranges from 1 to 4094, and VLAN has been created.</p> <p>The ERPS protocol VLAN of the created ring ranges from 1 to 4094, and VLAN has been created</p> <p>Note: The same ring protocol VLAN is also the same.</p>
Protection instance	<p>Ring protection instance, range is 0-15. ERPS ring only work for VLAN in protection instances.</p> <p>Note: VLAN settings for protected instances are set in spanning tree instance mapping settings</p>
Revertive mode	<p>Could configure Recovery or non-Recovery mode on Owner node.</p> <p>Owner node can be set to revertive or non-revertive mode</p>
Ring Port	<p>Loop Port, Optional Ethernet Physical Port or Aggregate Logic Port</p> <p>Note: The ring port should be set to Trunk mode and allow the VLAN and protocol VLAN that protect the instance to pass through.</p> <p>If it is an Owner or Neighbors node, the first Ping port is defaulted to RPL port, and the second Ring Port is a normal port.</p>

Chapter 7 Route Management

Note: Only layer3 series switch support the functions of this chapter. Specific reference is given to the actual equipment and mode

7.1 Virtual port

7.1.1 overview

The host computers of different VLANs cannot communicate directly. By configuring the virtual interface of VLAN on the device, three layers of interworking between VLANs can be realized

VLAN virtual interface is a layer 3 virtual interface, which does not exist on the device as a physical entity. Each VLAN corresponds to a VLAN virtual interface. After configuring the IP address for the VLAN virtual interface, the IP address can be used as the gateway address of the network equipment in the VLAN, and three-layer forwarding of messages that need to cross network segments based on IP address is carried out.

7.1.2 Virtual Interface Settings

In the navigation bar, select 'Router management>L3 route setting> Virtual interface setting' to enter 'Vlanif list'.

(1) In the 'Vlanif' interface, you can view all the current virtual interfaces and their related configuration information, as shown in Figure 7-1

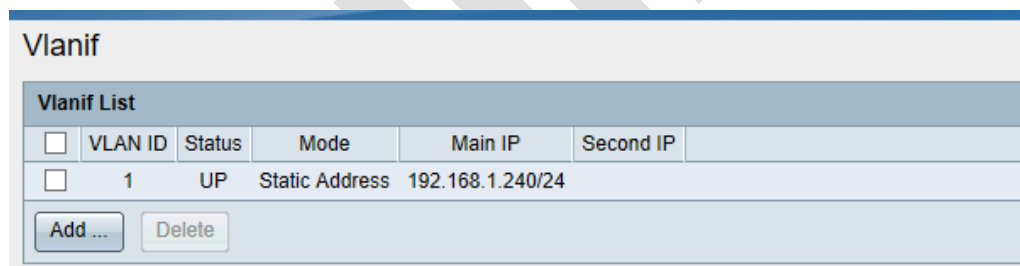


Figure7-1 Vlanif interface

- In 'Vlanif list' interface, you could add virtual interface
- Click<Add> below 'Vlanif' list to enter the 'Add virtual interface'. As shown in figure7-2.
- Fill in Vlanif configuration. Details configuration as show in table7-1
- Click< Apply> to complete operation.

Table7-1 Description of Virtual Interface Configuration Parameters

Title	Description
VLAN ID	Virtual interface VLAN
address type	IP address is divided to enter dynamic and static address ➤ Static:

	<p>You need to manually configure IP addresses and masks, no lease time.</p> <p>➤ Dynamic: No need to configure manually, get IP address automatically through DHCP server, with lease time.</p>
IP address	Static IPv4 address, which needs to be set when the IP address type is static. The format points are decimal, and the IPv4 address of each interface can't be in the same network segment.
Mask	IPv4 address's mask, 1 for match, 0 for mismatching.

(3) In 'Vlanif list' delete virtual port

- In 'Vlanif' list Select the virtual port that need to delete. Click < **Delete** > to complete operation.
- Select the virtual interface that needs to be deleted in the 'virtual interface' column table and click the < **Delete** > button to complete the operation.

Note: When deleting the IP address being logged in or the virtual interface of the VLAN, the WEB connection will be disconnected. Please reconfigure it through the command line or query the IP address that the device can connect before login.

7.2 ARP Management

7.2.1 Overview

ARP (Address Resolution Protocol) is a protocol that resolves IP addresses to enter Ethernet MAC addresses (or physical addresses).

In a LAN, when a host or other network device has data to send to another host or device, it must know the other's network layer address (that is, IP address). But only IP address is not enough, because IP data messages must be encapsulated to enter frames to be sent through the physical network, so the sending station must also have the physical address of the receiving station, so a mapping from IP address to physical address is needed. ARP is the protocol that implements this function.

(1) ARP table

After the device resolves to the destination MAC address through ARP, it will add the mapping table item from IP address to MAC address in its ARP table for subsequent forwarding to the same destination message

ARPtable items are divided to enter dynamic ARPtable items and static ARPtable items

(2) Dynamic ARP table

Dynamic ARP table item is automatically generated and maintained by ARP protocol through ARP message. It

can be aged, updated by new ARP message and covered by static ARP table item. The corresponding dynamic ARPtable items will be deleted when the aging time and interface downs are reached

(3) Static ARP table

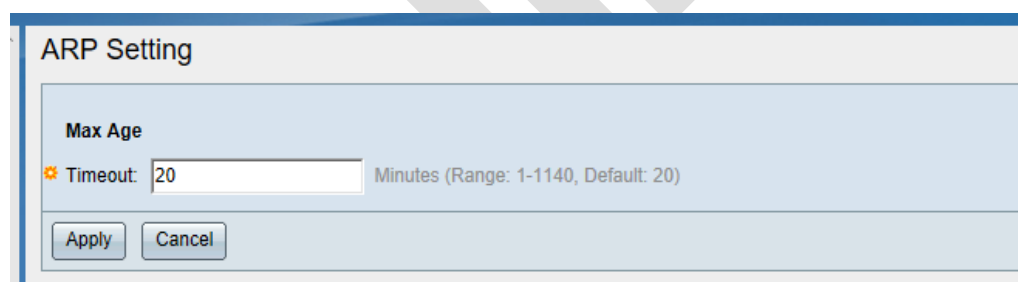
Static ARP table items are manually configured and maintained, and will not be aged and recover by dynamic ARP table items.

Configuring static ARPtable items can increase communication security. Static ARPtable item can restrict and specify only the specified MAC address when the device communicates with the specified IP address. In this case, the attack message cannot modify the mapping relationship between the IP address and MAC address of the table item, thus protecting the normal communication between the device and the specified device.

7.2.2 ARP properties

In the navigation bar, Select 'Route management> L3 interface setting>ARP properties ', you can view ARP aging time ,as shown in figure7-3.

Enter the aging time and click the < **Apply** > button to modify the ARP aging time (range 1-1140 minutes, default 20 minutes)



ARP Setting

Max Age

✱ Timeout: 20 Minutes (Range: 1-1140, Default: 20)

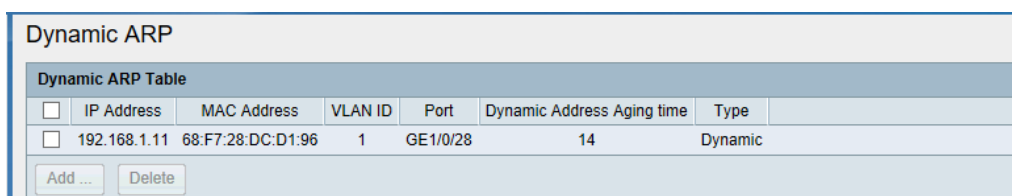
Apply Cancel

Figure7-3 ARP aging time

7.2.3 Dynamic ARP

Select 'Route management> L3 interface setting > dynamic ARP' to enter 'dynamic ARP table' interface.

Dynamic ARP table shows all the ARP entries learned, which can be viewed and deleted. As shown in Figure 7-4



Dynamic ARP

Dynamic ARP Table						
<input type="checkbox"/>	IP Address	MAC Address	VLAN ID	Port	Dynamic Address Aging time	Type
<input type="checkbox"/>	192.168.1.11	68:F7:28:DC:D1:96	1	GE1/0/28	14	Dynamic

Add ... Delete

Figure 7-4 Dynamic ARP table

7.2.3 Static ARP

(1) View dynamic ARP table

Select 'Rout management > L3 interface setting> Static ARP' to enter 'static ARP table'. As shown in figure 7-5, interface display all the static ARP item's information.

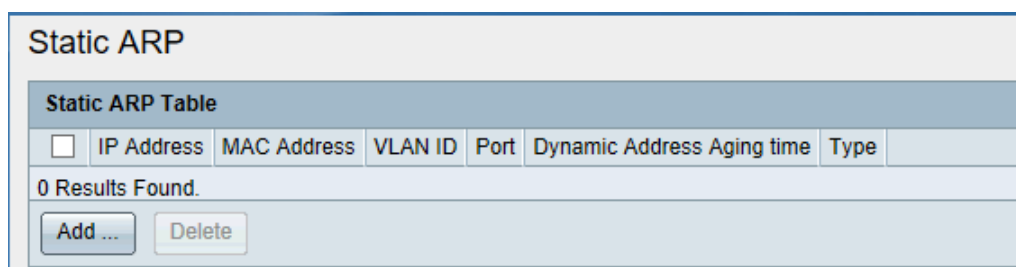


Figure 7-5 Static ARP table

Add static ARP table

- Click<**Add**> to enter 'add static ARP' interface, as shown in figure7-6.
- Configure static ARP table's information. Details configuration as shown in table 7-2.
- Click<**Apply**> to complete operation

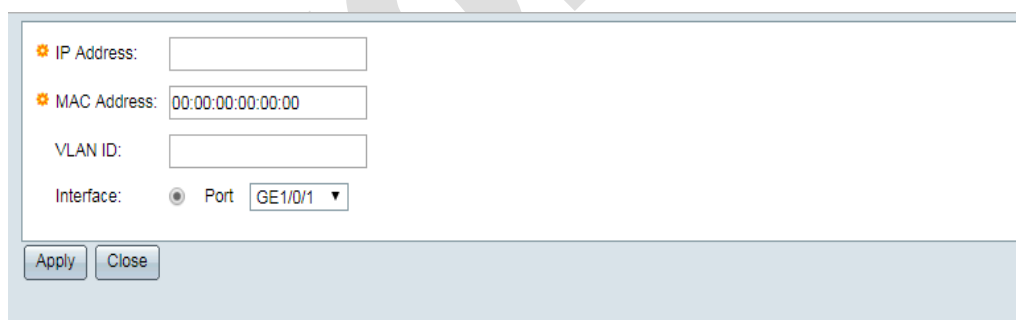


Figure 7-6 Add static ARP

Add static ARP configuration parameter.

Table 7-2 Description of Static ARP configuration

Title	Description
IP Address	Configure static ARP table's IP address.
MAC address	Configure ARP table's MAC address
VLAN ID	Configure VLAN that static ARP table belong to. VLAN ID request 1-4094 and created.
Port	Select static ARP's interface (Ethernet physical port).

Delete static ARP table.

Select single or several static ARP table items, click<**Delete**> to complete the deletion operation.

7.3 Route Table Management

7.3.1 Overview

In the network, the router chooses an appropriate path according to the destination address of the received message and forwards the message to the next router. The last router in the path is responsible for forwarding the message to the destination host. Routing is the path information of the message in the process of forwarding, which is used to guide the message forwarding.

This chapter 'Routing table management' is mainly used to maintain five types of routing tables: direct routing, dynamic routing, static routing, black hole routing and Reject routing.

(1) direct routing

Routing Discovered by Direct Link Layer Protocol, also known as Interface Routing

(2) dynamic routing

Dynamic routing refers to routing discovered by routing protocols. The software platform currently supports OSPF and RIP dynamic routing. Details can be found in chapters 7.4 and 7.5

(3) static routing

Static routing is a special kind of routing, which is manually configured by administrators. It is mainly used in networks with relatively simple network structure. However, static routing cannot automatically adapt to the changes of network topology. When the topology changes, there may be Reject routing, resulting in network interruption. At this time, network administrators need to manually modify the configuration of static routing.

- Static route also has following properties.

Destination reachable routing, normal routing is the case, that is, IP messages are sent to the next hop according to the route identified by the destination, which is the general use of static routing

When the static route to a destination has the 'reject attribute', any IP message to that destination will be dropped and the source host destination will be notified that the destination is Reject

Blackhole routing: When a static route to a destination has a 'blackhole' property, regardless of the next hop

address configured, the outgoing interface of the route is Null 0 interface, and any IP message to that destination will be dropped without notifying the source host

7.3.2 Direct Table

Select 'Route management> Route table management> Direct table' to enter direct table, as shown in figure 7-7.

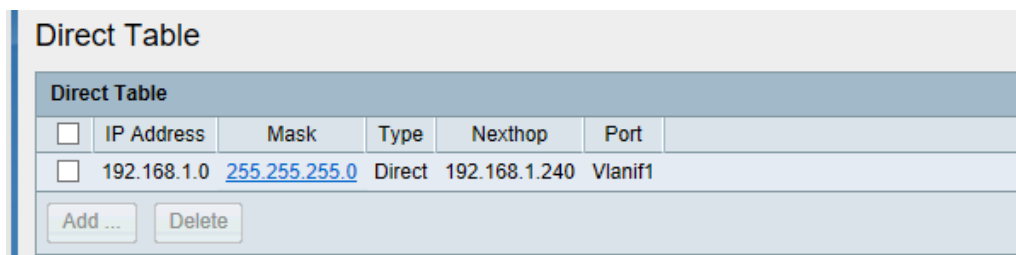


Figure 7-7 Direct Table

View the direct route table, details description as shown in following table.

Table 7-3 Detailed description of routing tables.

Title	Description
Ip address	The destination IP address and mask of routing
Mask	
Type	The type of routing, that is. discover the routing protocol for the IPv4 routing
Next hop	Next hop address of routing
Port	The routed outgoing interface, from which the packet to the destination segment will be sent

7.3.3 Dynamic Table

Select 'Route management> Route table management> Dynamic route' to enter dynamic route table, as shown in Figure7-8.

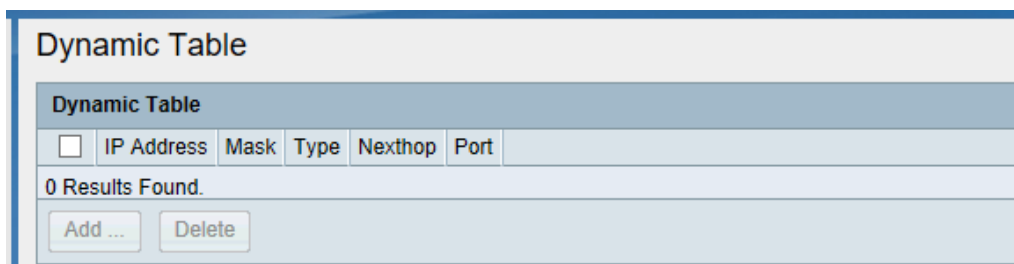


Figure 7-8 dynamic route table

7.3.4 Static Route Table

View static route table

Select 'Route management> Route table management> Static Table' to enter static route table, as shown in figure 7-9.

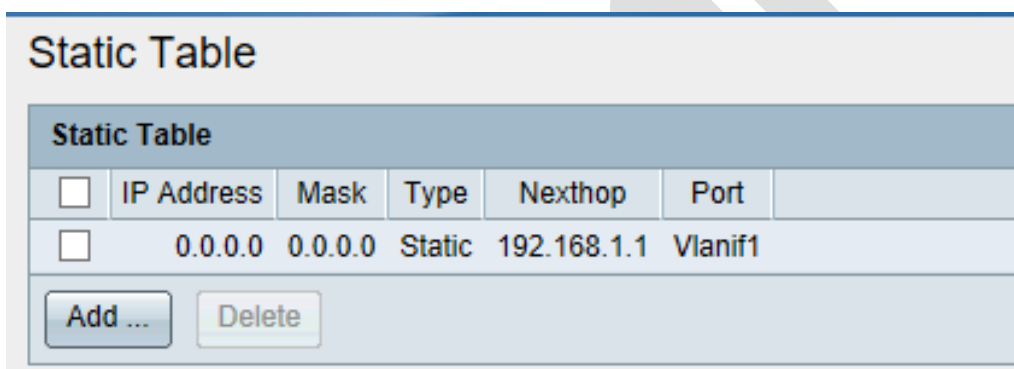


Figure 7-9 Static route table

Details of static routing tables, as shown in table7-3

(2) Add static route

- In 'Static route table' interface, click<Add> to enter create static route interface, as shown in figure 7-10.
- Configure static routing parameter. As shown in table 7-3(Notice: Select the type of 'static')
- Click<Apply> to complete operation

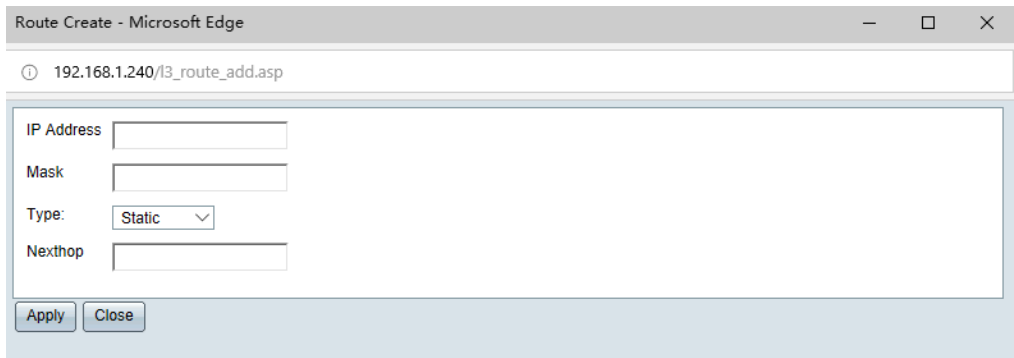


Figure 7-10 Static Route Create

Delete static route

In the 'Static routing table' interface, select one or a group of static routing entries that need to be deleted, and click the < Delete > button to complete the operation.

7.3.5 Blackhole Table

View blackhole table.

Select 'Route management> route table management> Blackhole route' to enter blackhole route table as shown in figure 7-11.

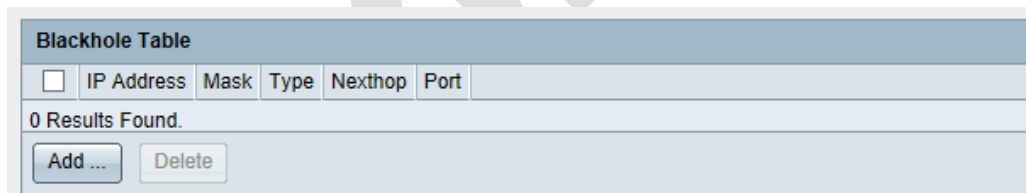


Figure 7-11 Blackhole route table

Details of black hole routing tables, as shown in table7-3

(2) Add blackhole route

In 'Blackhole table' interface click <Add> to enter blackhole route creating interface. As shown in figure 7-12.

- Click the < Add > button on the 'Black Hole Routing Table' interface to enter the Black Hole Routing Creation Interface, as shown in Figure 7-12.
- Configure blackhole routing parameters, as shown in table7-3. (Notice: select the type of blackhole)
- Click<Apply> to complete operation.

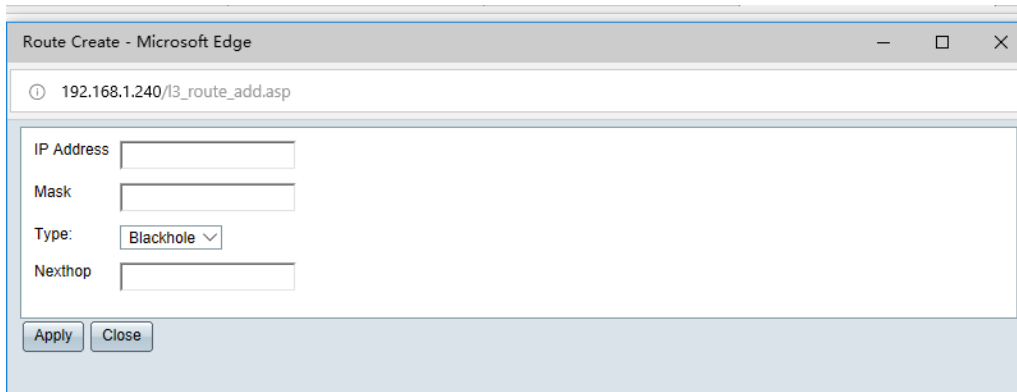


Figure 7-12 Blackhole creating interface

7.3.6 Reject Table

View Reject table

Select 'Route management> Route table management>Reject table' to enter reject table, as shown in figure 7-13.

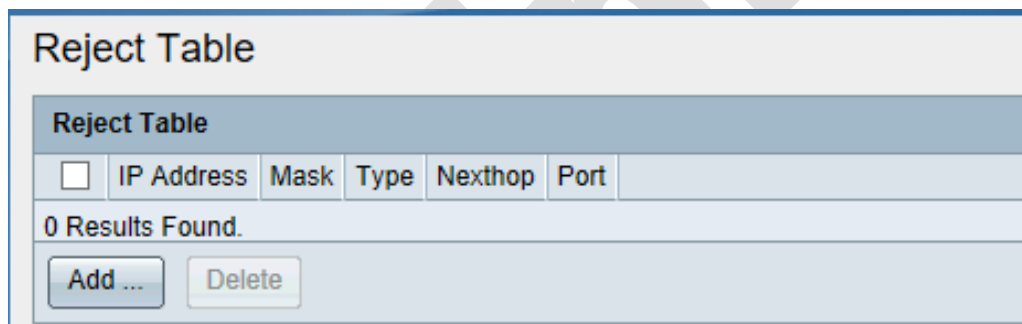


Figure 7-13 Reject Table

Details of Reject table, as shown in table7-3.

Add reject route

- In Reject table interface click<Add> to enter reject table creating interface, as shown in figure 7-14.
- Configure reject route parameter, as shown in table7-3(Notice: select the type of 'Reject')
- Click<Apply> to complete operation

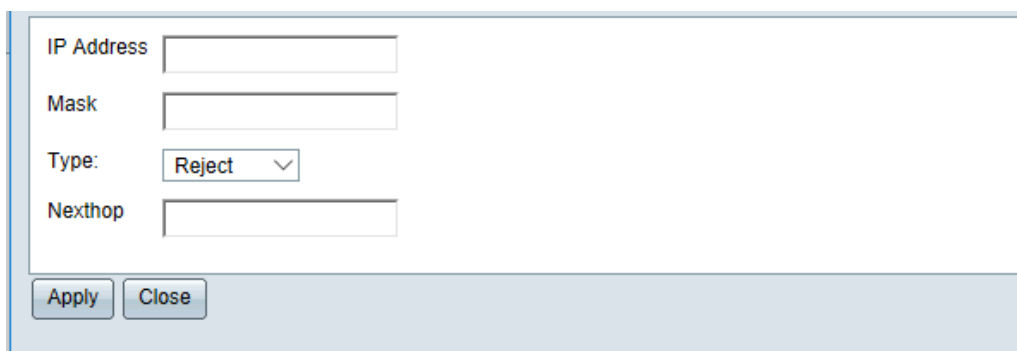


Figure 7-14

Delete Reject table

In the 'Reject table' interface, select one or a group of reject routing entries that need to be deleted, and click the < **Delete** > button to complete the operation

7.4 OSPF Management

7.4.1 Overview

OSPF (Open Shortest Path First) is an internal gateway protocol based on link state developed by IETF. Basic concepts of OSPF:

Router-ID:

Route-ID is the unique identifier of router in OSPF

DR/BDR:

DR/BDR: Designated router and backup designated router. In a LAN connection, OSPF elects one router as DR, and another as BDR. All other routers connected with DR and BDR form a fully adjacent state and only transmit LSA (link state). Announcement) to DR and BDR

OSPF Area:

OSPF area: Routers in an area will not need to know the topology details outside their area. In this environment, OSPF divides AS (Autonomous Region) into several regions and links them through backbone regions. Routers only need to have the same link state database as other routers in their region. The reduction of link state database means that less LSA notifications are processed and numbers of LSAs are processed. Floods are confined to an area

District communication classified to three type, they are Intra-Area Traffic\Inter-Area Traffic, External Traffic.

Regional traffic is also divided into three types: Intra-Area Traffic, Inter-Area Traffic and External Traffic

Intra-Area Traffic:

A router with the same area ID

Area Boundary Router:

A router located in one or more OSPF areas that connects the area to the backbone network

Backbone routers

(At least one interface of this kind of routers belongs to the backbone region (area ID 0).

All ABRs and internal routers in Area0 are backbone routers

ASBR (Autonomous System Boundary Router):

Routers that exchange routing information with other AS are called ASBR. ASBR does not necessarily lie at the boundary of AS. It may be either an intra-area router or an ABR. OSPF router introduces information about external routing, it becomes ASBR.

Area-id:

Routers must be configured in the same OSPF area, otherwise they cannot form neighbors

Hello time and Dead time:

That is to say, the Hello time and Dead time between routers must be the same, otherwise the neighbor Router time and Dead time cannot be formed

Authentication:

Routers must have the same authentication password, and if the passwords are different, they cannot form neighbors

7.4.2 OSPF setting

Select 'Route management>OSPF management>OSPF management' to enter OSPF configuration interface.

In the 'OSPF management' interface, you can open or close OSPF status and set Router ID, as shown in figure 7-15.

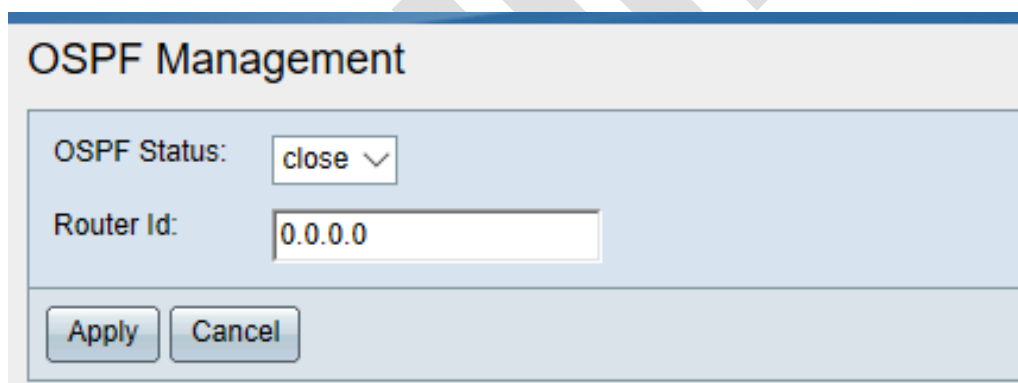


Figure 7-15 OSPF Global setting

Select or fill in the configuration items that need to be modified. Detailed configuration is shown in the table below.

Table 7-4 OPSF Global Configuration Information Description OPSF

Title	Description
OSPF state	Select whether to enable OSPF <ul style="list-style-type: none">➤ Open➤ Close: In this state, other OSPF configurations cannot be set.

Router Id	Router ID, default 0.0.0.0, configuration range is static IPv4 address, format point decimal
-----------	--

Click < **Apply** > to take effect. If the configuration item is filled in incorrectly, there will be corresponding prompts

7.4.3 OSPF Setting

Select 'Route Management > OSPF Management > OSPF Settings' from the navigation bar and go to the page shown in Figure 7-16. This page shows the OSPF network that has been configured.

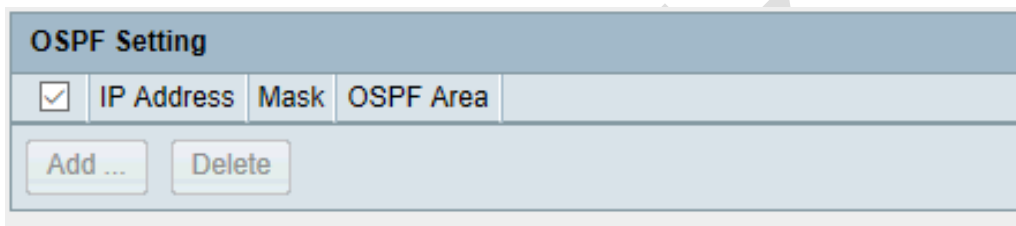


Figure 7-16 OSPF network setting interface

Click < **Add** > to enter the page as shown in figure 7-17. Configure OSPF networks and regions to be published on this page.

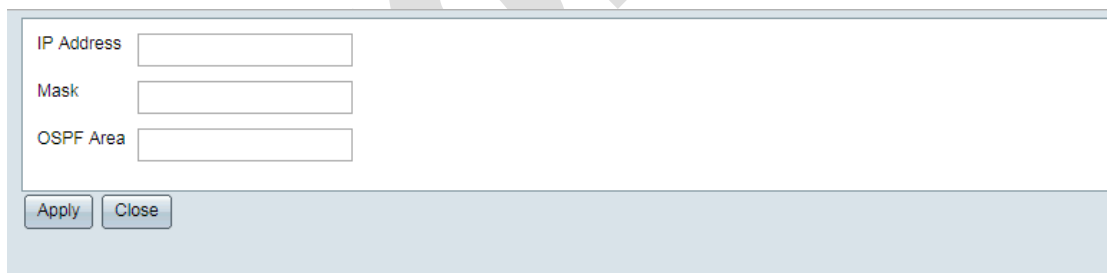


Figure 7-17 OSPF Network Configuration

Select the OSPF network and click < **Delete** > to delete the OSPF network

7.4.4 OSPF area

Select 'Route Management > OSPF Management > OSPF Domain Settings' and go to the page as shown in Figure 7-18. This page shows the OSPF fields that have been set up

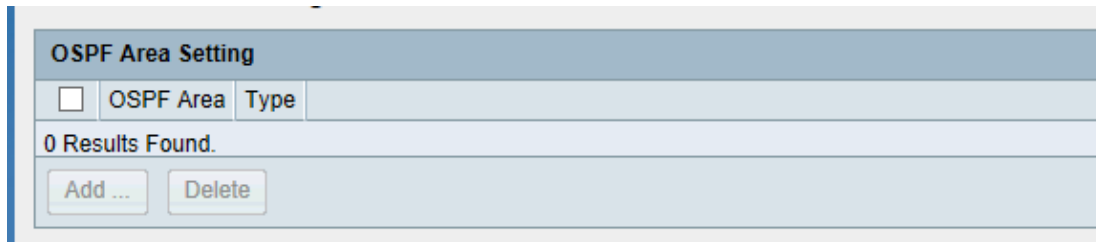


Figure 7-18 OSPF area setting interface

- On pages 7-18, you can add area settings to OSPF
- Click<**Add**> to enter OSPF area setting interface, as shown in figure 7-19.
- Fill in the appropriate configuration information, as shown in table7-5
- Click<**Apply**> to complete operation.
- The OSPF area can be deleted
- Check the area you want to delete and click < **Delete** > to complete the operation

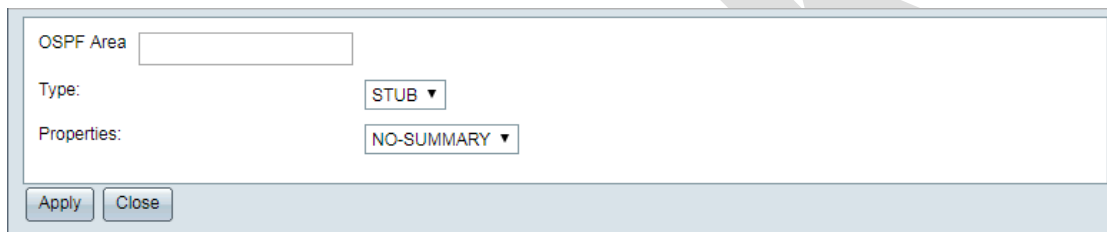


Figure 7-19 OSPF area setting

Detailed description of OSPF domain configuration information as shown in table7-5

Table 7-5 OSPF area setting description

Title	Description
OSPF area	ID of multiple regions in Autonomous Region, Format is 0-4294967295, or A.B.C.D.
Type	Select the type of region, two optional STUB, NSSA <ul style="list-style-type: none"> ➤ stub -- the peripheral region ➤ nssa -- incomplete peripheral region
Attributes	, Summary、 NO-Summary Select OSPF attributes, Summary, NO-Summary

7.4.5 OSPF status

Select 'Route Management > OSPF Management > OSPF Status' in the navigation bar and go to the page shown in Figure 7-20 to view the status information of OSPF operation, including global status, regional status, etc.

```

OSPF Status

OSPF Routing Process, Router ID: 192.168.1.240
Supports only single TOS (TOS0) routes
This implementation conforms to RFC2328
RFC1583Compatibility flag is disabled
OpaqueCapability flag is disabled
Initial SPF scheduling delay 200 millise(c)s
Minimum hold time between consecutive SPFs 1000 millise(c)s
Maximum hold time between consecutive SPFs 10000 millise(c)s
Hold time multiplier is currently 1
SPF algorithm has not been run
SPF timer is inactive
Refresh timer 10 secs
Number of external LSA 0. Checksum Sum 0x00000000
Number of opaque AS LSA 0. Checksum Sum 0x00000000
Number of areas attached to this router: 0

```

Figure 7-20 OSPF Status interface (Partially Shown above)

7.4.6 OSPF Neighbor

Select 'Route Management > OSPF Management > OSPF Neighbor Table' and enter the 'OSPF Neighbor Table' interface, as shown in Figure 7-21.

OSPF Neighbor						
Neighbor ID	Pri	State	Dead Time	Address	Interface	RXmtL RqstL DBsmL

Figure 7-21 OSPF neighbor

7.5 RIP Management

7.5.1 Overview

Routing Information Protocol (RIP) is a routing protocol based on distance vector algorithm, which uses hops as measurement standard. It has low bandwidth, configuration and management requirements and is mainly suitable for small-scale networks.

(1) Routing Establishment

After the router runs RIP, it will send the route update request first, and the router that receives the request will send its own RIP route to respond. After the network is stable, the router will send the route update information periodically.

(2) Calculation of Distance Vector

RIP measures the number of hops, which is 1, that is to say, the cost of each link is 1, regardless of the actual bandwidth, delay and other factors of the link, RIP allows up to 15 hops

RIP uses metrics to table the distance between it and all known destinations

When a RIP update message arrives, the receiver router compares with each item in its RIP routing table and modifies its RIP routing table according to the distance vector routing algorithm

(3) Timer

Update timer: Used to stimulate RIP router routing table updates, regularly broadcast their own routing table information to their neighbors.

Timeout: Used to determine whether a routing is available. When a route is activated or updated, the timer initializes and invalidates the route if no update is received within 180 seconds

Clearance Timer: Used to determine whether a route is cleared or not. When the router recognizes that a route is invalid, it initializes a clearance timer and deletes the route from the routing table if no update to the route has been received within 120 seconds

7.5.2 RIP Status setting

Select 'Route management> RIP management> RIP setting' to enter 'RIP setting' interface

In 'RIP setting' interface, could config Open or close RIP status, as shown in figure 7-22.

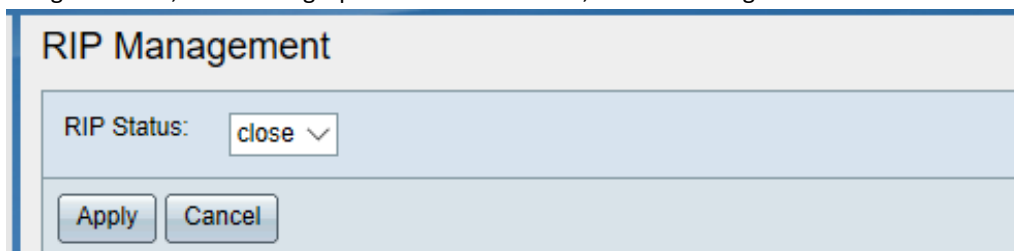


Figure 7-22 OSPF status settings

Note: When RIP status is close, other RIP configurations cannot be set

7.5.3 RIP Settings

Select 'Route Management > RIP Management > RIP Settings' in the navigation bar and go to the page shown in Figure 7-23. This page shows the configured RIP network

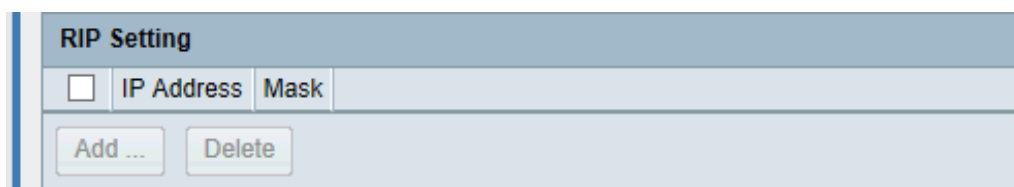


Figure 7-23 RIP network setting interface

Click <Add> to enter the page as shown in figure 7-24, I. Configure OSPF networks and regions to be published on this page.

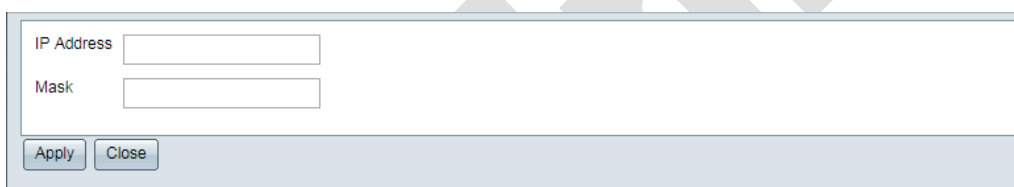


Figure 7-24 RIP Network Configuration

Select RIP network and click <Delete> to delete RIP network

7.5.4 RIP neighbor

In the navigation bar, select 'Route management> RIP management>RIP neighbor' to enter 'RIP neighbor table' interface, as shown in figure 7-25.

RIP Neighbor Table displays the running status of RIP, including timer, version number, published network, management distance, etc.

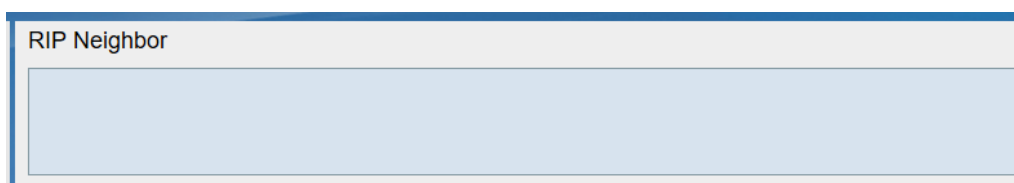


Figure 7-25 RIP neighbor table interface

Chapter 8 Network Security

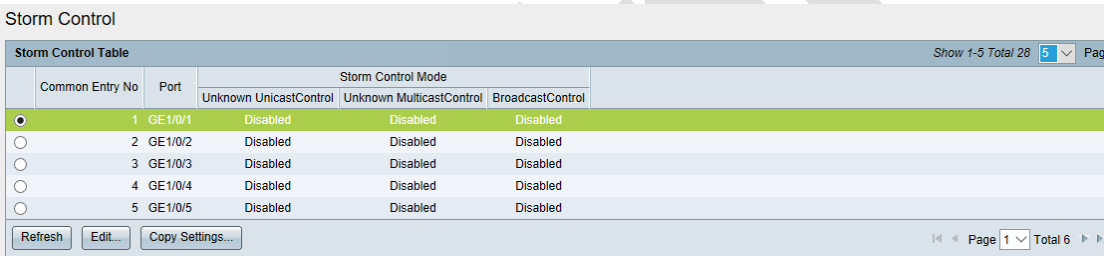
8.1 Broadcast Storm Suppression

8.1.1 Overview

Normal operation: when the broadcast/multicast/unknown unicast storm suppression function is configured on the interface, while the broadcast/multicast/unknown unicast traffic on the interface exceeds the threshold set by the user, the system will discard the messages that exceed the flow limit, thus reducing the broadcast/multicast/unknown unicast traffic of the interface to a limited range and ensuring network services.

8.1.2 Storm Control

To enter the 'Storm Control' interface (Figure 8-1), select 'Network Security > Port Security > Storm Suppression' in the navigation bar.



The screenshot shows the 'Storm Control' interface with a table titled 'Storm Control Table'. The table has columns for 'Common Entry No', 'Port', and 'Storm Control Mode' (subdivided into 'Unknown UnicastControl', 'Unknown MulticastControl', and 'BroadcastControl'). Five entries are listed, all with 'Disabled' status. The first entry is selected. Below the table are buttons for 'Refresh', 'Edit...', and 'Copy Settings...'. The bottom right corner shows pagination: 'Page 1 Total 6'.

Common Entry No	Port	Storm Control Mode		
		Unknown UnicastControl	Unknown MulticastControl	BroadcastControl
<input checked="" type="radio"/>	1 GE1/0/1	Disabled	Disabled	Disabled
<input type="radio"/>	2 GE1/0/2	Disabled	Disabled	Disabled
<input type="radio"/>	3 GE1/0/3	Disabled	Disabled	Disabled
<input type="radio"/>	4 GE1/0/4	Disabled	Disabled	Disabled
<input type="radio"/>	5 GE1/0/5	Disabled	Disabled	Disabled

Figure 8-1 'Storm Control' interface

On the interface, the storm control information of all ports can be viewed. The top right corner of the interface can set the items that are displayed on each page. Pages can be selected or changed by the arrow buttons located at the bottom right corner.

Click the <Refresh> button to refresh message suppression information.

On the 'Storm Control Table' interface, you can modify the port's storm control:

- Select the port entry and click the <Edit> button to enter the 'Storm Control Editing' interface, as shown in Figure 8-2.
- Modify configuration parameters, as shown in table 8-1.
- Click <Apply> to complete operation.
- By clicking <Copy>, storm control configuration of one port can be replicated to other ports.
- Select the port to be copied and click <Copy> to enter the 'Copy Settings' Interface.
- In the copy interface, enter the serial number of which the ports to be copy to.
- Click <Apply> to complete operation.

Port: GE1/0/1

Unknown Unicast Control Mode: 0 kbps

Unknown Multicast Control Mode: 0 kbps

Broadcast Control Mode: 0 kbps

kbps Range:1~1000000
(Default): 0 It indicates Storm Control disabled

Apply Close

Figure 8-2 'Storm Control Editing' interface

Table 8-1 Description of 'Storm Control' Configuration Item

Configure items	Description
Port	Select the port to be modified
Unknow unicast mode	Set the suppression value of unknown unicast in Kbps
Unknow multicast mode	Set the suppression value of unknown multicast in Kbps
Broadcast controlling mode	Set the broadcast suppression value in Kbps

In the 'Storm Control Table' interface, batch replication configuration can be achieved:

- Select the port to be copied and click < **Copy** >.
- In the 'Copy' dialog box that pops up, enter the serial number of the ports to which you copied.
- Click <**Apply**> to complete the operation.

8.2 IP Source Guard

8.2.1 Overview

According to the binding table, IP source protection restricts the IP traffic of the client.

'IP Source Binding Table' is the detection standard of data packets received by each port. Only in two cases can the switch forward data and the rest of the data packets be discarded by the switch:

1. The received IP packet satisfies the corresponding relationship of Port/IP/MAC in IP source binding table.
2. DHCP packets received.

IP source binding tables can be added statically on the switch by the user or be automatically learned by the switch from DHCP Snooping Binding Table.

Switches automatically generate IP source-binding tables based on DHCP listening for the content of the binding tables, and then filter all IP traffic according to the IP source-binding tables. In IP packets sent by clients, only the source IP address satisfies the source IP-binding table will be sent. For traffic with source IP address other than the source IP-binding table, it will be filtered.

8.2.2 Interface Setting

To enter the 'Interface Settings' (Figure 8-3), select 'Network Security > IP Source Protection > Interface Settings' in the navigation bar.

Common Entry No	Interface	IP Source Guard	Current Entry Number
<input type="radio"/> 1	GE1/0/1	Disabled	0
<input type="radio"/> 2	GE1/0/2	Disabled	0
<input type="radio"/> 3	GE1/0/3	Disabled	0
<input type="radio"/> 4	GE1/0/4	Disabled	0
<input type="radio"/> 5	GE1/0/5	Disabled	0

Figure 8-3 IP source guard 'Interface Settings'

In the 'Interface Settings', you can see the IP source protection status of all interfaces:

- Through the filters, you can choose to view IP source protection configurations for Ethernet interfaces or aggregation groups.
- The top right corner of the interface can set the items that are displayed on each page. Pages can be selected or changed by the arrow buttons located at the bottom right corner.

(1) Modify interface setting:

- In 'Interface Settings' (Figure 8-3), click <Edit> to enter modify interface as shown in Figure 8-4.
- Modify configuration parameters, as shown in table 8-2.
- Click <Apply> to complete the operation.

Figure 8-4 Edit interface setting

Table 8-2 Description of interface setting

Title	Description
Interface	Select the interface type and set the interface. Ethernet interface or aggregation group is optional.
IP source protection	Set whether IP source protection is enabled. Check 'Enable' to enable IP source protection on selected interfaces.

8.2.3 Binding Database

To enter the 'Binding Database Table' (Figure 8-5), select 'Network security>IP source guard> Binding database' in the navigation bar. The information of all binding databases can be viewed on the interface.

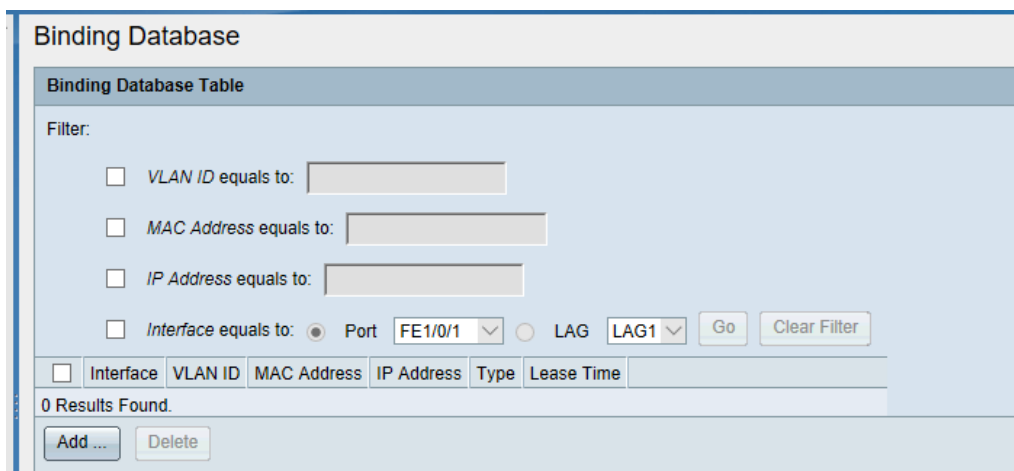


Figure 8-5 'Binding Database Table' interface

Through the filter, the information of specific conditions can be queried. The filtering conditions are: VLAN, MAC address, IP address, interface. When inquiring, select the filter and enter the parameters, then click <Apply>. To remove the filter, click <Clear Filter>.

(1) Binding database

- In 'binding database table' interface, click <Add> to enter the page shown in Figure 9-6.
- Configure the binding database parameters, as shown in Table 9-3.
- Click <Apply> to complete the operation.

Delete the binding database (single /batch)

- Select the required binding database entry and click <Delete>.

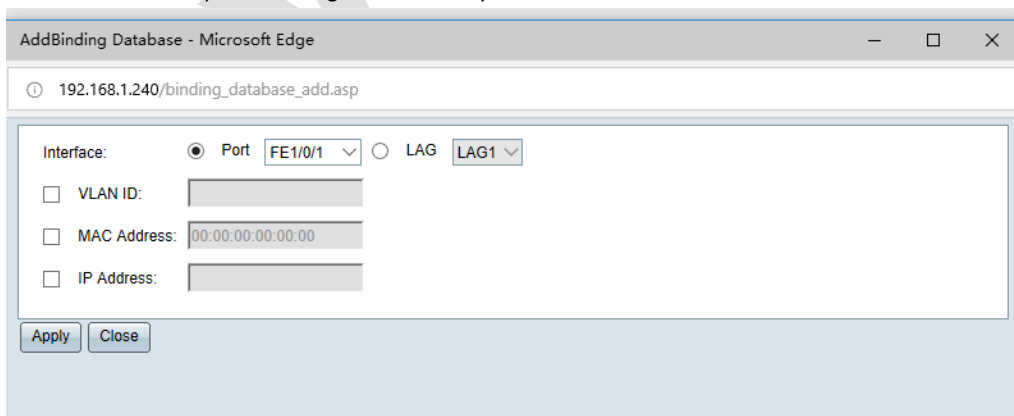


Figure 8-6 Add Binding database

Table 8-3 Description of add binding database's detail configuration items

Title	Description
Port	Select the interface type and port to set. Ethernet ports and aggregation groups are optional. (Mandatory)

VLAN ID	Select the VLAN ID to bind (optional)
MAC Address	Select the MAC address to bind to (optional)
Ip address	Select the IP address to bind to (optional)

8.3 DHCP Snooping

8.3.1 Overview

DHCP Snooping Function

DHCP Snooping is a security feature of DHCP. It has the following functions:

- a. Ensure that clients get IP addresses from legitimate servers.
- b. Enable DHCP clients to obtain IP addresses through legitimate DHCP servers, the DHCP Snooping security mechanism allows ports to be set to trust ports and untrusted ports:
 - Trust ports normally forward received DHCP messages.
 - After receiving DHCP-ACK and DHCP-OFFER messages from DHCP server, the untrusted port discards the message.

The ports connecting DHCP servers and other DHCP Snooping devices need to be set to trust ports and other ports to distrust ports, so as to ensure that DHCP clients can only obtain IP addresses from legitimate DHCP servers.

Record the corresponding relationship between DHCP client IP address and MAC address.

DHCP Snooping monitors DHCP-ACK broadcast messages received by DHCP-REQUEST and trust ports, and records DHCP Snooping table items, including the MAC address of the client, the IP address obtained, the port connected to the DHCP client and the VLAN to which the port belongs.

DHCP Snooping Support Option 82 Functionality

When the device receives the DHCP request message, it will process the message according to whether the message contains Option 82 and the processing strategy of user configuration, and forward the processed message to the DHCP server

Table 8-4 DHCP Snooping Support Option 82 Functionality

Receive DHCP request message	Processing strategy	DHCP Snooping Processing of Messages
Received message include Option82	Drop	Drop message
	Keep	Keep Option 82 unchanged and forward
	Replace	Fill Option 82 with normal mode, replace the original Option 82 in the message and forward it.
Received message without Option82	---	Filling Option 82 with normal mode and forwarding

8.3.2 Global settings

Select 'Network security > DHCP > DHCP Snooping> Global settings' to enter DHCP Snooping's global setting interface, as shown in figure 8-7.

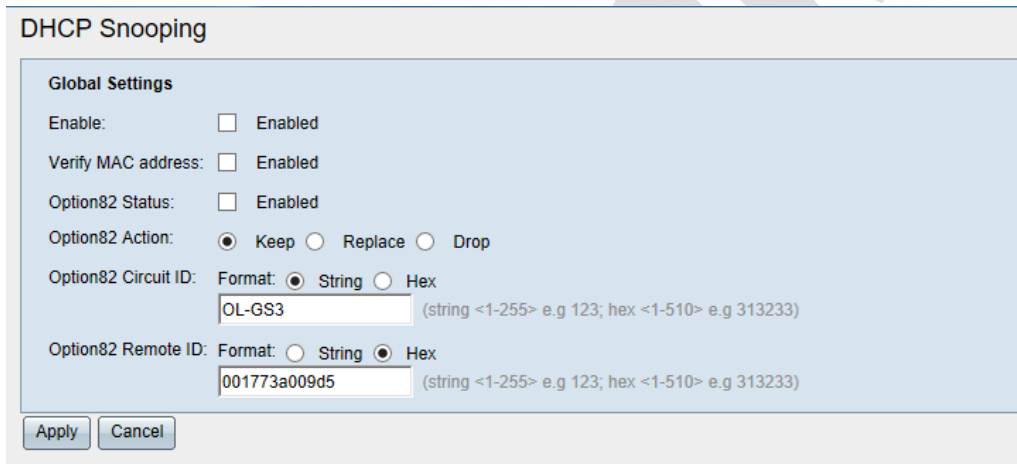


Figure 8-7 DHCP Snooping's Global Setting

Configure the global functionality of DHCP snooping, as shown in Table 8-5.

Click<Apply> to complete the operation.

Table 8-5 DHCP Snooping's Global Setting Table

Configuration items	Description
Enable	Set the global enabling state of DHCP Snooping to enable or disable.
MAC Verify	Set whether to enable MAC authentication Enable: When the MAC authentication function is enabled, DHCP Snooping compares the source MAC address of the request message with the hardware address of the DHCP client (i.e. CHADDR field), and forwards the same message, otherwise drop it.

	Disable: All request messages are forwarded without verifying the MAC address.
Option82 state	Set whether DHCP Snooping supports Option 82
Option82 Operation	Set DHCP Snooping's processing strategy for request messages containing Option 82, including: Drop: If the message has Option 82, the message is dropped Keep: If the message has Option 82, keep Option 82 unchanged and forward it Replacement: If there is Option 82 in the message, fill Option 82 with normal mode, replace the original Option 82 in the message and forward it.
Option82 Circuit ID	Configure Option 82 Circuit ID
Option82 Remote ID	Configure Option 82 Remote ID

8.3.3 Interface setting

In the navigation bar, select 'Network security> DHCP> DHCP Snooping> Interface setting', to enter DHCP Snooping interface, as shown in figure8-8.

The DHCP Snooping function configuration of all interfaces can be viewed on the interface

—Through filters, you can choose to view the DHCP Snooping configuration of the Ethernet port or aggregation group

—The top right corner of the interface can set the items displayed on each page, and the bottom right corner can be viewed by turning the page through the arrow button

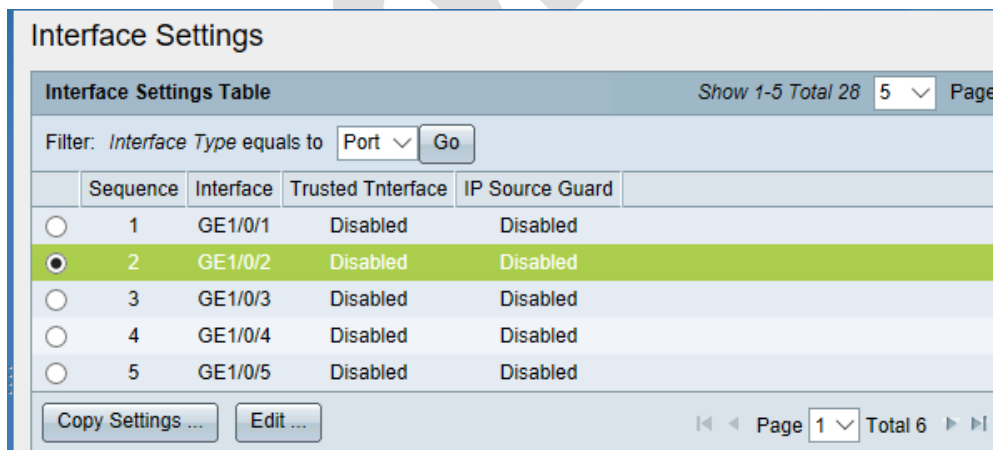


Figure 8-8 DHCP snooping' Interface Settings'

DHCP Snooping Function Configuration for Modifying Interfaces

—In the 'Interface Setting Table' interface, click < **Edit** > and enter the modification interface as shown in Figure 8-9

—Modify configuration parameters, as shown in table 8-6

—Click<**Apply**> to complete the operation.

(2) By<**Copy**> button, copy one port's DHCP Snooping configuration to other ports.

Copy the DHCP Snooping function of one interface to other ports through the < **Copy** > button.

—Select copied port, click < **Copy** > to enter modify interface.

Select the port to be copied and click < **Copy** > to enter the Copy Settings Interface

—In copy interface, enter port numbers that need to be copy to

In the copy setting interface, enter the serial number of which ports to copy to.

—Click < **Apply** > to complete the operation.

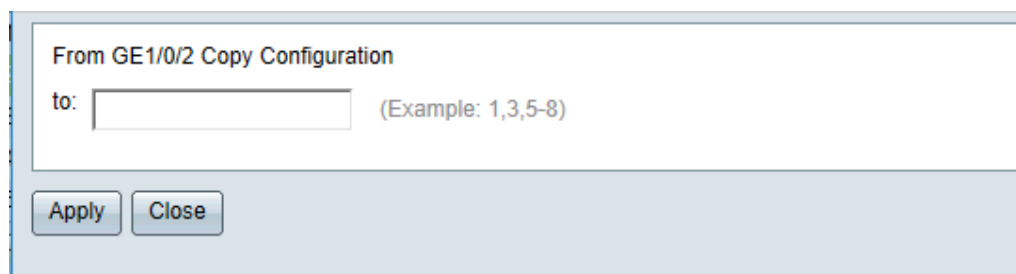


Figure 8-9 Modify DHCP Snooping interface setting

Table8-6 DHCP Snooping detail configuration items

Title	Description
Interface	Select the interface to modify. Ethernet interface or aggregation group is optional
Interface Trust	Set the trust attribute of the interface to trust or non-trust
Ip source protection	<p>Set whether to enable IP source protection</p> <p>Enable: DHCP monitor binding table will automatically generate IP source binding table. IP packets acquired from monitor port will be sent only if they match to the Port/IP/MAC in the IP source binding table, otherwise they will be dropped.</p> <p>Disable: Switches do not filter source IP data message.</p>

8.3.4 Snooping Bind Table

In the navigation bar, select 'Network security > DHCP > DHCP Snooping > Snooping Bind Table' to enter DHCP Snooping's bind table, as shown in figure 9-10

User table interface displays dynamic and static IP address lease binding entries

(1) Dynamic to Static

Select dynamic binding entries and click < **Dynamic to Static** > to convert dynamic binding entries into static binding entries.

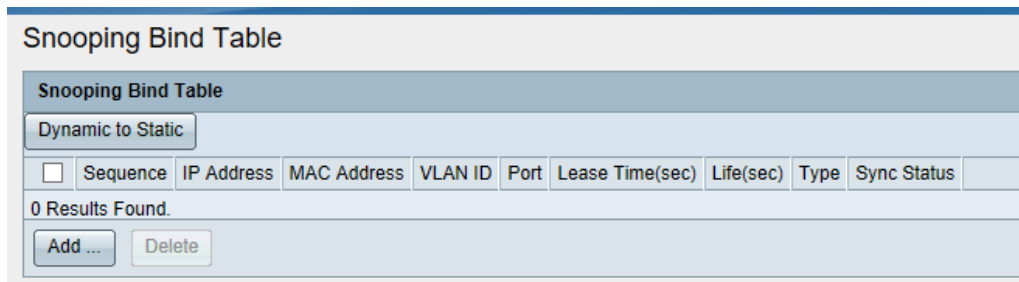


Figure 8-10 Snooping Bind Table Interface

(2) Add static bind items

—Click **<Add>** to enter 'Add Snooping Bind Table' interface, as shown in figure 8-11.

—Config bind table's information. Details parameter refer to table 8-7.

Configure the binding table information, and detailed configuration as shown in table8-7.

—Click**<Apply>** to complete the operation.

(3) Delete binding entries

In Snooping bind table interface, select bind items that need to be deleted. Click**<Delete>** to complete operation.

In the user table display interface, select the binding entries that need to be deleted and click the **< Delete >** button to complete the operation

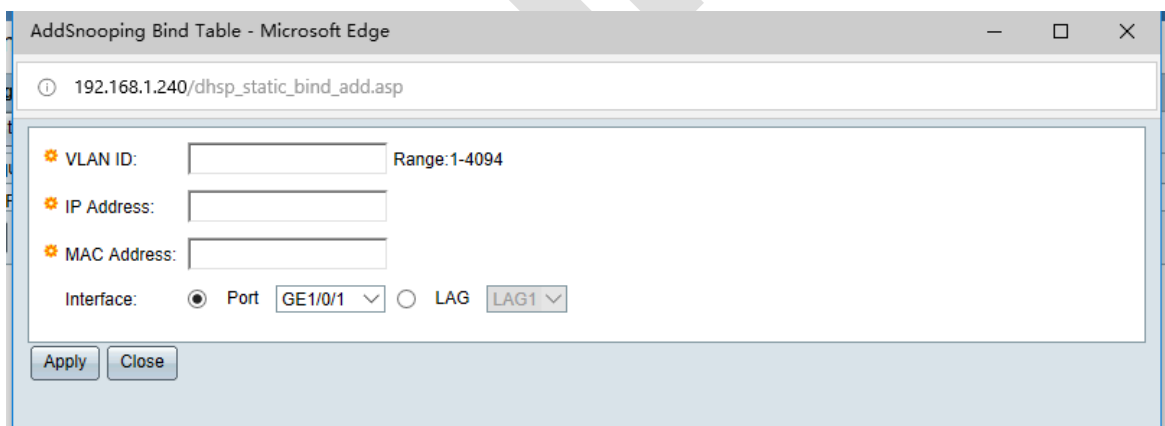


Figure 8-11 Add Snooping bind Table

Table9-7 DHCP Snooping Detailed description of user information

Title	Description
IP Address	IP Address Assigned by DHCP Server for DHCP Client
MAC Address	MAC address of DHCP client
VLAN ID	VLAN to which device ports connected to DHCP clients belong
Port	Device Port Connected with DHCP Client
Lease Time	Client acquire IP address' lease time Lease time for client to get IP address

Aging Time	The remaining time of the binding lease
Type	Binding type with values including: Dynamic: Table shows dynamically generated IP address and MAC address bindings, lease time expiration aging Static: The table shows the IP address and MAC address binding of the static configuration, and does not age
Synchronization state	Whether to synchronize to IP source protected database

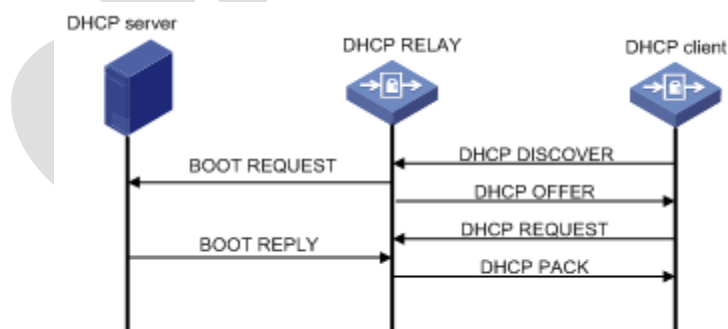
8.4 DHCP RELAY

Note: Only Layer3 series switch equipment is supported to support the functions of this chapter. Specific reference is given to the actual equipment and model

8.4.1 Overview

DHCP Relay Agent Principle Diagram :

DHCP relay agent is used to forward DHCP requests of one segment to DHCP Server of other segments, and DHCP Server of other segments assigns IP addresses. The reason why DHCP relay agent exists is that the DHCP client has not set up an IP environment. At this time, DHCP Relay takes over the DHCP request of the client, then passes the DHCP message to DHCP Server, and then passes the DHCP server's reply message to the client, and the client obtains the IP address.



8.4.2 Global setting

In the navigation bar, select 'Network security> DHCP> DHCP Relay> Global setting' to enter DHCP Relay's global setting, as shown in figure 8-12.

In the global settings, you can view the global enabling status of DHCP Relay, or modify the enabling status in the configuration box, and then click the < **Apply** > button

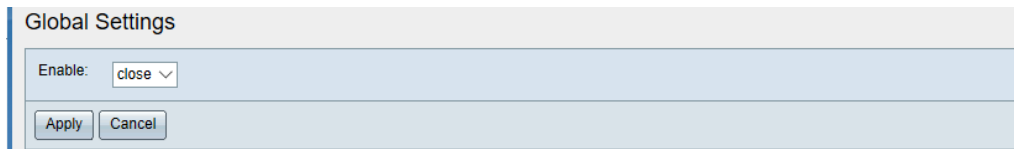


Figure 9-12 DHCP Global Settings

Table 9-8 DHCP Relay 'Global Setting'

Title	Description
Enable	Set the DHCP Relay global enable state ➤ Enable: Enable DHCP Relay function ➤ Close: Disable DHCP Relay function Note: Close by default.

8.4.3 DHCP Relay Vlanif set

In the navigation bar, select 'Network security>DHCP>DHCP Relay>Global settings', you can view DHCP Relay's Vlanif set, as shown in figure 8-13.

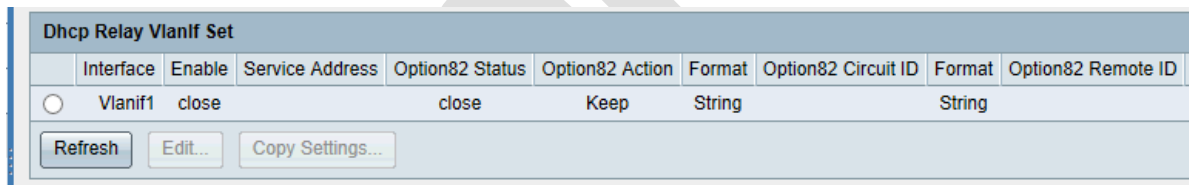


Figure 8-13 DHCP Relay interface setting

In the DHCP Relay interface setting, you can view the DHCP Relay settings of the virtual interface currently created

Click the < **Refresh** > button to refresh the DHCP Relay settings of the virtual interface

Editing and modifying interface settings

—Select the virtual interface that needs to be modified, click the < **Edit** > button, and enter the edit interface, as shown in Figure 8-14

—Modify port configuration.

—Click<**Apply**> to complete the operation

(1) By<**Copy**>button, copy DHCP Relay configuration of one interface to other ports

—Select the port to be copied, click < **Copy** > and enter the Copy Settings interface

—In the copy interface, enter the serial number of which ports to copy to.

—Click<**Apply**> to complete the operation.

Interface: Port Vlanif1

Enable: Enabled

DHCP Server:

Option82 Status: Enabled

Option82 Action: Keep Replace Drop

Option82 Circuit ID: Format: String Hex
 (string <1-255> e.g 123; hex <1-510> e.g 313233)

Option82 Remote ID: Format: String Hex
 (string <1-255> e.g 123; hex <1-510> e.g 313233)

Figure 8-14 Modify the interface settings of DHCP Relay

Table 8-9 DHCP Relay 'Interface Settings'

Title	Description
interface	Select the virtual interface name to configure Note: The virtual interface to connect the client needs to be selected
Enable	Set whether to enable DHCP relay function on the interface
DHCP Server	Setting the IP address of DHCP server Note: If the DHCP server is not set up, the DHCP message from the client cannot be forwarded. After setting up the DHCP server, the message will be forwarded from the interface connecting the server.
Option 82 State	Set whether DHCP Relay supports Option 82 functionality.
Option 82 Operation	Set DHCP Relay's processing strategy for request messages containing Option 82, including: Drop: If the message has Option 82, drop the message Keep: If the message has Option 82, keep Option 82 unchanged and forward it Replacement: If the message has Option 82, fill Option 82 with normal mode, replace the original Option 82 in the message and forward it.
Option 82 Circuit ID	Configure Option 82 Circuit
Option 82 Remote ID	Configure Option 82 Remote ID

8.4.4 Snooping Bind Table

(1) In the navigation bar, select 'Network Security > DHCP > DHCP Relay > User Table' and enter the user table interface of DHCP Relay, as shown in Figure 8-15.

Display all dynamic user address table items in the 'Snooping bind table' interface (currently not supported for dynamic configuration). Detailed parameter descriptions, as shown in table8-10

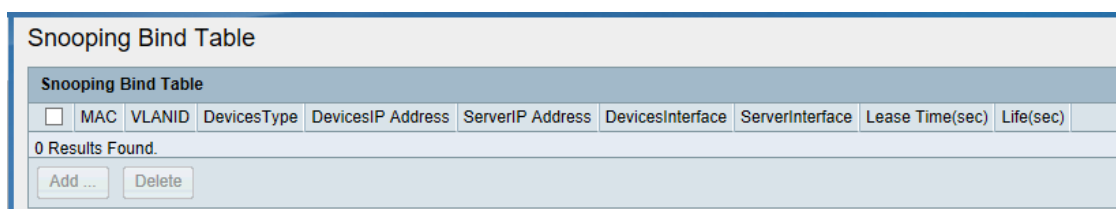


Figure 8-15 DHCP Relay DHCP Relay User Table Interface

Table8-10 DHCP Relay

Title	Description
MAC	MAC address of DHCP client
VLAN ID	VLAN to which device ports connected to DHCP clients belong
Device Type	---
Device IP address	IP Address Assigned by DHCP Server for DHCP Client
Server IP address	The IP address of the server that assigns addresses to the client
Device Port	Device Port Connected with DHCP Client
Server port	Device ports connected to servers
Lease Time	Lease Time for client acquired IP address
Aging Time	The remaining time of the binding lease

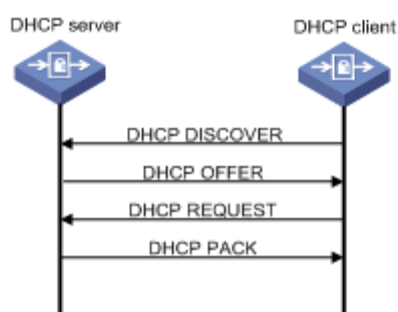
8.5 DHCP SERVER

Note: Only Layer3 series switch equipment is support the functions of this chapter. Specific reference is given to the actual equipment and model.

8.5.1 Overview

DHCP servers select and assign IP addresses and other related parameters to clients from the address pool. When a device as a DHCP server receives a DHCP request from the client, it will select an appropriate address pool according to its configuration and select an idle IP address from it, which will be sent to the client together with other relevant parameters (such as DNS server address, address lease period, etc.).

DHCP Server schematic:



8.5.2 Global setting

In the navigation bar, select 'Network Security> DHCP>DHCP Server>Global Setting', to enter 'Global Setting' Interface

Global Setting

In the 'Global Settings' interface, you can view the global enable status of DHCP Server, or configure it to open or close in the configuration box, and then click <Apply> to complete the settings. As shown in Figure 8-16

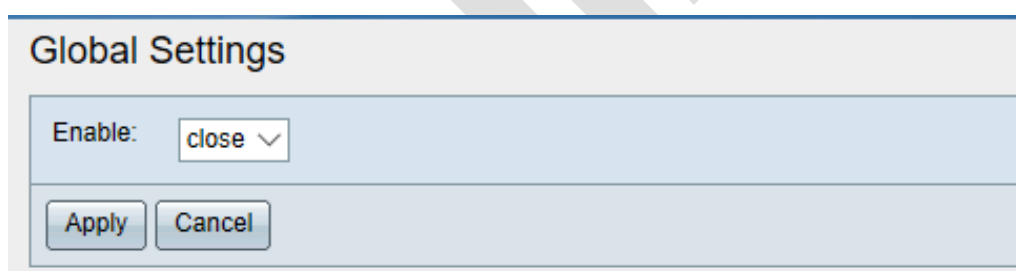


Figure 8-16 DHCP Server Global Setting Interface

DHCP server interface setting

In the lower part of the 'Global Settings' interface, you can view the DHCP server interface settings, as well as refresh, edit and copy operations, as shown in Figure 8-17

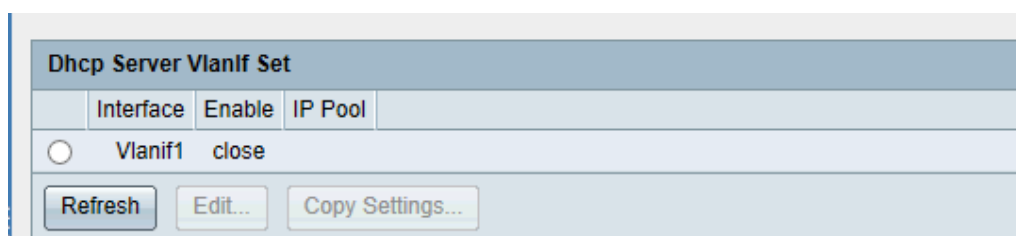


Figure 8-17 DHCP Server Interface Setting Display Interface

Click the < Refresh > button to refresh the interface settings

(1) Modify interface setting

—Select the interface that needs to be modified, click the < **Edit** > button, and enter the interface that modifies the interface settings of DHCP server, as shown in Figure 8-18

—Modify the interface settings, as shown in table 8-11

—Click<**Apply**>button to complete the operation

By <**Copy settings**>, copy one port’s DHCP server setting to other ports.

—Select the port to be copied and click on <**Copy Settings**> to enter the Copy Settings Interface

—In the copy interface, enter the serial number of which ports to copy to.

—Click<**Apply**> to complete the operation.

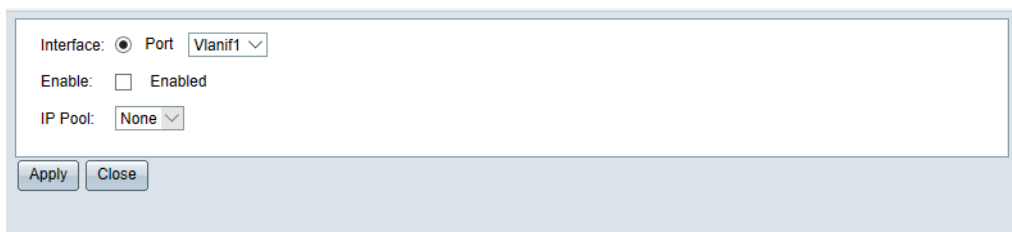


Figure 8-18 Edit interface setting

Table9-11 DHCP Relay ‘Interface setting’ configuration

Title	Description
Interface	Select the virtual interface name to configure
Enable	Set whether to start DHCP Server function on the interface
Resource pool	Select the resource pool to which the interface is binding, requiring that the resource pool has been created

8.5.3 IP Resource Pool

In the navigation bar, select ‘Network security>DHCP>DHCP server>IP Pool to enter IP pool display interface, as shown in figure 8-19

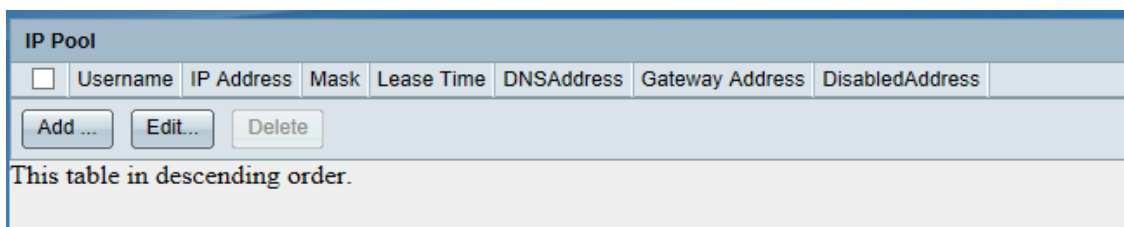


Figure 8-19 Resource Pool interface

The configuration information of all created resource pools can be viewed in the resource pool display interface.

(1) Add resource pool

—In the resource pool display interface, click the < **Add** > button to enter the resource pool add interface,

as shown in Figure 8-20

—Configure resource IP pool information, as shown in table 8-12

—Click **Apply** to complete the operation

(2) Edit IP pool

—In the resource pool display interface, select the resource pool that needs to be modified. Click the **Edit >** button to enter the resource pool modification interface

—Modify the IP pool information and configure it in detail as shown in table 8-12 (user name, IP address and mask cannot be modified)

— Click **Apply** to complete the operation

(3) Delete IP pool

—In the IP pool display interface, select the IP pool that needs to be deleted. Click the **Delete >** button to complete the operation

The screenshot shows a web-based configuration interface titled "IP Pool". It contains several input fields and a table. The fields are: Username (text input), IP Address (text input), Mask (text input), Lease Time (1 Day, 00 Hour, 00 Minutes), DNS Address (text input), Gateway Address (text input), and Disabled Address (table with 8 rows). The Disabled Address table has two columns: a text input field and a dropdown menu. At the bottom of the form are "Apply" and "Cancel" buttons.

Figure 8-20 add IP pool interface

Table 8-12 DHCP Server IP pool config description

Title	Description
User name	Configure IP pool's name
Ip address	Configure IP pool's network segment address and mask

Mask	
Lease Time	<p>Set the lease time for dynamic IP addresses. Range of values:</p> <ul style="list-style-type: none"> ➤ Day: 0~24854 ➤ Hour: 0~23 ➤ Minute: 0~59 <p>When the value is 0:0 on the day, the table is the largest.</p> <p>Note: For different address pools, DHCP servers can specify different address lease periods, but addresses in the same DHCP address pool have the same duration</p>
DNS Server	Enter the IP address of DNS server, you can configure more than 8 IP addresses.
Gateway address	Set the IP address of the gateway. More than 8 IP addresses can be added
Disable address	<p>Set IP addresses that do not participate in the allocation. Requires the same segment as the resource pool IP address.</p> <p>Note: Some addresses are assigned to specific services, such as DNS servers, which cannot be allocated. In this case, these addresses can be configured as IP addresses that do not participate in the allocation in the DHCP address pool.</p>

8.5.4 Static binding configuration

In the navigation bar, select 'Network security>DHCP>DHCP server>Static bind' to enter static bind interface. As shown in figure 8-21.

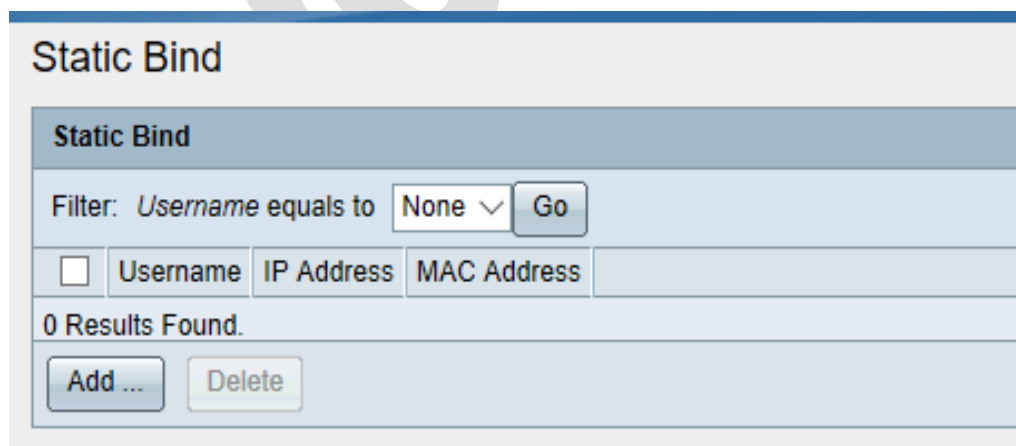


Figure 8-21 static bind interface

In static bind interface you can view all static bind items. By filter, could appoint query any user name's static bind item.

All static binding entries can be viewed in the static binding table interface, and static binding entries for querying a user name can be specified by filters.

—Select the user name through the drop-down list. Click the <Apply> button.

(1) Add static binding items

- In the static binding table interface, click the < **Add** > button to enter the static binding settings interface, as shown in Figure8-22
- Set the static binding entry information and configure it in detail as shown in table8-13
- Click<**Apply**>to complete the operation.

(2) Delete static binding entries

- In static bind interface, select bind items need to delete. Click<**Delete**>to complete operation.
- In the static binding table interface, select the static binding entries that need to be deleted and click <**Delete**> to complete the operation.

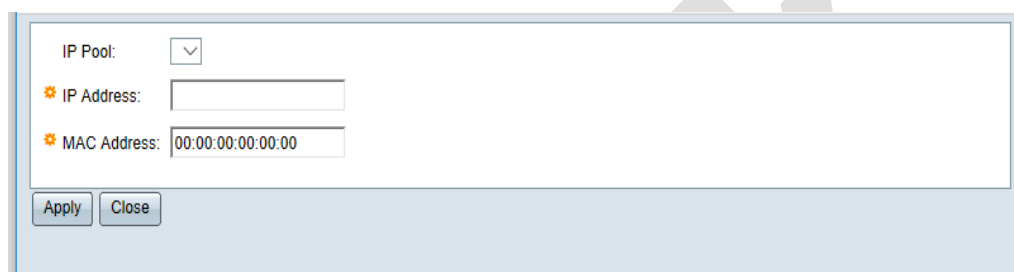


Figure 8-22 add static bind interface

Table8-13 DHCP Server config description of Static bind Configuration instructions for static binding

Title	Description
User name	Select the pool of resources to set static addresses
IP address	Set the binding static IP address, requiring the same segment as the resource pool IP address
Mac address	Setting the MAC address of the binding client

8.5.5 Snooping Bind Table

In the navigation bar, select 'Network security>DHCP>DHCP Server>Snooping Bind Table, to enter DHCP server user interface

Select 'Network Security DHCP > DHCP Server > User Table' in the navigation bar and enter the user table interface of DHCP server, as shown in Figure 8-23.

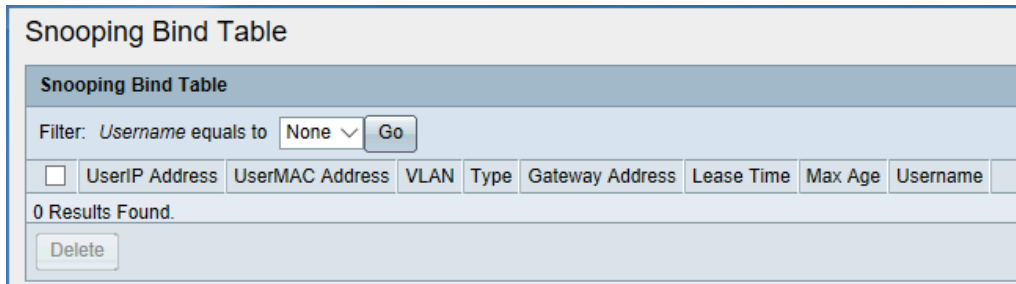


Figure 8-23 DHCP server user table interface of DHCP server

Snooping Bind Table display all IP address' lease information. Details information description show on table 8-14. User table displays all IP address lease information, as shown in Table 8-14.

The lease information of a user name can be specified and queried through a filter

—Select the user name through the drop-down box and click the < **Apply**> button

Select the user lease entry and click the < **Delete** > button to complete the deletion operation

Table 8-14 Information description of user table

Title	Description
User IP address	IP address obtained by Client
User MAC address	Client's MAC address
VLAN	VLAN to which device ports connected to DHCP clients belong
Type	The types of lease information are static and dynamic
Gateway address	Gateway Address Obtained by Client
Lease Time	Lease time for client to get IP address
Aging Time	The remaining time of the binding lease
Username	Resource pool name to assign IP address to client

8.6 ACL

8.6.1 Traffic Setting

In the navigation bar, select 'Network security>ACL>Traffic setting' to enter traffic setting interface as shown in figure 9-24.

Select 'Network Security > ACL > Traffic Settings' in the navigation bar and enter the display interface of 'Traffic Settings', as shown in Figure 8-24.

Traffic SettingTable			
	Common Entry No	Port	Traffic Count
<input checked="" type="radio"/>	1	FE1/0/1	0
<input type="radio"/>	2	FE1/0/2	0
<input type="radio"/>	3	FE1/0/3	0
<input type="radio"/>	4	FE1/0/4	0
<input type="radio"/>	5	FE1/0/5	0
<input type="radio"/>	6	FE1/0/6	0
<input type="radio"/>	7	FE1/0/7	0
<input type="radio"/>	8	FE1/0/8	0
<input type="radio"/>	9	FE1/0/9	0
<input type="radio"/>	10	FE1/0/10	0

Sequence Action Direction ACL ID IPv4/IPv6 Rule ID CIR Mirror Port Redirect Port Vlan DSCP Cos

0 Results Found.

Figure 9-24 'Traffic Settings' Interface

In the 'Traffic Settings' interface, you can view the number of Traffic bars bound to all ports. By clicking on the selected port, you can see the details of the Traffic bound to that port.

In 'Traffic setting' interface, could add Traffic item to port

- Select the port and click the <Add> button to enter the edit 'Traffic Settings' interface, as shown in Figure 8-25
- Configure Traffic parameters, as shown in Table 8-15
- Click<Apply> to complete the operation

In the 'Traffic Settings' interface, you can delete the Traffic entry of the port.

- Select the port, in the Traffic column table shown below, select the Traffic entry to delete, and click <Delete> to complete the operation

192.168.1.240/traffic_item_add.asp

Port: FE1/0/1
 Action: Filter
 Direction: Ingress
 ACL ID: (Range: IPv4/IPv6: 2000-3999; MAC: 4000-4999)
 IPv4/IPv6: IPv4
 Rule ID: (Range: 1 - 8)

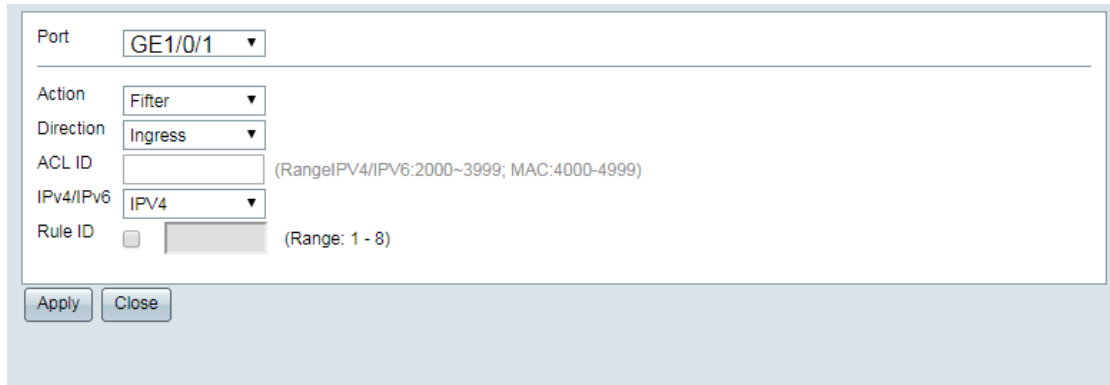


Figure 8-25 Edit 'Traffic setting' interface

Table 8-15 Traffic setting

Title	Description
Port	Select the port to set traffic
动作 Action	<p>Set the action of traffic. When the message matches the rules binding by traffic, the action is executed</p> <ul style="list-style-type: none"> ➤ Filter: Filter the traffic of matching rules ➤ Limit: Limit the traffic of matching rules ➤ Mirror: Mirror the traffic of matching rules to the specified port ➤ Redirect: Redirecting traffic to a specified port for matching rules ➤ Re-mask: Traffic Remarking VLAN Labels for Matching Rules ➤ Re-priority: Remarking COS or DSCP Priorities for Traffic of Matching Rules ➤ Statistic: Traffic statistics for matching rules
Direction	Set the direction of traffic, divided into entrance and exit
ACL ID	Enter ACL ID to be bound
IP version	Setting ACL based on IPv4 or IPv6
Rule ID	Enter the RULE identity of the ACL to be bound

8.6.2 MAC-Based ACL

In the navigation bar, select 'Network Security >ACL>ACL configuration> MAC-Based ACL' to enter Mac based ACL's interface

In 'MAC based ACL', you can view all ACL items based on MAC, as shown in figure 8-26.

On the 'MAC-based ACL' interface, you can view all MAC-based ACL entries, as shown in Figure 8-26

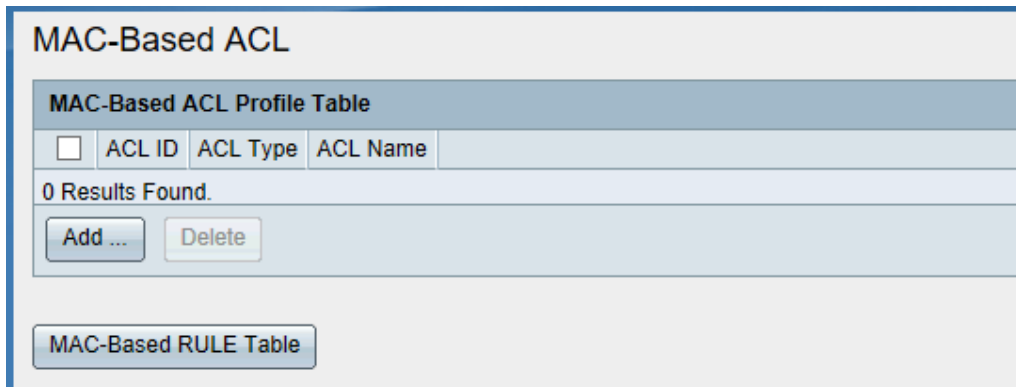


Figure 8-26 Mac-Based ACL interface.

Add MAC-based ACL

- In MAC based ACL interface, click <Add> to enter 'Add ACL interface'
- In the 'MAC-based ACL table' interface, click the < Add > button to enter the 'Add ACL' interface, as shown in Figure 8-27
- Enter the ACL ID and name, as shown in Table 8-16
- Click on the < Apply > button to add a new ACL entry

Delete MAC based ACL

- In the MAC-based ACL table interface, you can delete ACL entries by selecting ACL entries and clicking the < Delete > button
- Click <MAC Based Rule table>, to enter MAC-Based Rule interface. As shown in figure 8-27
- Click on the < MAC Based Rule table > button to enter the 'MAC-based Rule' interface, as shown in Figure 8-27

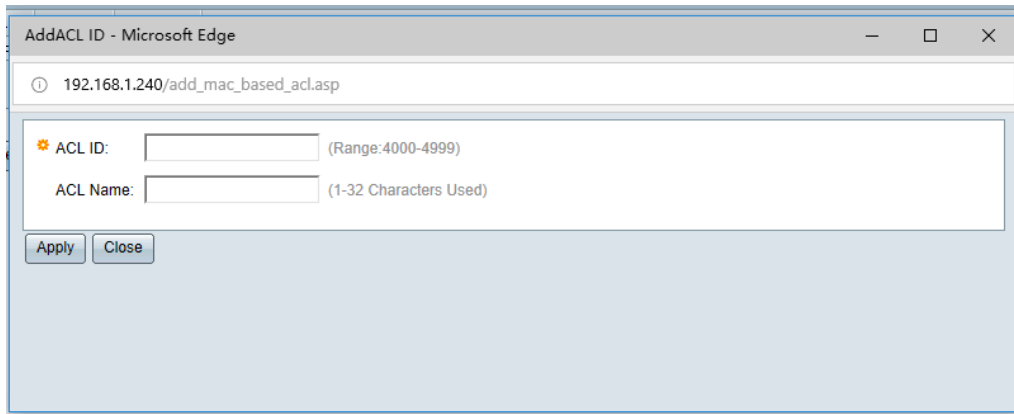


Figure 8-27 Add MAC-Based ACL interface

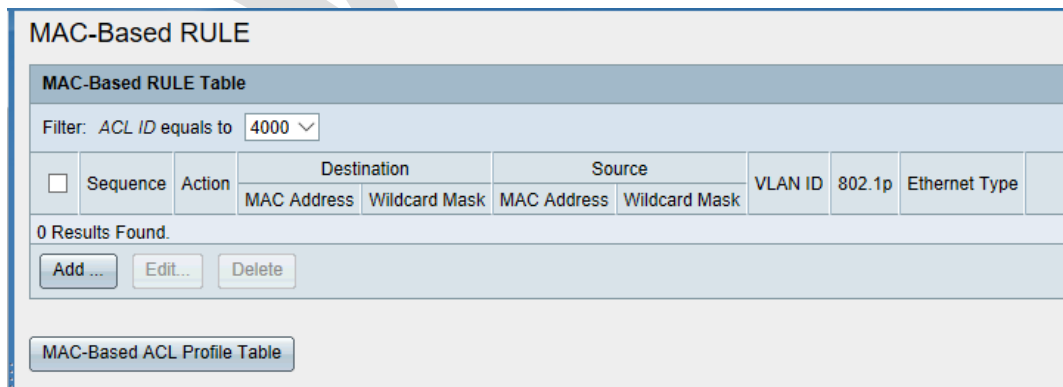
Table 8-16 Add MAC based ACL configure description

Title	Description
ACLID	Set the created ACL ID, range 4000-4999
ACL Name	Set the ACL name

8.6.3 MAC based RULE

Select 'Network Security > ACL > ACL Settings > MAC-based Rule' in the navigation bar and enter the 'MAC-Based Rule' interface

On the 'MAC-based Rule' interface, you can view all MAC-based Rule entries, as shown in Figure 8-28



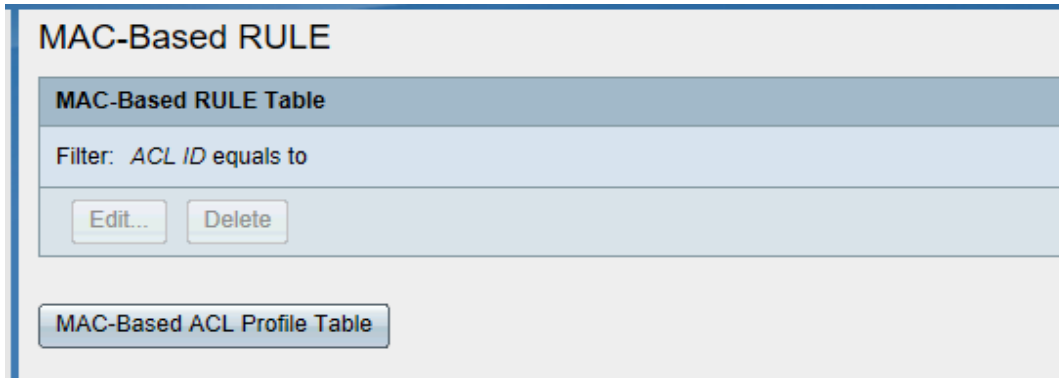


Figure 8-28 MAC-Based Rule Table

Add Mac-Based Rule

- Select ACL on the filter that needs to add Rule
- Click <Add>, pop up the 'Add MAC-based Rule' dialog box, as shown in Figure 8-29
- Configure Rule parameters, as shown in table8-17
- Click<Apply> to complete the operation

(1) Program Rule based on Mac

Edit Mac-Based Rule

- Select ACL that needs to add Rule
- Click <Add> to pop up the 'Edit MAC-based Rule' dialog box
- Modify Rule parameters, detailed configuration as shown in table8-17
- Click<Apply> to complete the operation

Delete MAC based Rule

- Select the Rule need to delete
- Click<Delete> to complete the Operation

ACL ID:	4000
✱ Sequence:	<input type="text"/> (Range: 1 - 8)
Action:	<input checked="" type="radio"/> Permit <input type="radio"/> Deny
Destination MAC Address:	<input checked="" type="radio"/> Any <input type="radio"/> User Defined
✱ Destination MAC Address Value:	<input type="text"/> (Format:xxxxxxxxxx)
✱ Destination MAC Wildcard Mask:	<input type="text"/> (0 represents match, 1 represents no match)
Source MAC Address:	<input checked="" type="radio"/> Any <input type="radio"/> User Defined
✱ Source MAC Address Value:	<input type="text"/> (Format:xxxxxxxxxx)
✱ Source MAC Wildcard Mask:	<input type="text"/> (0 represents match, 1 represents no match)
VLAN ID:	<input type="text"/> (Range: 1 - 4094)
802.1p:	<input type="checkbox"/> Include
✱ 802.1p Value:	<input type="text"/> (Range: 0 - 7)
Ethernet Type:	<input type="text"/> (Range: 0x0600 - 0xFFFF)

Apply Close

Figure 8-29 Add Mac-Based Rule

Table 8-17 Mac Based Rule Configuration

Title	Description
ACL ID	Display the ACL ID to add Rule
Number (Mandatory)	Enter the serial number of the configured Rule, rang 1- 8
Operation (Mandatory)	Select the operation on the message matching the rule Permit: Table indicates that a message matching this rule is allowed to pass through Deny: table indicates that messages that do not match this rule are prohibited from passing through.
Destination address (Mandatory)	Setting the destination address of the message Any: When choosing any, it is not necessary to specify the destination MAC address and wildcard of the message, that is, to match all destination MAC addresses ➤ User-defined: Customization: When selecting user-defined, you need to specify the destination MAC address value and wildcard of the message (0 generation table matching, 1 generation table mismatching)
Destination MAC address	
Destination MAC	
Source MAC address(Mandatory)	Setting the source address of the message ➤ Any: When choosing any destination MAC address, it is not necessary to specify the destination MAC address and wildcard of the message, that is, to match all destination MAC addresses. ➤ User-define: When selecting user-define, you need to specify the destination MAC address value and wildcard character of the message (0 generation table matching, 1 generation table mismatching)
Source MAC address value	
Source MAC wildcard mask	
VLAN ID (optional)	Set the VLAN value of the message, range is 1~4094
802.1p (optional)	Sets whether to specify 802.1p for a message
802.1p value (optional)	Select the check box in front of '802.1p' and set the value of 802.1p, range 0-7
Ethernet type (optional)	Set the Ethernet type of the message, range is 0x0600~0xFFFF

8.6.4 IPv4-Based ACL

Select 'Network security>ACL> IPv4-Based ACL' to enter 'IPv4-Based ACL' interface

In IPv4-Based ACL interface, you can view all the IPv4-Based ACL items, as shown in figure 8-30

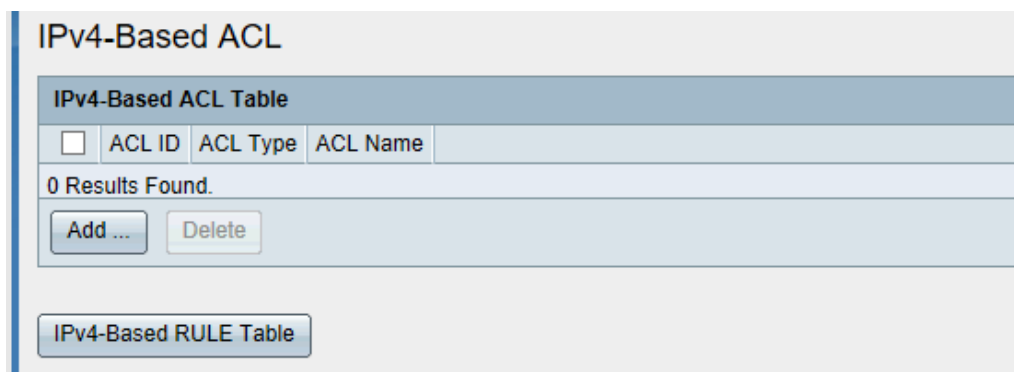


Figure 8-30 IPv4 based ACL

Add IPv4-Based ACL

- In the 'IPv4-based ACL table' interface, click the < **Add** > button to enter the 'Add ACL' interface, as shown in Figure 8-31

Enter ACL ID and name, detailed configuration as shown in table 8-18

- Click <**Apply**> could add ACL entries.

Delete IPv4-Based ACL

- In IPv4-Based ACL interface, Select ACL item, click<**Delete**> could delete ACL item
- In the IPv4-Based ACL interface, you can delete ACL entries by selecting ACL entries and click the < **Delete** > button.

Click the <**IPv 4-based RULE table**> button to enter the 'IPv4-based RULE' interface, as shown in Figure 8-31

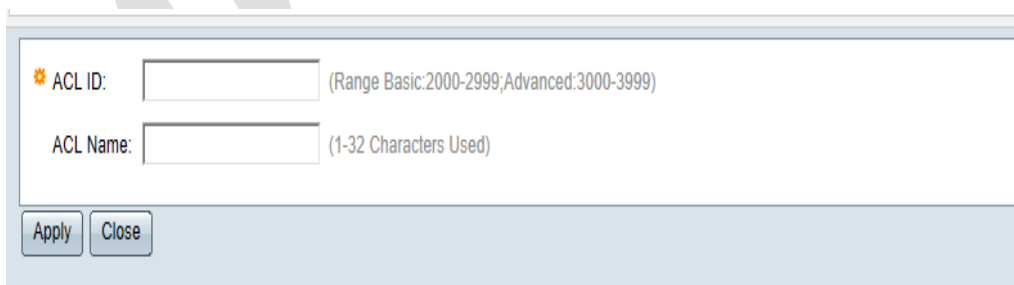


Figure 8-31 Add IPv4 Based ACL interface

Table 8-18 Add IPv4 Based ACL Configuration

Title	Description
ACL ID	Configure created ACL ID, rang is basic:2000-2999; Advanced: 3000-3999
ACL Name	configure ACL name

Note:

- There are two types of IPv4-Based ACL, one is basic (ACL ID is 2000-2999), one is Advanced (ACL ID is 3000-3999)
- Rule based on basic IPv4 can only set matching source IP address;
- Rule based on extended IPv4 can set multiple matching parameters

8.6.5 IPv4 Based RULE

In the navigation bar, select 'Network Security > ACL > ACL Settings > IPv4-based Rule' and enter the 'IPv4-based Rule' interface

On the 'IPv4-based Rule' interface, you can view all IPv4-based Rule entries, as shown in Figure 8-32.

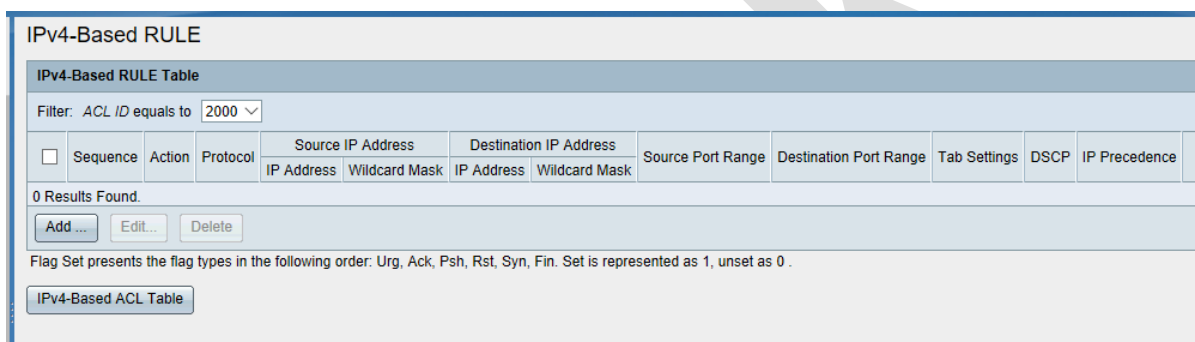


Figure 8-32 IPv4 Based Rule Table

Add IPv4 Based Rule

- Select ACL on the filter that needs to add Rule
- Click<Add>, pop up 'Add IPv4 based Rule' dialog box, as shown in Figure 8-33.
- Configure Rule parameters, as shown in table8-19
- Click the <Apply> button to complete the operation.

Edit Ipv-4 based Rule

- Select ACL that needs to add Rule
- Click<Add>, pop up the 'Edit Rule Based on IPv4' dialog box.
- Modify the Rule parameter, detailed configuration as shown in table8-19
- Click<Apply> to complete the operation

Delete IPv4 based Rule

- Select the rule need to delete
- Click<Delete> to complete the operation.

ACL ID: 2000

Sequence: (Range: 1 - 8)

Action: Permit
 Deny

Protocol: Select from list
 Protocol ID to match

Source IP Address: Any
 User Defined

Source IP address value:

Source IP Wildcard Mask: (0 represents match, 1 represents no match)

Destination IP Address: Any
 User Defined

Destination IP Address Value:

Destination IP Wildcard Mask: (0 represents match, 1 represents no match)

Source Port: Any
 Single (Range: 0 - 65535)

Destination Port: Any
 Single (Range: 0 - 65535)

TCP Flags:

Urg:	Ack:	Psh:	Rst:	Syn:	Fin:
<input type="radio"/> Settings	<input type="radio"/> Settings	<input type="radio"/> Settings	<input type="radio"/> Settings	<input type="radio"/> Settings	<input type="radio"/> Settings
<input type="radio"/> Unset	<input type="radio"/> Unset	<input type="radio"/> Unset	<input type="radio"/> Unset	<input type="radio"/> Unset	<input type="radio"/> Unset

Type of Service: Any
 DSCP to match (Range: 0 - 63)
 IP Precedence to match (Range: 0 - 7)

Apply Close

Figure 8-33 Add IPv4 based Rule

Table 8-19 IPv4 Based Rule config description

Title	Description
ACL ID	Display the ACL ID to add Rule
No (Mandatory)	Enter the serial number of configured Rule.Range1-8
Operation (Mandatory)	Select the operation on the message matching the rule Permit: Table indicates that a message matching this rule allows pass through Deny: Table indicates that messages that do not match this rule are prohibited from passing through
Protocol (Mandatory)	Select protocol type that packet matching

	Select from the column table: TCP or UDP ➤ Protocol ID need to match
Source IP address (Mandatory)	Setting the source IP address of the message Any: When choosing any, it is not necessary to specify the source IP address and the wildcard, that is, to match all the source IP addresses
Source IP address (Mandatory)	User-Define: When selecting user-define, you need to specify the source address value of the message and wildcard (0 generation table matching, 1 generation table mismatching)
Source IP wildcard	
) Destination IP address(Mandatory)	Configure message's destination IP address Any: When choosing any, it is not necessary to specify the destination IP address and wildcard, that is, to match all destination IPv4 addresses. User-defined: When selecting user-defined, you need to specify the destination IP address value and wildcard (0 generation table matching, 1 generation table mismatching)
Destination IP address value	
Destination IP wildcard mask	
Source Port	Setting source port information and destination port information for TCP/UDP messages Configuration can only be done if the configuration item 'protocol' is selected as '6 TCP' or '17 UDP' Individual: need to specify port number (0-65535)
Destination Port	
TCP label	When protocol type is TCP, could select whether configure TCP label or not.
Service Type	Setting DSCP and COS Priorities for Messages

8.6.6 IPv6 Based

Select 'Network security>ACL>ACL setting>IPv6 based ACL' to enter the 'IPv6 based ACL' interface.

On the 'IPv6-based ACL' interface, you can view all IPv6-based ACL entries, as shown in Figure 8-34

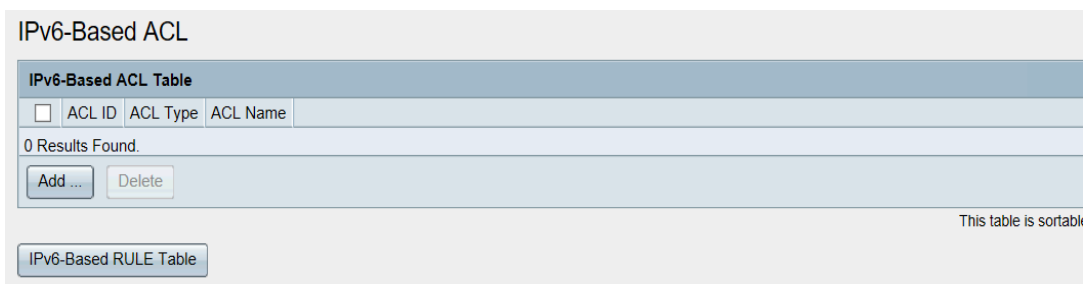


Figure 8-34 IPv6 based ACL.

Add IPv6 based ACL

- In the 'IPv6 based ACL table' interface, click the < **Add** > button to enter the 'Add ACL' interface, as shown in Figure 8-35
- Enter ACL ID and name, detailed configuration as shown on table 8-20.
- Click<**Apply**>, could add new ACL entries.

Delete IPv6 based ACL

- In the IPv6 based ACL interface, select ACL entries, click<**Delete**> , you can delete ACL entries
- Click the <IPv6-based RULE table> button to enter the 'IPv6-based RULE' interface, as shown in Figure 8-36

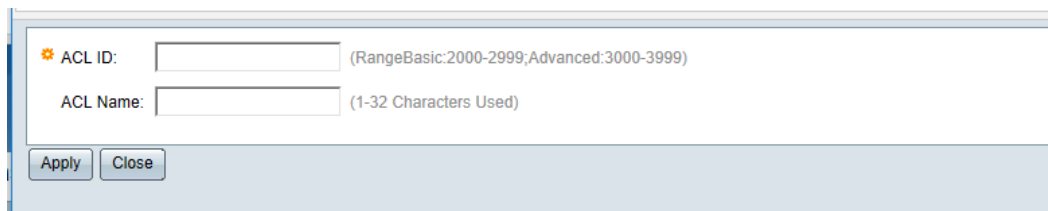


Figure 8-35 Add IPv6 based ACL interface

Table 8-20 Add'IPv6 based ACL' config description.

Title	Description
ACL ID	Set the created ACL logo, range is basic type: 2000-2999; extended type: 3000-3999
ACL Name	Set the ACL name

Note:

- There are two types of IPv6 based ACL, one is basic (ACL identification 2000-2999) and the other is extended (ACL identification 3000-3999).
- Rule based on basic IPv6 can only set matching source IP address; Rule based on extended IPv6 can set multiple matching parameters

8.6.7 IPv6 Based Rule

Select 'Network security> ACL> ACL configuration> IPv6 based rule', to enter the IPv6 based rule.

On the 'IPv6-based Rule' interface, you can view all IPv6-based Rule entries, as shown in Figure 8-36

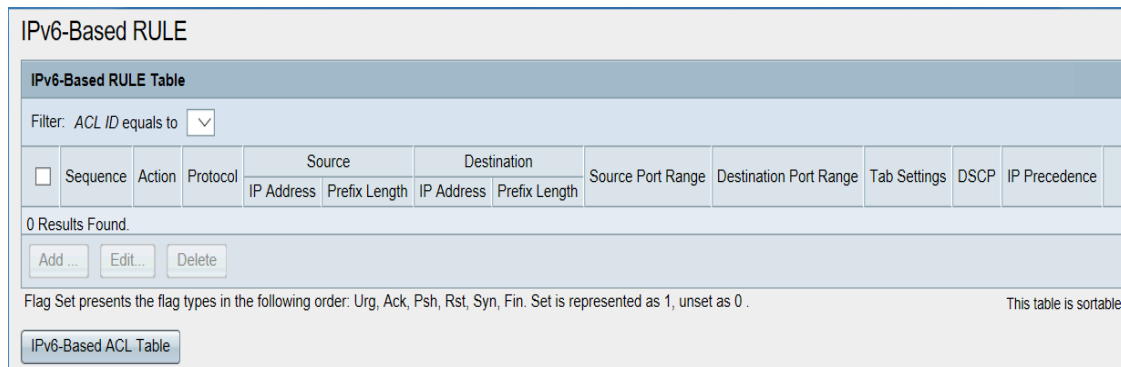


Figure 8-36 IPv6 based Rule Table

Add IPv6 based Rule

- Select ACL on the filter that needs to add Rule
- Click<**Add**> pop up the window of add IPv6 based Rule. As shown in figure 8-37
- Click < Add >, pop up the 'Add IPv6 Based Rule' dialog box, as shown in Figure 8-37
- Configure Rule parameter, details show on table 8-21
- Click<**Apply**> to complete the operation

Edit IPv6 based Rule

Select ACL that need to add Rule

- Click<**Add**>, pop up the 'edit IPv6 based Rule' dialog box.
- Modify Rule parameter, detailed configuration as show on table 8-21.
- Click<**Apply**> to complete the operation

Delete IPv6 based Rule

- Select the rule that need to delete
- Click<**Delete**> to complete the operation

ACL ID: 2000

Sequence: (Range: 1 - 8)

Action: Permit
 Deny

Protocol: Select from list
 Protocol ID to match

Source IP Address: Any
 User Defined

Source IP address value:

Source IP prefix length: (Range: 0 - 128)

Destination IP Address: Any
 User Defined

Destination IP Address Value:

Destination IP Prefix Length: (Range: 0 - 128)

Source Port: Any
 Single (Range: 0 - 65535)

Destination Port: Any
 Single (Range: 0 - 65535)

TCP Flags:

Urg:	Ack:	Psh:	Rst:	Syn:	Fin:
<input type="radio"/> Settings	<input type="radio"/> Settings	<input type="radio"/> Settings	<input type="radio"/> Settings	<input type="radio"/> Settings	<input type="radio"/> Settings
<input type="radio"/> Unset	<input type="radio"/> Unset	<input type="radio"/> Unset	<input type="radio"/> Unset	<input type="radio"/> Unset	<input type="radio"/> Unset

Type of Service: Any
 DSCP to match (Range: 0 - 63)
 IP Precedence to match (Range: 0 - 7)

Figure 8-37 Add IPv6 based Rule

Table 8-21 IPv6 Based Rule config description

Title	Description
ACL ID	ACL ID that need to add Rule.
Series Number (Mandatory)	Enter configured Rule ID, range 1-8
Operation (Mandatory)	<p>Select operation to the message matching the rule. Select the operation on the message matching the rule</p> <ul style="list-style-type: none"> ➤ Permission: table indicates that a message that matches this rule allows to pass ➤ Deny: table indicates that messages that do not match this rule are prohibited from passing

		Choosing Protocol Types for Packet Matching
Protocol (Mandatory)		Select from the column table: TCP or UDP Protocol ID to match
Source IP address(Mandatory)		Setting the source IP address of the message
Source Ip address value		➤ Any: When you choose any, you do not need to specify the source IP address and wildcard of the message, that is, to match all source IP addresses
Prefix-length of source IP address		➤ User-defined: When selecting user-defined, you need to specify the source address value of the message and wildcard mask (0-128)
Destination Ip address9(Mandatory)		Setting the destination IP address of the message
Destination Ip address value		➤ Any: When choosing any destination IP address and wildcard, it is not necessary to specify the destination IP address and wildcard of the message, that is, to match all destination IPv6 addresses.
Prefix length of Destination Ip		User define: When selecting user-define, you need to specify the destination IP address value and wildcard of the message (0-128)
Source port		Setting source port information and destination port information for TCP/UDP messages
Destination port		Configuration can only be done if the configuration item 'protocol' is selected as '6 TCP' or '17 UDP' ➤ Any ➤ Individual: need to specify port number(0-65535)
TCP label		When the protocol type is TCP, you can choose whether to set the TCP label or not
Type of Service		Setting DSCP and COS Priorities for Messages

8.7 POE

Note: Only switch with POE functions support this feature of this chapter. Specific reference is to actual equipment and model.

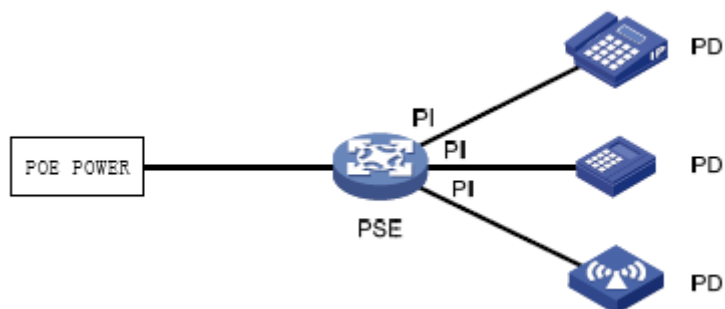
8.7.1 Overview

PoE (Power over Ethernet, also known as remote power supply) refers to the device through the Ethernet port, using twisted pair to connect PD (Power Device, power equipment) for remote power supply. POE has many advantages:

Reliable: centralized power supply, convenient backup

Simple connection: the network terminal does not need external power supply, only needs a network cable
Standards: Complying with the standard of IE802.3af/IE802.3at, using a unified global power interface
Wide application prospects: it can be used in IP phone , wireless AP (Access Point), portable device charger, card switcher, network camera, data acquisition, etc.

The PoE system is shown in the following figure, including PoE power supply, PSE (Power Sourcing Equipment), PI (Power Interface), and PDs.



PSE equipment refers to the equipment that directly supplies power to PD. PSE can be divided into two types: Endpoint and Midspan. Built-in means that PSE is integrated into switch/router, and external means that PSE is independent of switch/router. Our equipment is built-in.

PI refers to the Ethernet interface with PoE power supply capability, also known as PoE interface, including FE and GE interfaces

PDs are devices that receive PSE power supply, such as IP phone, wireless AP (Access Point), portable device charger, POS, network camera, etc. While receiving the power supply from PoE power supply, the PD device can connect other power sources and make redundant backup of power supply.

The PD equipment is divided into standard PD and non-standard PD. Standard PD refers to the PD equipment that meets the standard of 802.3af/at. Generally, PSE can only detect and supply standard PD. Only when the function of PSE detecting non-standard PD is turned on, can PSE detect non-standard PD and supply power for it.

8.7.2 PoE configuration

Select 'Network security>POE> POE configuration' to enter POE configuration interface, as shown in figure 8-38
In the 'POE Configuration' interface, you can view the configuration information of POE functions for each port
Click <Refresh> could refresh port configuration and state.

POE Config							
	Common Entry No	Port	Enable	LEGACY	Limit(W)	Priority	
<input type="radio"/>	1	GE1/0/1	Open	Close	15(AF)	Low	
<input type="radio"/>	2	GE1/0/2	Open	Close	15(AF)	Low	
<input type="radio"/>	3	GE1/0/3	Open	Close	15(AF)	Low	
<input type="radio"/>	4	GE1/0/4	Open	Close	15(AF)	Low	
<input type="radio"/>	5	GE1/0/5	Open	Close	15(AF)	Low	
<input type="radio"/>	6	GE1/0/6	Open	Close	15(AF)	Low	
<input type="radio"/>	7	GE1/0/7	Open	Close	15(AF)	Low	
<input type="radio"/>	8	GE1/0/8	Open	Close	15(AF)	Low	
<input type="radio"/>	9	GE1/0/9	Open	Close	15(AF)	Low	
<input type="radio"/>	10	GE1/0/10	Open	Close	15(AF)	Low	
<input type="radio"/>	11	GE1/0/11	Open	Close	15(AF)	Low	
<input type="radio"/>	12	GE1/0/12	Open	Close	15(AF)	Low	
<input type="radio"/>	13	GE1/0/13	Open	Close	15(AF)	Low	
<input type="radio"/>	14	GE1/0/14	Open	Close	15(AF)	Low	
<input type="radio"/>	15	GE1/0/15	Open	Close	15(AF)	Low	
<input type="radio"/>	16	GE1/0/16	Open	Close	15(AF)	Low	
<input type="radio"/>	17	GE1/0/17	Open	Close	15(AF)	Low	
<input type="radio"/>	18	GE1/0/18	Open	Close	15(AF)	Low	
<input type="radio"/>	19	GE1/0/19	Open	Close	15(AF)	Low	
<input type="radio"/>	20	GE1/0/20	Open	Close	15(AF)	Low	
<input type="radio"/>	21	GE1/0/21	Open	Close	15(AF)	Low	
<input type="radio"/>	22	GE1/0/22	Open	Close	15(AF)	Low	
<input type="radio"/>	23	GE1/0/23	Open	Close	15(AF)	Low	
<input type="radio"/>	24	GE1/0/24	Open	Close	15(AF)	Low	

Refresh Edit... Copy Settings...

Figure 8-38 'POE config' interface

In the 'POE Configuration' table interface, you can modify the configuration of the port.

- Select the corresponding port, click <Edit> to enter the interface as shown in Figure 8-39
- Modify the corresponding configuration items, as shown in table 9-22
- Click<Apply> complete modify. Click<Cancel> cancel modify

Figure 8-39 Edit POE configuration

Table 8-22 POE settings

Title	Description
Port	current configured Port 's name
Port open/close	<p>POE power supply function of enabling port, it's open by default</p> <ul style="list-style-type: none"> ➤ Open: Enable POE Power Supply Function of the Port ➤ Disable: Close POE Power Supply Function of the Port. <p>Note: The default POE function refers to the standard POE power supply mode, which only supports the standard PD equipment power supply.</p>
Legacy	<p>The non-standard POE power supply function of enabling port is close by default.</p> <p>Open: Enable port's non-POE power supply function</p> <p>Close : Disable port's non-POE power supply function</p> <p>Note: In order to support the power supply of non-standard PD devices, it is necessary to keep the power supply function of the enabling port open before turning on the power supply function of non-standard POE</p>
Limit	<p>Set the maximum power supply of POE port. The range is 1 to 30 watts. By default, the maximum power supply of the PoE interface is 15 watts</p> <p>Note: The maximum power supply of the PoE interface refers to the maximum power that the PoE interface can provide for the downlink PD. When the power required by the PD is greater than the maximum power of the PoE interface, the PD will not be powered</p>
Priority	<p>Set the priority level of the port, which is divided into three levels: high, medium and low, and the default is low.</p> <p>Note: When the external power supply of the equipment is insufficient, priority should be given to the PoE interface with higher priority.</p>

In the 'POE Configuration' table interface, batch replication configuration can be achieved

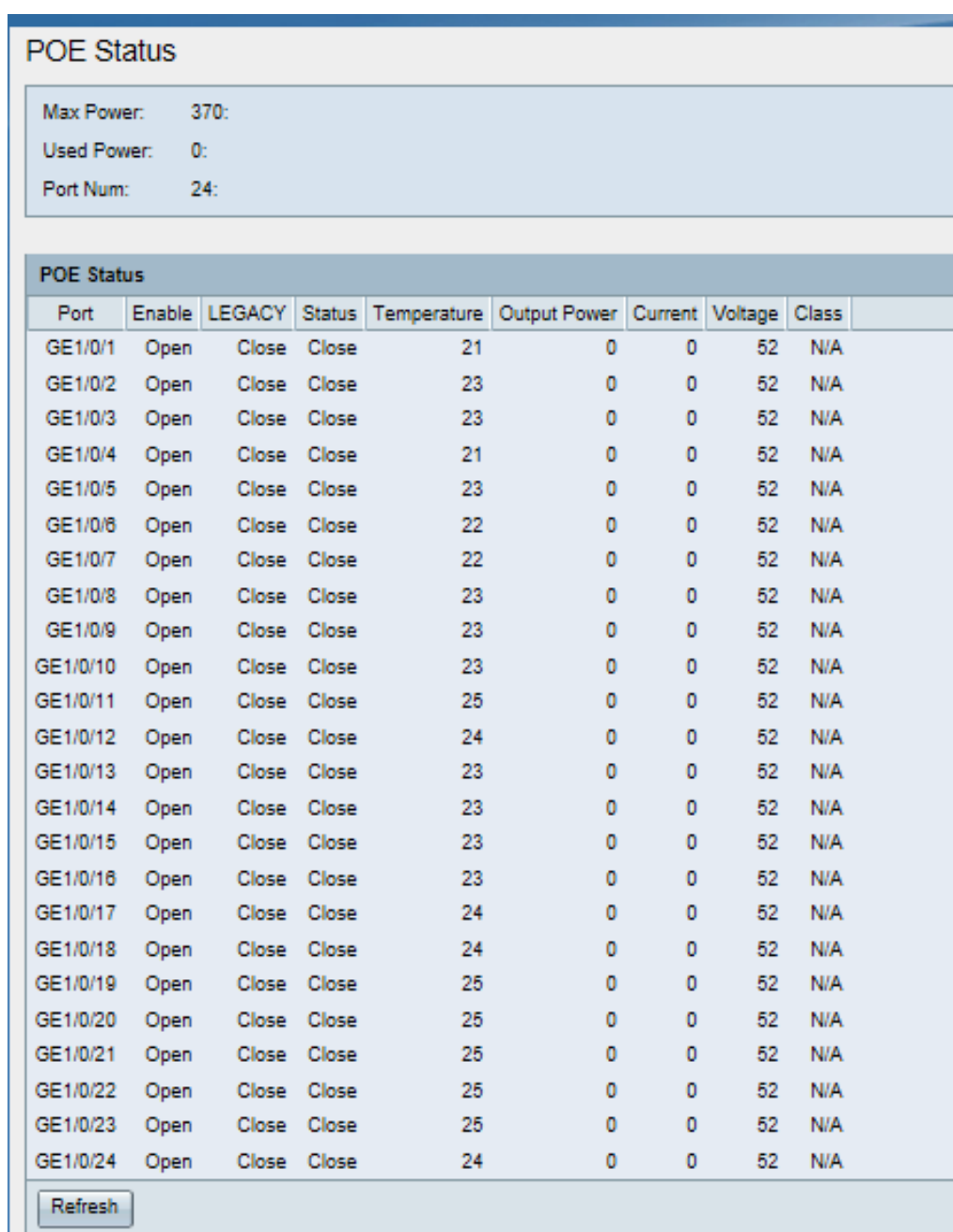
- Select the port to be copied and click the < **Copy Settings** > button
- In pop up 'copy' window, enter port's number that need to copy to
- In the 'Copy' dialog box that pops up, enter the serial number of the ports to which you copied.
- Click<**Apply**> to complete the operation.

8.7.3 POE status

Select 'Network security>POE>POE status', to enter 'POE status' interface, as shown in figure 8-40.

In the 'POE status' interface, you can see the maximum total power supported by the switch, the total power used, the number of ports supporting POE, and the configuration information, temperature, status and power usage of each port POE function. The parameter descriptions are shown in table8-23.

Click<Refresh> refresh latest state



The screenshot displays the 'POE Status' interface. At the top, there is a summary section with the following values: Max Power: 370, Used Power: 0, and Port Num: 24. Below this is a table with the following columns: Port, Enable, LEGACY, Status, Temperature, Output Power, Current, Voltage, and Class. The table lists 24 ports (GE1/0/1 to GE1/0/24) with their respective configurations and power usage. All ports are currently 'Open' and 'Close' in status, with zero power usage. A 'Refresh' button is located at the bottom of the table.

POE Status								
Max Power:	370:							
Used Power:	0:							
Port Num:	24:							
POE Status								
Port	Enable	LEGACY	Status	Temperature	Output Power	Current	Voltage	Class
GE1/0/1	Open	Close	Close	21	0	0	52	N/A
GE1/0/2	Open	Close	Close	23	0	0	52	N/A
GE1/0/3	Open	Close	Close	23	0	0	52	N/A
GE1/0/4	Open	Close	Close	21	0	0	52	N/A
GE1/0/5	Open	Close	Close	23	0	0	52	N/A
GE1/0/6	Open	Close	Close	22	0	0	52	N/A
GE1/0/7	Open	Close	Close	22	0	0	52	N/A
GE1/0/8	Open	Close	Close	23	0	0	52	N/A
GE1/0/9	Open	Close	Close	23	0	0	52	N/A
GE1/0/10	Open	Close	Close	23	0	0	52	N/A
GE1/0/11	Open	Close	Close	25	0	0	52	N/A
GE1/0/12	Open	Close	Close	24	0	0	52	N/A
GE1/0/13	Open	Close	Close	23	0	0	52	N/A
GE1/0/14	Open	Close	Close	23	0	0	52	N/A
GE1/0/15	Open	Close	Close	23	0	0	52	N/A
GE1/0/16	Open	Close	Close	23	0	0	52	N/A
GE1/0/17	Open	Close	Close	24	0	0	52	N/A
GE1/0/18	Open	Close	Close	24	0	0	52	N/A
GE1/0/19	Open	Close	Close	25	0	0	52	N/A
GE1/0/20	Open	Close	Close	25	0	0	52	N/A
GE1/0/21	Open	Close	Close	25	0	0	52	N/A
GE1/0/22	Open	Close	Close	25	0	0	52	N/A
GE1/0/23	Open	Close	Close	25	0	0	52	N/A
GE1/0/24	Open	Close	Close	24	0	0	52	N/A

Refresh

Figure 8-40 PoE Status

Table 8-23 PoE Status

Title	Description
Max power	Display the maximum global PoE power supported by PoE switches
Used power	Display the total power used by the current PoE power supply
Port Number	Display the total number of ports that PoE switch equipment can support PoE power supply function
Port	Display the PoE-enabled port sequence table
Enable	Display PoE power supply function is open or close
Non-standard POE	Display open or close non-standard PoE power supply function
Temperature	Real-time display of current PoE port temperature
Output power	Real-time display of current PoE port output power
Current	Real-time display of current PoE port output current
Voltage	Real-time display of current PoE port output voltage
Power class	Real-time display of current PoE port hanging standard PD load power CLASS level, the standard is 0-4 five levels

Chapter 9 Maintenance diagnosis

9.1 System log

System log contains a lot of information about network and equipment, including running status, configuration changes, etc. It is an important way for network administrators to monitor network and equipment operation. The information provided by the system log can help network administrators to find network problems or security risks, so as to take targeted measures.

(1) log class:

Table 10-1

Class	Class no.	Description
(emergencies)	0	System unavailability information
(alerts)	1	Information that needs to be processed immediately, such as an attack on a device, etc.
(critical)	2	Crisis information. For example, hardware error
(errors)	3	error information

(warnings)	4	alert information
(notifications)	5	Non-error messages, but need to special handling
(informational)	6	notice
(debug)	7	Usually used as debugging information within modules

(2) log output

Log information can be exported to different destinations, supporting the following several log information output destinations, users can specify according to their own needs.

Table10-2 log output

Destination	Description
Server	The system can send logs to the syslog server
Local	By default, the system logs to a local database

9.1.2 Log Setting

Select 'Maintenance diagnosis> system log> log setting' to enter 'Log Settings' interface, as shown in figure 9-1.

Figure 9-1 Log Settings Interface

Depending on the requirements, configure the parameters related to the system logs in the 'Log Settings' interface, and configure them in detail as shown in Table 9-3 below

Click< **Apply**> to complete system log setting

Table 9-3 'log settings' config description

Title	Description
log status	Setting the global enable state of the system log
save minimum severity	Set the minimum level of storage, 7 log levels are optional (see table 10-1 for log level description). When a certain level is selected, a more serious level can also be preserved If 'debugging' is selected, all levels of log information can be saved; if 'emergency' is selected, only the level of 'emergency' log information can be saved;
Remote log servers	Set whether remote log server output is supported
log server IP address	Setting IP Address of Remote Log Server
UDP Port	Setting UDP port number of remote log server
Send minimum severity	Set the minimum level for sending to the remote log server. Seven log levels are optional (see table 10-1 for the log level description). When a certain level is selected, a severer level can also be sent to the server. If 'debugging' is selected, all levels of log information are sent to the server; if 'emergency' is selected, only the level of 'emergency' log information can be sent

9.1.3 Check log

Select 'Maintenance Diagnosis > System Log > View Log', enter the 'Log Display' interface, as shown in Figure 9-2

(1) Log display

- 'Log display' interface could check system log's information.
- The 'Log Display' interface allows you to view information about the system logs, as shown in Table 9-4

(2) Log output

- In the 'Log Display' interface, all system logs saved in the log buffer of Web pages can be exported to PC in file form through the <Export> button

(3) Clear log

- You can clear all system logs saved in the Web page log buffer by clicking <Clear Log> button

(4) Refresh log

- Click<Refresh> button, manually refresh system log information display on current page
- You can manually refresh the system log information displayed on the current page by clicking the <Refresh> button

The screenshot shows a web interface titled "Log Information". It contains a table with the following data:

Log Information Table					
Log Time	Type	Severity	Category	Description	
Jan 1 00:00:46	authpriv	info	dropbear[84]	Running in background	
Jan 1 00:00:50	user	info	syslog	udhcpd(v1.20.2) started	
Jan 1 00:10:08	user	notice	SYSTEM	gigabitethernet 1/0/28 is UP.	
Jan 1 00:10:08	user	notice	SYSTEM	Vlan-interface1 is UP.	
Jan 1 00:13:20	user	notice	WEB	admin logged in from 192.168.1.11	
Jan 1 00:34:32	user	err	SYSLOG	erps is disabled.	
Jan 1 00:35:01	user	err	SYSLOG	erps is disabled.	

Below the table are three buttons: "Export", "Clear Log", and "Refresh".

Figure 9-2 Log information table

Table 9-4 Detailed description of system log information

Title	Description
log time	Time and date of system log generation
Type	system log type
Severity	Log level (see table 8-1 for detailed level description)
Category	A process module that generates logs
Description	Detailed description of system log

9.2 Port Maintain

9.2.1 Overview

The software platform provides port-based mirroring, which copies messages from one or more specified ports to the mirror port for message analysis and monitoring. For example, the message on port 2 can be copied to the specified mirror port 1, and the working state of port 2 can be tested and recorded by the protocol analyzer connected to the mirror port 1.

9.2.2 Mirror

In the navigation bar, select 'Maintenance diagnosis > port maintenance> port mirror' to enter the port mirror interface, as shown in figure9-3.

In the port mirror main interface, you can create the image group and display the port mirror column table.

Figure9-3 Port Mirror Main interface

The process of configuring port mirrors is as follows:

(1) Create mirror group and set monitor port

--In Monitor session enter group1, select monitor port

--Click<**Create**>

(2) Setting the mirror source port of Mirror Group 1

--Select the mirror group in the 'Port Mirror' column table, click the <**Edit**> button, and enter the mirror port configuration interface. As shown in Figure 9-4.

--Select whether to mirror or not in the drop-down table box corresponding to the port number

--Click <**Apply**> to complete the configuration

Example: As shown in Figure 9-4, port mirroring is configured to enable monitoring port GE1/0/1 to analyze and monitor incoming and outgoing ports of port GE1/0/2, outgoing ports of port GE1/0/3 and all messages of port GE1/0/4.

Port Mirror

Monitor Port:

Notice: When Mirror port configuration is more, the mirror port may cause a larger flow monitor port congestion, affecting port forwarding performance..

Port	Mirror Direction	Port	Mirror Direction
GE1/0/1	No Mirror	GE1/0/2	No Mirror
GE1/0/3	No Mirror	GE1/0/4	No Mirror
GE1/0/5	No Mirror	GE1/0/6	No Mirror
GE1/0/7	No Mirror	GE1/0/8	No Mirror
GE1/0/9	No Mirror	GE1/0/10	No Mirror
GE1/0/11	No Mirror	GE1/0/12	No Mirror
GE1/0/13	No Mirror	GE1/0/14	No Mirror
GE1/0/15	No Mirror	GE1/0/16	No Mirror
GE1/0/17	No Mirror	GE1/0/18	No Mirror
GE1/0/19	No Mirror	GE1/0/20	No Mirror
GE1/0/21	No Mirror	GE1/0/22	No Mirror
GE1/0/23	No Mirror	GE1/0/24	No Mirror
GE1/0/25	No Mirror	GE1/0/26	No Mirror
GE1/0/27	No Mirror	GE1/0/28	No Mirror

Figure9-4 Config interface of Mirror port

9.3 LLDP

LLDP (Link Layer Discovery Protocol) is a standard link layer discovery method. It can organize the main capabilities, management addresses, device identifiers, interface identifiers and other information of local devices into different TLVs (Type/Length/Value, Type/Length/Value) and encapsulate them in LLDPDU (Link Layer Discovery Protocol). Very Protocol Data Unit (PDU) is distributed to the neighbors who are directly connected to them. After receiving the information, the neighbors save it in the form of standard MIB (Management Information Base) for the network management system to query and judge the communication status of the link.

The basic principle of LLDP is as follows:

LLDP module updates its own LLDP local system MIB through the interaction between LLDP agent and physical topology MIB, entity MIB, interface MIB and other types of MIB on the device, as well as the LDP extension MIB customized by the local device.

Encapsulating local device information into LLDP frames and sending it to remote devices

Receiving LDP frames from remote devices, updating their own LLDP remote system MIB, and extending LDP MIB customized by remote devices

By sending and receiving LLDP frames through LLDP proxy, the device knows the information of the remote device very clearly, including which interface the remote device is connected to, the MAC address of the remote device and so on.

LLDP local system MIB is used to store local device information. Including device ID, interface ID, system name,

system description, interface description, network management address and other information.

LLDP remote system MIB is used to save remote device information. Including device ID, interface ID, system name, system description, interface description, network management address and other information.

9.3.2 Global setting

(1) In the navigation bar, select 'maintenance diagnosis> LLDP> Global setting' to enter LLDP global setting interface.

In the LLDP 'Global Settings' interface, you can view and modify the configuration information of the current LLDP parameters of the port, as shown in Figure 9-5.

Configure the LDP parameters of the port, as shown in Table 9-5

Click<Apply> to complete parameter configuration

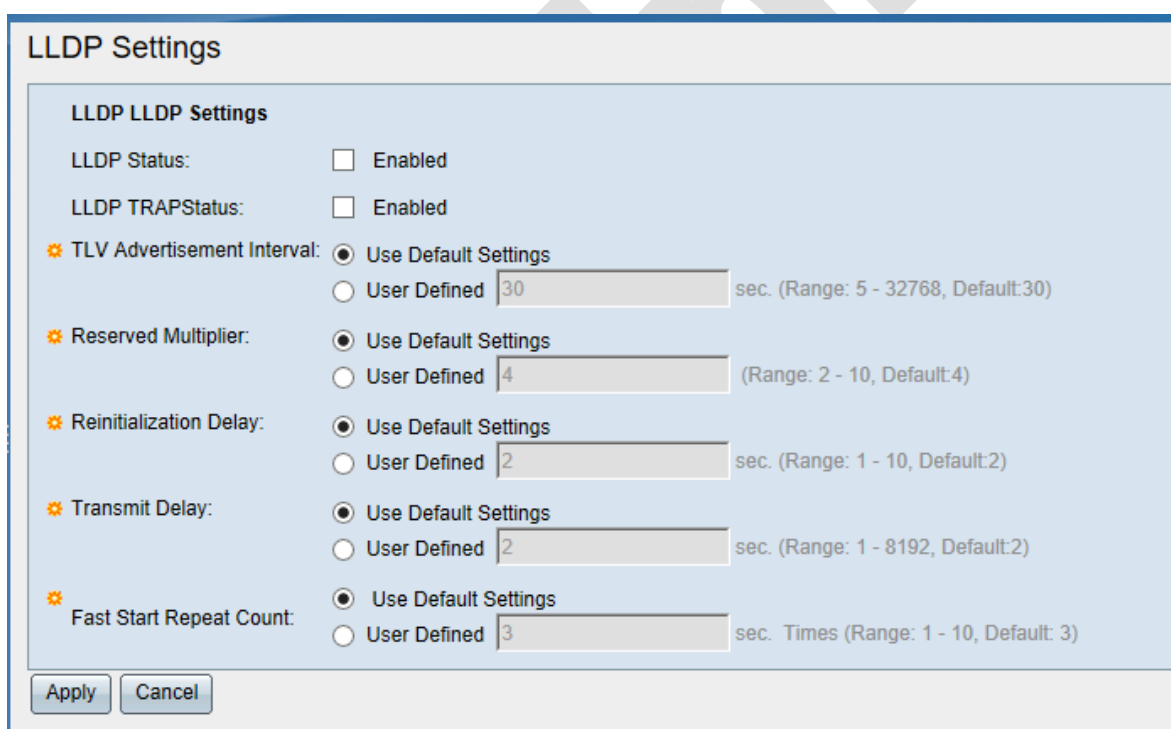


Figure 9-5 LLDP Settings interface

LLDP functioning

Table10-5 LLDP Settings

Title	Description
LLDP status	Setting LLDP Global Enabling State ➤ Enable: enable LLDP function

	<ul style="list-style-type: none"> ➤ Disable: Disable LLDP function Notice: Disable by default
LLDP TRAP Status	Setting LLDP TRAP Global Enabling State
TLV advertisement interval	Setting LLDPDU Send Time Interval
Reserved multiplier	Setting the value of TTL multiplier The value of TTL in TTL TLV carried by LLDPDU is used to set the aging time of neighbor information on local devices. $TTL = TTL \text{ multiplier} * \text{the time interval of sending LLDP message}$, so by adjusting TTL multiplier, we can control the aging time of the device information on neighbor devices
Reinitialization Delay	When the working mode of LLDP on the port changes, the port will initialize the protocol state machine. By configuring the delay time of the initialization of the port, it can avoid the continuous initialization of the port due to frequent changes in the working mode
Transmit delay	Setting LLDPDU Delay Time
Fast Start Repeat Count	Set the number of LLDP fast sending messages

9.3.3 Port Settings

In the navigation bar, select 'Maintenance diagnosis> LLDP> port setting', you can view LLDO port settings Table, as shown in figure 9-6.

Common Entry No	Port	LLDP Enable	Work Mode	Selected TLVs
1	FE1/0/1	Disable	brx	Port Descriptions, System Name, System Description, System Capabilities, 802.3 MAC-PHY, 802.3 Link Aggregation, 802.3 Max Frame Size
2	FE1/0/2	Disable	brx	Port Descriptions, System Name, System Description, System Capabilities, 802.3 MAC-PHY, 802.3 Link Aggregation, 802.3 Max Frame Size
3	FE1/0/3	Disable	brx	Port Descriptions, System Name, System Description, System Capabilities, 802.3 MAC-PHY, 802.3 Link Aggregation, 802.3 Max Frame Size
4	FE1/0/4	Disable	brx	Port Descriptions, System Name, System Description, System Capabilities, 802.3 MAC-PHY, 802.3 Link Aggregation, 802.3 Max Frame Size
5	FE1/0/5	Disable	brx	Port Descriptions, System Name, System Description, System Capabilities, 802.3 MAC-PHY, 802.3 Link Aggregation, 802.3 Max Frame Size

Figure 9-6 LLDP Port settings table

Select the port in the 'Port Settings' interface, click the < **Edit** > button, and enter the display and configuration page of the port LLDP parameters. You can view and modify the configuration information of the current LLDP parameters of the port, as shown in Figure 9-7.

Configure the LDP parameters of the port, as shown in Table 9-6

Click<**Apply**> to complete parameter configuration

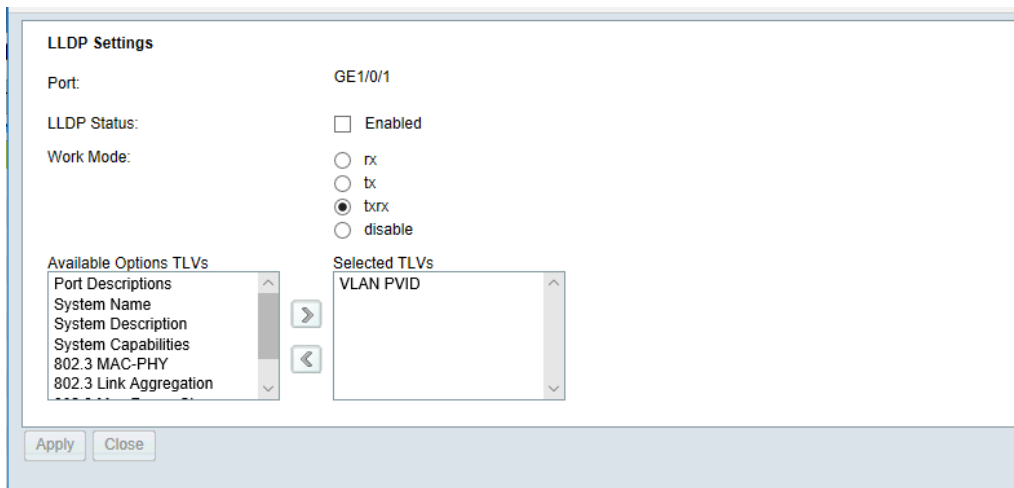


Figure 9-7 Edit port LLDP parameter

Table 9-6 LLDP port settings description

Title	Description
Port	Port name
LLDP status	<p>Port LLDP enable status</p> <ul style="list-style-type: none"> ➤ Enable: Enable port's LLDP function ➤ Disable: Disable port's LLDP function <p>Note: it's disabled by default.</p>
work mode	<p>Port's LLDP state</p> <ul style="list-style-type: none"> ➤ tx: Enable LLDP tx function for the port only. ➤ rx: Enable LLDP rx function for the port only. ➤ txrx: Enable LLDP tx/rx function for the port only. ➤ disable: Disable LLDP tx/rx function for the port only. <p>Note: Port is disable by default</p>
Available options TLVS	Select the information to be published by the switch by moving the TLV to the 'Selected TLVs' column table. Available TLV contains:
Selected TLVS	<p>Port Description - Port information, including manufacturer, product name and hardware/software version.</p> <p>System name - the specified name of the system (in alphanumeric format).</p>

	<p>System Description - Description of network entities (in alphanumeric format). It includes system name, hardware version, operating system and network software supported by switch</p> <p>System Function - The main function of the switch and whether these functions have been enabled in the switch. These functions are represented by two octal tables. The 0-7 bits tables show other, repeaters, bridges, WLAN AP, routers, telephones, DOCSIS cable equipment and workstations. Eight to fifteen bits are reserved.</p> <p>802.3 MAC-PHY-Duplex and Bit Rate Functions and Current Duplex and Bit Rate Settings of Transmitting Devices. It also points out whether the current settings are generated through automatic negotiation or manual configuration</p> <p>802.3 Link Aggregation LAG - Whether Links can be Aggregated (associated with ports used to transmit LLDP PDUs). It also indicates whether the link is currently aggregated; if so, the aggregated port identifier is provided</p> <p>Maximum frame size- Maximum Frame Size Function Implemented by MAC/PHY</p> <p>➤ Manage IP address</p>
--	--

9.3.4 LLDP Local information

Select 'Maintenance diagnosis>LLDP>LLDP local information', you can view LLDP local information, as shown in figure 9-8

Local Information	
Port:	GE1/0/1
Global	
Chassis ID Subtype ID:	MAC address
Chassis ID:	00:17:73:a0:09:d5
System Name:	SW1
System Description:	OL-GS3428CP-4C
Supported System Capabilities:	Bridge
Enabled System Capabilities:	Bridge
Port ID Subtype	Interface name
Port ID:	GE1/0/1
Port Descriptions:	GE1/0/1
Management Address	
Address Subtype:	IPv4
Address:	192.168.1.240
Interface Subtypes:	3
Interface Numbering:	28
802.1 VLAN and Protocol	
VLAN PVID:	1
VLAN Name:	
MAC / PHY Details	
Auto Negotiation Supported:	Supported
Auto Negotiation Enabled:	Enabled
Run MAU Types:	speed(1000)/duplex(full)
802.3 Max Frame Size:	1522
802.3 Link Aggregation	
Aggregation Capability:	support
Aggregation Status:	NO
Aggregation Port ID:	0

Figure 9-8 LLDP Local information

9.3.5 LLDP Neighbor

Select 'Maintenance diagnosis>LLDP>LLDP neighbor', you can view LLDP neighbor information. As shown in figure 9-9.

LLDP neighbor table display all ports' neighbor information. By filter, could select one port's neighbor information. Click<Clear filter> restore all port's neighbor information.

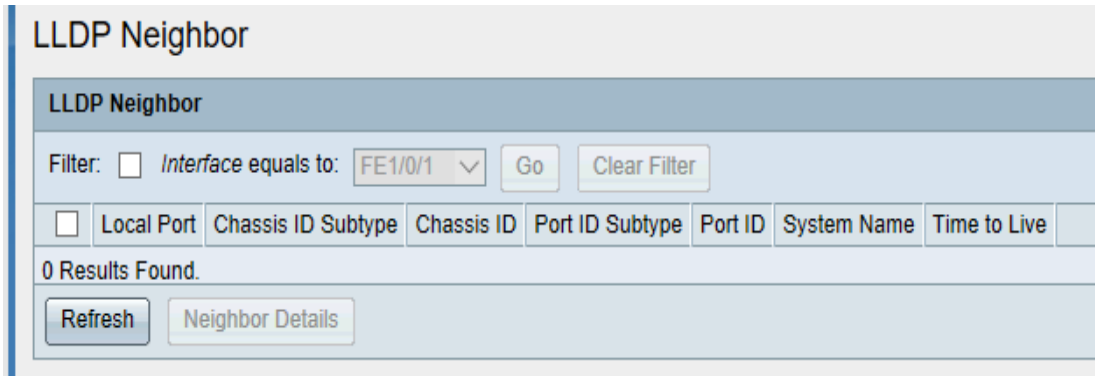


Figure 9-9 LLDP Neighbor table

Select LLDP neighbor items, click <Neighbor details> could check the LLDP neighbor item's detail information, as shown in figure 9-10.

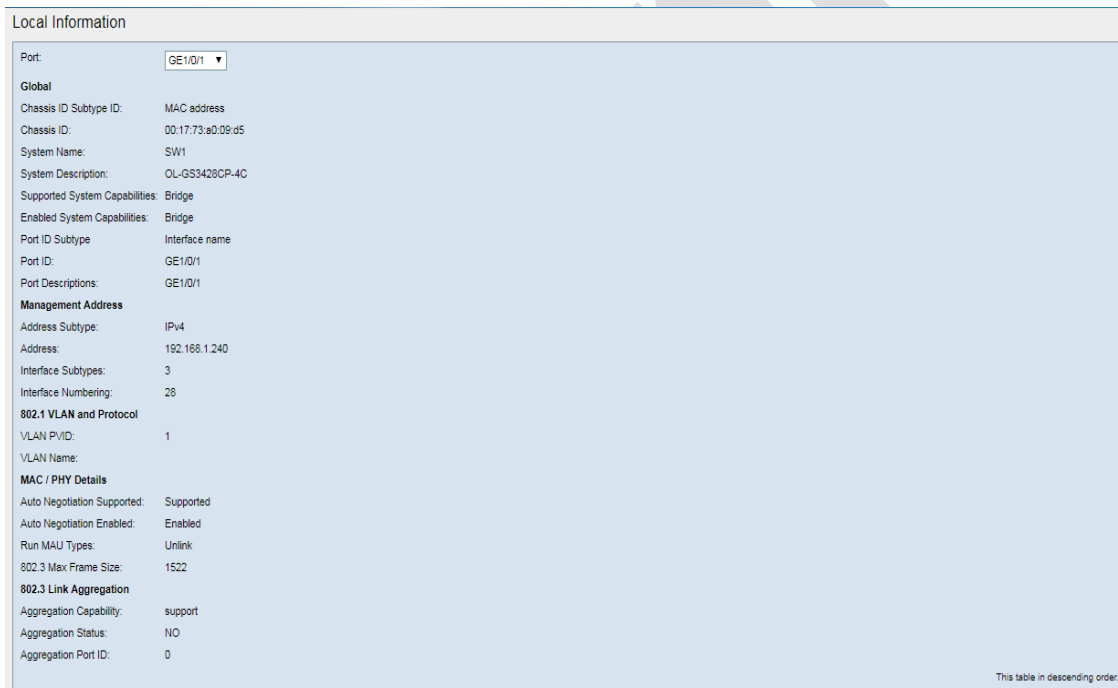


Figure9-10 LLDP detail

9.3.6 LLDP statistic

(1) In the navigation bar, select 'Maintenance diagnosis> LLDP>LLDP statistic', you can view LLDP statistic information, as shown in figure 9-11.

(2) Check the check box and click the < **Refresh** > button to refresh the LLDP statistics of the selected port manually.

(3) Check the check box and click the <**Clear**> button to clear the LLDP statistics of the selected port.

LLDP Statistics Table											Show 1-5 Total 28 <input type="text" value="5"/> Page	
<input type="checkbox"/>	Common Entry No	Port	Tx Frames Total	Rx Frames			Rx TLVs		Nerghbors Information Deletion Count			
				Total	Discard	Error	Discard	Unrecognized				
<input type="checkbox"/>	1	GE1/0/1	0	0	0	0	0	0	0	0		
<input type="checkbox"/>	2	GE1/0/2	0	0	0	0	0	0	0	0		
<input type="checkbox"/>	3	GE1/0/3	0	0	0	0	0	0	0	0		
<input type="checkbox"/>	4	GE1/0/4	0	0	0	0	0	0	0	0		
<input type="checkbox"/>	5	GE1/0/5	0	0	0	0	0	0	0	0		

Refresh Clear Page 1 Total 6

Figure 9-11 LLDP statistics