COMXUS

L3 Managed Ethernet

WEB Network Management Operation Guide

Ver 1.01

COMXUS A Brand of Willstrong Solution Pvt Ltd
Head Office- I-128, UPSIDC Site-C, Industrial Area, Surajpur,
Greater Noida, (U.P.) 201307
E-mail: info@comxus.com
Web: www.comxus.com
Toll-Free: 1800-890-8412

Declare

Copyright, all rights reserved

The copyright of this manual belongs to our company. Without the written permission of our company, no unit or individual may extract or copy part or all of the contents of this book without authorization, and may not disseminate it in any form.

Introduction

This manual mainly describes the WEB of the COMXUS L3 network switch. The user can manage the switch through the WEB page. This manual only gives a brief introduction to the operation of each WEB page. Please refer to the User Manual for the introduction of each function.

The preamble contains the following

- Audience Object
- Product Introduction
- Product Features

Audience Object

- Network Planner
- On-site technical support and maintenance personnel
- Responsible for the Network administrator responsible for network configuration and maintenance

Product Introduction

COMXUS L3 network switch is independently designed and developed by our company, which is specially designed for building high security and high-performance network. The system adopts a new software and hardware platform, which is an ideal convergence layer switch for office network, campus network, small and medium-size enterprises and branch offices.

Highlighted Features

- Support Port Shutdown
- Support auto negotiation, port speed of 10000M, 2500M, 1000M, 100m, half 100m, 10m and half 10m
- Supports full-duplex IEEE 802.3x, half-duplex backpressure flow control
- Supports rate limit for broadcast, multicast, and DLF packets
- Supports detection of broadcast, multicast, or unicast packets on a port and shuts down the port if the rate exceeds a threshold
- Port mirroring is supported
- Support port ingress and egress rate limit
- Support manual link aggregation
- Support LACP dynamic link aggregation
- Supports up to 32 aggregation groups, each group up to 8 ports
- Support source MAC, destination MAC, source destination MAC, source IP, destination IP, source destination IP routing strategy
- Supports port isolation
- Support up to 12KB packet
- Support for redundant port
- DDM with Fiber Port support
- Support Large MAC table capacity
- Support MAC table management
- Support IVL forwarding mode
- Support static MAC address, MAC address binding, and MAC address filtering
- Support Control the MAC learning based on port
- Supports 4K VLANs
- Support for 802.1Q-based VLAN

- Support for MAC-based VLAN
- Supports IP-based, protocol-based VLAN
- Voice VLAN support
- Support 1:1 VLAN mapping
- Q in Q Support basic Q in Q and support flexible Q in Q
- GVRP support
- Supports STP/RSTP/MSTP Spanning Tree Protocol
- Support Port Loop Detection
- Support for EAPS RFC3619
- Support ERPS (ITU-T G.8032/Y.1344)
- Support LLDP & LLDP-MED
- Support Fully compatible with CISCO's UDLD protocol
- Support for VLLP only with VRRP
- Support static and dynamic ARP
- Support static route based on IPv4 and IPv6
- Support 32 VLAN interfaces
- Support RIP v1/v2 & IPv6 RIPng
- Support OSPFv2 & IPv6 OSPFv3
- Support BGP4 & IPv6 BGP4+
- Support Policy Line, VRRP support
- Supports static multicast MAC address
- Support IGMP SNOOPING v1/v2/v3
- Support for IGMP Querier, IGMP Snoop Filter,
- Support MVR, GMRP, PIM-SM
- Support IGMP v1/v2/v3
- Standard and extended IP-based ACLs are supported

- Support for IP-based Extended ACL
- Supports MAC-based ARP, time-based ACL. Support ACL port filtering
- Support port queue number 8
- Port queue scheduling mode supporting WRR, WFQ, SP
- Supports port-based classification, 802.1p-based classification, DSCP based classification, and ACL-based classification
- Support packets mapping to queue
- Support COS or DSCP Remarking
- Support data flow statistics
- Support rate limits of data flow
- Support mirroring of data flow
- Supports DHCP Client, DHCP Snooping, DHCP Relay, DHCP Server, DHCP Option 82
- Support Console, Telnet and SSH
- Supports multiple Telnet links, SSH connections over IPv4 and IPv6
- Supports HTTP, HHTTPS over IPV4 and IPv6
- Support SNMP v1, v2, v3, SNMP trap
- Support lots of standard and private MIBs
- Support SNMP and TRAP based on IPv4 and IPv6
- Support multiple user management
- support switch authentication via TACACS+ server remote username and password
- Support password encryption in PAP and CHAP mode
- Support TACACS+ server to authorize the switch's commands
- Support TACACS+ based on IPv4 and IPv6
- Support local log management

- Support SYSLOG
- Support RMON 1, 2, 3 and 9 groups
- Support NDP, NTDP
- Support manual and automatic joining of cluster groups
- Support cluster unified management
- Support uploading and downloading configuration file
- Support TFTP transmission based IPv4 and IPv6
- Support local clock management
- Support SNTP
- Support enabling and disabling TELNET, SSH, HTTP, HTTPS and SNMP services
  Support TELNET, SSH, HTTP
- HTTPS and SNMP services to bind to standard IP ACLs
- Support for limiting the number of TELNET and SSH connections
- Supports authentication, authorization, and accounting through RADIUS server
- 802.1XSupport port-based and MAC-based 802.1x
- Support 802.1x guest VLAN
- Support static configuration of IP, MAC and port binding
- Support dynamic ARP binding to prevent ARP spoofing
- Support dynamic IP, MAC and port binding
- Support fixed port to connect to DHCP server to prevent private connection to DHCP server
- Support manually configuring MAC ARP-based ACL rules to prevent ARP spoofing.
- Support the DHCP SNOOPING function. During the process of obtaining an IP address by DHCP, the switch dynamically binds ARP to the port to prevent ARP spoofing.

- Supports PoE
- Support PoE powering of ports on and off
- Support setting total power
- Support PoE scheduling policy and PD online query, etc.
- Support IPv4/IPv6 dual protocol stack, IPv6 neighbor discovery, ICMPv6, and IPv6 path MTU discovery
- Support manual address configuration and stateless address auto-configuration
- Support PING, PING 6, Traceroute
- Support TELNET client based IPv4 and IPv6
- Support SSH client based IPv4 and IPv6

[Version Update]

Ver 1.0.1

User experience optimization

Resolves known issues and provides faster response.

Related functions are optimized to make management easier.

Directory

WEB PAGE OVERVIEW 11

1. Characteristics of web access 11
2. System requirements for web browsing 12
3. Login of web browsing session 12
4. Basic composition of web page 13
5. Introduction to page button 14
6. Error message.....15
7. Entry field.....15

Web page introduction 16

1. System configuration.....16

1) System information page.....16
2) IP address configuration page 17
3) User management page 17
4) Serial port information 18
5) SNTP configuration.....18
6) SNMP community configuration page 18
7) SNMP trap configuration page.....19
8) Log information.....20

2. Port configuration 20

1) Port basic configuration page.....20
2) Port statistics page.....21
3) Port storm suppression page.....22
4) Port speed limit page.....22
5) Protection port.....23

3, CONFIGURATION.....26
(1) Port mirroring configuration page.....23
(2) Link Aggregation Configuration Part.....24
(3) DDM information.....26
4, VLAN CONFIGURATION.....28
(1) Configuration Page.....28
(2) Access Port Configuration Page.....29
(3) Trunk Port Configuration Part.....30
(4) Hybrid Port Configuration Page.....30
(5) GVRP Configuration.....31
5, THREE-TIER CONFIGURATION.....32
(1) IP Basic Configuration.....32
(2) RIP configuration.....35
(3) OSPF Configuration.....36
(4) VRRP configuration.....37
6, SECURITY CONFIGURATION.....38
(1) MAC configuration.....38
(2) ACL Configuration.....40
(3) AAA Configuration.....45
(4) Native Management Security Configuration.....47
7, DHCP CONFIGURATION.....48
(1) DHCP client.....48
(2) DHCP Relay.....49
(3) DHCP server.....49
(4) DHCP snooping.....50
8, MULTICAST CONFIGURATION.....52
(1) IGMP SNOOPING Configuration.....52

(2) GMRP Configuration.....52
(3) Multicast routing configuration 54
(4) IGMP configuration 54
(5) PIM-SM Configuration 55
9, RING NETWORK CONFIGURATION 57
(1) Spanning Tree Configuration 57
(2) ERPS Configuration.....58
(3) EAPS Configuration.....60
10, ADVANCED CONFIGURATION.....62
(1) QoS Configuration 62
(2) LLDP configuration 63
11, SYSTEM TOOLS 64
(1) Save Configuration 63
(2) Backup configuration films.....63
(3) Restore Configuration File 63
(4) Software upgrade.....64
(5) Restore Factory Configuration 65
(6) Restart 65
12, PoE CONFIGURATION 65
(1) PoE Port Configuration 65
(2) PoE scheduling configuration 66
(3) PD Query Configuration ..... ….….…66

WEB page operation manual

This manual mainly describes the WEB page of the switch. The user can The WEB page manages the switch. This manual only briefly introduces the operation of each WEB page. For the introduction of each function of the switch, see User Operation Manual. This manual mainly includes the following contents:

1, WEB Page Overview
2, WEB page introduction

WEB Page Overview

1, Characteristics of WEB access

The switch provides Web access to the user. Users can access the switch through a Web browser to manage and configure the switch. The main features of WEB access are:

- Easy access: Users can easily access the switch from anywhere on the network.
- Users can use familiar browsers such as Firefox, Google Chrome, Opera and Microsoft Internet Explorer (8.0 and above) to access the WEB page of the switch. The WEB page is presented to the user in graphical and tabular form.
- The switch provides rich WEB pages, through which the user can configure and manage most of the functions of the switch.
- The classification and integration of WEB page functions are convenient for users to find relevant pages for configuration and management.

2, System requirements for WEB browsing

The system requirements for Web browsing are shown in Table 1.

Table 1:

Hardware and software	System Requirements
CPU	Pentium 586Up
Memory	128MB or more
Resolution	1024 x768-up
color	More than 256 colors
Browser	Internet Explorer 8.0 or above or Firefox or Google Chrome or Opera, etc.
Operating system	Microsoft ® Windows XP ®/Windows Vista ®/Windows 7 ®/Windows 8 ®, MAC, Linux, Unix, etc.

notice：

Microsoft®, Windows xp®, Windows Vista®, Windows 7®, Windows8® are registered trademarks of Microsoft Corporation. All other product names, trademarks, registered trademarks, and service marks are copyrighted by their respective owners.

3, Login of WEB browsing session

Before starting a Web browsing session, the user needs to confirm:

- The switch has been configured for IP, and by default, the interface IP address for VLAN 1 on the switch is 192.168.0.5
- The subnet mask is 255.255.255.0
- A host with a Web browser installed is connected to the network and is able to ping the switch.

After completing the above two tasks, the user enters the address of the switch in the address bar of the browser and presses Enter to enter the Web login page of the switch, as shown in Figure 1. The Web can be accessed only if the correct password is entered. The default user is comxus, and the password is comxus by default.

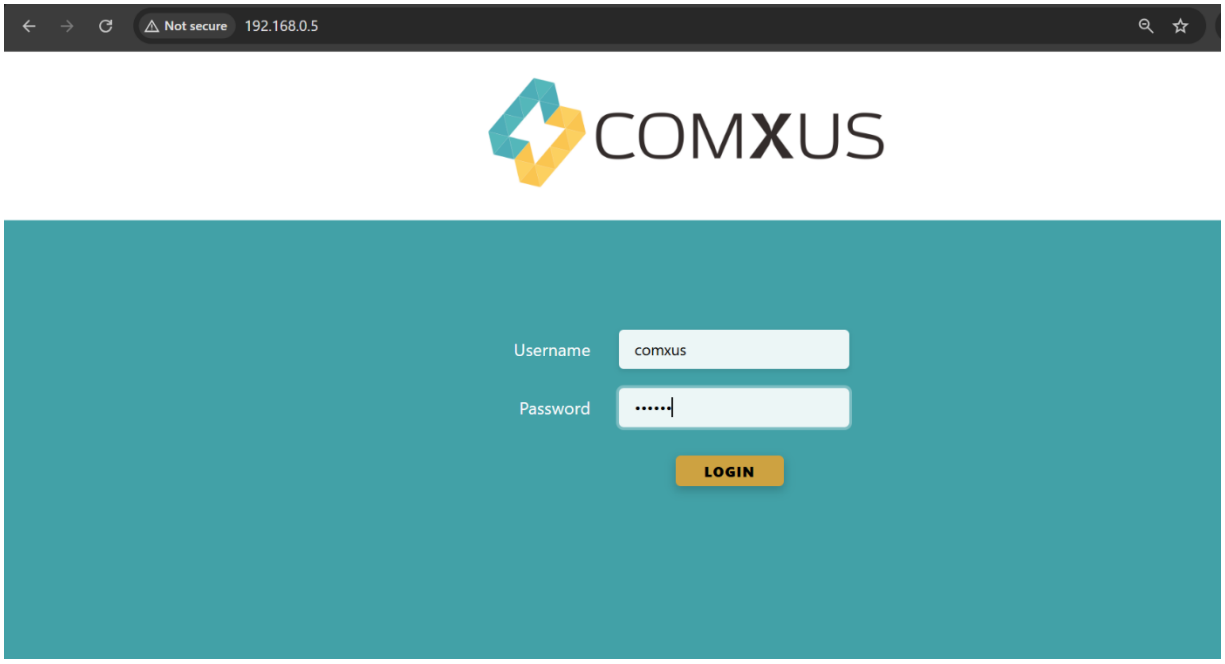


Figure 1 Login page for a WEB browsing session

4, Basic composition of WEB page

As shown in Figure 2, the WEB page is mainly composed of four parts: title page, category navigation page, menu page and main page.

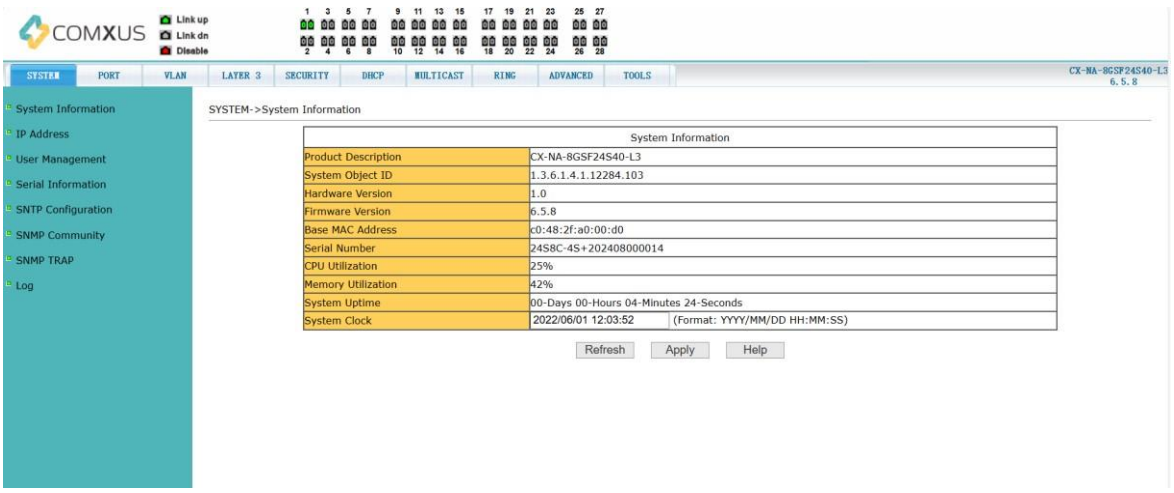


Figure 2 Basic Composition Page of Switch WEB Page

The **banner page** is used to display the logo and the real-time port status, as shown in the following figure：

- A green light indicates that the port is connected;
- A gray light indicates that the port is in an unconnected state;
- A red light indicates that the port is down

The **category navigation page** is the function category entry of WEB. The user can click a button to view the corresponding category menu. The right side of the page is the switch model version and login user name.

The **menu page** displays the category menu selected by the user from the category navigation page. There may be a primary or secondary menu. Click the menu item to open the corresponding page.

The **main page** is used to display the page selected by the user from the menu page.

5, Introduction to Page Button

There are some common buttons on the page. The functions of these buttons are generally the same. Table 2 describes the functions of these buttons.

Table 2:

button	Action
Refresh	Update all domains on the page
application	Place the updated value in memory. Because error checking is done by the Web server, there is no error checking until the user selects the button
delete	Delete the current record
help	Open the help page to view the configuration instructions for each pack

6, Error Message

If an error occurs when the WEB server of the switch processes a user request, a corresponding error message is displayed in a dialog box. For example, Figure 4 shows an error message dialog box.

Figure 3 Error Information Page

7, Entry Field

Some pages have an entry field at the beginning, as shown in Figure 4, through which different entries can be accessed. When you select a value in an entry field, the corresponding information for that row is displayed on the page, and the contents of the row are edited. The row is also called the active row.

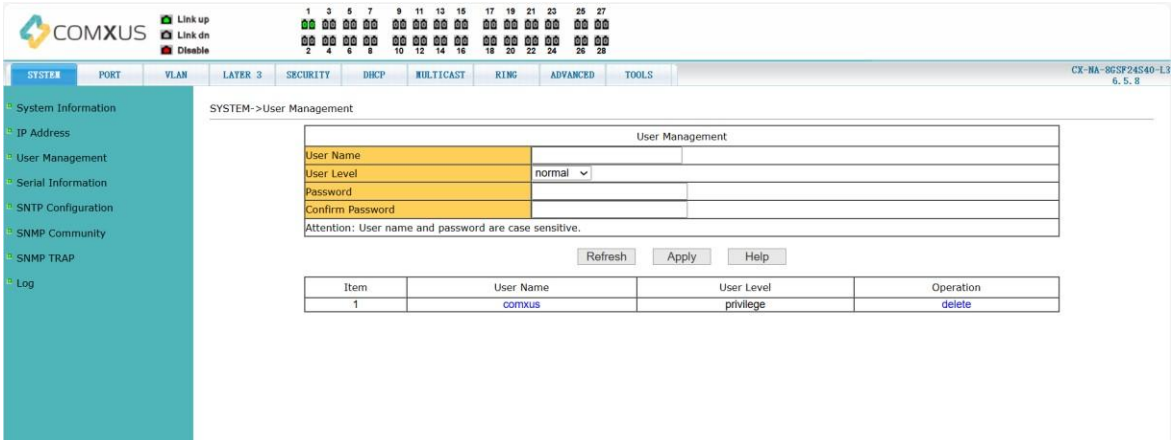


Figure 4 Entry field page

WEB page introduction

The WEB pages of the switch are organized into groups, and each group includes one or more WEB pages. Each page is described below one by one.

1, System configuration

(1) System Information Page

Figure 1-1 is the system information configuration page, through which the user can configure and view the system information of the switch.

Product Model: The product model description of the switch

Firmware Version Information: The firmware version currently used by the switch

Bootrom version information: The version of Bootrom currently used by the switch

Base MAC Address: The base MAC address of the switch

Serial Number: The serial number of the switch

Serial port baud rate: serial port baud rate used by the switch

System startup time: The time since the switch was started

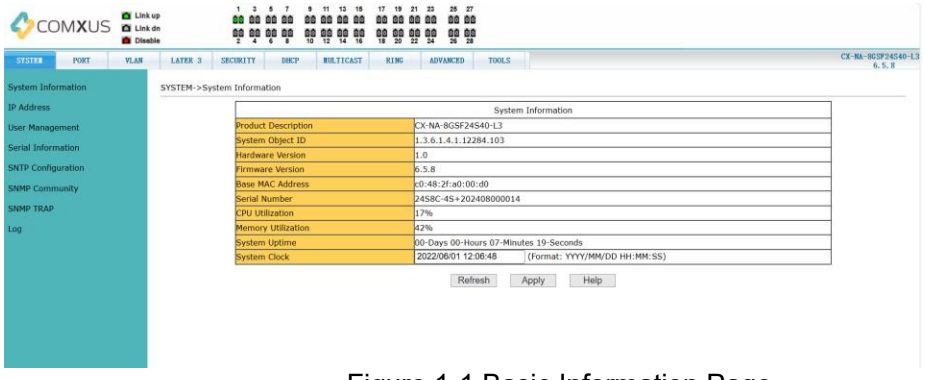


Figure 1-1 Basic Information Page

System clock (modifiable): the current clock of the system; year, month, day, hour, minute and second are required to be input

(2) IP address configuration page

Figure 1-2 is the IP address configuration page. The user can configure the IP address, subnet mask, and gateway address of the switch through this page. The management VLAN is 1 by default and cannot be modified.

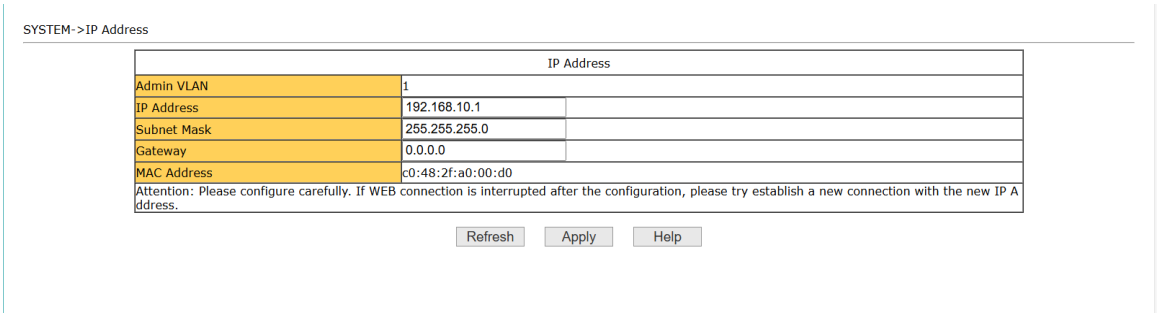


Figure 1-2 IP Address Configuration Page

(3) User management page

Figure 1-3 is the user management page, through which user information can be configured. The default user of the switch is comxus, which cannot be deleted, but the password can be modified.

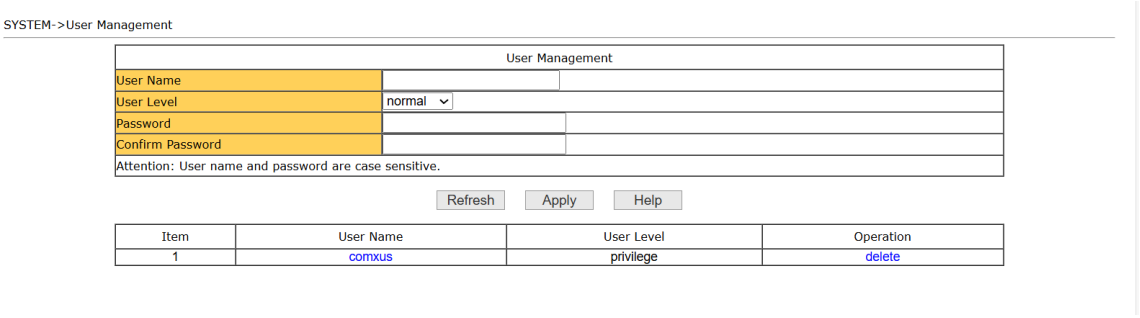


Figure 1-3 User Management Page

(4) Serial port information

Figure 1-4 is the serial port information page, through which you can view the serial port information.

Figure 1-4 Serial Port Information Page

(5) SNTP Configuration

Figure 1-5 is the SNTP configuration page, through which the administrator can configure and view the system clock.

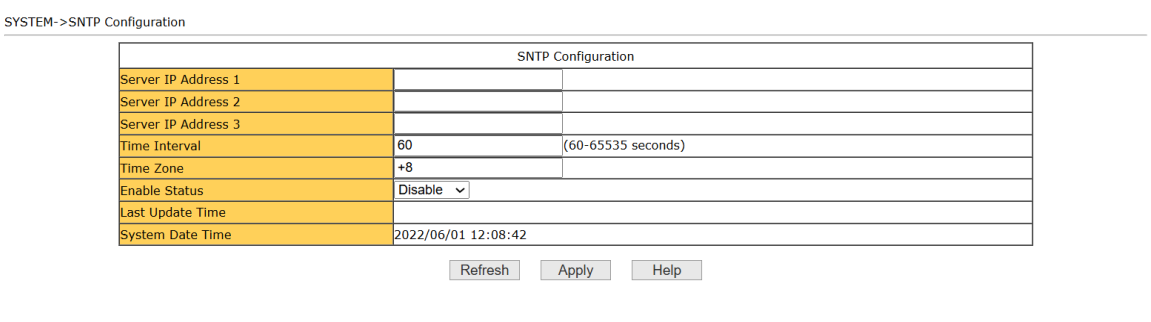


Figure 1-5 SNTP Configuration Page

(6) SNMP Community Configuration Page

Figure 1-6 shows the SNMP Community Configuration page. This page allows the user to configure the name and read and write permissions of the community of the switch. A total of eight entries can be configured.

By default, the switch has a community with a public name that is read-only

When the switch needs to be managed through SNMP, it is necessary to configure a common body with readable and writable permissions.

The configured community cannot be modified and cannot be added with the same name as the existing one. However, you can click the corresponding delete link to delete the community and then reconfigure it.

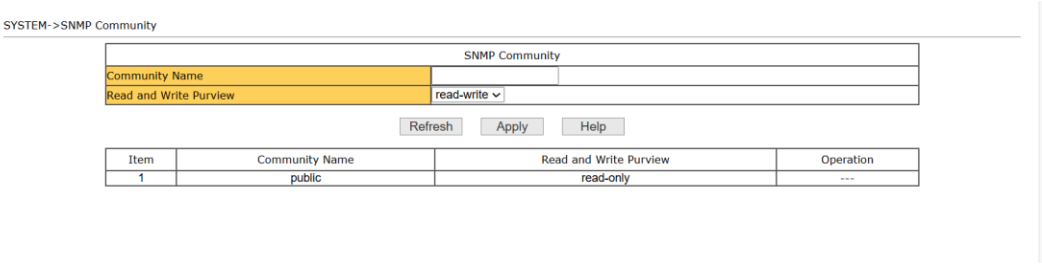


Figure 1-6 SNMP Community Configuration Page

(7) SNMP TRAP Configuration Page

Figure 1-7 shows the SNMP TRAP configuration page, which allows the user to configure the IP address of the station receiving the TRAP message and some parameters of the TRAP protocol package.

Enter the TRAP name, the IP address of the TRAP server, and select the version number. If the configuration is successful after submission, the SNMP TRAP function will work. Once link up or link down occurs, the switch will automatically send the TRAP packet to the target address.

Configured TRAP targets cannot be modified and added without duplicating an existing name. However, you can click the corresponding delete link to delete the TRAP target and then reconfigure it.

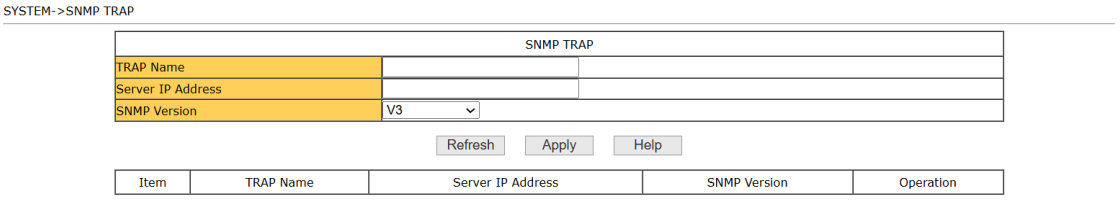


Figure 1-7 SNMP TRAP Configuration Page

(8) Log information

Figure 1-8 is the log information page through which the user can view the log. Select the priority from the drop-down list to view the log of this level. Click Refresh to view the latest log.

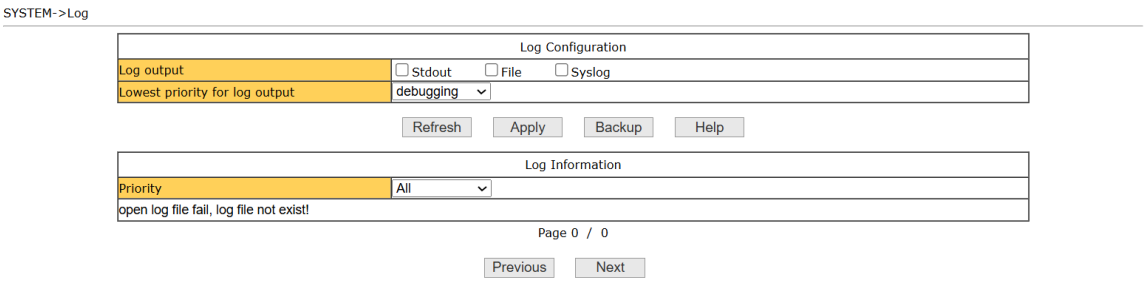


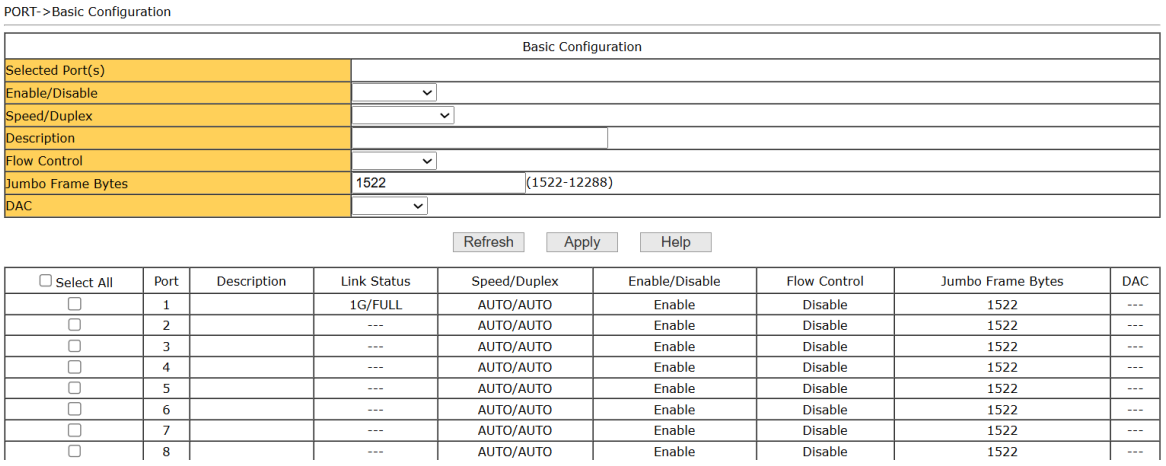
Figure 1-8 Log Information Page

2, Port configuration

(1) Port Basic Configuration Page

Figure 2-1 shows the port basic configuration page. From this page, users can enable or disable ports, set port rates and flow control, or view the basic information of all ports.

To modify the port configuration, the user needs to check the left side of the corresponding port or use the "Select All" function. The selected ports will be displayed at the top of the page, and several consecutive ports will be represented by connection numbers. After successful setting, the selected port will be configured with the same parameters. The list on the page shows the configuration information for all ports.


PORT->Basic Configuration

Basic Configuration	
Selected Port(s)	
Enable/Disable	
Speed/Duplex	
Description	
Flow Control	
Jumbo Frame Bytes	1522 (1522-12288)
DAC	

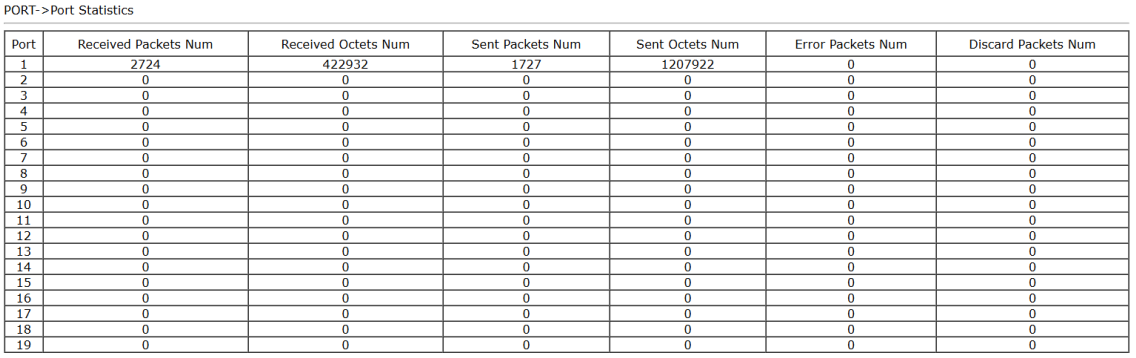
Refresh Apply Help

Select All	Port	Description	Link Status	Speed/Duplex	Enable/Disable	Flow Control	Jumbo Frame Bytes	DAC
	1		1G/FULL	AUTO/AUTO	Enable	Disable	1522	---
	2		---	AUTO/AUTO	Enable	Disable	1522	---
	3		---	AUTO/AUTO	Enable	Disable	1522	---
	4		---	AUTO/AUTO	Enable	Disable	1522	---
	5		---	AUTO/AUTO	Enable	Disable	1522	---
	6		---	AUTO/AUTO	Enable	Disable	1522	---
	7		---	AUTO/AUTO	Enable	Disable	1522	---
	8		---	AUTO/AUTO	Enable	Disable	1522	---

Figure2-1 Port Configuration and Port Display Page

(2) Port Statistics Page

Figure 2-2 is the Port Statistics page. The page lists the number of packets sent, bytes sent, packets received, bytes received, error packets, and dropped packets for all ports.


PORT->Port Statistics

Port	Received Packets Num	Received Octets Num	Sent Packets Num	Sent Octets Num	Error Packets Num	Discard Packets Num
1	2724	422932	1727	1207922	0	0
2	0	0	0	0	0	0
3	0	0	0	0	0	0
4	0	0	0	0	0	0
5	0	0	0	0	0	0
6	0	0	0	0	0	0
7	0	0	0	0	0	0
8	0	0	0	0	0	0
9	0	0	0	0	0	0
10	0	0	0	0	0	0
11	0	0	0	0	0	0
12	0	0	0	0	0	0
13	0	0	0	0	0	0
14	0	0	0	0	0	0
15	0	0	0	0	0	0
16	0	0	0	0	0	0
17	0	0	0	0	0	0
18	0	0	0	0	0	0
19	0	0	0	0	0	0

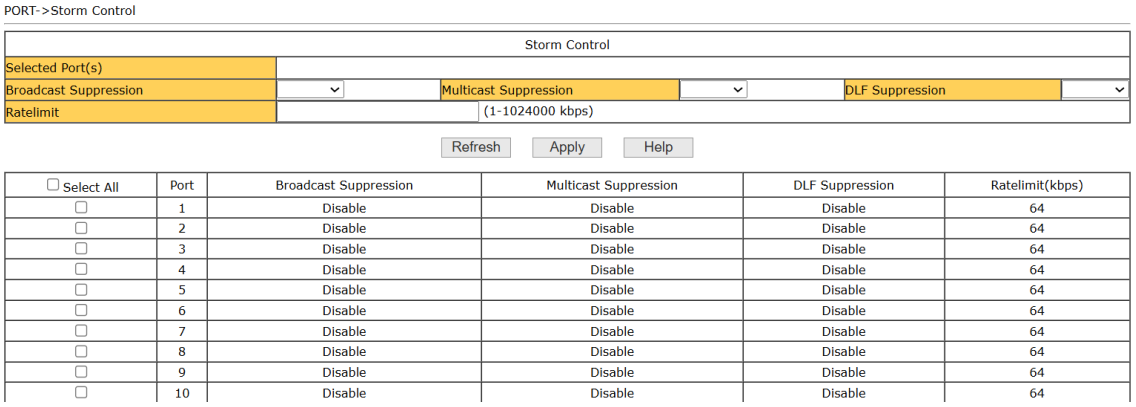
Figure2-2 Port Statistics Page

(3) Port Storm Suppression Page

Figure 2-3 shows the port storm suppression page. This page is used to configure the suppression of broadcast, multicast, and DLF packets on a port.

Check on the left side of the corresponding port, or use the "Select All" function to select the port to turn on and off the broadcast suppression,

multicast suppression and DLF suppression of the port. The suppression rate type item and the suppression rate item are used to select the suppression rate type and suppression rate value to be configured. The suppression rate range is 1-1024000, and the unit is kbits. The suppression rates of broadcast suppression, multicast suppression and DLF suppression can be configured independently. The list on the page shows the configuration information for all ports.


PORT->Storm Control

Storm Control

Selected Port(s)					
Broadcast Suppression		Multicast Suppression		DLF Suppression	
Ratelimit	(1-1024000 kbps)				

Refresh Apply Help

Select All	Port	Broadcast Suppression	Multicast Suppression	DLF Suppression	Ratelimit(kbps)
	1	Disable	Disable	Disable	64
	2	Disable	Disable	Disable	64
	3	Disable	Disable	Disable	64
	4	Disable	Disable	Disable	64
	5	Disable	Disable	Disable	64
	6	Disable	Disable	Disable	64
	7	Disable	Disable	Disable	64
	8	Disable	Disable	Disable	64
	9	Disable	Disable	Disable	64
	10	Disable	Disable	Disable	64

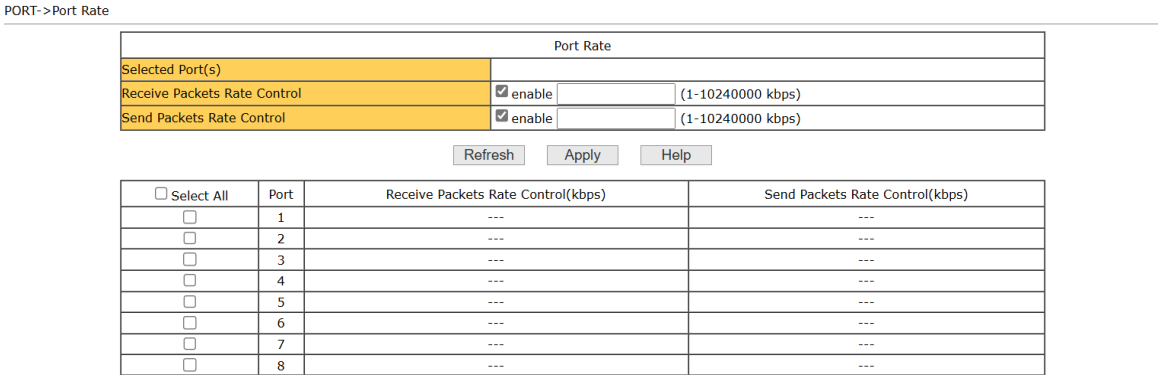
Figure2-3 Broadcast Storm Suppression Page

(4) Port speed limit page

Figure 2-4 shows the port speed limit page. This page is used to configure the port ingress and egress speed limits.

Check on the left side of the corresponding port, or use the "Select All" function to select the port. The inlet/outlet port speed limit can be enabled independently by checking. The speed limit range is 1-1024000, and the unit is kbits.

If the check is cancelled, the speed is not limited. The list on the page shows the configuration information for all ports.


PORT->Port Rate

Port Rate

Selected Port(s)	
Receive Packets Rate Control	☑ enable (1-10240000 kbps)
Send Packets Rate Control	☑ enable (1-10240000 kbps)

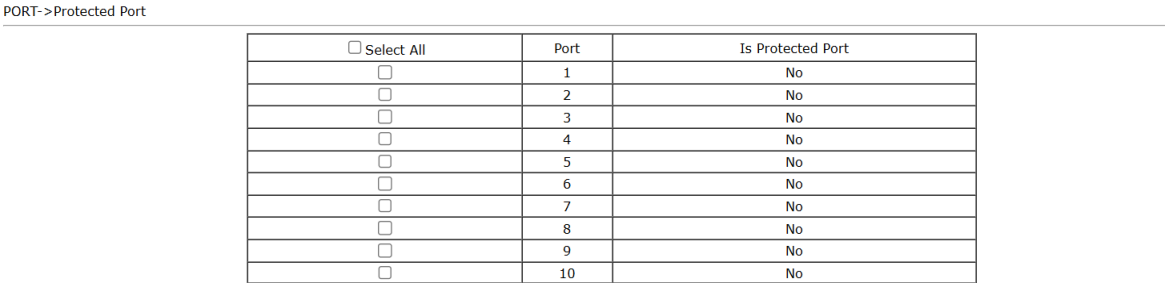
Refresh Apply Help

☐ Select All	Port	Receive Packets Rate Control(kbps)	Send Packets Rate Control(kbps)
☐	1	---	---
☐	2	---	---
☐	3	---	---
☐	4	---	---
☐	5	---	---
☐	6	---	---
☐	7	---	---
☐	8	---	---

Figure2-4 Port Speed Limit Page

(5) Protection Port

Figure 2-5 is the protection port setting interface. This page is used to configure/display protection port information.


PORT->Protected Port

☐ Select All	Port	Is Protected Port
☐	1	No
☐	2	No
☐	3	No
☐	4	No
☐	5	No
☐	6	No
☐	7	No
☐	8	No
☐	9	No
☐	10	No

Figure2-5 Protection Port Page

(3) Port configuration page

(1) Port mirroring configuration page

Figure 2-6 shows the port mirroring configuration page, which allows the user to configure port mirroring. Port mirroring is to monitor the data packets output by the mirrored output port and the data packets input by the mirrored

input port through the mirroring port. Only one mirror port can be selected, and multiple mirrored output ports and mirrored input ports can be selected. When configuring, select a mirror port first, and select "Do not mirror" to cancel the mirror configuration. Then select the port and direction to be mirrored from the other ports. When the ingress port in the monitoring direction is selected, it means to monitor the received data packets, and the egress port means to monitor the sent data packets. Ticking both means to monitor all the sent and received data packets.

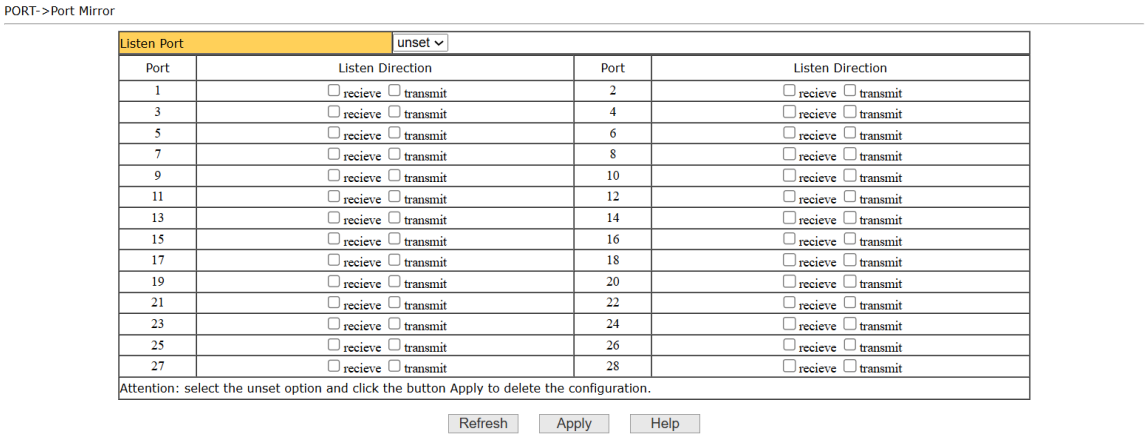


Figure2-6 Port Mirror Configuration Page

(2) Link Aggregation Configuration Part

The following figure shows the link aggregation configuration page. The page lists all ports vertically and all aggregation groups horizontally. To add a port to an aggregation group, just click the radio box at the intersection of the row and column. You can also select the aggregation method at the bottom of

each aggregation group. If you want to cancel the aggregation configuration of the specified port, click the leftmost radio box corresponding to the port.

① Create an aggregation group

Figure 2-7-1 shows the link aggregation creation interface. This page is used to configure aggregation groups.

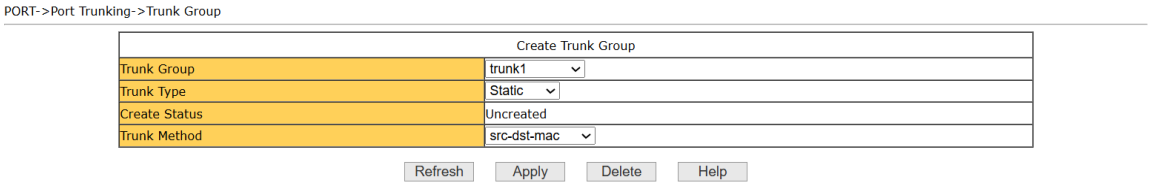


Figure 2-7-1 Create Aggregation Group Page

② Configure Aggregation Group

Figure 2-7-2 shows the interface for configuring the aggregation group. This page is used to configure the aggregation group.

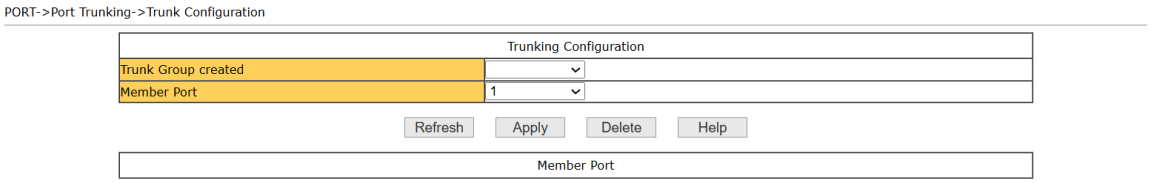


Figure 2-7-2 Configure Aggregation Group Page

③ Aggregate Information

Figure 2-7-3 shows the interface for viewing aggregated information. This page is used to view aggregation information for a link aggregation.

Figure 2-7-3 Aggregate Information Page

(3) DDM information

Figure 2-8 shows the DDM information viewing interface. This page is used to view the corresponding information of the optical module.

Figure 2-8 DDM Information Page

4, VLAN Configuration

(1) Configuration Page

Figure 4-1 shows the VLAN configuration page. This page allows the user to create VLANs and displays information for all VLANs.

If you want to create a new VLAN, enter the VID in the active line from 2 to 4094. The switch creates VLAN 1 by default, and VLAN 1 cannot be deleted.

The VLAN list displays all created VLANs and indicates the port membership of each VLAN. A port may not be a member of a VLAN, and may be a tagged or untagged member of a VLAN. The characters before the port on the page have the following meanings:

T Tagged The port is a tagged member of this VLAN

U Untagged The port is an untagged member of this VLAN

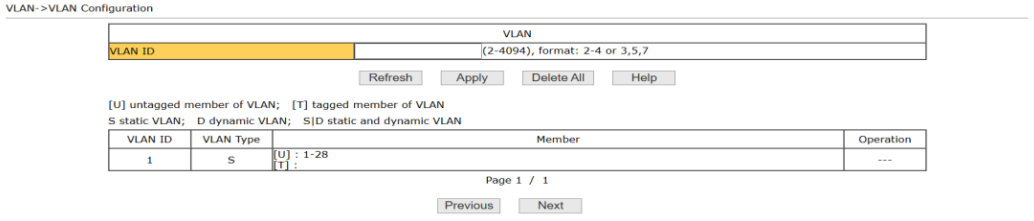


Figure 4-1 VLAN Configuration Page

(2) Access Port Configuration Page

Figure 4-2 shows the Access Port Configuration page, which displays and configures the Port Access Mode and the VLAN to which it belongs. The page is divided into two parts: port list and VLAN list. Hover the mouse on the port to see the VLAN mode of the port. Click a port to display/configure the VLAN of the port. If the port is in Access mode, its VLAN can be displayed when it is selected. If other VLANs are selected and applied, the VLAN of the port is changed. If the port is not in Access mode, the port is changed to Access mode after configuration and the VLAN is set. Note that only one VLAN can be selected in Access mode.

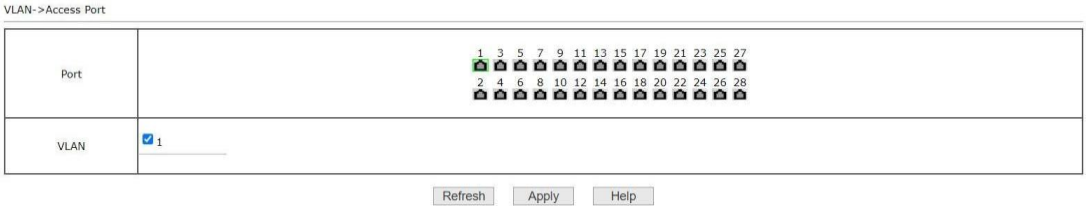


Figure 4-2 Access Port Configuration Page

(3) Trunk Port Configuration Part

Figure 4-3 shows the Trunk Port Configuration page, which displays and configures the port Trunk mode and the VLAN to which it belongs. This page is divided into two parts: port list and VLAN list. For the operation of port part, please refer to Section 2 (Access Port Configuration Page). If the port is in Trunk mode, its VLAN can be displayed when it is selected. If other VLANs are selected and applied, the VLAN of the port is changed. If the port is not in Trunk mode, after configuration, the port is changed to Trunk mode and the VLAN is set. Multiple VLANs can be selected in Trunk mode. To select a group of consecutive VLANs, select the first one, press and hold the Shift key, and then select the last one.

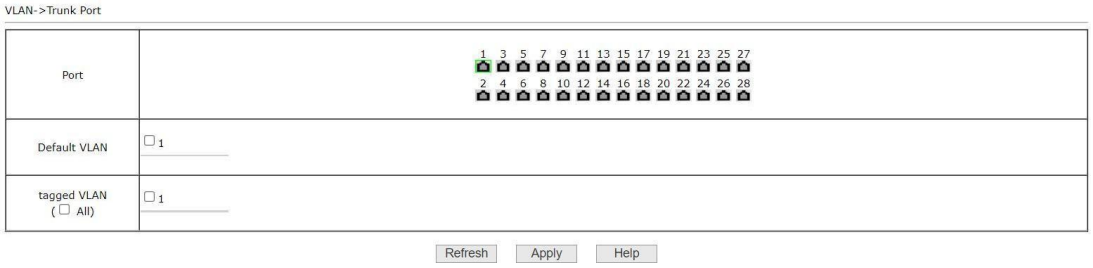


Figure 4-3 Trunk Port Configuration Page

(4) Hybrid Port Configuration Page

Figure 4-4 shows the Hybrid port configuration page, which displays and configures the port in Hybrid mode and the VLAN to which it belongs. This page is divided into two parts: port list and VLAN list. For the operation of port part, please refer to Section 2 (Access Port Configuration Page). If the port is in Hybrid mode, its VLAN can be displayed when it is selected. If other VLANs are selected and applied, the VLAN of the port is changed. If the port is not in Hybrid mode, after configuration, the port is changed to Hybrid mode and the VLAN is set. The default VLAN must be configured and only one can be selected. Any number of tagged VLANs and untagged VLANs can be selected. However, for a VLAN, only one of the three modes can be selected. If a VLAN is configured with a tagged VLAN, The VLAN cannot be designated as a default VLAN or an untagged VLAN, and so on.

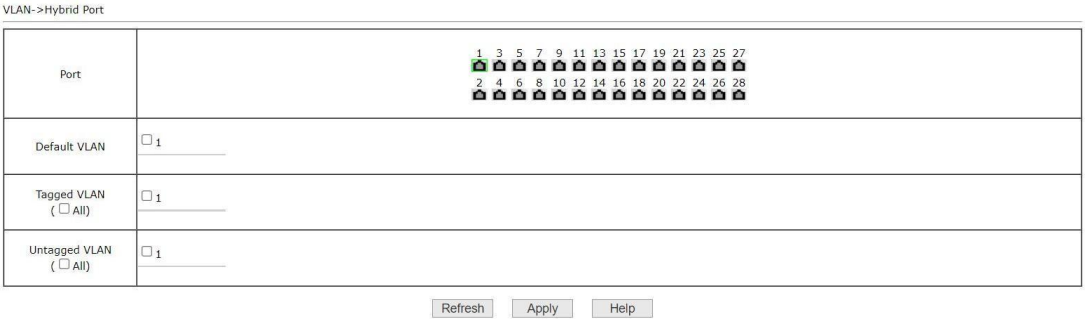


Figure 4-4 Hybrid Port Configuration Page

(5) GVRP Configuration

① GVRP Global Configuration

Figure 4-5-1 shows the GVRP global configuration page, through which the user can enable GVRP.

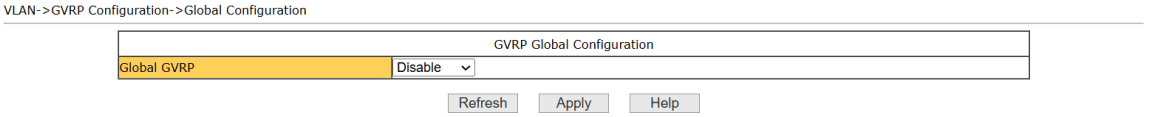


Figure 4-5-1 GVRP Global Configuration Page

② GVRP Port Configuration

Figure 4-5-2 is the GVRP port configuration page, through which the user can enable port GVRP and view port information.

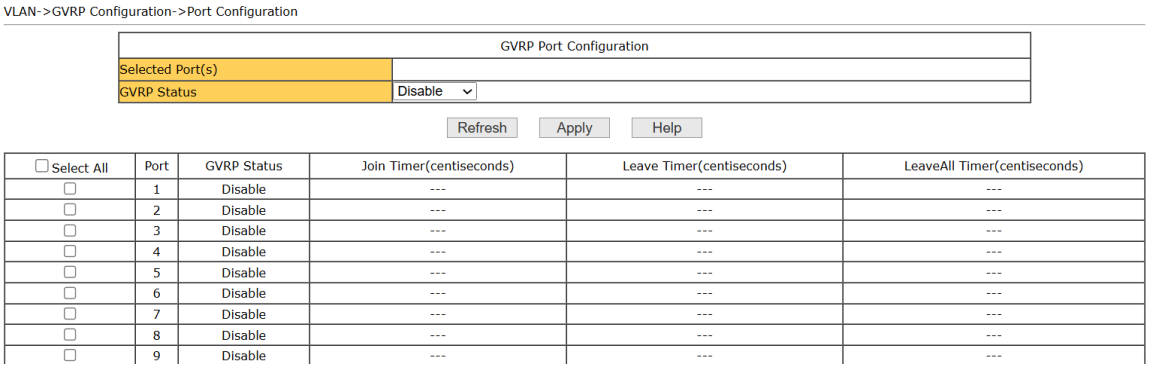


Figure 4-5-2 GVRP Port Configuration Page

③ GVRP state machine

Figure 4-5-3 is the GVRP state machine page, through which the user can view the state machine information established by GVRP.

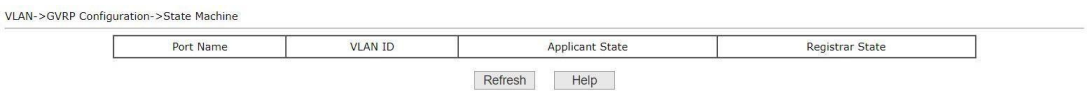


Figure 4-5-3 GVRP State Machine Page Diagram

5, Three-tier configuration

(1) IP Basic Configuration

① VLAN interface configuration

Figure 5-1-1 is the VLAN interface configuration page, through which the user can configure the IP address of the interface, delete the IP address of the interface and view the interface information.

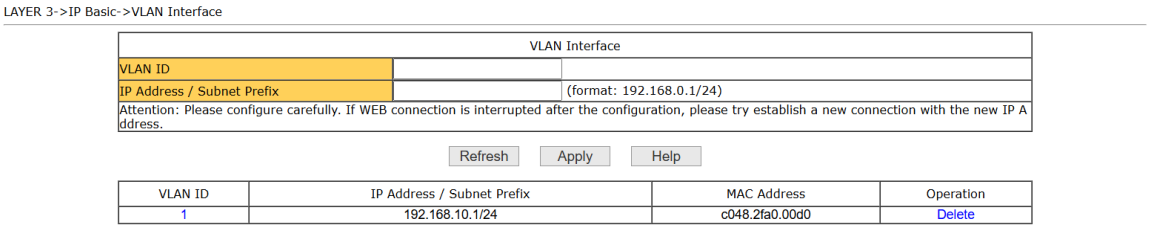


Figure 5-1-1 VLAN Interface Configuration Page

The switch has a VLAN 1 interface by default, which cannot be deleted. Only one VLAN interface can be configured for each VLAN.

② ARP interface configuration

Figure 5-1-2 is the ARP configuration page. This page can display all the information of the ARP table of the switch. At the same time, the user can configure the static ARP entry, delete the ARP entry, and modify the dynamic ARP entry to the static ARP entry through this page.

When configuring a static ARP entry, the user needs to enter the IP address and MAC address. The MAC address must be a unicast MAC address, and then click the Apply button.

When the user deletes an ARP entry, click the corresponding delete link in the list.

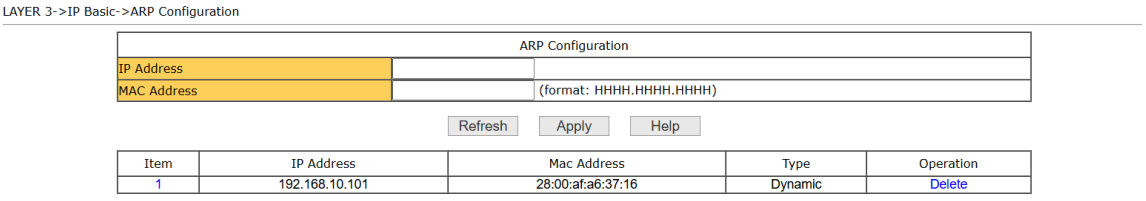


Figure 5-1-2 ARP Interface Configuration Page

③ Static route configuration

Figure 5-1-3 is the static route configuration page, through which the user can add or delete the static route of the switch. By default, the switch is not configured with a static route. The user can also use this page to configure a default route, that is, a route with a destination address/subnet prefix of 0.0.0.0/0.

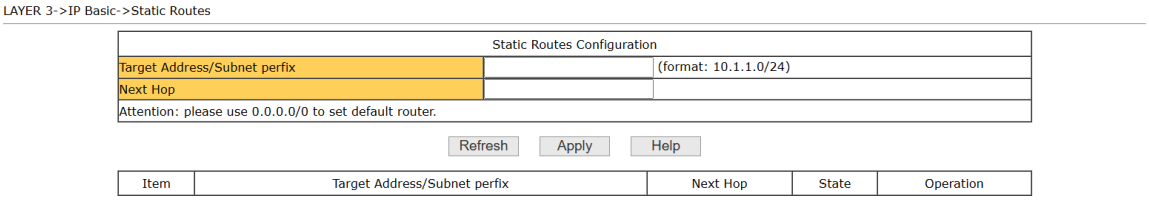


Figure 5-1-3 Static Route Configuration Page

④ _ Routing table information

Figure 5-1-4 shows the Routing Table Information page, which displays the routing table entries of the switch. Users can filter the displayed routes by route state and route type to view the required routing information.

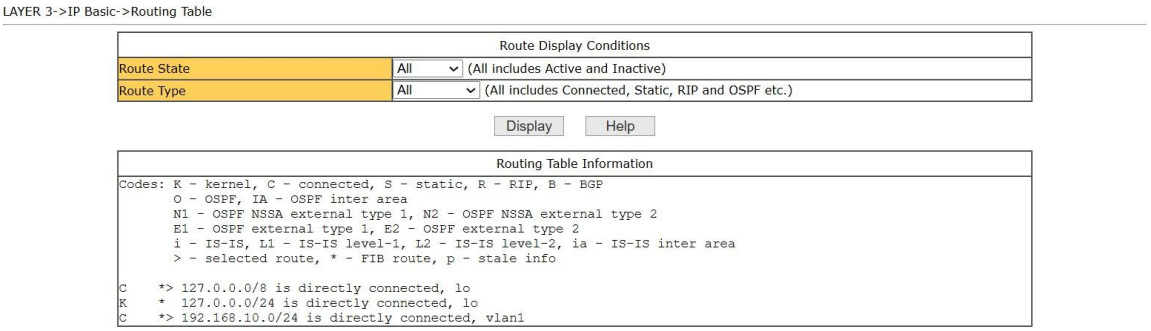


Figure 5-1-4 Routing Table Information Page

(2) RIP configuration

① RIP configuration

Figure 5-2-1 shows the RIP configuration page, through which the user

can turn on/off the RIP state and declare the corresponding network segment.

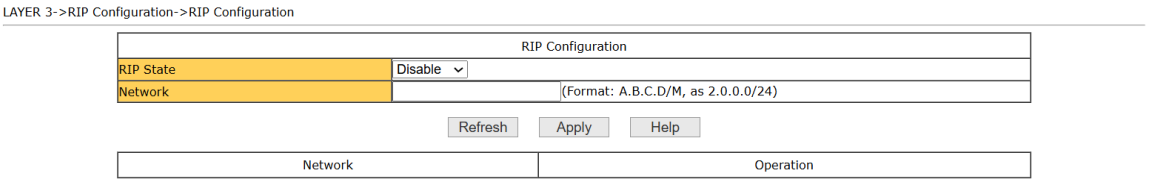


Figure 5-2-1 RIP Configuration Page

② RIP Interface Information

Figure 5-2-2 is the RIP interface information interface, and the user can view the RIP interface information.

Figure 5-2-2 RIP Interface Information Page

③ RIP routing information

Figure 5-2-3 shows the RIP routing information interface. The user can view the RIP routing information configured by RIP.

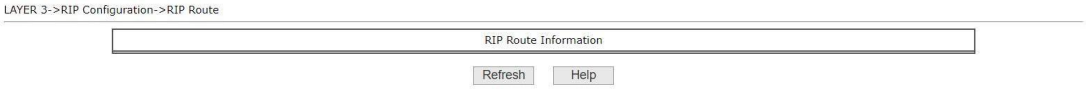
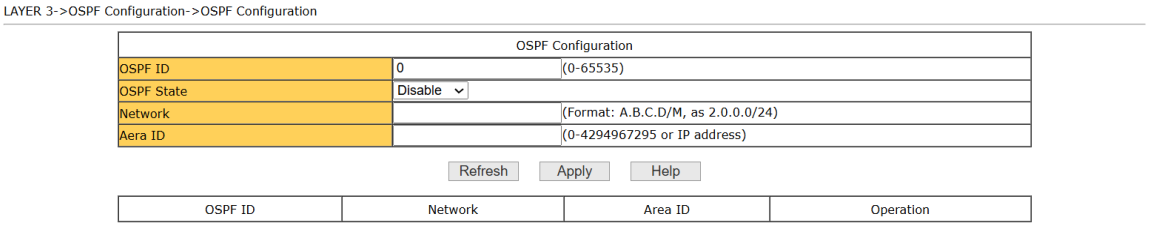


Figure 5-2-3 RIP Routing Information Page

(3) OSPF Configuration

① OSPF Configuration

Figure 5-3-1 shows the OSPF configuration. This page is used to configure the OSPF configuration.



② OSPF interface information

Figure 5-3-2 shows the interface for viewing OSPF interface information. This page is used to view interface information for OSPF.

Figure 5-3-2 OSPF Interface Information Page

③ OSPF Neighbor Information

Figure 5-3-3 shows the OSPF neighbor information viewing interface. This page is used to view neighbor information for OSPF.

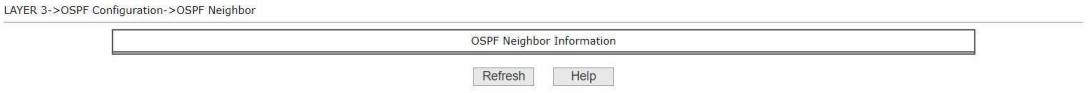


Figure 5-3-3 OSPF Neighbor Information Page

④ OSPF link-state information

Figure 5-3-4 is the OSPF link status information viewing interface. This page is used to view the link state information for the OSPF configuration.

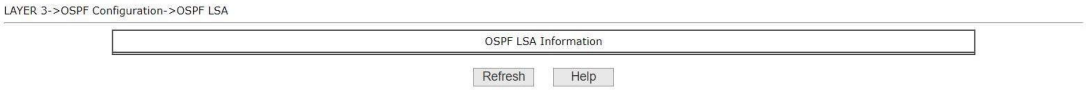


Figure 5-3-4 OSPF Link State Information Page

⑤ OSPF routing information

Figure 5-3-5 shows the OSPF routing information viewing interface. This page is used to view routing information for an OSPF configuration.

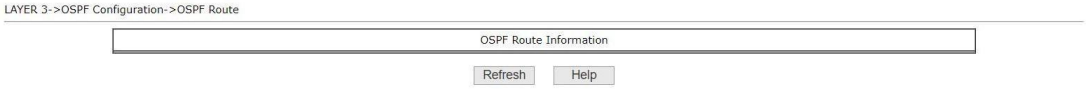


Figure 5-3-5 OSPF Routing Information Page

(4) VRRP configuration

① VRRP configuration

Figure 5-4-1 shows the VRRP configuration. This page is used to configure the VRRP configuration.

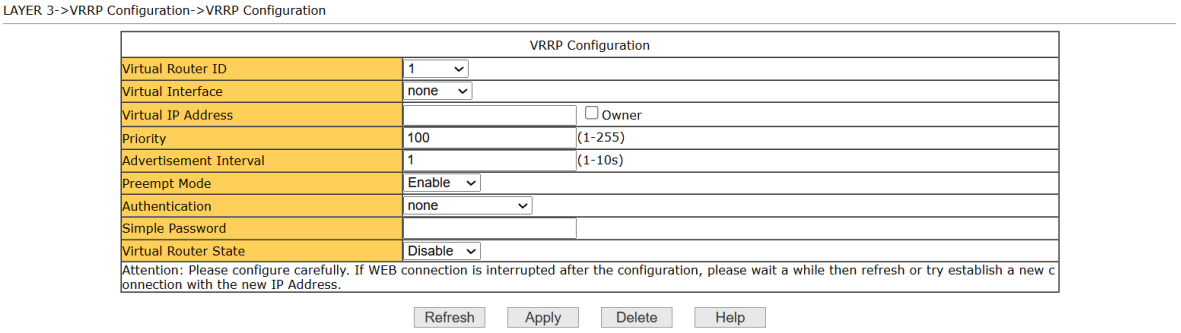


Figure5-4-1 VRRP configuration page

② VRRP Information

Figure 5-4-2 shows the VRRP information viewing interface. This page is used to view the VRRP information of the VRRP configuration.

Figure 5-4-2 VRRP information page

6, Security Configuration

(1) MAC configuration

① MAC address manual binding

Figure 6-1-1 is the MAC binding configuration page. This page is used to implement the binding of port and MAC address.

The MAC entry on the page is used to enter the bound MAC address, and the VLAN ID entry is used to enter the VLAN to which the MAC address belongs.

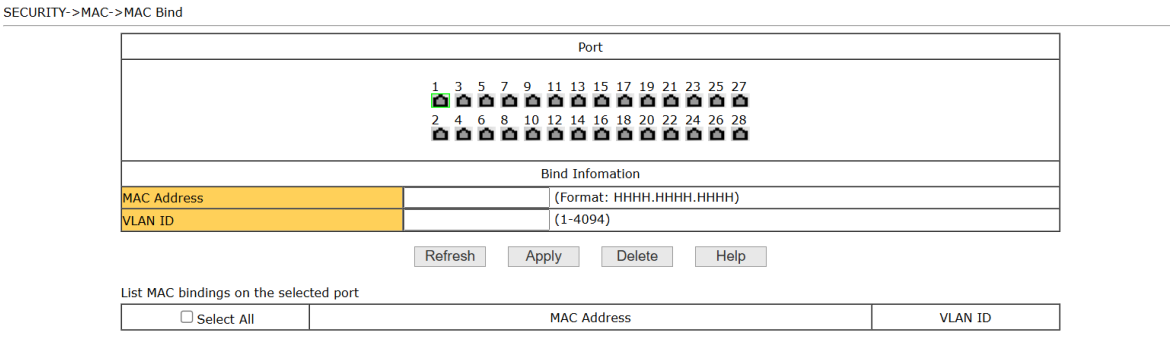


Figure 6-1-1 MAC address manual binding page

② Automatic MAC address binding

Figure 6-1-2 shows the MAC address automatic binding page. This page is used to automatically bind the MAC address to the port.

Displays the existing dynamic MAC address of the port in the Layer 2 hardware forwarding table and the VLAN to which the port belongs. You can select one of the entries and convert it to a static binding.

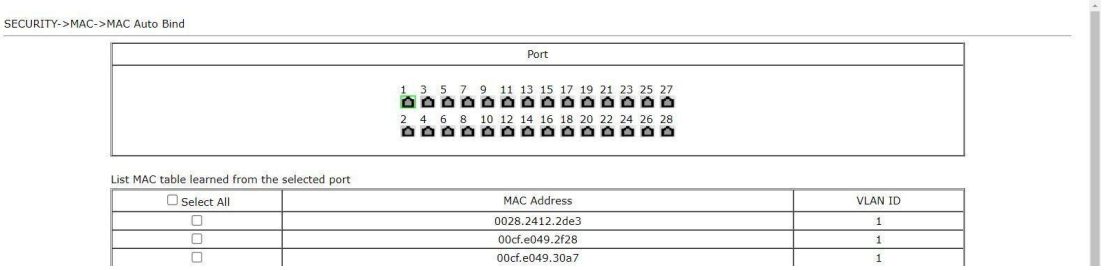


Figure 6-1-2 MAC address automatic binding page

③ MAC address filtering configuration

Figure 6-1-3 shows the MAC address filtering configuration page. This page is used to configure port MAC address filtering.

The MAC entry on the page is used to enter the MAC address for filtering, and the VLAN number entry is used to enter the VLAN to which the MAC address belongs.

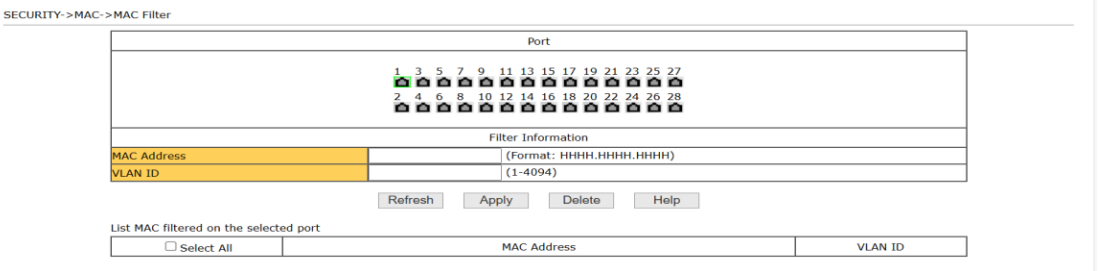


Figure 6-1-3 MAC Address Filtering Configuration

④ MAC address table

Figure 6-1-4 is the MAC address table. This page is used to configure the

MAC display condition of the port.

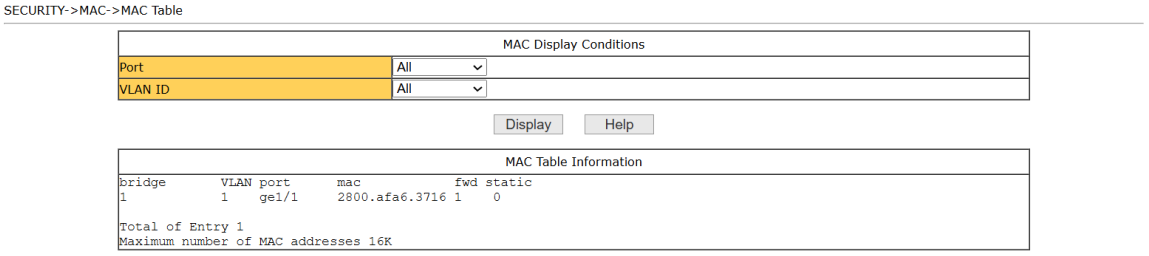


Figure 6-1-4 MAC Address Table

(2) ACL Configuration

① Standard IP group ACL

Figure 6-2-1 is the standard IP group ACL page, through which the user can establish the rule base of ACL standard IP. Users can select an ACL group number (in the range of 1-99, or 1300-1999) to create one or more rules in that group. The only field that can be matched in a rule is the source IP address (with a mask).

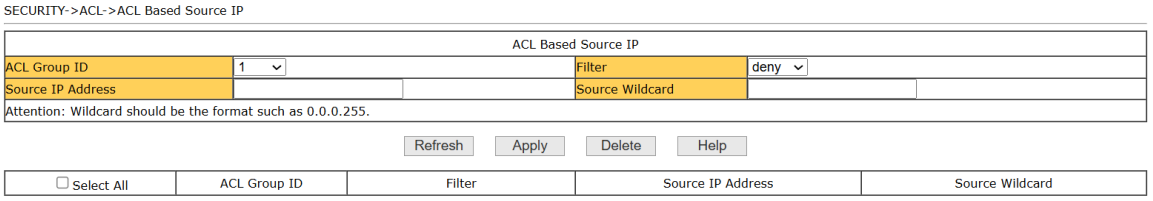


Figure 6-2-1 Standard IP Group ACL Page

When the user configures the rule, the source IP address needs to be masked, and the rule can match the set of IP addresses. The mask of the address is represented by the complement. If the rule is to match the IP address range 192.168.0.0 to 192.168.0.255, the IP address can be 192.168.0.1 and its mask is 255.0.0.0

When the user configures rules, each rule must have a filter mode: Allow or Deny. When a user creates a rule in a rule group, the system will automatically

assign a rule number to the rule. When a rule in a rule group is deleted, other rules remain unchanged, and the system will automatically sort the rules in a rule group. If the user wants to delete the whole rule group, he can select all first, and then click the delete button.

② Extended IP Group ACL

Figure 6-2-2 is the ACL page of the extended IP group, through which the user can establish the rule base of the ACL extended IP. Users can select an ACL group number (in the range of 100-199, or 2000-2699) to create one or more rules in that group. Fields that can be matched in a rule are source IP address (with mask), destination IP address (with mask), protocol type (such as ICMP, TCP, UDP, etc.), source port and destination port (valid only for TCP and UDP protocols), and TCP control flags.

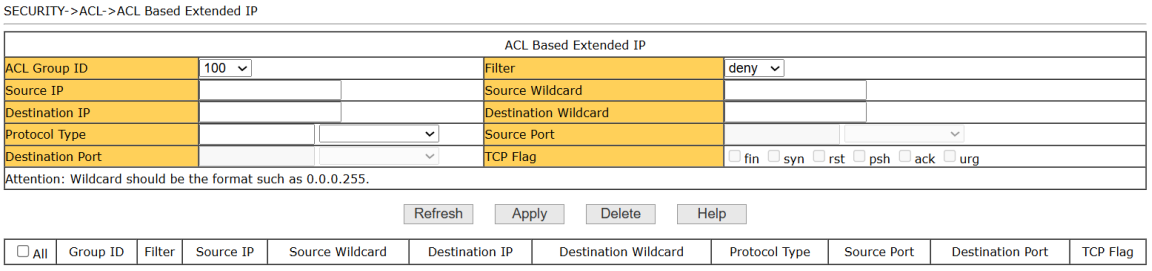


Figure 6-2-2 Extended IP Group ACL Page

When the user configures the rule, the source IP address needs to be masked, and the rule can match the set of IP addresses. The mask of the address is represented by the complement. If the rule is to match the IP address range 192.168.0.0 to 192.168.0.255, the IP address can be 192.168.0.1 and its mask is 0.0. 0.255.

When the user configures rules, each rule must have a filter mode: Allow or Deny. When a user creates a rule in a rule group, the system will automatically assign a rule number to the rule. When a rule in a rule group is deleted, other rules remain unchanged, and the system will automatically sort the rules in

a rule group. If the user wants to delete the whole rule group, he can select all first, and then click the delete button.

③ MAC IP Group ACL Part

Figure 6-2-3 is the MAC IP group ACL page, through which the user can establish the rule base of ACL MAC IP. Users can select an ACL group number (in the range of 700-799) to create one or more rules in that group. The fields that can be matched in a rule are source MAC address (with address match bits), source IP address (with address match bits), and destination IP address (with address match bits).

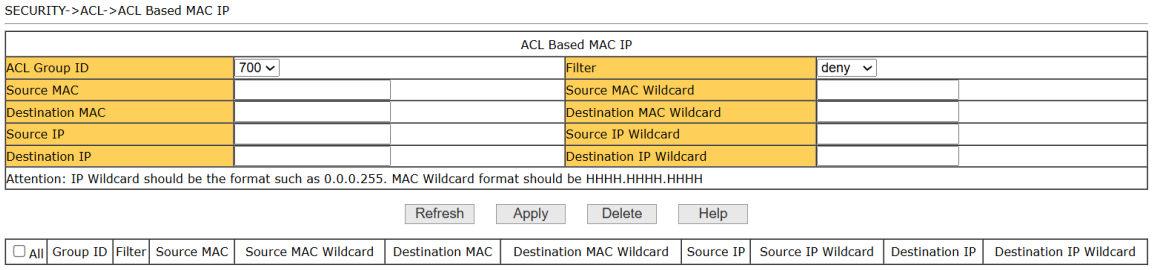


Figure 6-2-3 MAC IP Group ACL Page

When the user configures the rule, the source IP address needs to be masked, and the rule can match the set of IP addresses. The mask of the address is represented by the complement. If the rule is to match the IP address range 192.168.0.0 to 192.168.0.255, the IP address can be 192.168.0.1 and its mask is 0.0.0.255.

When the user configures rules, each rule must have a filter mode: Allow or Deny. When a user creates a rule in a rule group, the system will automatically assign a rule number to the rule. When a rule in a rule group is deleted, other rules remain unchanged, and the system will automatically sort the rules in a rule group. If the user wants to delete the whole rule group, he can select all first, and then click the delete button.

④ MAC ARP Group ACL Part

Figure 6-2-4 is the MAC ARP group ACL page, through which the user can establish the rule base of ACL MAC ARP. Users can select an ACL group number (in the range of 1100-1199) to create one or more rules in that group. The fields that can be matched in a rule are the ARP operation type, the sending MAC address (with address match bits), and the sending IP address (with address match bits).

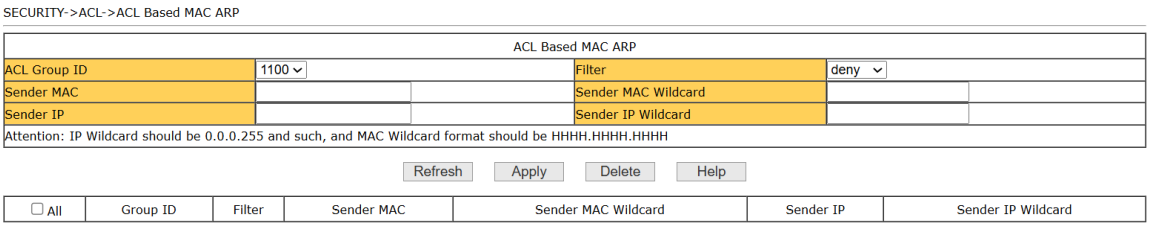


Figure 6-2-4 MAC ARR Group ACL Page

When the user configures the rule, the source IP address needs to be masked, and the rule can match the set of IP addresses. The mask of the address is represented by the complement. If the rule is to match the IP address range 192.168.0.0 to 192.168.0.255, the IP address can be
192.168.0.1 and its mask is 0.0.0.255.

When the user configures rules, each rule must have a filter mode: Allow or Deny.

When a user creates a rule in a rule group, the system will automatically assign a rule number to the rule. When a rule in a rule group is deleted, other rules remain unchanged, and the system will automatically sort the rules in a rule group. If the user wants to delete the whole rule group, he can select all first, and then click the delete button.

⑤ Port Apply ACLs pack

Figure 6-2-5 is the port application ACL page, through which the user can select an ACL group for a port, write the rules in this ACL group into the port hardware logic, and make the port perform ACL filtering on the received packets according to these rules.

When selecting an ACL group on a port, you can select IP Standard, IP Extended, MAC IP, and MAC ARP ACL groups. The selected ACL group must exist. Select from the ACL Rule Group list and press the Add key. To delete an ACL group, select an ACL group from the list of referenced rule groups and press the Delete key.

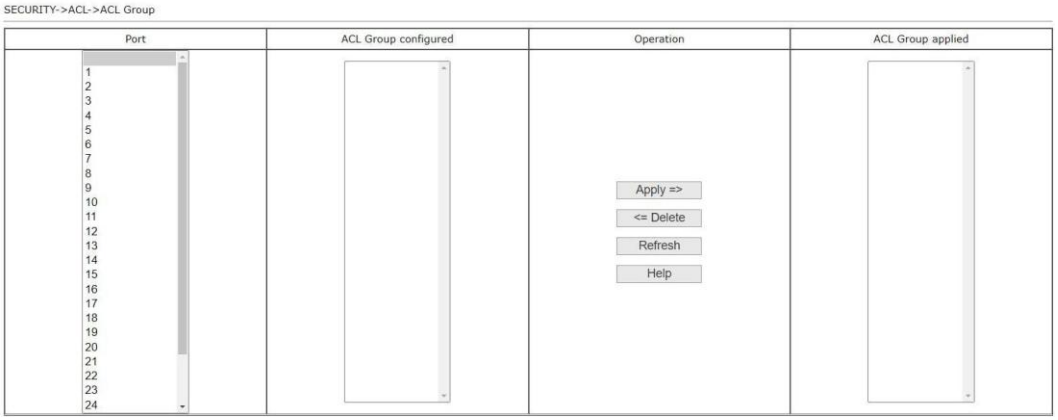


Figure 6-2-5 Port Application ACL Page

⑥ ACL Configuration Information Part

Figure 6-2-6 shows the ACL configuration information page, which displays all the rules and reference information configured in the current ACL.

Figure 6-2-6 ACL Configuration Information Page

(3) AAA Configuration

① AAA Global Configuration Page

Figure 6-3-1 is the AAA global configuration page. The user can configure the

information related to AAA. The information that can be set includes:

- Whether to start the 802.1x protocol, the 802.1x protocol must be started during authentication and accounting.
- Whether to enable the re-authentication function is not enabled by default, and it is determined according to the actual situation when performing authentication billing. Turning on the recertification function will make users more reliable when using authentication billing, but it will slightly increase the traffic of the network.
- Set the time interval for re-authentication, which is valid only when the re-authentication function is enabled. The default value is 3600 seconds. Set the value according to the actual situation when performing authentication billing, but the value should not be too small.
- The IP address of the RADIUS server. This field must be set during authentication and accounting.
- Backup RADIUS server IP address. This field can be set if there is a backup RADIUS server.
- The shared key is used to set the encrypted shared password between the switch and the Radius server. This field must be set during authentication and billing, and must be the same as the setting on the Radius server.
- Whether to start charging, it is started by default. Charging is generally started during authentication and charging.

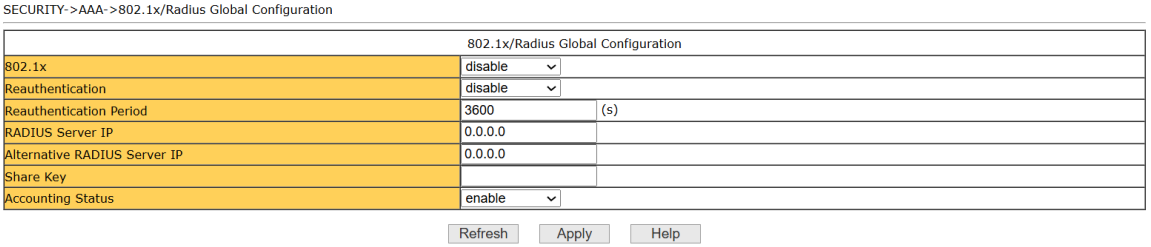
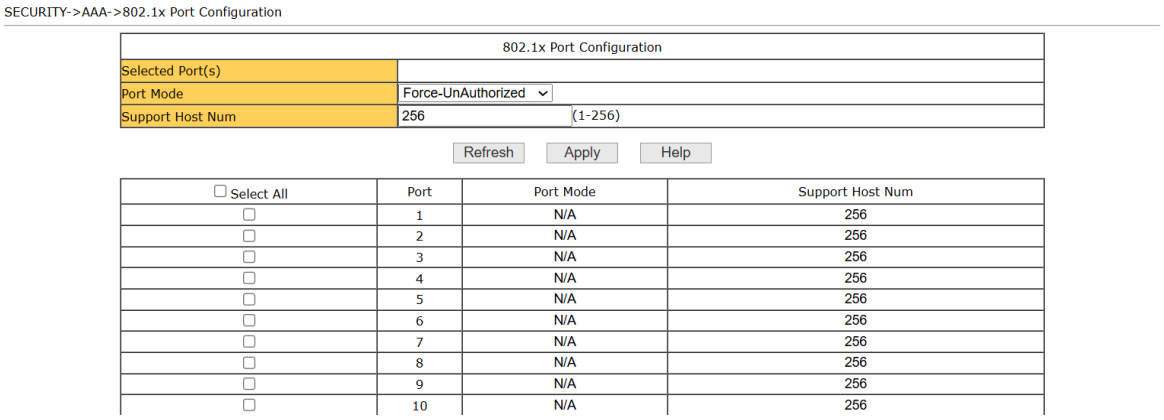


Figure 6-3-1 AAA Global Configuration Page

② AAA Port Configuration Part

Figure 6-3-2 is the AAA port configuration page, through which the user can configure the authentication port mode and the maximum number of hosts

supported, and view the configuration of each port. To modify the port AAA configuration, the user needs to check the left side of the corresponding port, or use the "Select All" function. The selected ports will be displayed at the top of the page, and several consecutive ports are represented by connection numbers. After successful setting, the selected port will be configured with the same parameters. There are four types of AAA port modes: N/A state, Auto state, Force-authorized state, and Force-unauthorized state. When 802.1 authentication is required for a port, the port must be set to the Auto state. If the port is not authenticated, it can access the network. The port must be set to the N/A state. The other two States are rarely used in practical applications.


SECURITY->AAA->802.1x Port Configuration

802.1x Port Configuration

Selected Port(s)	
Port Mode	Force-UnAuthorized
Support Host Num	256 (1-256)

Refresh Apply Help

Select All	Port	Port Mode	Support Host Num
	1	N/A	256
	2	N/A	256
	3	N/A	256
	4	N/A	256
	5	N/A	256
	6	N/A	256
	7	N/A	256
	8	N/A	256
	9	N/A	256
	10	N/A	256

Figure 6-3-2 AAA Port Configuration Page

During 802.1x authentication, the maximum number of hosts accessed by the port is 256 by default. The user can modify this field to support 256 hosts at most.

③)AAA User Information Page

Figure 6-3-3 is the AAA user information page, through which the user can view the status information of all users connected to a port.

SECURITY->AAA->AAA User Information

AAA User Information

User name	MAC Address	Authentication state	Authenticator state	Back-End state	Reauthentication state

Refresh Help

Figure 6-3-3 AAA User Information Page

(4) Native Management Security Configuration

①)Management permission configuration page

Figure 6-4-1 is the management authority configuration page.

Through the configuration of this page, the administrator can control the network management services TELNET, WEB and SNMP, enable or disable these services, and attach these services to the ACL group of IP standard to implement source IP address control. Controls host access to these services.

By default, the TELNET, WEB, and SNMP services of the switch are turned on without ACL filtering, that is, all hosts can access these three services of the switch. If the administrator does not want to provide one or more of these services to other users for the sake of security, one or more of these services can be turned off. If the administrator only wants specific hosts to access one or more of these services, one or more of these services can be filtered by ACL. When a service needs ACL filtering, the service needs to be opened and an ACL group (1-99) of IP standard needs to be selected. At this time, the ACL group must exist.

It should be noted that if the administrator controls the WEB service on this page (such as closing the WEB service), the user may no longer be able to use the WEB page. At this time, the user can log in to the switch in other ways and control the WEB service so that the user can use the WEB page (such as opening the WEB service).

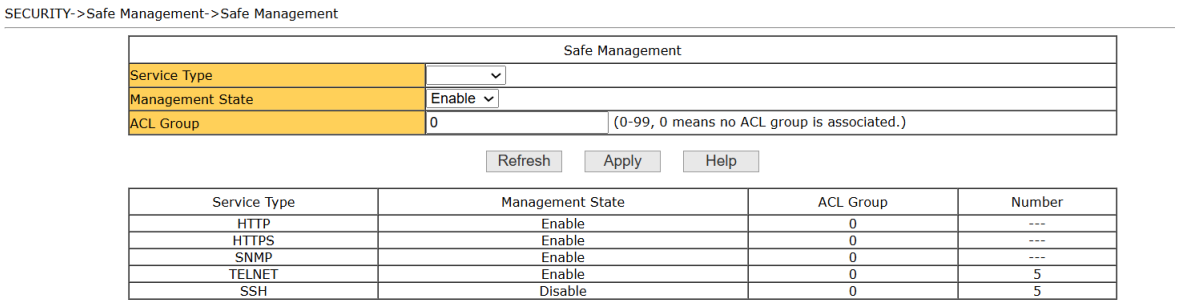


Figure 6-4-1 Management Authority New Configuration Page

7, DHCP Configuration

(1) DHCP client

Figure 7-1 shows the DHCP client configuration. This page is used to configure the DHCP client configuration.

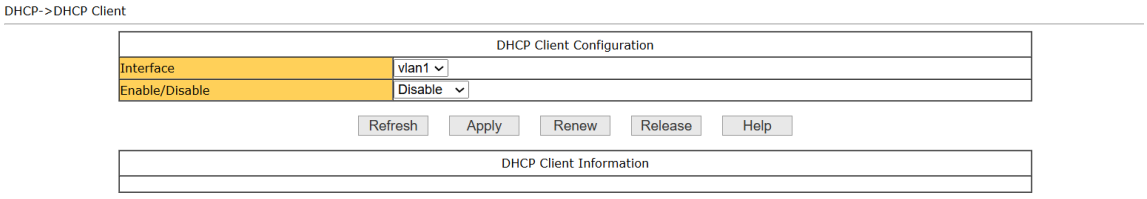


Figure 7-1 DHCP Client Page

(2) DHCP Relay

Figure 7-2 shows the DHCP relay configuration. This page is used to configure the DHCP relay configuration.

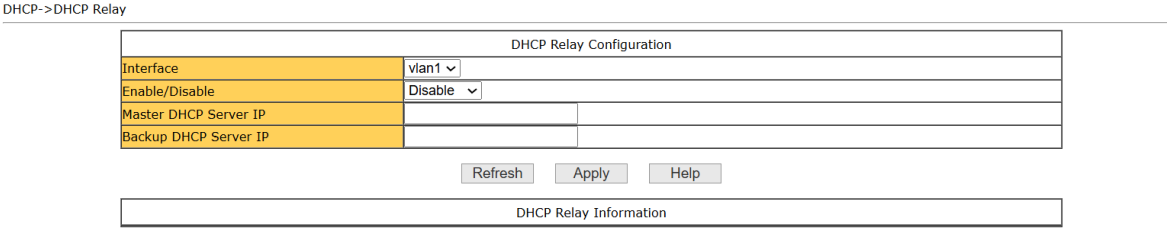


Figure 7-2 DHCP Relay Page

(3) DHCP server

① Global and interface configuration

Figure 7-3-1 shows the DHCP server interface configuration. This page is used to configure the DHCP server interface configuration.

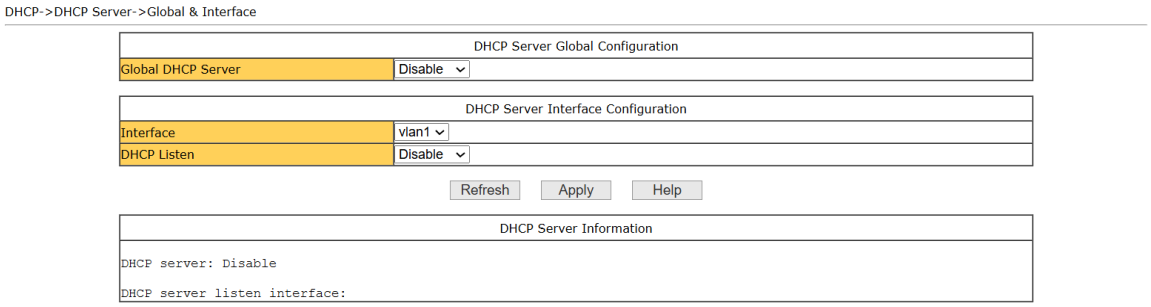


Figure 7-3-1 Global and Interface Configuration Page

② Address Pool Configuration

Figure 7-3-2 shows the DHCP server address pool configuration. This page is used to configure the DHCP server address pool configuration.

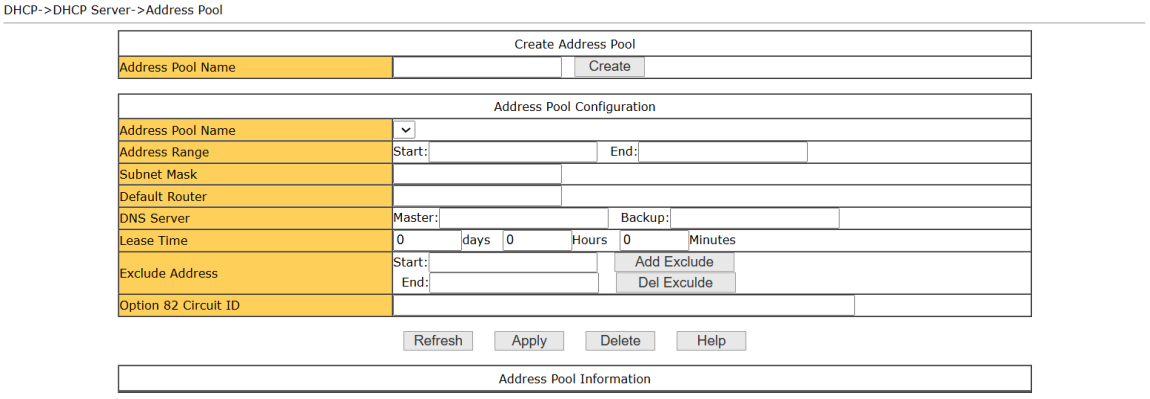


Figure 7-3-2 Address Pool Configuration Page

③ Address Information

Figure 7-3-3 is the DHCP server address information viewing interface. This page is used to view the address information of the DHCP server.

Figure 7-3-3 Address information page

(4) DHCP snooping

① Global Configuration

Figure 7-4-1 is the global DHCP snooping configuration interface, which is used to configure the global DHCP snooping configuration.

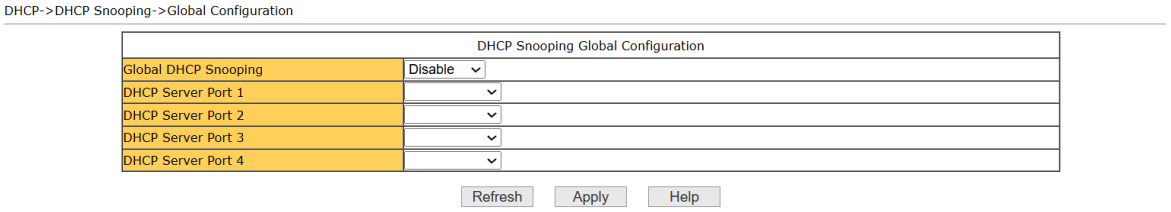


Figure 7-4-1 Global Configuration Page

② Interface configuration

Figure 7-4-2 is the DHCP listening port configuration interface, which is used to configure the DHCP listening interface configuration.

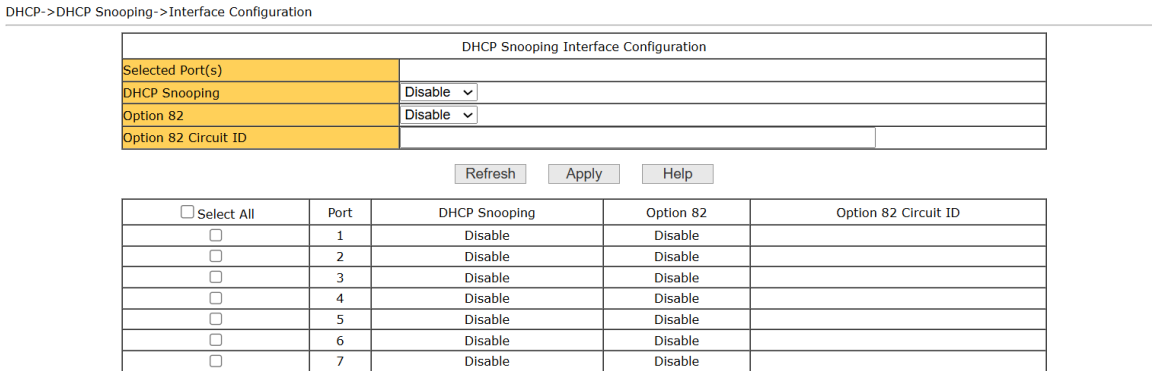


Figure 7-4-2 Interface configuration page

③ Binding Table Information

Figure 7-4-3 is the interface for viewing the address information of the DHCP server. This page is used to view the address information of the DHCP server.

Figure 7-4-3 Binding Table Information Page

8, Multicast configuration

(1) IGMP SNOOPING Configuration

① IGMP SNOOPING Configuration Page

Figure 8-1-1 is the IGMP SNOOPING configuration page. Users can enable IGMP Snooping from this page.

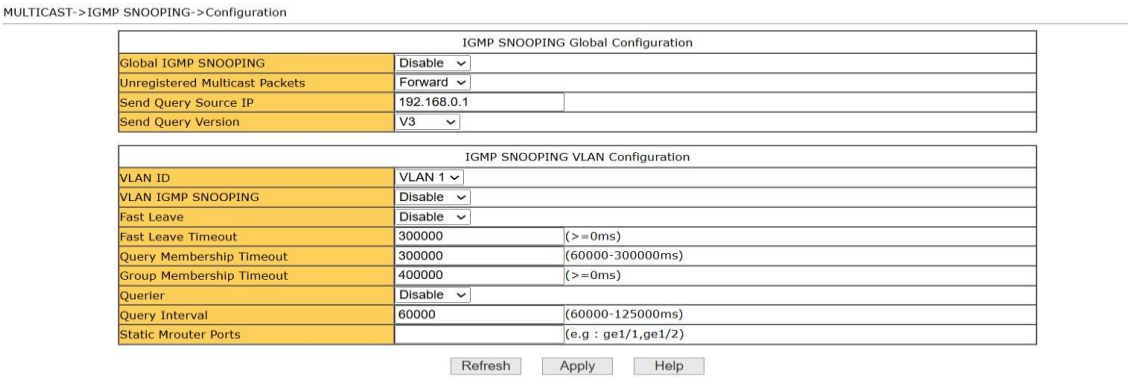


Figure 8-1-1 IGMPSNOOPING Configuration Page

② Multicast group information page

Figure 8-1-2 is the multicast group information page, through which the user can view the IGMP SNOOPING multicast information.

Figure 8-1-2 Multicast Group Information Page

(2) GMRP

① GMRP Global Configuration

Figure 8-2-1 is the GMRP omnipotent configuration interface, which is used to configure the global GMRP.

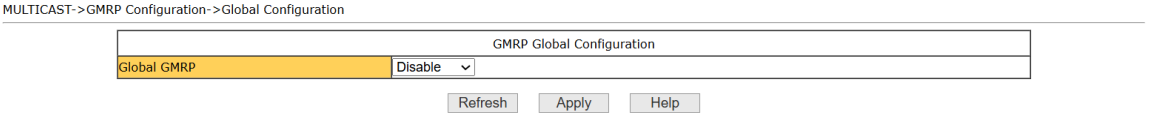
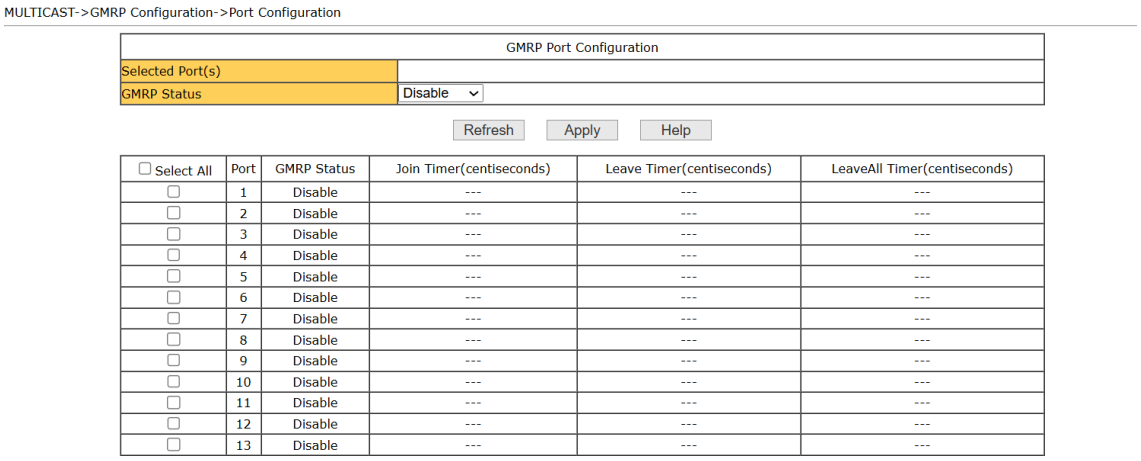


Figure 8-2-1 GMRP Global Configuration Page

② GMRP Port Configuration

Figure 8-2-2 shows the GMRP port configuration interface, which is used to configure the GMRP port status.



MULTICAST->GMRP Configuration->Port Configuration

GMRP Port Configuration

Selected Port(s)	
GMRP Status	Disable

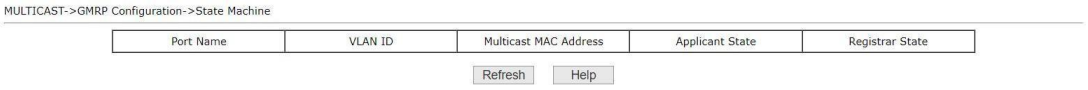
Refresh Apply Help

Select All	Port	GMRP Status	Join Timer(centiseconds)	Leave Timer(centiseconds)	LeaveAll Timer(centiseconds)
	1	Disable	---	---	---
	2	Disable	---	---	---
	3	Disable	---	---	---
	4	Disable	---	---	---
	5	Disable	---	---	---
	6	Disable	---	---	---
	7	Disable	---	---	---
	8	Disable	---	---	---
	9	Disable	---	---	---
	10	Disable	---	---	---
	11	Disable	---	---	---
	12	Disable	---	---	---
	13	Disable	---	---	---

Figure 8-2-2 GMRP Port Configuration

③ GMRP state machine

Figure 8-2-3 is the GMRP state machine viewing interface. This page is used to view the status of the GMRP state machine for the GMRP configuration



MULTICAST->GMRP Configuration->State Machine

Port Name	VLAN ID	Multicast MAC Address	Applicant State	Registrar State

Refresh Help

Figure 8-2-3 GMRP State Machine

(3) Multicast routing configuration

Figure 8-3-1 shows the multicast routing configuration. This page is used to configure the multicast routing switch.

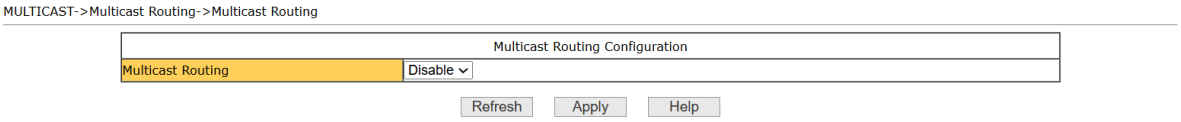


Figure 8-3-1 Multicast Routing Configuration Page

② Multicast routing table

Figure 8-3-2 is the multicast routing table viewing interface. This page is used to view the multicast routing table of the multicast routing configuration.

Figure 8-3-2 Multicast Routing Table Page

(4) IGMP configuration

① IGMP configuration

Figure 8-4-1 is the IGMP port configuration interface, which is used to configure the IGMP switch parameters.

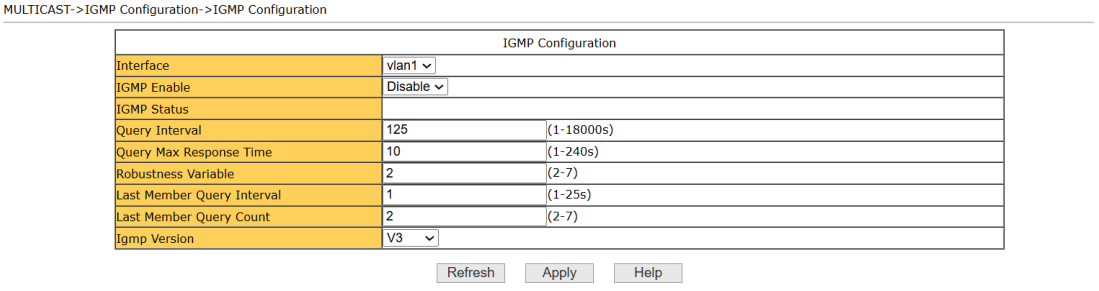


Figure 8-4-1 IGMP Configuration Page

① IGMP Interface Information

Figure 8-4-2 is the IGMP interface information viewing interface. This page is used to view the IGMP interface information for the IGMP configuration.

Figure 8-4-2 IGMP Interface Information Page

② Figure 8-4-3 is the IGMP group information viewing interface. This page is used to view IGMP group information for the IGMP configuration.

Figure 8-4-3 IGMP Group Information Page

(5) PIM-SM Configuration

① Global Configuration

Figure 8-5-1 shows the PIM-SM global configuration interface, which is used to configure the global PIM-SM parameters.

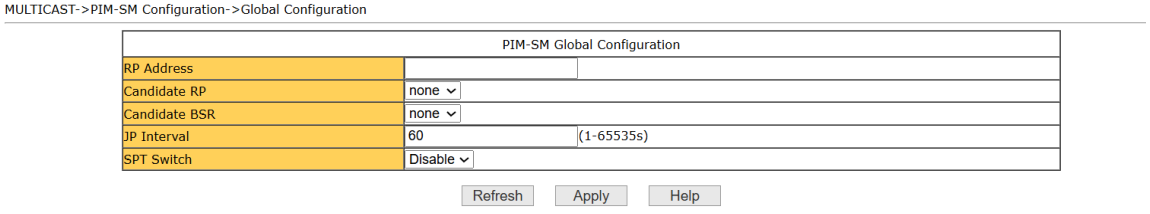


Figure 8-5-1 Global Configuration Page

② Interface configuration

Figure 8-5-2 is the PIM-SM interface configuration interface, which is used to configure PIM-SM interface parameters.

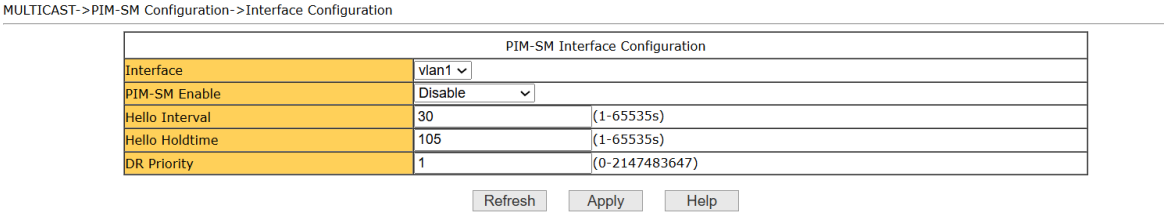


Figure 8-5-2 Interface Configuration Page

③ Multicast routing information

Figure 8-5-3 is the multicast routing information viewing interface. This page is used to view the multicast routing information configured by PIM-SM.

Figure 8-5-3 Multicast routing information

④ Interface information

Figure 8-5-4 is the interface for viewing interface information. This page is used to view the interface information configured by PIM-SM.

Figure 8-5-4 Interface information page

⑤ Neighbor information

Figure 8-5-5 is the neighbor information viewing interface. This page is used to view the neighbor information configured by PIM-SM.

Figure 8-5-5 Neighbor Information Page

⑥ RP information

Figure 8-5-6 shows the RP information viewing interface. This page is used to view the RP information for the PIM-SM configuration.

Figure 8-5-6 RP information page

⑦ BSR information

Figure 8-5-7 is the BSR information viewing interface. This page is used to view the BSR information for the PIM-SM configuration.

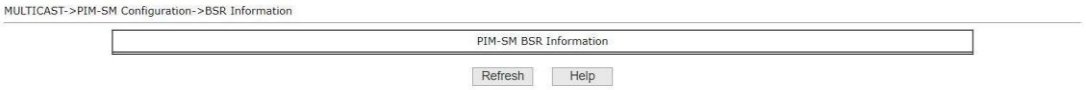


Figure 8-5-7 BSR Information Page

9, Ring Network Configuration

(1) Spanning Tree Configuration

① Spanning Tree Global Configuration

Figure 9-1-1 shows the global configuration page of spanning tree, through which the user can configure global spanning tree parameters.

RING->MSTP->Global Configuration

Global Configuration		
MSTP	disable	
Priority	32768	(0-61440, must be an interger multiple of 4096)
Forward-Time	15	(4-30, meet 2*(Forward-Time - 1) >= Max-Age)
Hello-Time	2	(1-10, meet 2*(Hello-Time + 1) <= Max-Age)
Max-Age	20	(6-40)
Max-Hops	20	(1-40)

Refresh Apply Help

Figure 9-1-1 Spanning Tree Global Configuration Page

② Spanning Tree Port Configuration

Figure 9-1-2 is the Spanning Tree Port Configuration page, through which the user can view the specific status of the port MSTP.

RING->MSTP->Port Configuration

Port Configuration	
Selected Port(s)	
Port Priority	
Path-Cost	
Force-Version	STP
Portfast	disable

Refresh Apply Help

All	Item	Port	Priority	Path-Cost	Force-Version	Portfast	STP State
	1	1	128	20000	MSTP	disable	Forwarding
	2	2	128	20000000	MSTP	disable	Blocked
	3	3	128	20000000	MSTP	disable	Blocked
	4	4	128	20000000	MSTP	disable	Blocked
	5	5	128	20000000	MSTP	disable	Blocked
	6	6	128	20000000	MSTP	disable	Blocked

Figure 9-1-2 Spanning Tree Port Configuration Page

(2) ERPS Configuration

① ERPS Predefined Configuration

Figure 9-2-1 is the ERPS Predefined Configuration page, which enables

the ERPS Predefined Configuration. When you enable the ERPS predefined configuration, you can specify the node type: Primary or Transport.

Specific predefined configuration: ERPS instance number is 1, ERPS change number is 1, ring mode is main ring mode, protocol VLAN is VLAN3001, data VLAN is VLAN1, RPL port is 51, RL port is 52, recovery

behavior is recoverable, hold-off time is 0, guard time is 500 ms, The WTR time is 5 minutes, the WTB time is 5 seconds, and the protocol message sending time is 5 seconds.

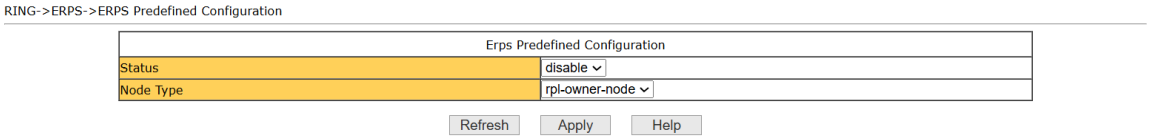


Figure 9-2-1 ERPS Predefined Configuration Page

② ERPS Instance Configuration

Figure 9-2-2 shows the ERPS instance configuration page, through which the ERPS instance can be configured. When an instance is not created, click Apply to create and assign a role. When an instance is created but not associated with a ring, you can modify the role. If an instance is created and associated with a ring, you cannot modify the instance. Click Delete to delete the selected instance. You can configure up to 8 instances.

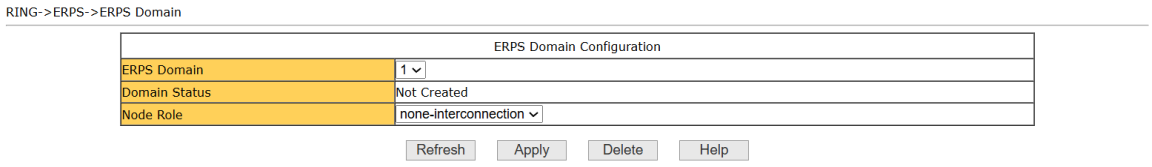


Figure 9-2-2 ERPS Instance Configuration Page

③ ERPS Ring Configuration

Figure 9-2-3 is the ERPS Ring Configuration page, which allows you to create and configure an ERPS ring. Select a ring. Click the Apply button to create the ring and set the configuration information when the ring is not created. If the ring is created, the configuration information

can be modified. Click the Delete button to delete the selected ring. A ring must and can only be associated to one instance. A maximum of 32 rings can be configured. When a ring fault is detected, click the Manual Recovery button to recover.

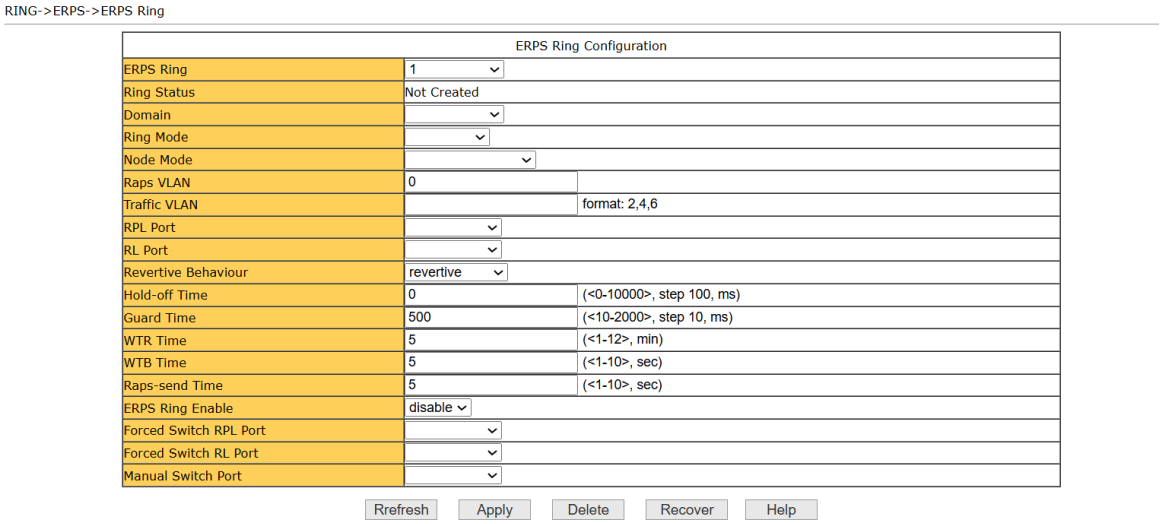


Figure 9-2-3 ERPS Ring Configuration Page

④ ERPS Information

Figure 9-2-4 is the ERPS information page. Select the ring number to display the configuration and status information of the relevant ERPS ring.

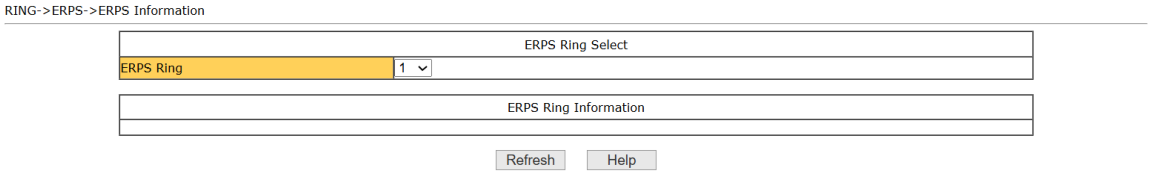


Figure 9-2-4 ERPS Information Page

(3) EAPS Configuration

① EAPS Ring Configuration

Figure 9-3-1 This page is used to create and configure EAPS information, and also to delete and display EAPS information.

EAPS ring number: specific ring number, value range 1-16, can be

selected according to the drop-down box

Creation status: Not Created and Created. In case of no creation, it is necessary to create first

Modes: Master and Transit, which can be configured according to specific needs.

Main port: EAPS main port, such as fe1/1, ge1/1

Alternate port: EAPS 2nd port

Control VLAN: control VLAN of EAPS ring, value 2-4094

Protected VLAN: EAPS ring protected VLAN

Hello Interval The interval at which Hello messages are sent. The default is 1s

Fail time: the time to detect the fault, which is 3s by default

In the case of data trans-ring forwarding and multi-ring forwarding, this Function shall be enabled when the data needs to be trans-ring forwarded. Not turned on by default Extreme Interoperability Compatibility with other network devices, on by default

Enable status, last EAPS ring enable condition

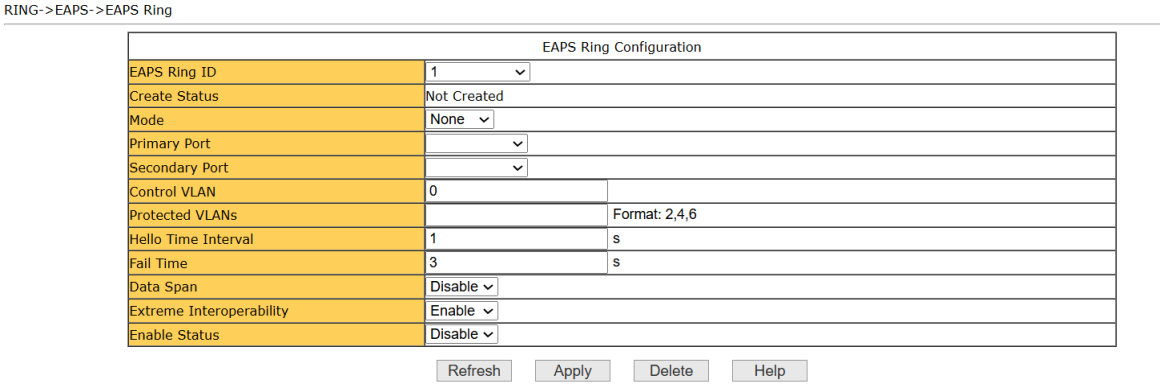


Figure 9-3-1 EAPS Ring Configuration Page

② EAPS Information

Figure 9-3-2 is the EAPS information page, through which the user can view the EAPS configuration information.

RING->EAPS->EAPS Information

Figure 9-3-2 EAPS Information Page

10, Advanced Configuration

(1) QoS Configuration

① QoS application configuration

Figure 10-1-1 is the QoS application page, through which the user can configure the QoS type of the port and modify the default user priority. The list shows the port's QoS type and user default priority in real time.

ADVANCED->QoS Configuration->QoS Apply

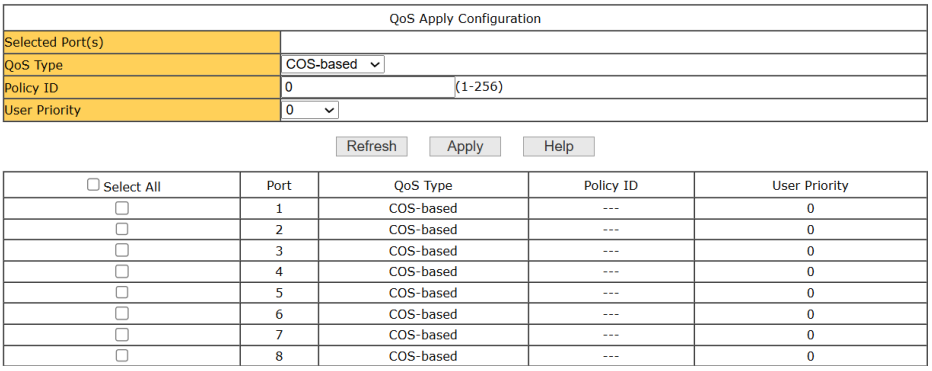


Figure 10-1-1 QoS Application Configuration Page

QoS scheduling configuration

Figure 10-1-2 is the QoS scheduling page, through which the user can configures the QoS scheduling mode of the port and modify the priority of the queue. The list displays the scheduling mode of the port and the weight value of each queue in real time.

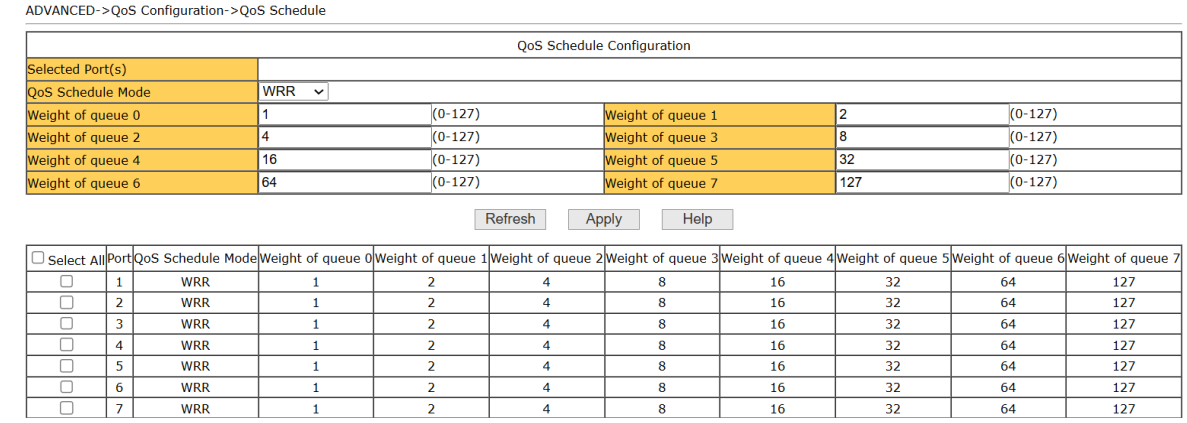


Figure 10-1-2 QoS Scheduling Configuration Page

(2) LLDP configuration

① LLDP Global Configuration

Figure 10-2-1 shows the LLDP global configuration interface, which is used to display and configure global LLDP parameters.

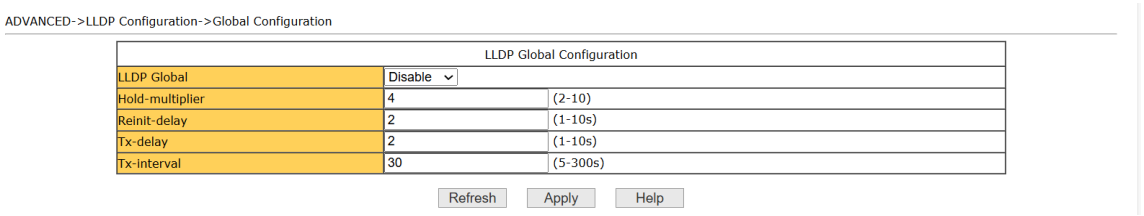


Figure 10-2-1 LLDP Global Configuration

② LLDP Port Configuration

Figure 10-2-2 shows the LLDP port configuration interface, which is used to display and configure LLDP port parameters.

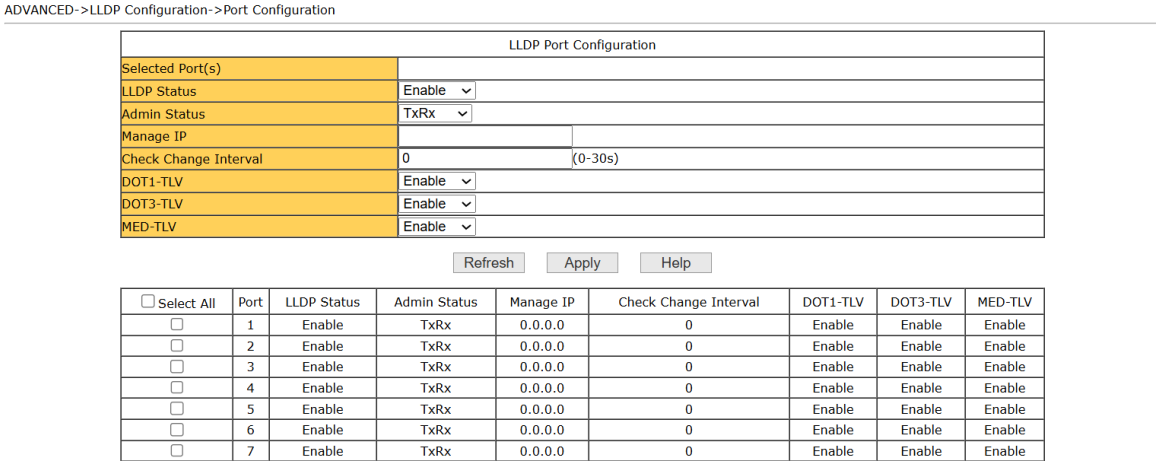


Figure 10-2-2 LDP Port Configuration

③ LLDP Neighbor Table

Figure 10-2-3 shows the LLDP neighbor table viewing interface. This page is used to view the LLDP neighbor table information for the LLDP configuration.

Figure 10-2-3 LLDP Neighbor Table

11, System Tools

(1) Save Configuration

Figure 11-1 is the Save Configuration page. This page allows the user to view the current configuration of the switch. The Save button is used to save

the current configuration of the system to the configuration file. Because the storage operation needs to erase the FLASH chip, which takes a certain amount of time. When the user has made the configuration on the page and

wants to restart the switch without losing the configuration, he must click the Save button on the current configuration page before exiting the page.

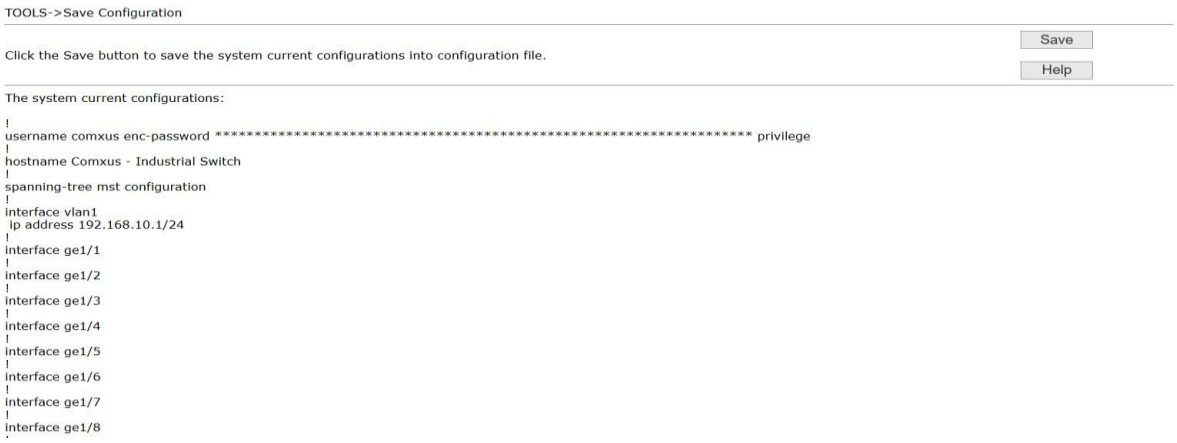


Figure 11-1 Save Configuration Page

(2) Backup configuration films

Figure 11-2 is the Backup Profile page. This page allows the user to view the initial configuration of the system. The initial configuration is actually the configuration file in FLASH. When there is no configuration file in FLASH, the default configuration is used when the system is started. Click the Backup button, a dialog box will pop up, and the user can select the directory path and save the configuration file. The filename of the downloaded configuration file defaults to the switch. CFG.

Figure 11-2 Backup Profile Page

(3) Restore Configuration File

Figure 11-3 shows the Restore Configuration File page, which allows the user to upload a configuration file to the switch. Click the Browse button to select the directory path of the uploaded configuration file on the PC. Click the Upload button to upload the configuration file. The suffix of the configuration file must be *.cfg. Please do not click other pages or restart the switch before

returning to the transfer result page; otherwise, the file transfer will fail and the system will crash.

Figure 11-3 Restore Profile Page

(4) Software upgrade

Figure 11-4 shows the Software Upgrade page, which allows users to upload image files to the switch. Click the Browse button to select the directory path of the uploaded image file on the PC. Click the Upload button to upload the image file, which must be provided by the manufacturer and the file name suffix must be *.img. Please do not click other pages or restart the switch before returning to the transfer result page; otherwise, the file transfer will fail and the system will crash.

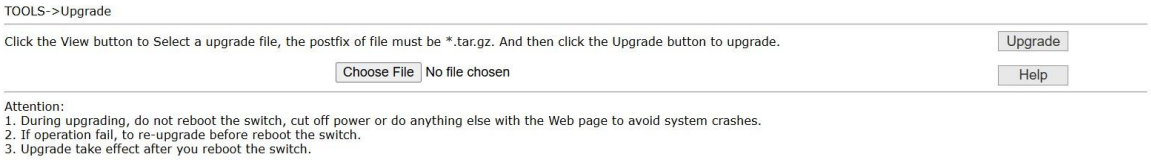
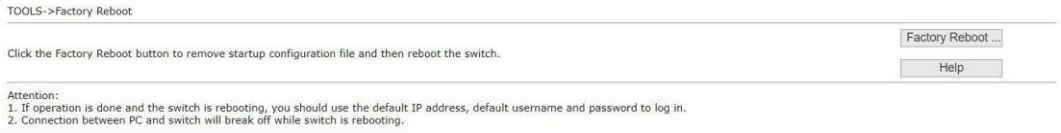


Figure 11-4 Software Upgrade Page

(5) Restore Factory Configuration

Figure 11-5 shows the Restore Factory Configuration page. This page allows the user to delete the configuration file in FLASH to return to the factory configuration. Click the Restore Factory Configuration button, and a dialog box will pop up to prompt the user whether to confirm. After the factory configuration



is restored, the switch will automatically restart to make the factory configuration take effect. Please use the factory default IP address and password when logging in next time.

Figure 11-5 Restore Factory Configuration Page

(6) Restart

Figure 11-6 shows the restart page through which the user restarts the switch. When the Restart button is clicked, a dialog box will pop up to prompt the user whether to restart the switch. If yes, press the OK button, otherwise press the Cancel button. Web pages will no longer open when you restart.

Figure 11-6 Restart Page

12, PoE Configuration

(1) PoE Port Configuration

Figure 12-1 is the PoE port configuration page, through which you can con figure the total power of the PoE device (to be updated by the system), PoE single-port power (to be updated by the system), and PoE on or off; through this page, you can view the relevant information of the current PoE device.

PoE port: Select the power supply port number (1-

24) PoE port status: enable or disable

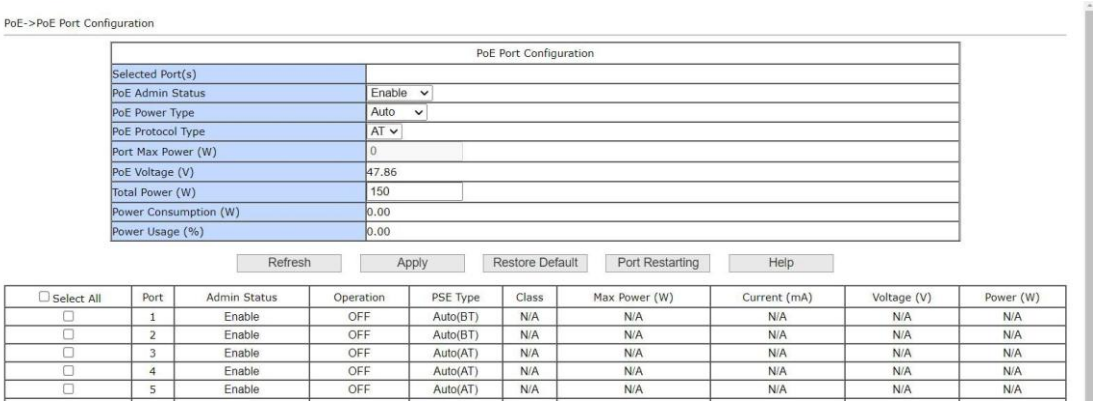


Figure 12-1 PoE Port Configuration Page

(2) PoE scheduling configuration

Figure 12-2 is the PoE scheduling configuration page. Through the

scheduling management, the PoE power supply can be turned on or off according to the actual needs. The control mode is hour + week.

Control Port: Used to select the port (1-24) to be scheduled for management

Control function: enable or disable

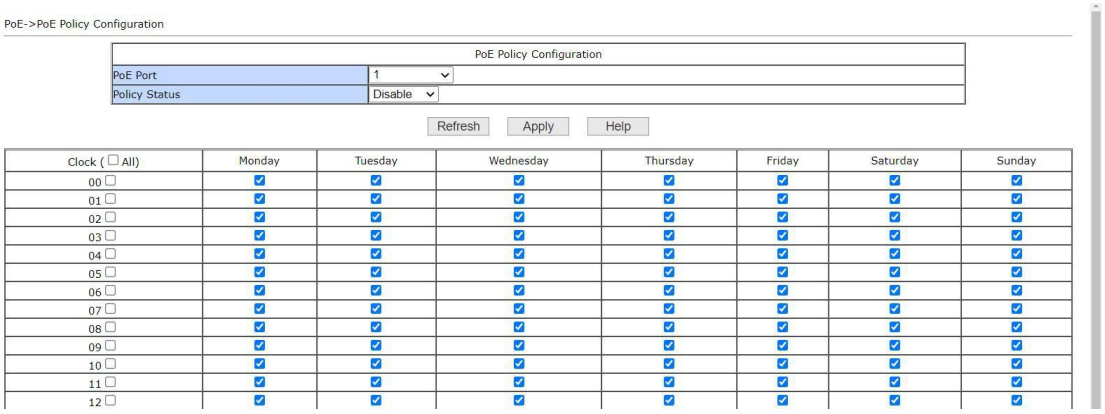


Figure 12-2 PoE Schedule Configuration Page

(3) PD Query Configuration

Figure 12-3 shows the PD query configuration page, through which the PD online device status detection can be realized.

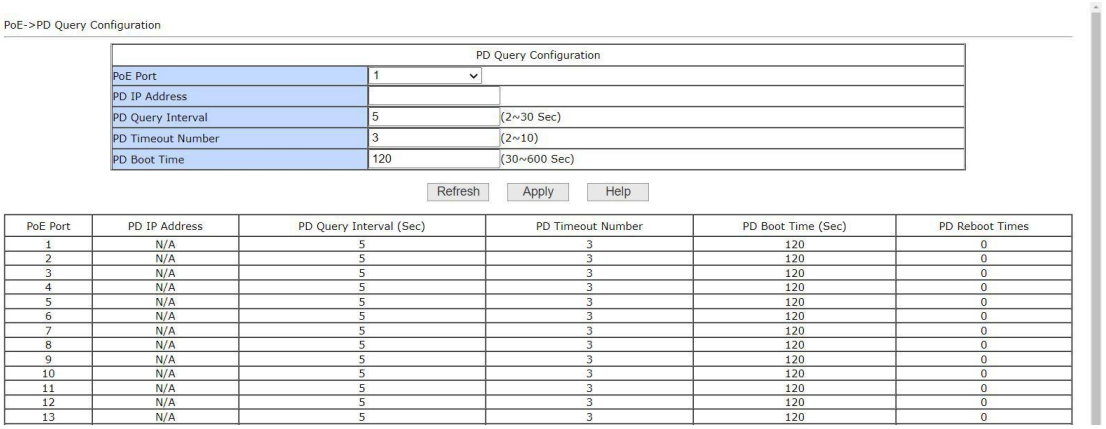
PoE Port: used to select the port connected to the PD device to be queried

PD IP address: IP address of the PD device.

PD query interval: the time interval for querying PD devices (5 seconds by default).

Maximum times of PD query without response: used to query the maximum times of PD device without response (3 times by default)

Maximum time required for PD startup: used to query the maximum time required for PD device startup (default 120 seconds)



PoE->PD Query Configuration

PD Query Configuration

PoE Port	1	
PD IP Address		
PD Query Interval	5	(2~30 Sec)
PD Timeout Number	3	(2~10)
PD Boot Time	120	(30~600 Sec)

Refresh Apply Help

PoE Port	PD IP Address	PD Query Interval (Sec)	PD Timeout Number	PD Boot Time (Sec)	PD Reboot Times
1	N/A	5	3	120	0
2	N/A	5	3	120	0
3	N/A	5	3	120	0
4	N/A	5	3	120	0
5	N/A	5	3	120	0
6	N/A	5	3	120	0
7	N/A	5	3	120	0
8	N/A	5	3	120	0
9	N/A	5	3	120	0
10	N/A	5	3	120	0
11	N/A	5	3	120	0
12	N/A	5	3	120	0
13	N/A	5	3	120	0

Figure 12-3 PD Query Configuration Page