All Gigabit Managed Ethernet Switch

WEB Network Management Operation Guide

Ver 6.7.3

COMXUS A Brand of Willstrong Solutions Pvt Ltd
Head Office- I-128, UPSIDC Site-C, Industrial Area,
Surajpur, Greater Noida, (U.P.) 201307
E-mail: info@comxus.com

Declaration

All rights reserved.

The copyright of this manual belongs to Comxus. 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.

Preface

This manual mainly describes the WEB page of the all-gigabit managed ethernet switch. Users can manage the switch through the WEB page of the all-gigabit managed Ethernet switch. 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 of the all-gigabit managed Ethernet switch.

The preamble contains the following

- Audience Object
- Product Introduction
- Product function

Audience Object

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

Product Introduction

The all-gigabit managed Ethernet switch is independently designed and developed by COMXUS, which is specially designed for building a high-security and high-performance network. The system adopts a brand-new software and hardware platform, provides a comprehensive security protection system, a perfect QoS strategy and rich VLAN functions, is simple in management and maintenance, and is an ideal convergence layer switch for an office network, a campus network, a small and medium-sized enterprise and a branch office.

Product Features

- Supports IEEE 802.3x
- Supports IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3 Z
- Supports IEEE 802.3ad
- Supports IEEE 802.1Q, IEEE 802.1Q/p
- Supports IEEE 802.1w, IEEE 802.1d, EEE 802.1S
- Support MAC address table, automatic update, two-way learning
- Supports port-based VLANs up to 4096 VLAN
- Supports 802.1Q standard VLAN
- Support STP Spanning Tree Protocol
- Support for RSTP Rapid Spanning Tree Protocol
- Supports MSTP Rapid Spanning Tree Protocol
- Support ERPS ring network protocol
- Support EAPS ring network protocol
- Support 802.1x authentication protocol
- Support 8 groups of aggregation, with each group supporting up to 8 ports
- Port mirroring supporting bidirectional transmission and reception

- Support loop protection function, real-time detection, rapid alarm, accurate positioning, intelligent blocking, automatic recovery
- Support the isolation of downlink ports from each other and communicate with the uplink port at the same time
- Supports half-duplex backpressure-based control
- Supports full-duplex PAUSE-based frame
- Supports port-based I/O bandwidth management
- Support for IGMPv1/2/3 and MLDv1/2 Snooping
- Support GMRP agreement registration
- Support multicast address management, multicast VLAN, multicast routing port and static multicast address
- Supports DHCP Snooping
- Support storm suppression of unknown unicast, multicast, unknown multicast, broadcast type
- Supports storm suppression based on bandwidth throttling, storm filtering
- Support user port + IP address + MAC address
- Supports IP, MAC-based ACL
- Support the security nature of the number of MAC addresses based on the port
- Supports 802.1 p-port queue priority algorithm
- Support Cos/Tos, QOS marking
- Support WRR (Weighted Round Robin), weighted priority rotation algorithm
- WRR, SP and WFQ priority scheduling modes are supported
- Support Auto-MDIX function, automatically identify straight-through network cable and crossover network cable
- Support port supports auto-negotiation function (auto-negotiation transmission rate and duplex mode)

- Updating package upload is supported
- Support system log viewing
- Support WEB to restore the factory configuration
- Support for opening or closing ports
- Support standard POE scheduling management
- Support the function of automatic detection of online equipment (automatic, no operation required)
- Support WEB interface management
- Support for Telnet, Console based CLI management
- Support SNMP V1/V2/V3 management
- Support SSHV1/V2 management
- Support RMON management

[Version Update]

Ver 6.7.3

User experience optimization

Resolves known issues and provides faster response.

Related functions are optimized to make management easier.

Directory

Table of Contents

— Overview of WEB pages....10

1. Characteristics of WEB access....10
2. System requirements for WEB browsing: 10
3. Login for WEB browsing session 11
4. Basic composition of WEB page....12
5. Navigation Tree Structure 13
6. Introduction to Page Button 14
7. Error Message....15
8. Entry Field 15
9. State Field 16

WEB Page Introduction 17

1. Login Dialog 17
2. Main Page 18
3. System configuration 18

(1)Basic Information 18

(1) Serial information 20

(2) User Management....20

(3)

(4) SNTP configuration 22

(5) Jumbo Frame Configuration....23

(6) Save Current configuration....23

(7) Configuration file 24

(8) File upload 24

(9) System Reboot....25

4. Port configuration 26

(1) Common configuration 26

(2) Port Statistics 26

(3) Flow Control 27
(4) Broadcast Storm....28
(5) Port rate limit 28
(6) Protection Port 29
(7) Learn limit 30
(8) Prot Trunking 30
(1) Mirror....32
(2) DDM information 33
5. MAC Configuration 33
(1) MAC table 33
(2) MAC Binding 34
(3) MAC auto binding....34
(4) MAC Filter 35
(5) MAC auto filter 35
6. VLAN Configuration....36
(1) VLAN information 36
(2) VLAN Configuration....36
(3) VLAN Port Configuration 37
7. SNMP Configuration....39
(1) Community Name 39
(2) TRAP Target 39
8. ACL Configuration 40
(1) Standard IP 40
(2) Extended IP....41
(3) MAC IP 42
(4) MAC ARP....43
(5) ACL Information 44
(6) ACL Reference....44
9. Qos configuration 45
(1) Qos apply....45
(2) Qos Schedule....45

10. IP Basic Configuration 46
(1) VLAN interface 46
(2) ARP configuration and display 47
(3) Host static route configuration 48
11. AAA Configuration 48
(1) AAA Authentication 48
(2) Tacacs + Configuration 49
(3) Radius Configuration 49
(4) 802.1x configuration 50
(5) 802.1x Port Configuration 52
(6) 802.1x user authentication information 53
12. MSTP configuration 53
(1) Global Configuration 53
(2) Port configuration 53
(3) Port information 54
13. IGMPSNOOPING configuration 54
(1) IGMP SNOOPING Configuration 54
(2) Multicast group information 55
14. GMRP Configuration 55
(1) GMRP Global Configuration 55
(2) GMRP Ports Configuration 56
(3) GMRP State Machine 56
15. CVRP Configuration 57
(1) GVRP Global Configuration 57
(2) GVRP Ports Configuration 57
(3) GVRP state machine 57
16. EAPS Configuration 58
(1) EAPS Configuration 58
(2) EAPS Information 59
17. RMON Configuration 59

(1) Statistics Configuration....59
(2) History Configuration....60
(3) Alarm Configuration....61
(4) Event Configuration....61
18. Cluster Management....62
(1) NDP configuration....62
(2) NTDP Configuration....**Error! Bookmark not defined.**
(3) Cluster configuration....64
19. ERPS Configuration....65
(1) ERPS Configuration....65
(2) ERPS Information....67
20. LLDP Configuration....67
(1) LLDP global configuration....67
(2) LLDP Ports Configuration....67
(3) LLDP Neighbor....68
21. Log Management....68
(1) Log Configuration....68
(2) Log Information....69
22. POE Port Configuration....69
(1) POE Port Configuration....69
(2) POE Policy Configuration....70
(3) PD Query Configuration....71

— Overview of WEB pages

1. Characteristics of WEB access

The all-gigabit managed Ethernet switch provides Web access for users. 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 Netscape Communicator and Microsoft Internet Explorer to access the WEB page of the all-gigabit managed Ethernet switch, and the WEB page is presented to users in a graphical and tabular form.
- The all COMXUS switch provides rich WEB pages, through which users 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 586 or above
Memory	128MB or more
Resolution	Above 800 × 600

color	More than 256 colors
Browser	IE 4.0 or above or Netscape 4.01 or above
Operating system	Microsoft® ,Windows95®,Windows98®,WindowsNT®, Windows2000®,WindowsXP®,WindowsME®, Windows Vista®, Windows7®, Windows8®, Windows10® Windows11®, MAC, Linux, Unix-like operating system

notice：

Microsoft®, Windows95®, Windows98®, WindowsNT®, Windows2000®, Windows XP ®, Windows ME®, Windows Vista®, Windows7®, Windows8®, Windows10®, Windows11® is a registered trademark of Microsoft Corporation. All other product names, trademarks, registered trademarks, and service marks are copyrighted by their respective owners.

3. Login for 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 VLAN1 on the switch is 192.168.0.5
- The subnet mask is 255.255.255.0
- A host with a Web browser has been connected to the network and is able to ping to 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. When the multiuser management is not enabled, the user needs to verify the password of the anonymous user (comxus) when logging in the Web. Only by entering the correct password can the user access the Web. The default password of the anonymous user is comxus.

If the system enables multi-user management and configures privileged users, the anonymous user password will not take effect. Users accessing the Web will not verify the anonymous user password, but verify the user name and password of multi-user management.

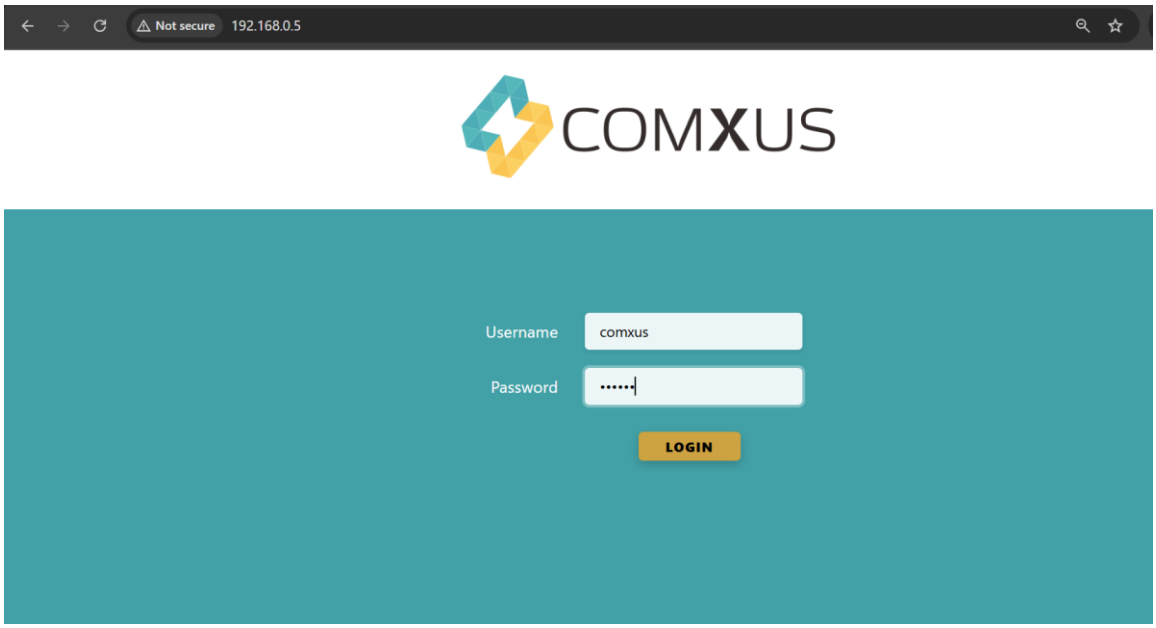


Figure 1 Login page for WEB browsing session

4. Basic composition of WEB page

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

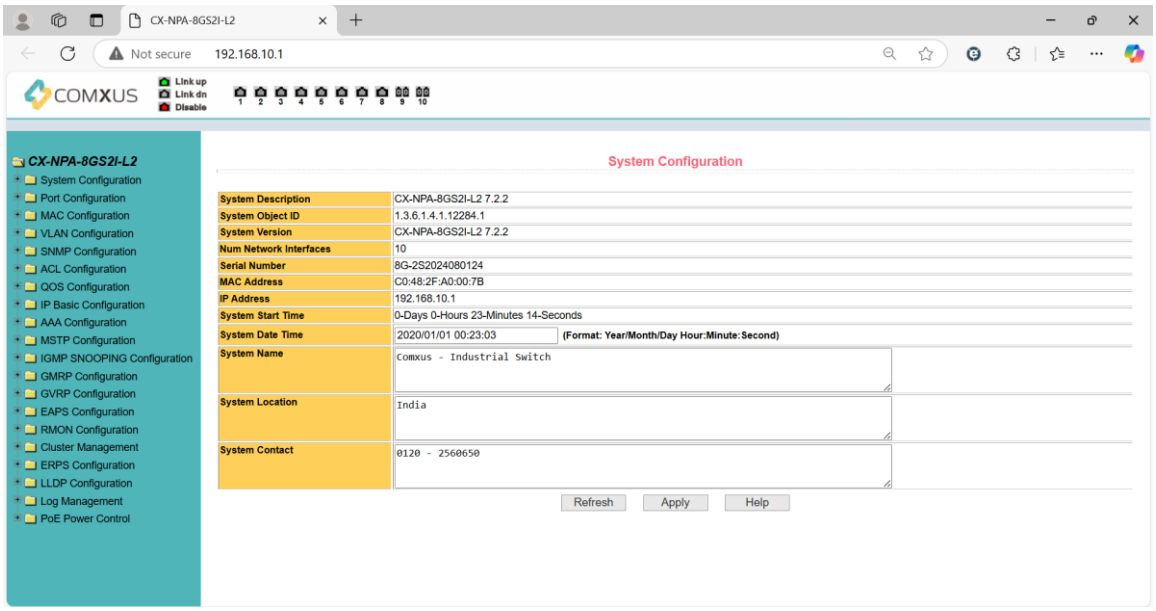


Figure 2　Basic composition page of switch WEB page

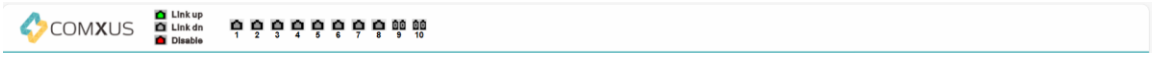
Title Page

It is used to display the logo and the real-time port status, as shown in the foll owing figure

A green light indicates that the port is connected;

A gray light indicates that the port is not connected;

Red light indicates that the port is closed (refer to the port configuration for specific settings)



Main Page　Displays the page that the user selects from the navigation tree.

5. Navigation Tree Structure

Figure 3 shows the organization of the navigation tree.

The navigation tree is located at the bottom left of each page, and displays the nodes of the WEB page in the form of a tree, so that the user can easily

find the WEB page to be managed. Web pages are divided into different groups according to their functions, and each group includes one or more pages. The page name in most navigation trees is an abbreviation of the page title above the corresponding page.

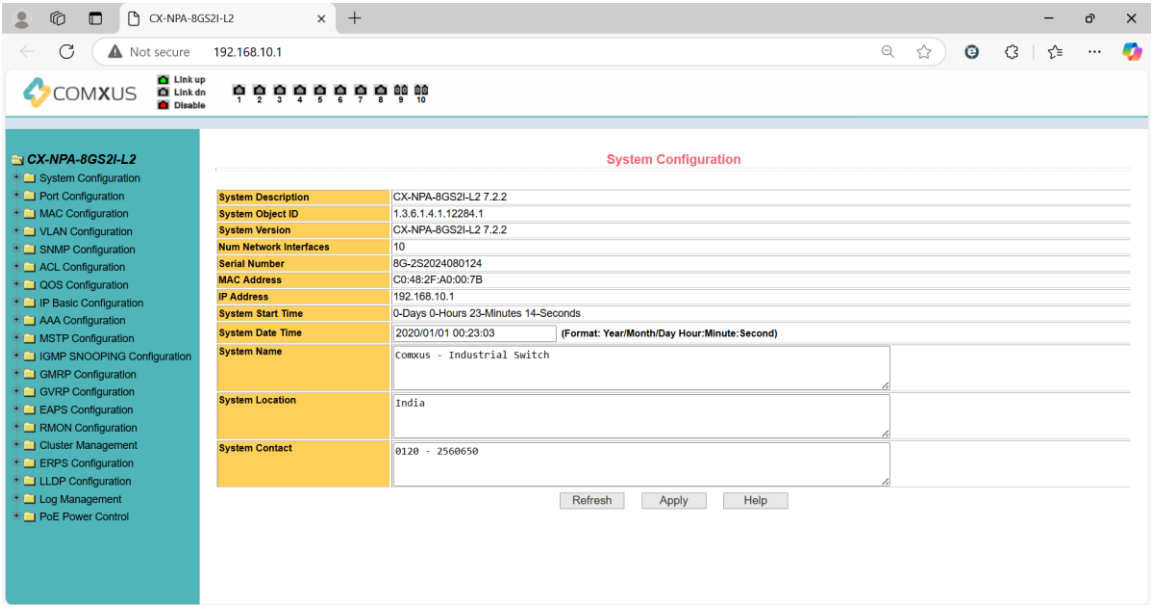


Figure 3 Organization page of the switch navigation tree

6. Introduction to Page Button

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

Table 2：

button	Function
Refresh	Update all fields on the pack
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

7. Error Message

If an error occurs while the switch & apos;s WEB server is processing a user request, a corresponding error message is displayed in a dialog box. For example, Figure 4 shows an error message dialog box.

Figure 4 Error Information Page

8. Entry Field

Some pages have an entry field in the leftmost column of the table, as shown in Figure 5, through which different rows in the table can be accessed. When you select a value in an entry field, the corresponding information for that row is displayed on the first row. Only that row can be edited. It is also called the active row. When a page is initially loaded, the entry field displays new and the active line is empty.

To add a new row, select New from the drop-down menu in the entry field, enter the new row information, and press the Apply key.

If you want to edit an existing row, select the appropriate row number from the drop-down menu in the entry field, edit the row as needed, and then press the Apply key. You will see the corresponding changes displayed in the table.

If you want to delete a row, select the corresponding row number from the drop-down menu in the entry field and press the Delete key. The row will disappear from the table.

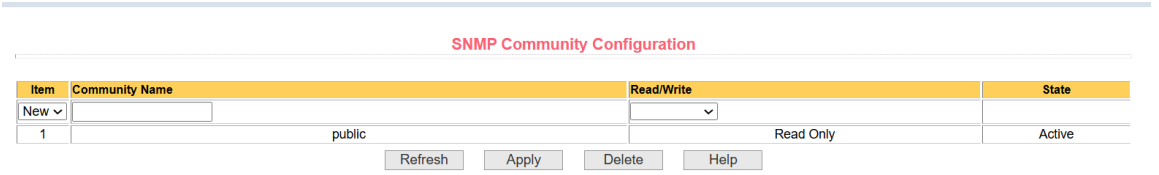


Figure 5 Entry Domain Page

9. State Field

Some pages have a status field in the rightmost column of the table, as shown in Figure 6, which shows the status of the row. Since all row state changes are handled internally, this state field is read-only. Once all the domain information in a row is in effect, the row status automatically changes to active.

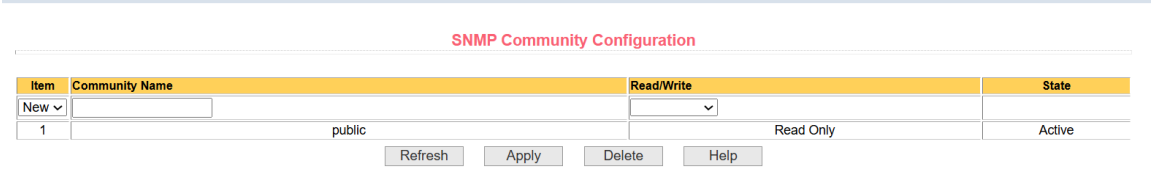


Figure 6 Status Field Page

WEB Page Introduction

1. Login Dialog

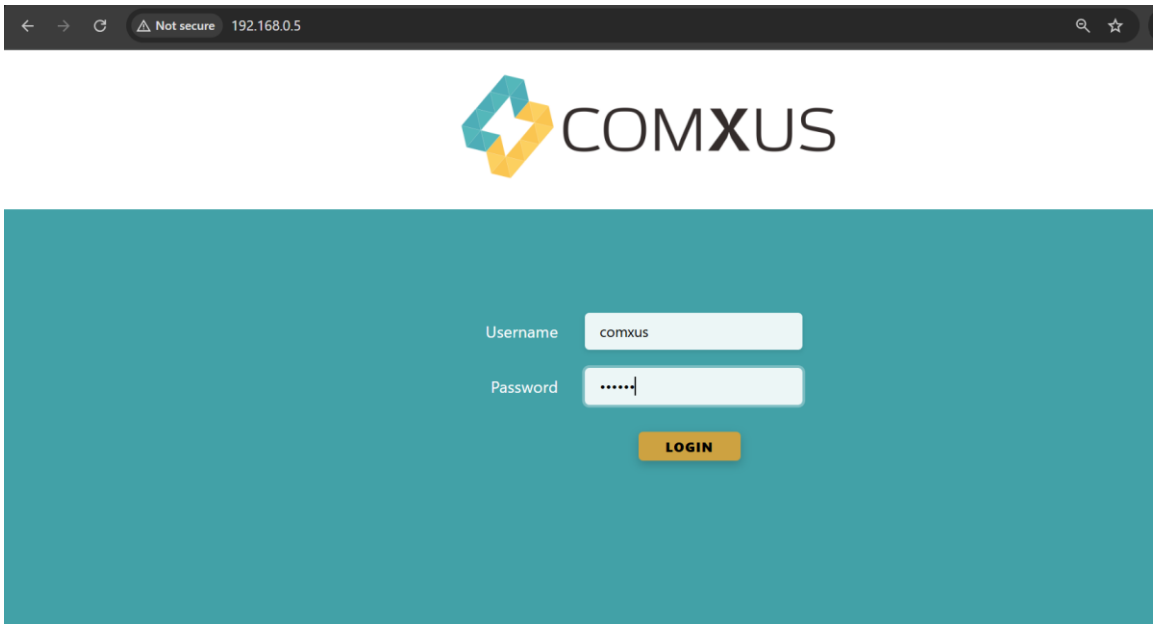


Figure 1-1 Login page for WEB browsing session

Figure 1-1 shows the login dialog box that appears the first time a user logs on to a Web page. The user can log in to the Web server of the switch by entering the user name and password in the corresponding fields and then clicking the OK button. Passwords are case-sensitive. Anonymous user password s can be up to 16 characters, while multiple user names and passwords can be up to 16 characters. The default user name of the managed switch is the anonymous user name comxus, the default password is the anonymous user pass word, and the default anonymous user password is comxus.

2. Main Page

Figure 2-1 shows the main WEB page of the managed switch. This page Is displayed after the user logs in to the web page.

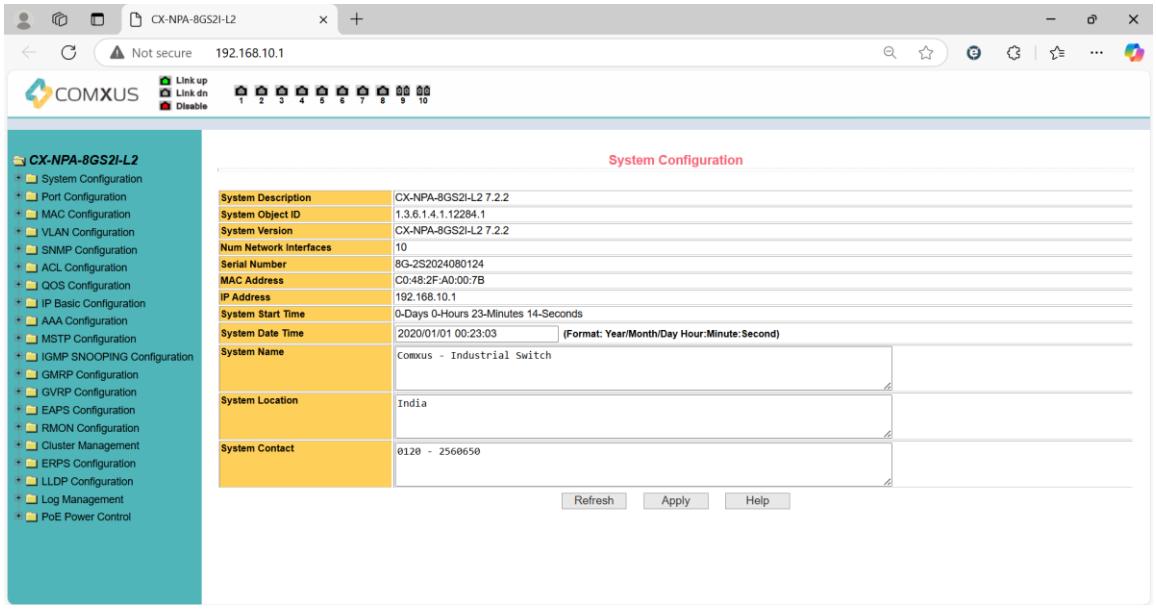
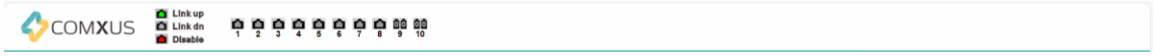


Figure 2-1 Switch Home Page

3. System configuration

Language switching: Use the language settings option in the upper-right corner to switch between available system interface languages.



(1) Basic Information

Figure 3-1 is the basic information configuration page, through which the user can configure the basic information of the switch.

System Description displays a description of the relevant parameters of the system.

The system descriptor identification number shows the identification of the system in network management.

System Version Number displays the version number of the software currently in use on the switch.

Network Interfaces displays the current number of network interfaces in the switch.

System Startup Time displays the time since the switch was started.

The system clock displays the current clock of the system. The user can modify the current clock of the system by inputting the parameters of year, month, day, hour, minute and second.

System Name displays the system name of the switch on the network. You can change the system name.

System Location displays the physical location of the switch in the network. You can modify the system location.

System Contacts displays the Manage Contact Information page for the current node.

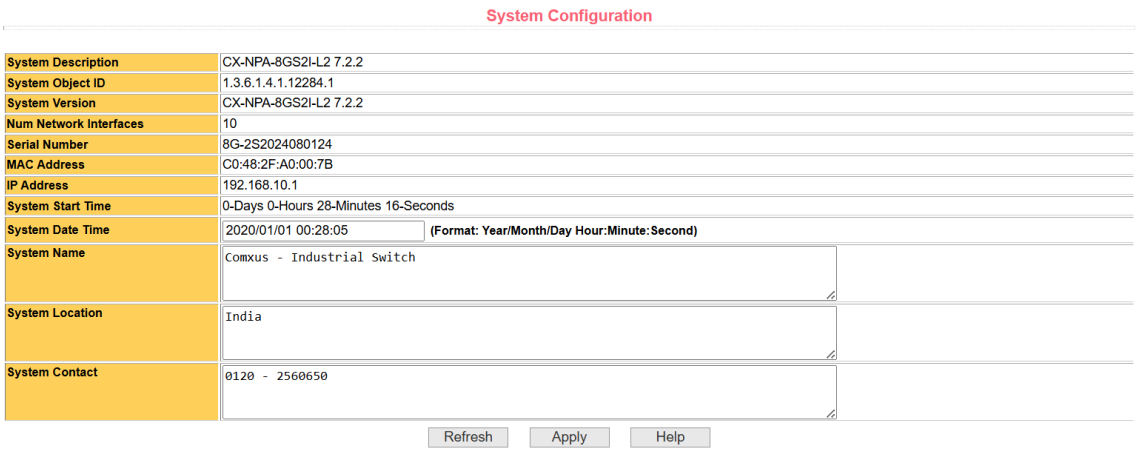


Figure 3-1 Basic information configuration page

(2) Serial Information

Figure 3-2 shows the interface for displaying switch serial port information. Through this page, you can view the configuration information of the switch serial port.

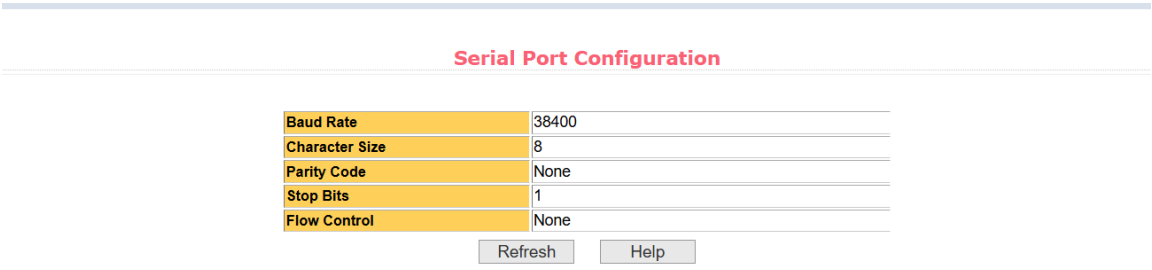


Figure 3-2 Serial Port Configuration Information Page

(3) User Management

Figure 3-3 shows the user management page, where users can modify the anonymous user (comxus) password of the switch. Telnet and Web use the same anonymous user password when multiple users are not enabled. Passwords are case sensitive and can be set to a maximum of 16 characters. If you want to change the password, the user needs to enter the new password twice. Once the user clicks the application button, the new password will be activated. At this time, if the switch does not enable multiple users, a login dialog box will be displayed. The user needs to log in to the webpage again, and must enter the new anonymous user password to log in to the WEB page.

At the same time, users can configure multiple users through this page. The switch does not have multiple users by default, which means that the multiuser management function is not enabled by default. At this time, login does not require verification of multiple user names and passwords. For Telnet, when a username

is added, the multi user management function is enabled, and when all users are deleted, the multi user management function is turned off a gain. For the Web, when adding a username, the multi user management function is only enabled if it is a privileged user. When all privileged users are deleted, the multi user management function is turned off again. When the multiuser management function is enabled, anonymous user passwords will not take effect, and logging into Telnet and the Web requires multiuser username and password verification. When the multi user management function is turned off, if an anonymous user password is configured, logging in to Telnet and Web requires anonymous user password verification.

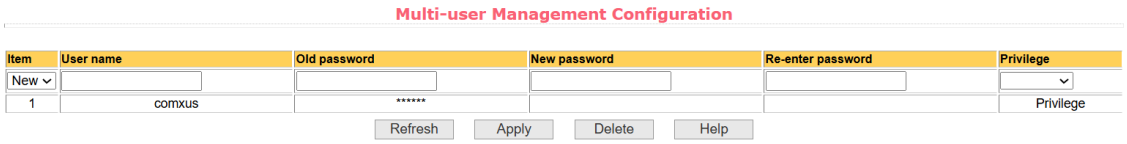


Figure 3-3 User Management Page

(4) safe management

Figure 3-4 is the security management 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, attach these services to the ACL group of IP standard, and implement source IP ad dress 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 on 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).

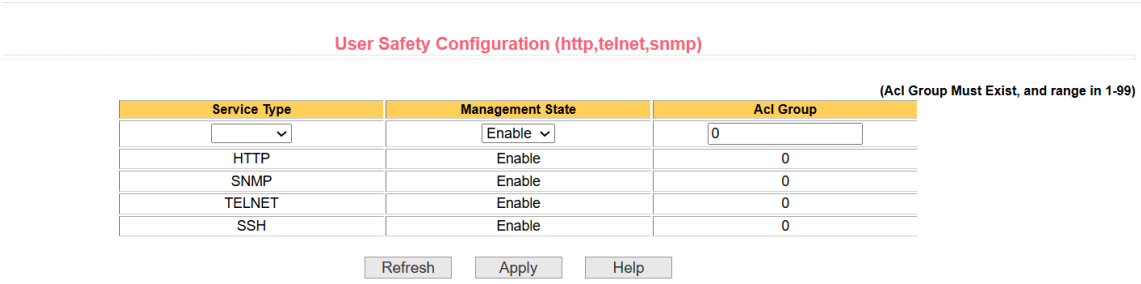


Figure 3-4 Security Management Page

(5) SNTP configuration

Figure 3-5 shows the SNTP configuration page, which allows administrators to configure and view the system clock.

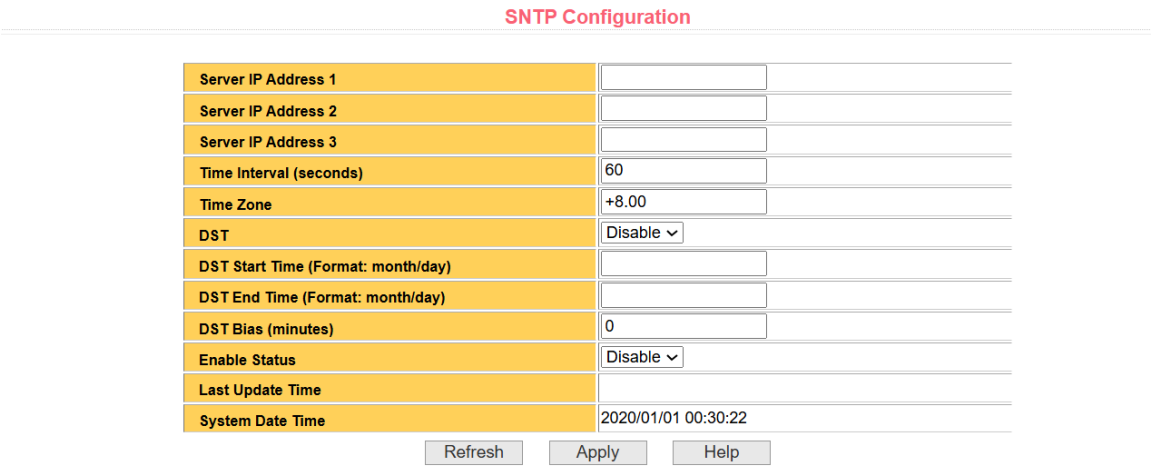


Figure 3-5 SNTP Configuration Page

(6) Jumbo Frame Configuration

Figure 3-6 Jumbo Frame Configuration Interface. Through this page, the user can configure the switch frame. The frame number range (1522-16383) sets the point application.

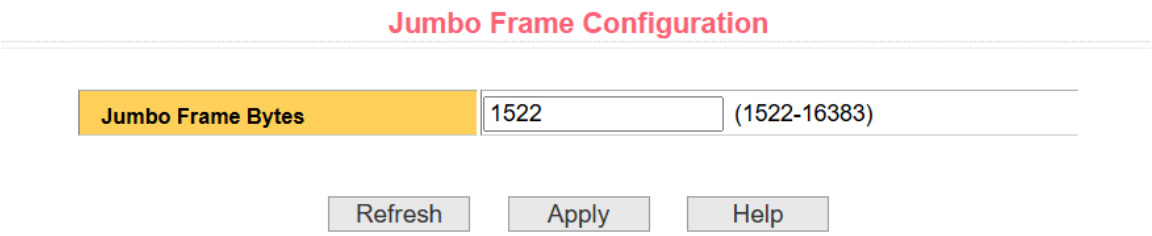


Figure 3-6 Jumbo Frame Page

(7) Save Current configuration

Figure 3-7 is the current configuration page. This page allows the user to view the current configuration of the switch. The save key 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 makes a configuration on the page and wishes that the configuration will not be lost after restarting the switch, the must click Save in the current configuration page before exiting the page.

Figure 3-7 Current Configuration Page

(8) Configuration file

Figure 3-8 is the 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. The delete key is used to delete the configuration file in FLASH. Click the delete key, and a dialog box will pop up. The dialog box prompts the user to confirm whether to delete the configuration file. If yes, press the OK key on the dialog box. Otherwise, press the cancel key. The download key is used to download the configuration file to the PC. Click the download button, a dialog box will pop up, and the user will select the directory path and save the configuration file.

The file name of the downloaded configuration file is the switch .cfg.

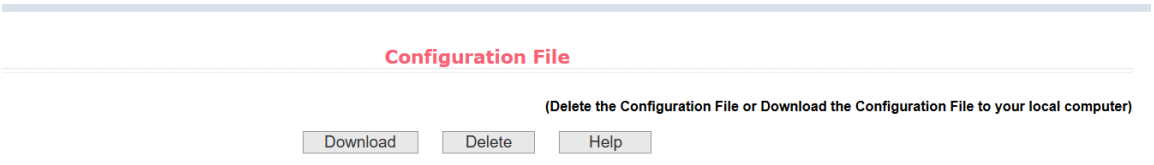


Figure 3-8 Configuration File Page

(9) File upload

Figure 3-9 shows the file upload page, which allows users to upload configuration files and image files to the switch. Click the Browse button to select the directory path of the uploaded profile or image file on the PC. Click the Upload button to upload the configuration file or image file. The suffix of the configuration file must be *.cfg. The image file must be provided by the manufacturer and the suffix of the file name 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.

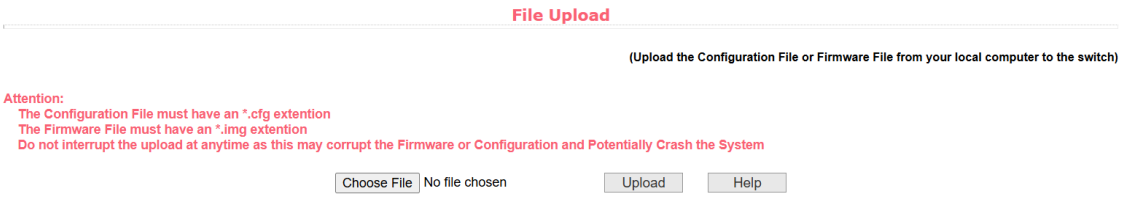


Figure 3-9 File Upload Page

(10) System Reboot

Figure 3-10 shows the system reset 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. When clicking the Restore Factory Switch, a dialog box will pop up to prompt the user whether to confirm the restoration of the factory switch. If yes, press the OK key, otherwise press the Cancel key. Web pages will no longer open when you restart.

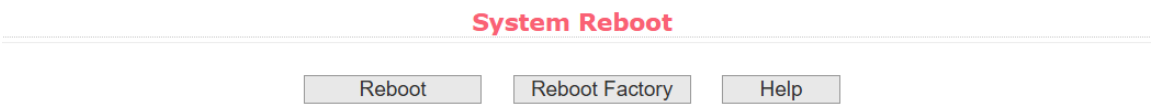


Figure 3-10 System Reset Page

4. Port configuration

(1) Common configuration

Figure 4-1 is the Port Configuration/Port Display page. This page allows users to enable or disable ports, set port speeds, or view basic information for all ports. To set a specific port, the user needs to select the corresponding port name in the drop-down menu of the port. The port status defaults to up, and you can disable the port by selecting down from the drop-down menu.

The user can also select the Set Speed drop-down menu to set the speed of the port, such as forcing the port to be half-duplex 10 M (half-10). This page allows the user to view additional basic information for all ports.

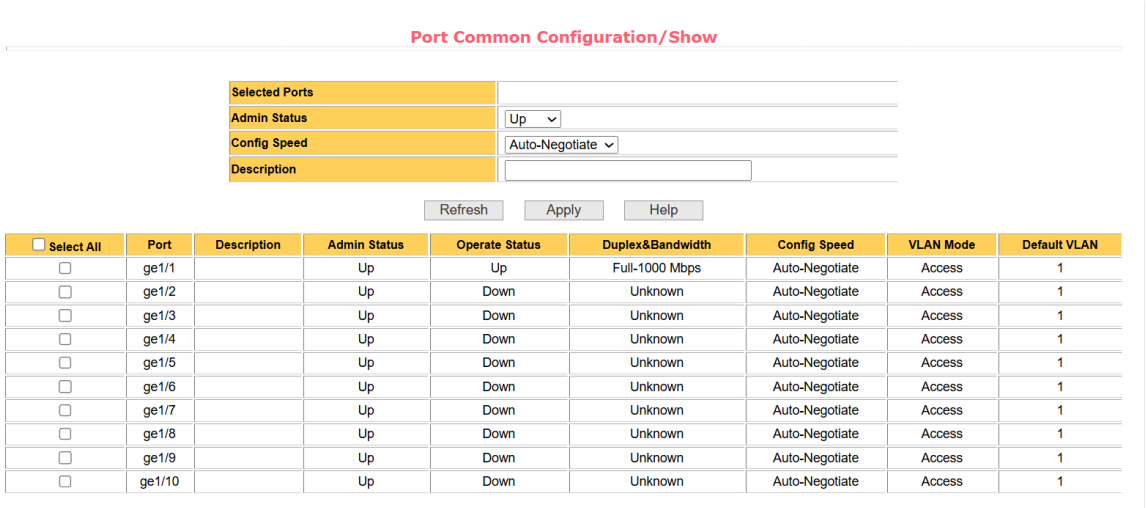


Figure 4-1 Port Configuration and Port Display Page

(2) Port Statistics

Figure 4-2 is the Port Statistics page. To view a particular port, the user needs to select the appropriate port name from the drop-down menu for the port. This page allows the user to view the statistics of packets sent and received by the port.

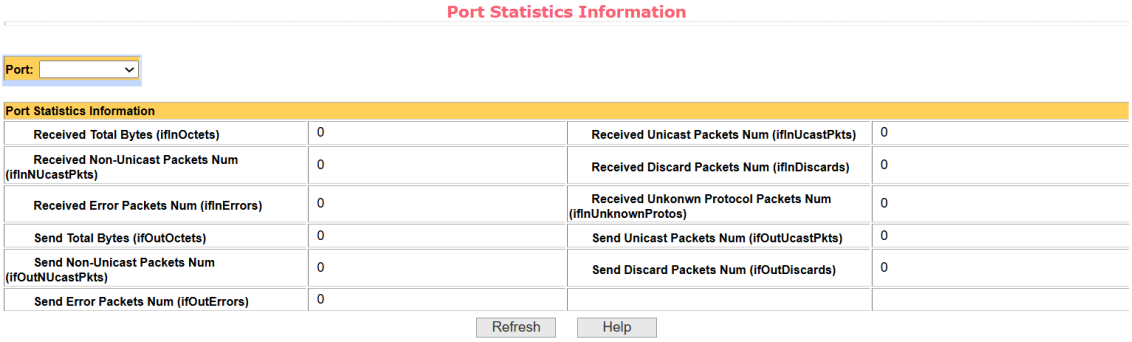


Figure 4-2 Port Statistics Page

(3) Flow Control

Figure 4-3 is the flow control page. The user can turn on and off the flow control of each port through this page. Flow control of a port is turned on or off by the pull-down on or off of the flow control. At the same time, the flow control status of all ports can be viewed through this page.

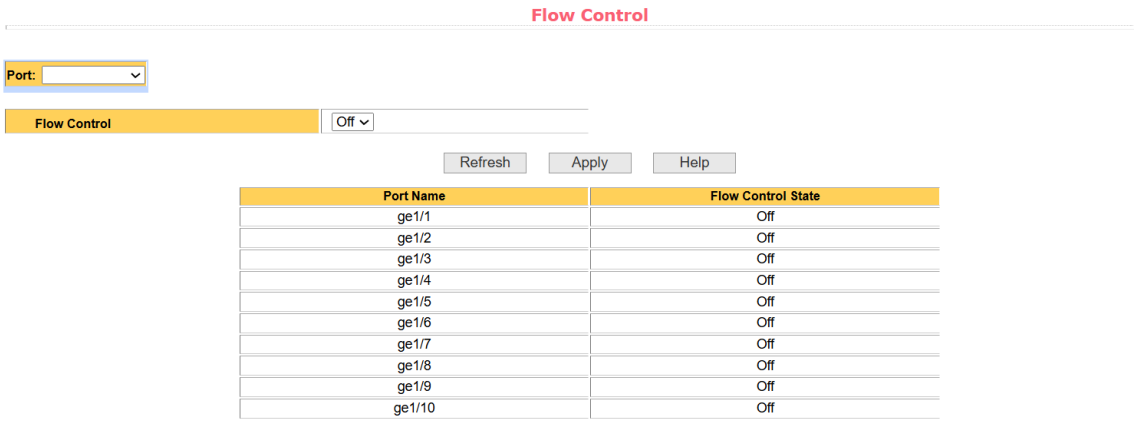
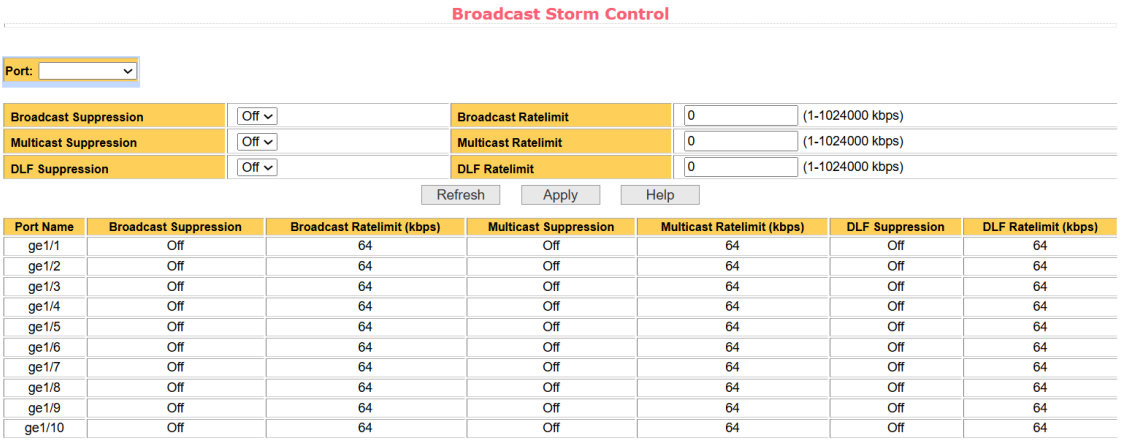


Figure 4-3 Flow Control Page

(4) Broadcast Storm

Figure 4-4 is the Broadcast Storm Control page. This page is used to configure the suppression function of broadcast packets, multicast packets and DLF packets for the port.

Select the port to be configured from the drop-down bar of the port. Use on and off to turn on and off broadcast suppression, multicast suppression, and DLF suppression for the port. Throttle rate item is used to configure the throttle rate of the port. Range 1-1024000, unit: kbits. The suppression rates of broadcast suppression, multicast suppression and DLF suppression on the same port are equal. At the same time, you can view the broadcast storm control configuration of all ports through this page.



Port Name	Broadcast Suppression	Broadcast Ratelimit (kbps)	Multicast Suppression	Multicast Ratelimit (kbps)	DLF Suppression	DLF Ratelimit (kbps)
ge1/1	Off	64	Off	64	Off	64
ge1/2	Off	64	Off	64	Off	64
ge1/3	Off	64	Off	64	Off	64
ge1/4	Off	64	Off	64	Off	64
ge1/5	Off	64	Off	64	Off	64
ge1/6	Off	64	Off	64	Off	64
ge1/7	Off	64	Off	64	Off	64
ge1/8	Off	64	Off	64	Off	64
ge1/9	Off	64	Off	64	Off	64
ge1/10	Off	64	Off	64	Off	64

Figure 4-4 Broadcast Storm Control Page

(5) Port rate limit

Figure 4-5 shows the port speed limit page. This page is used to configure the rate at which the port sends and receives.

Select the port to be configured from the drop-down bar of the port. The b and width control of sending data packet is used to configure and display the bandwidth control of sending data packet. The range is 1-1024000, and the unit is kbits. After

input, press the application key to take effect. Displays off if the port is not configured for bandwidth control. The corresponding cancel key is used to cancel the bandwidth control of the transmitted data packet. The bandwidth control of the received data packet is used to configure and display the bandwidth control of the received data packet. The range is 1-1024000, and the unit is kbits. After input, press the application key to take effect. Displays off if the port is not configured for bandwidth control. The corresponding cancel key is used to cancel the bandwidth control of the received packet.

If the port is configured with bandwidth control, it is displayed in the list.

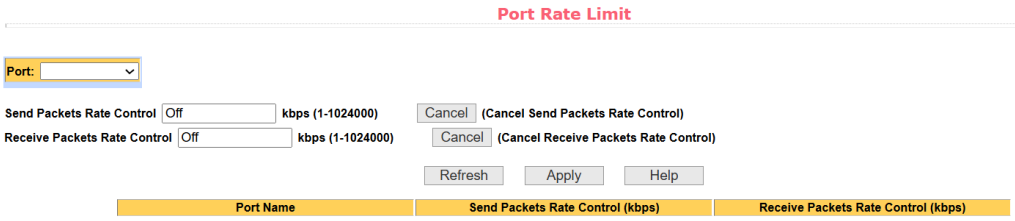


Figure 4-5 Port Speed Limit Page

(6) Protection Port

Figure 4-6 is the protection port page. This page is used to configure protection ports. Protected ports cannot communicate with each other, only with unprotected ports.

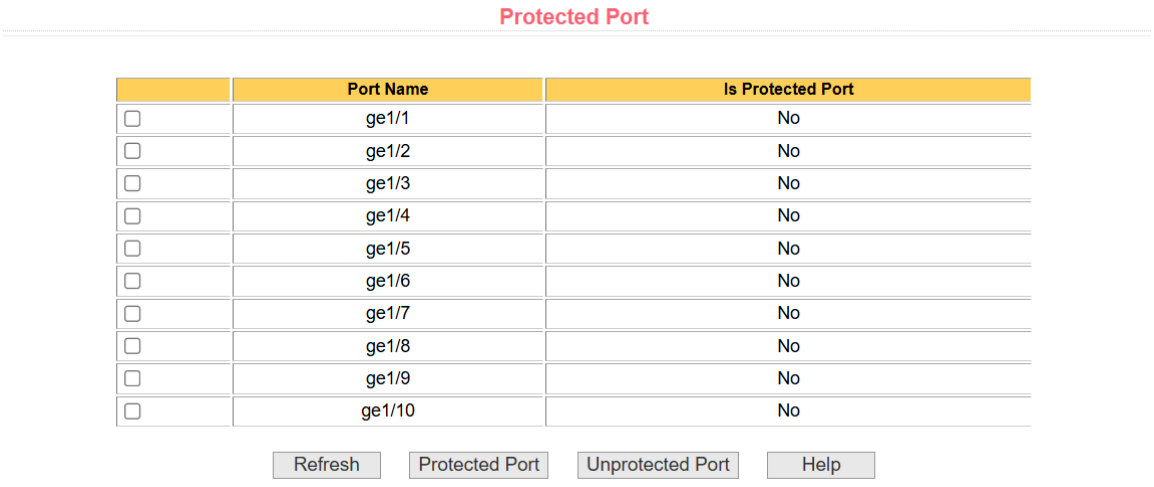
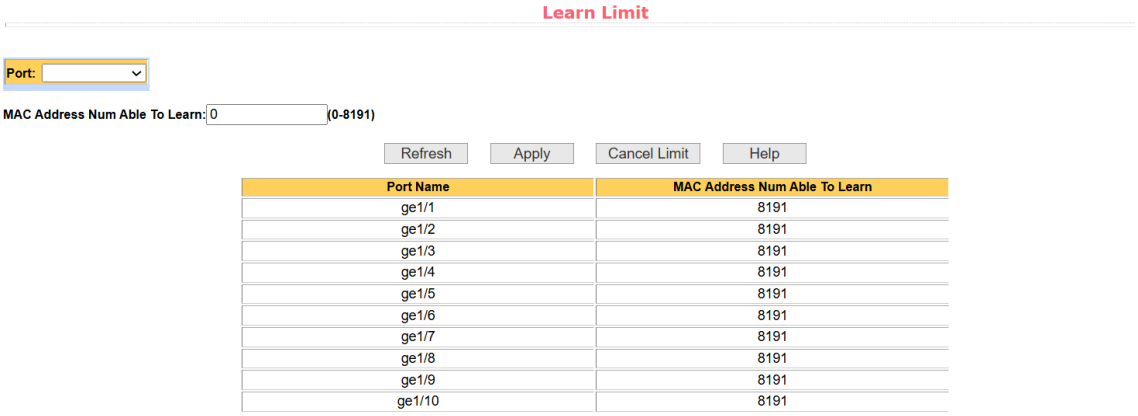


Figure 4-6 Protection Port Page

(7) Learn limit

Figure 4-7 is the Port Learning Limits page. This page is used to limit the number of MAC addresses that the port can learn. The range is 0-8191. The default value is 8191, which is also the maximum value, indicating that the port has no learning limit configured. The list shows the learning limits for all ports.



Port Name	MAC Address Num Able To Learn
ge1/1	8191
ge1/2	8191
ge1/3	8191
ge1/4	8191
ge1/5	8191
ge1/6	8191
ge1/7	8191
ge1/8	8191
ge1/9	8191
ge1/10	8191

Figure 4-7 Port Learning Limit Page

(8) Prot Trunking

Figure 4-8 is the Port Aggregation Configuration page. This page allows the user to configure port aggregation. This page consists of four sections: Tr group ID selection, port aggregation method, configurable ports, and group member ports.

To create or modify a port aggregation, the user needs to select a Tr group ID from 1 to 8. The user clicks the corresponding Tr group ID in the list box, and the information of the Tr group is displayed in the group member port. To create a Trunk group, select the corresponding ID in the Trunk group ID, and click "Create Trunk Group". If the creation is successful, the ID display column will be marked with parentheses. If a Tr group is not created, Not created is marked in parentheses in the ID display column. To set the port aggregation method, select an aggregation method from the drop-down box

above the list and click the button Set Aggregation Method. To add an aggregated port, select the aggregated port in Configurable Ports and click Member Port = >. To delete a port from the existing aggregated ports, select the aggregated port from the group member ports and click the "Non-member port < =" button. To delete the entire Tr group, click the Delete Tr Group button.

In the page configuration process, the configured aggregation method corresponds to the selected Trunk group ID. Only the existing Trunk group can configure the aggregation method; only the existing Trunk can add or delete member ports; only the Trunk group without member ports can be deleted.

The switch provides six types of port aggregation: based on source MAC address, based on destination MAC address, based on source and destination MAC address, based on source IP address, based on destination IP address, and based on source and destination IP address.

The managed switch supports up to 8 groups of port aggregation. Each group of port aggregation supports up to 8 ports. Each Tr group can configure its own port aggregation method.

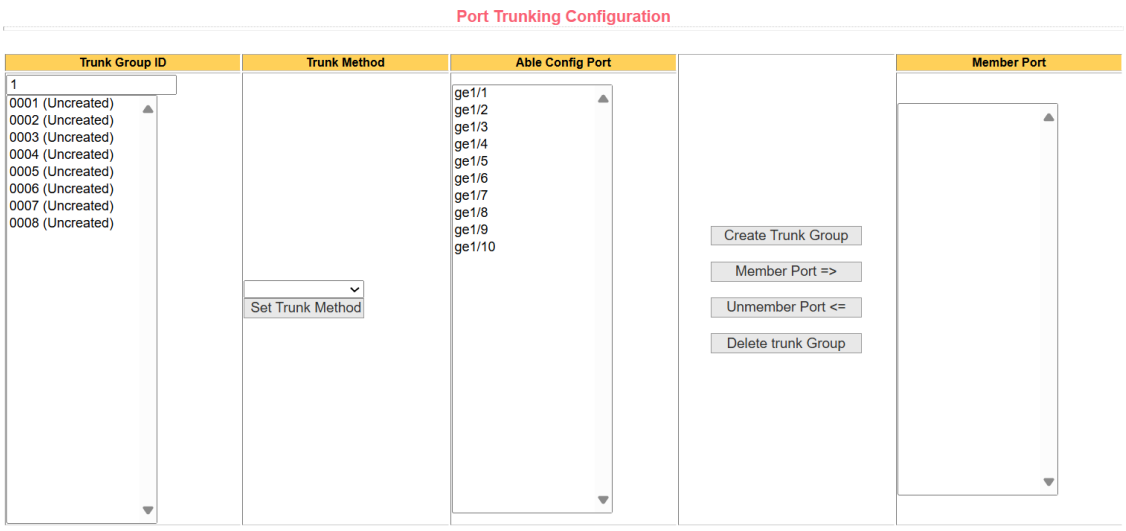


Figure 4-8 Port Aggregation Configuration Page

(9) Mirror

Figure 4-9 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 in put port through the mirroring port. Only one mirror port can be selected, and multiple mirrored output ports and mirrored input ports can be selected. This page consists of four parts: listening port, configurable port, listening direction and mirror configuration information. When configuring a mirror port, first configure the mirror port from the monitoring port. There can only be one mirror port. Then select the mirrored port from the configurable ports. Select the monitoring direction from the monitoring direction. Finally, press the Apply key to take effect. The result will be displayed in the mirror configuration information.

When RECEIVE is selected in the monitoring direction, it means to monitor the received data packets, and TRANSMIT means to monitor the transmitted data packets. BOTH means to monitor all sent and received packets, NOT _ RECEIVE means to cancel monitoring received packets, NOT-Transmit means to cancel monitoring sent packets, and NEITHER means to cancel monitoring received and sent packets, that is, to cancel the monitored port.

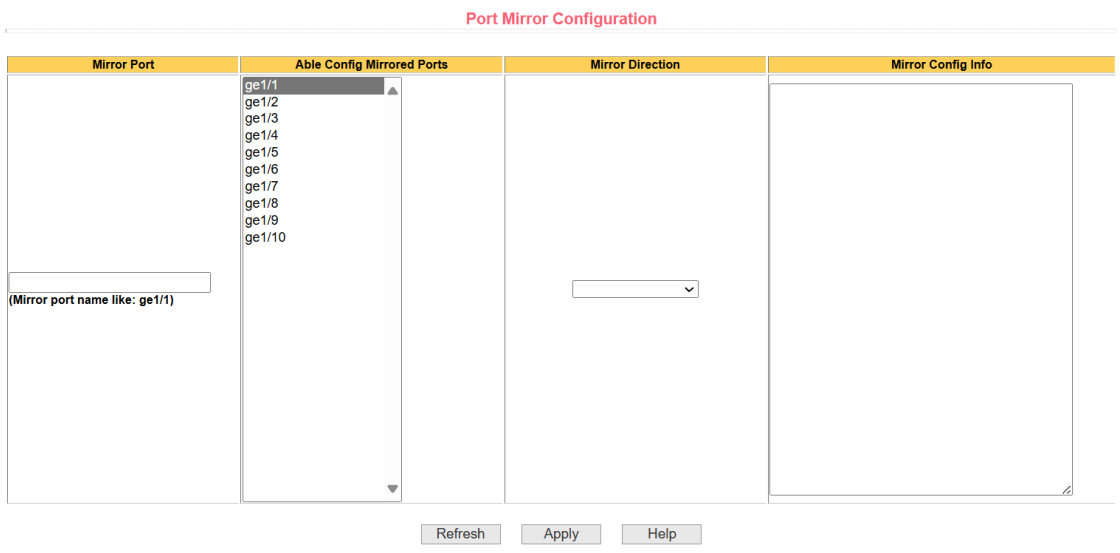


Figure 4-9 Port Mirror Configuration Page

(10) DDM information

Figure 4-10 shows the DDM information viewing interface. This page is used to view the corresponding information of the optical module.

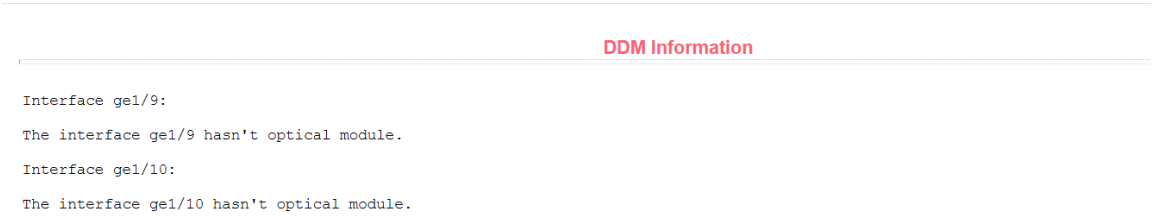


Figure 4-10 DDM information viewing interface

5. MAC Configuration

(1) MAC table

Figure 5-1 is the MAC address table display interface. This page is used to view the MAC address of the VLAN corresponding to the port.

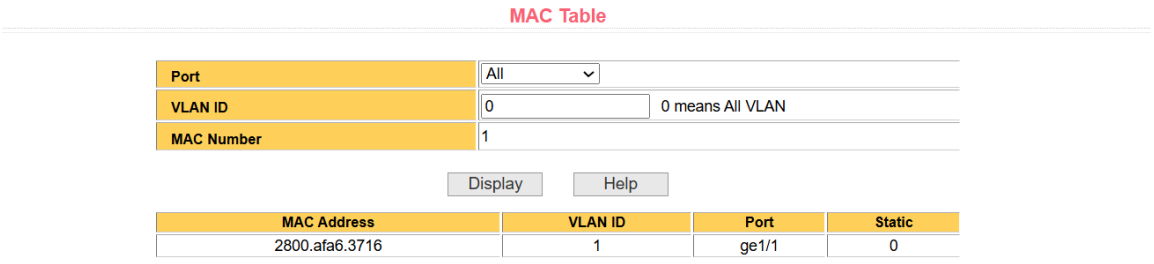


Figure 5-1 MAC Address Table

(2) MAC Binding

Figure 5-2 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.

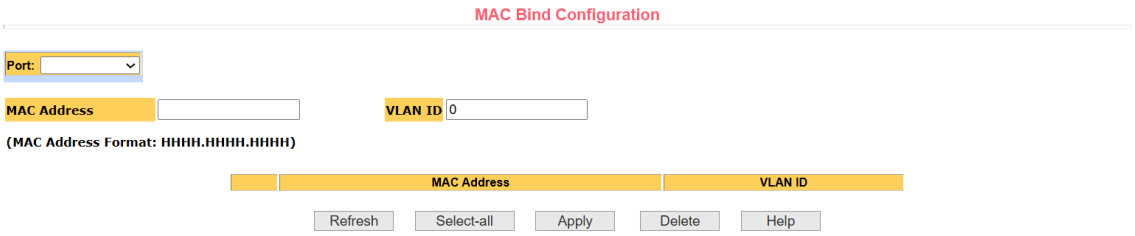


Figure 5-2 MAC Binding Configuration Page

(3) MAC auto binding

Figure 5-3 is the MAC Binding Auto Conversion page. This page is used to automatically bind the MAC address of the port.

Displays the existing dynamic MAC address of the port in the Layer 2 hardware forwarding table and the VLAN to which it belongs. You can select an

entry and convert it to a static binding.

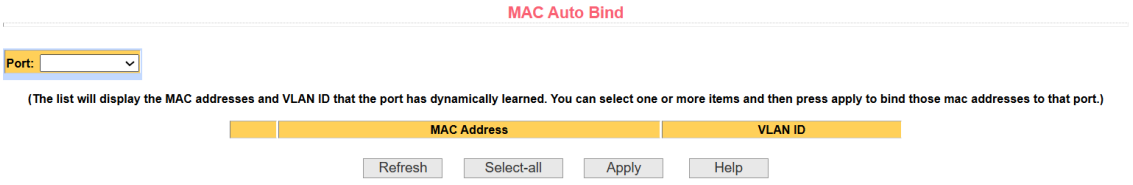


Figure 5-3 MAC Binding Automatic Conversion Page

(4) MAC Filter

Figure 5-4 is the MAC filtering configuration page. This page is used to configure the port to filter MAC addresses.

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

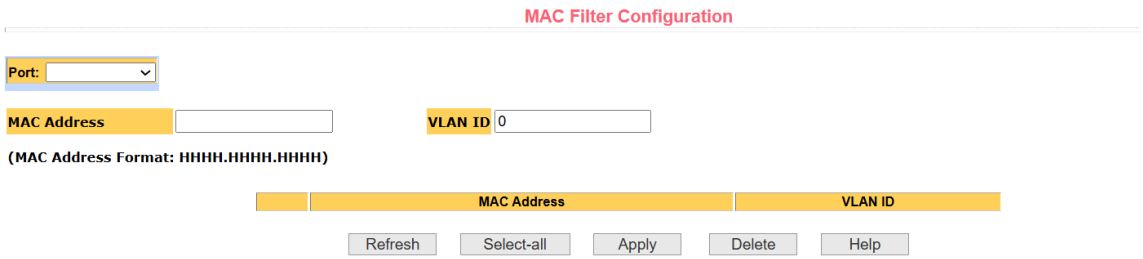


Figure 5-4 MAC Filtering Configuration Page

(5) MAC auto filter

Figure 5-5 shows the MAC filtering automatic transition 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 hard ware forwarding table and the VLAN to which it belongs. You can select an entry and convert it to a static filtering configuration.

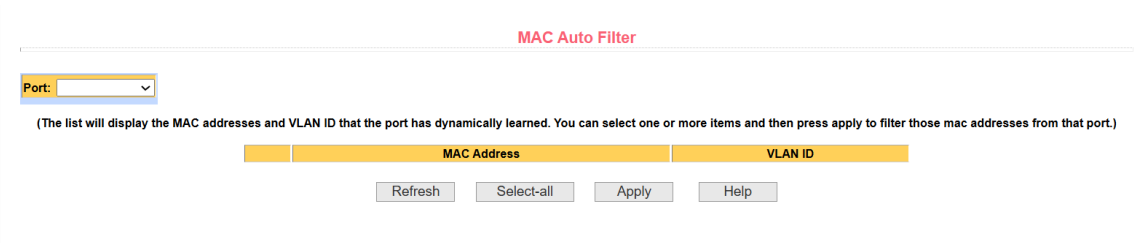


Figure 5-5 MAC Filtering Auto Conversion Page

6. VLAN Configuration

(1) VLAN information

Figure 6-1 shows the Current VLAN Information page. This read-only page displays the current VLAN, the status of the VLAN, and the port membership of the VLAN. The drop-down box displays all current VLANs, and the list displays the VID, status, and port membership for up to 30 VLANs. Select a VLAN from the drop-down box. The list displays information for up to 30 VLANs with a VID greater than the VLAN. However, if there are no more than 30 VLANs, no matter which VLAN is selected from the drop-down box, the information of all VLANs will be displayed in the list.

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

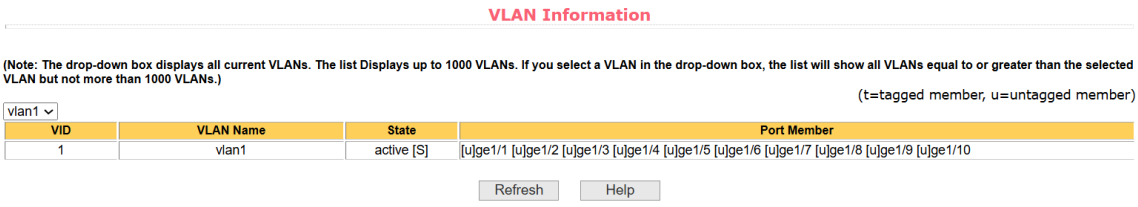


Figure 6-1 VLAN Information Page

(2) VLAN Configuration

Figure 6-2 is the Static VLAN Configuration page, which allows the user to create VLANs.

To create a new VLAN, the user enters a VID in the active line from 2 to 4

094. The VLAN name is generated by the system based on the VLAN ID and cannot be modified. Click the Apply button, and the list box displays the VID and VLAN name of the VLAN created by the user. The switch creates VLAN 1 by default, and VLAN 1 cannot be deleted.

To delete a VLAN, the user needs to click on the corresponding VLAN in the list box. The VLAN will be displayed in the active line. Click the Delete key to delete the VLAN, and the information of the VLAN will be removed from the list box.

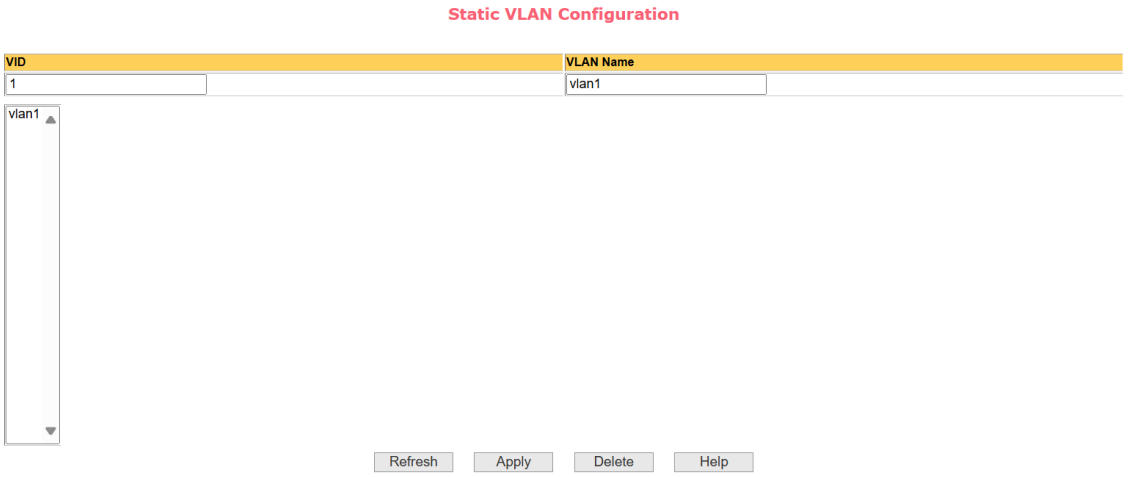


Figure 6-2 VLAN Configuration Page

(3) VLAN Port Configuration

Figure 6-3 is the VLAN Port Configuration page, which is used to configure VLANs on the ports and displays the results of the configuration. This page mainly consists of eight parts: port, mode, all current VLANs, VLAN to which the port belongs, and the keys "Default VLAN = >", "tagged = >", "untagged = >" and "Non-member < =".

Port is the port that specifies the VLAN to be configured.

Access Mode specifies that the port & apos; s VLAN mode is ACCESS mode In this VLAN mode, the port defaults to an untagged member of VLAN1, and the port & apos; s default VLAN is 1. Hybrid specifies that the VLAN mode of the port is

HYBRID mode. In this VLAN mode, the port is an untagged member of VLAN1 by default, and the default VLAN of the port is 1. Trunk specifies that the VLAN mode of the port is TRUNK mode. In this VLAN mode, the port is a tagged member of VLAN1 by default, and the default VLAN of the port is 1.

All current VLANs refer to the currently created VLANs, that is, the VLANs configured by the port. The user can select more than one VLAN from the list.

The VLAN to which the port belongs displays the result of the VLAN port configuration. [P] indicates that the VLAN is the default VLAN for the port. [T] indicates that the port is a tagged member of the VLAN. [U] indicates that the port is an untagged member of the VLAN. When a VLAN is deleted, the user selects the VLAN from the list. Multiple selections are allowed.

Press "Default VLAN = >" to configure the default VLAN of the port, and select a VLAN from all the current VLANs.

Press "tagged = >" to configure that the port is a tagged member of the specified VLAN, and select one or more VLANs from all current VLANs.

Press "untagged = >" to configure the port to be an untagged member of the specified VLAN. Select one or more VLANs from all the current VLANs.

Press the key "Non-member < =" to delete the port from one or more specified VLANs, and select one or more VLANs from the VLANs to which the port belongs.

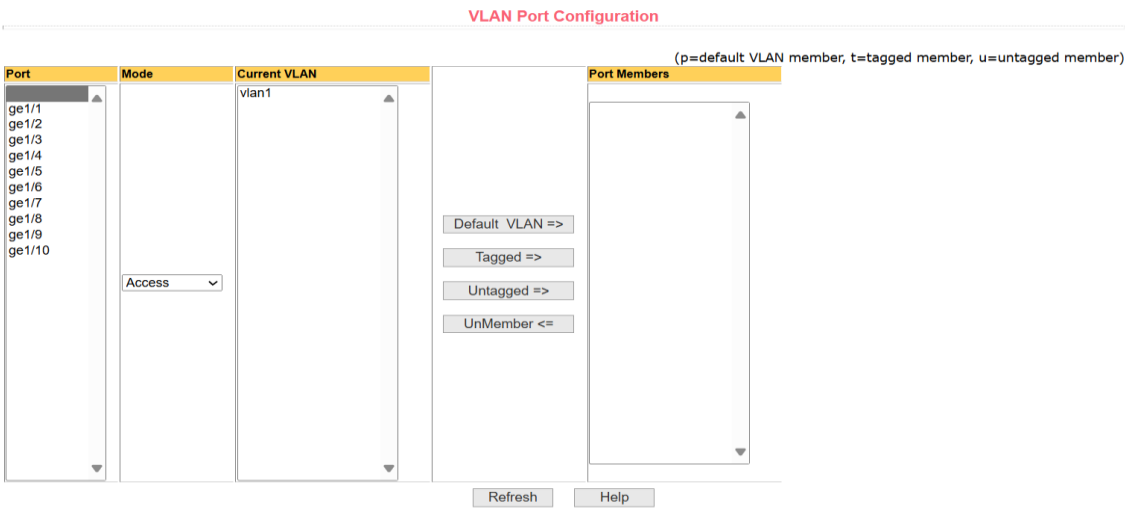


Figure 6-3 VLAN Port Configuration Page

7. SNMP Configuration

(1) Community Name

Figure 7-1 shows the SNMP community configuration page, which 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. Correspondingly, there is only one active entry on the page, the community name is public, and the permissions are read-only. When the switch needs to be managed through SNMP, it is necessary to configure a common body with readable and writable permissions.

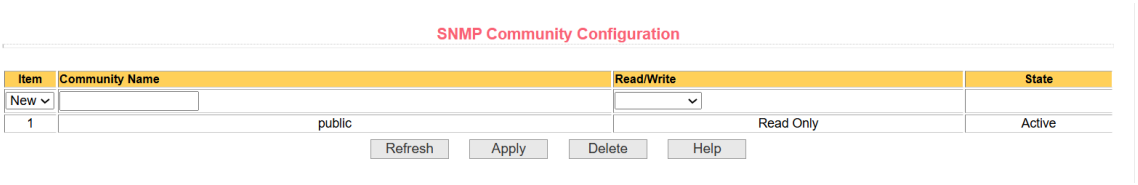


Figure 7-1 SNMP Community Configuration Page

(2) TRAP Target

Figure 7-2 is the TRAP Destination Configuration page, which allows the user to configure the IP address of the workstation that receives the TRAP message and some parameters of the TRAP packet.

When configuring the entry, the name is used to enter the trap name, the transport IP address is used to enter the destination address, and the SNMP version is used to select the version of the trap packet. If the setting is successful, the status in the entry will be displayed as active. If the configuration is

successful, the SNMP TRAP feature will work and the switch will automatically send TRAP packets to the destination address in the event of a link up or link down condition, for example.

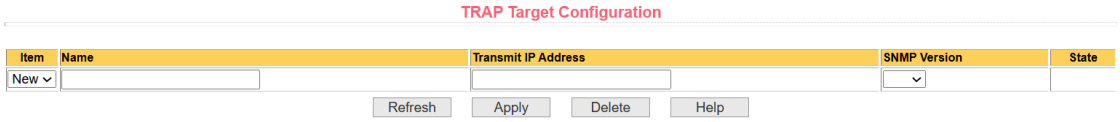


Figure 7-2 TRAP Target Configuration Page

8. ACL Configuration

(1) Standard IP

Figure 8-1 is the ACL Standard IP Configuration page, which allows the user to create a rule base for 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).

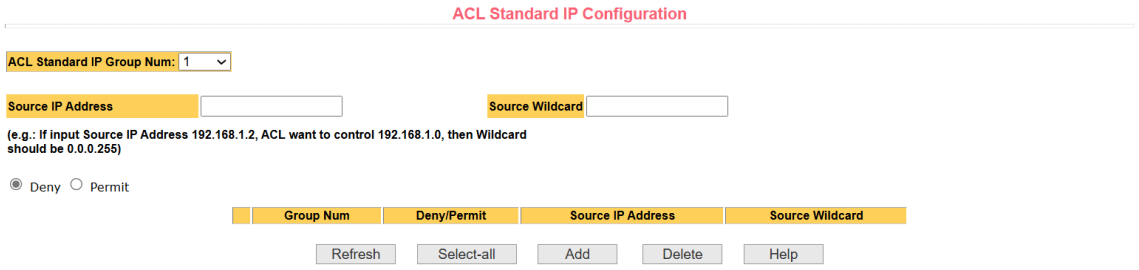


Figure 8-1 ACL Standard IP Configuration Page

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 a user configures a rule, 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

Figure 8-2 shows the ACL extended IP configuration page, which allows the user to create a rule base for 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 IC MP, TCP, UDP, etc.), source port and destination port (valid only for TCP and UDP protocols), and TCP control flags.

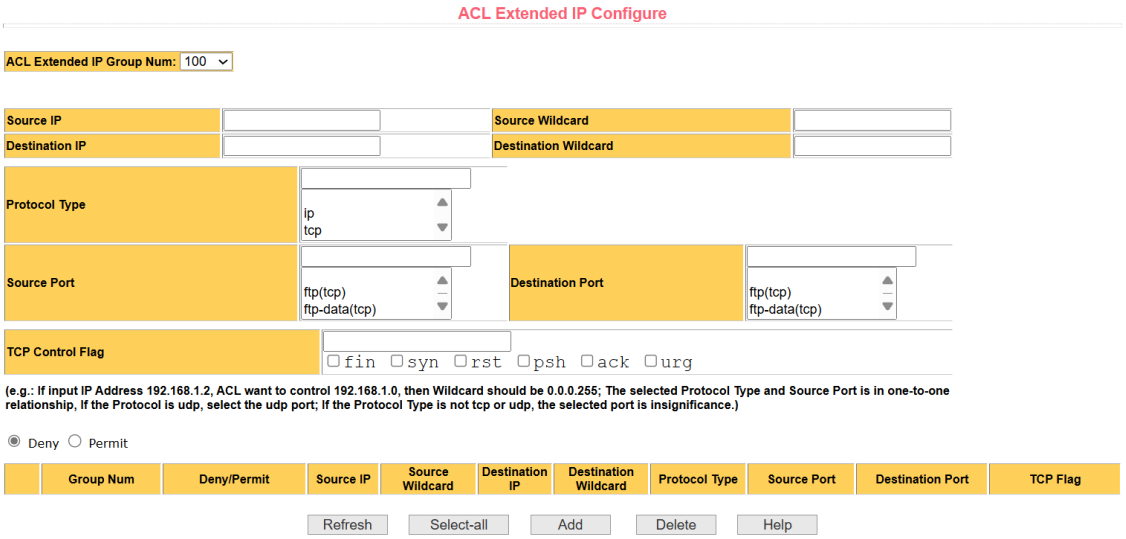


Figure 8-2 ACL Extended IP Configuration Page

When the user configures a rule, both the source IP address and the destination IP address need to be masked, and the rule can match the set of IP addresses. The mask of the address is represented by one & apos; s 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 a user configures a rule, 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 press the delete key.

(3) MAC IP

Figure 8-3 shows the ACL MAC IP configuration page, which allows the u ser to create a rule base for the 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. Th e fields that can be matched in a rule are source MAC address (with address match bits), source IP address (with address match bits), destination IP address (with address match bits), VLAN ID.

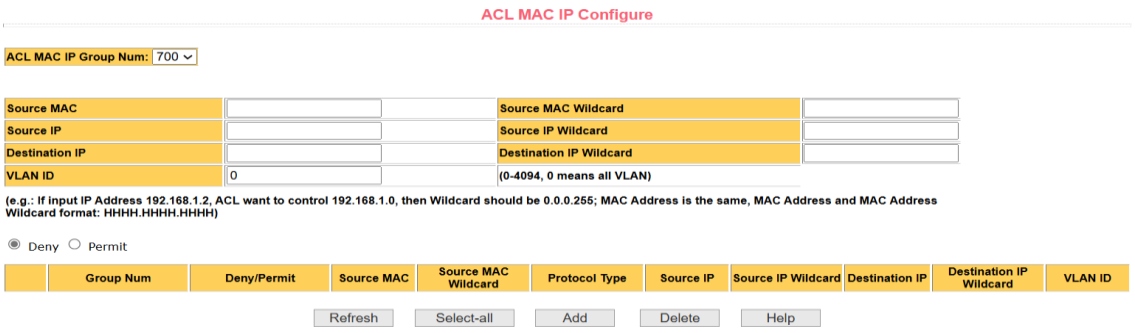


Figure 8-3 ACL MAC IP Configuration Page

When the user configures a rule, the source MAC address, source IP address, and destination IP address must all have an address match bit, and the rule can match a set of MAC addresses and IP addresses. For example, 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 a user configures a rule, 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 r ule group. If the user wants to delete the whole rule group, he can select all first and then press the delete key.

When the user configures the rule, the VLAN ID must be in the range of 0 to 4094, inclusive, where 0 represents all.

(4) MAC ARP

Figure 8-4 shows the ACL MAC ARP configuration page, which allows the user to create a rule base for 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 sending MAC address (with address match bits) and the sending IP address (with address match bits).

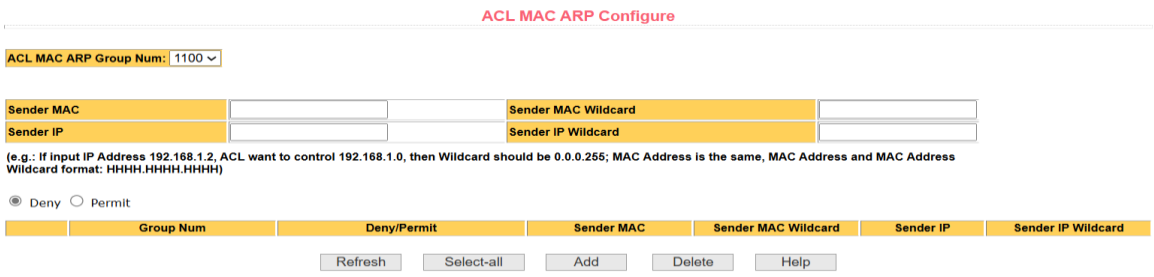


Figure 8-4 ACL MAC ARP Configuration Page

When the user configures the rule, both the sending MAC address and the sending IP address need to have the address matching bit, and the rule can match the set of MAC address and IP address. For example, 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 a user configures a rule, 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 press the delete key.

(5) ACL Information

Figure 8-5 shows the ACL Repository Information page, which displays all the rules and references configured in the current ACL.

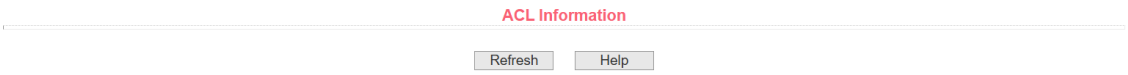


Figure 8-5 ACL Resource Library Information Page

(6) ACL Reference

Figure 8-6 is the ACL reference configuration page, through which the user can select an ACL rule group for a port, write the rules in the ACL rule 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 rule group on a port, you can select IP Standard, IP Extended, MAC IP, and MAC ARP ACL groups. The selected ACL rule group must exist. Select from the ACL rule group list and press the Add key. To delete an ACL rule group, select an ACL rule group from the list of referenced rule groups and press the Delete key.

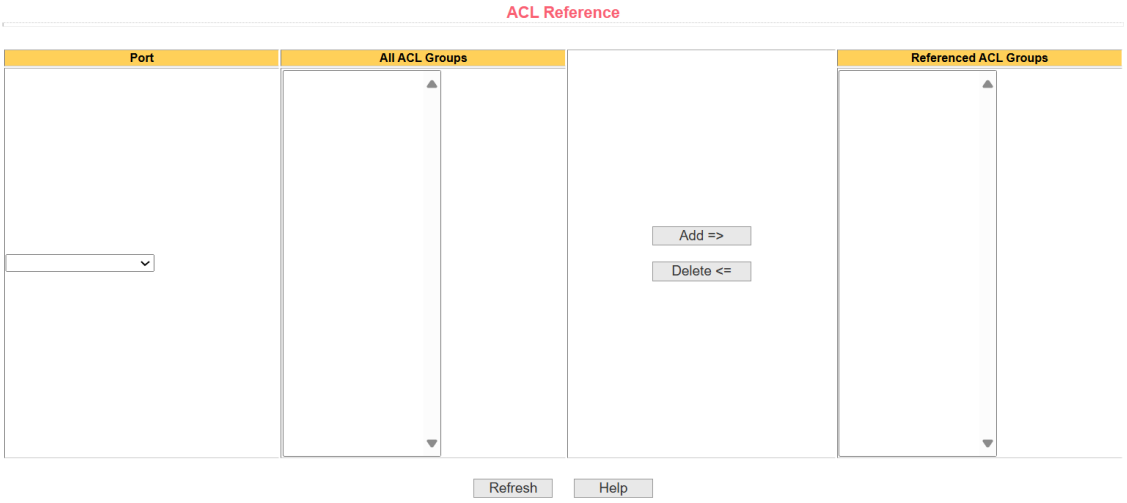


Figure 8-6 ACL Reference Configuration Page

9. Qos configuration

(1) Qos apply

Figure 9-1 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 & apos; s Qos type and user default priority in real time.

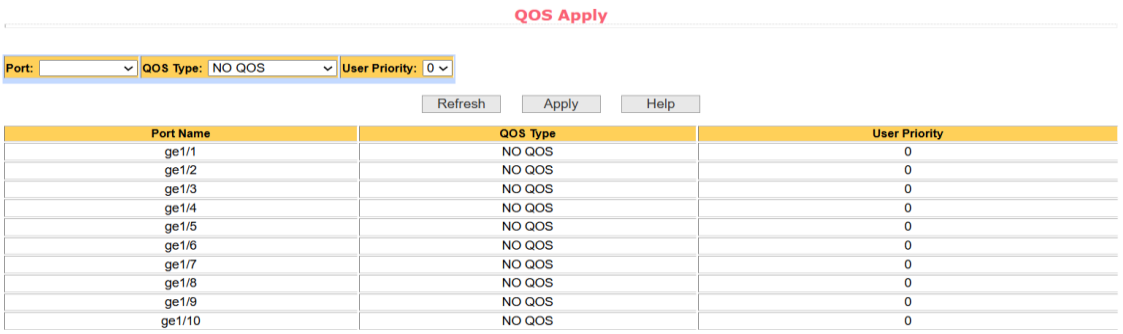
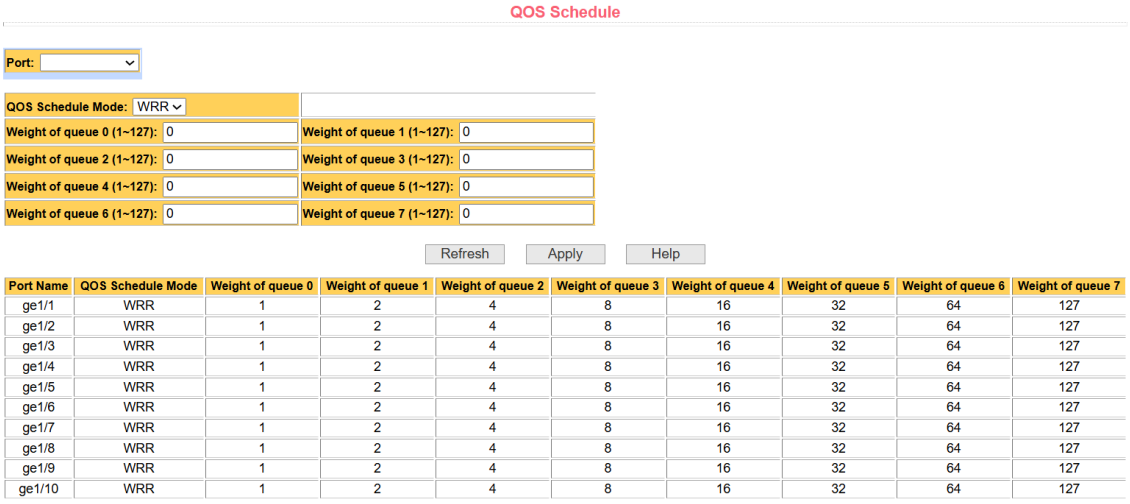


Figure 9-1 Qos Application Page

(2) Qos Schedule

Figure 9-2 is the Qos scheduling page, through which the user can configure 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.



Port Name	QOS Schedule Mode	Weight of queue 0	Weight of queue 1	Weight of queue 2	Weight of queue 3	Weight of queue 4	Weight of queue 5	Weight of queue 6	Weight of queue 7
ge1/1	WRR	1	2	4	8	16	32	64	127
ge1/2	WRR	1	2	4	8	16	32	64	127
ge1/3	WRR	1	2	4	8	16	32	64	127
ge1/4	WRR	1	2	4	8	16	32	64	127
ge1/5	WRR	1	2	4	8	16	32	64	127
ge1/6	WRR	1	2	4	8	16	32	64	127
ge1/7	WRR	1	2	4	8	16	32	64	127
ge1/8	WRR	1	2	4	8	16	32	64	127
ge1/9	WRR	1	2	4	8	16	32	64	127
ge1/10	WRR	1	2	4	8	16	32	64	127

Figure 9-2 Qos Scheduling Page

10. IP Basic Configuration

(1) VLAN interface

Figure 10-1 is the VLAN interface configuration page, through which the user can configure the VLAN interface, delete the VLAN interface, configure the IP address of the interface, delete the IP address of the interface, and view the interface information. A VLAN can only be set as an interface if it already exists, and an interface address can only be configured on an already set interface.

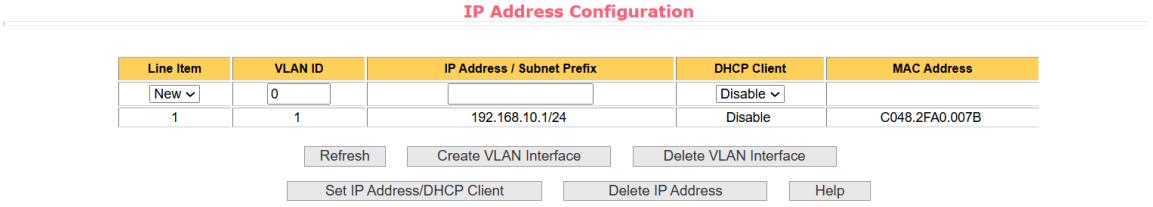


Figure 10-1 VLAN Interface Configuration Page

Managed switches have a VLAN 1 interface by default, which cannot be deleted. Only one interface can be configured for a VLAN.

(2) ARP configuration and display

Figure 10-2 is the ARP configuration and display 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 Add.

When deleting an ARP entry, the user can select to delete an ARP entry of an IP, delete an ARP entry of a network segment, delete all ARP entries, delete all dynamic ARP entries, and delete all static ARP entries. To delete the ARP table entry of an IP or delete the ARP table entry of a network segment, enter the specified IP address or IP network segment in the input box. Then click the delete button.

When the dynamic ARP table entry is modified into the static ARP table entry, the dynamic ARP table entry in a certain network segment or all the dynamic ARP table entries can be modified into the static ARP table entry. In the case of a certain network segment, you need to enter the specified network segment in the input box. Then click the Apply button.

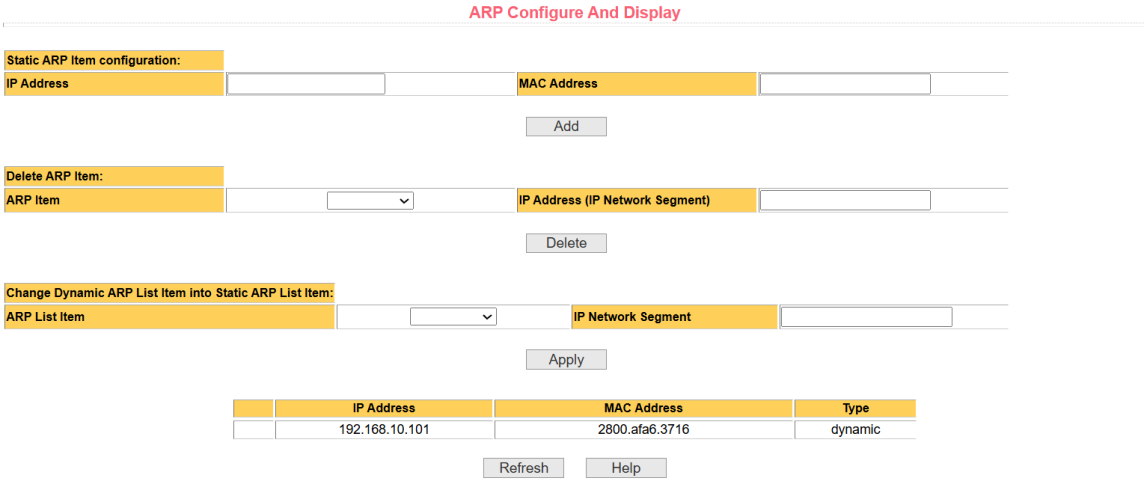


Figure 10-2 ARP Configuration and Display Page

(3) Host static route configuration

Figure 10-3 is the host static route configuration page, through which the user can add or delete the host static route of the switch. By default, the switch is not configured with a host static route. The user can use this page to configure a default route, that is, a route with a destination address/subnet prefix of 0.0.0.0/0.

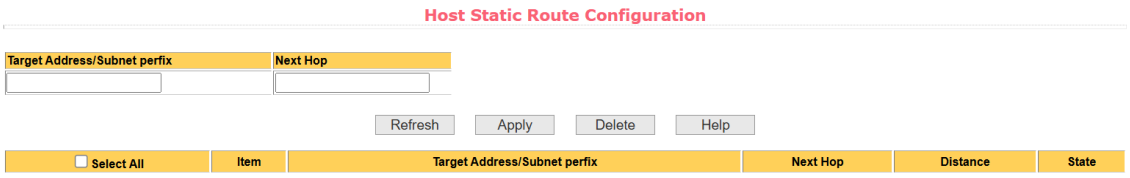


Figure 10-3 Host Static Route Configuration Page

11. AAA Configuration

(1) AAA Authentication

Figure 11-1 is the AAA authentication configuration interface, through which the user can select the authentication type.

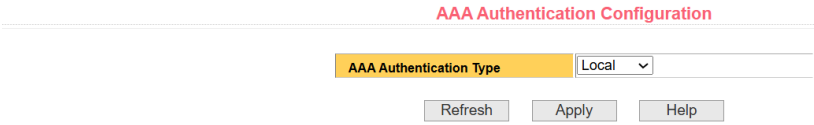


Figure 11-1 AAA Authentication Configuration Page

(2) Tacacs + Configuration

Figure 11-2 shows the Tacacs + configuration page. Users can configure information related to Tacacs +. The information that can be set includes: enabling Tacacs + functions, configuring the IP address of the Tacacs + server, the authentication type, and the shared secret key.

The Tacacs + feature must be enabled before it can be used. The default configuration is not enabled.

Configure the IP address of the Tacacs + server. This field must be set when using Tacacs + functionality.

Authentication type: PAP and CHAP authentication types are provided, and the default configuration is PAP authentication.

The shared key is used to set the encrypted shared password between the switch and the Tacacs + server. This field must be set during authentication and authorization, and must be the same as the setting on the Tacacs + server

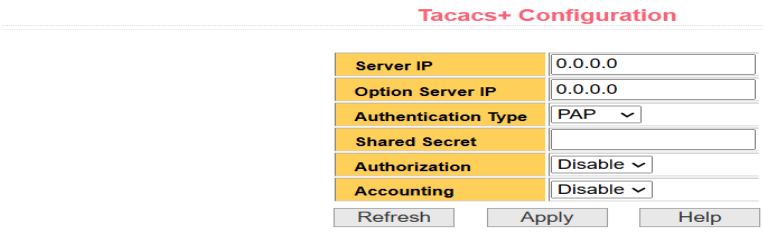


Figure 11-2 Tacacs + Configuration Page

(3) Radius Configuration

Figure 11-3 is the Radius configuration page. The user can configure the information related to Radius. The settable information includes:

- IP address of Radius server. This field must be set during authentication and accounting.
- Optional Radius Server IP Address. This field can be set if there is an alternate radius server.
- Authentication UDP port. The default value is 1812. Users generally do not need to modify this field.
- Whether to start charging? It is started by default. Charging is generally started during authentication charging.
- Billing UDP port, default value is 1813.
- 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.
- Vendor specific information. Users generally do not need to modify this field.
- NAS port, NAS port type, and NAS service type. Users generally do not need to modify these three values.
- Whether Radius roaming is turned on or off.

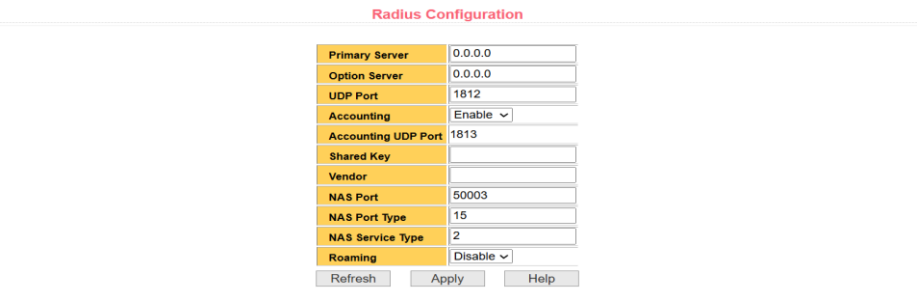


Figure 11-3 Radius Configuration Page

(4) 802.1x configuration

Figure 11-4 is the 802.1x configuration page, through which the user can configure some information related to 802.1x, mainly including:

- Whether to start the 802.1x protocol? The 802.1x protocol must be started during authentication and accounting.
- Whether the switch uses general authentication or extended authentication.
- Whether to turn on the re-authentication function is not turned on by default, and it is determined according to the actual situation when making authentication billing. Turning on the re-authentication function will make users more reliable when using authentication billing, but it will slightly increase the traffic of the network.
- Set the re-authentication time interval, which is valid only when the re-authentication function is enabled. The default is 3600 seconds. Set the value according to the actual situation when performing authentication billing, but the value should not be too small.
- Quiet Period timer. Users generally do not need to modify this field.
- Tx-Period timer. Users generally do not need to modify this field.
- Server timeout timer. Users generally do not need to modify this field.
- For the supplicant timeout timer, the user generally does not need to modify this field.
- The number of Max Requests. Users generally do not need to modify this field.
- Displays the Reauth Max size.
- Client Version. The client version number.
- Check Client, whether to check the timing traffic packet of the client after passing the authentication.

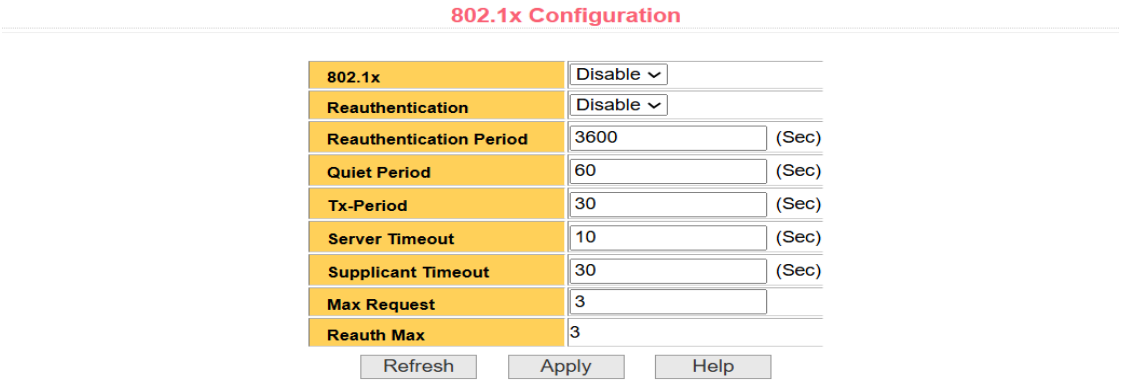


Figure 11-4 802.1x Configuration Page

(5) 802.1x Port Configuration

Figure 11-5 is the X port configuration page of the 802.1. Through this page, the user can configure the X port mode of the 802.1 and the maximum number of hosts supported, and view the X configuration of the 802.1 of each port. 802.1x port modes include four types: N/A state, Auto state, Force-authorized state, and Force-unauthorized state.

When 802.1 X 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.

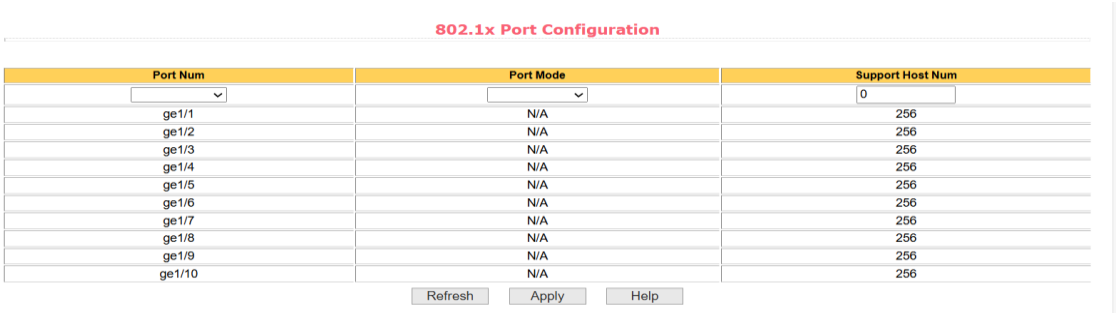


Figure 11-5 802.1x Port Configuration Page

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

maximum of 256 hosts.

(6) 802.1x user authentication information

Figure 11-6 is the 802.1x user authentication information page, through which the user can view the status information of all users connected to a port

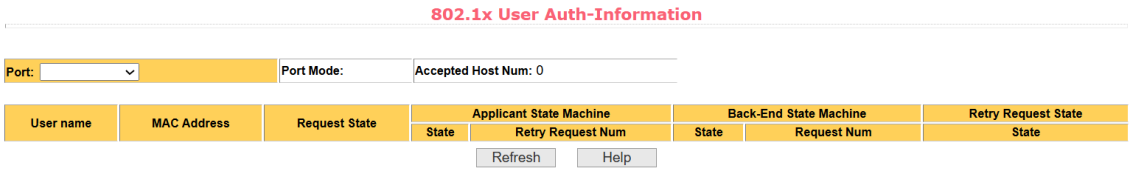


Figure 11-6 802.1x User Authentication Information Page

12. MSTP configuration

(1) Global Configuration

Figure 12-1 shows the MSTP global configuration page, through which the user can configure global MSTP parameters.

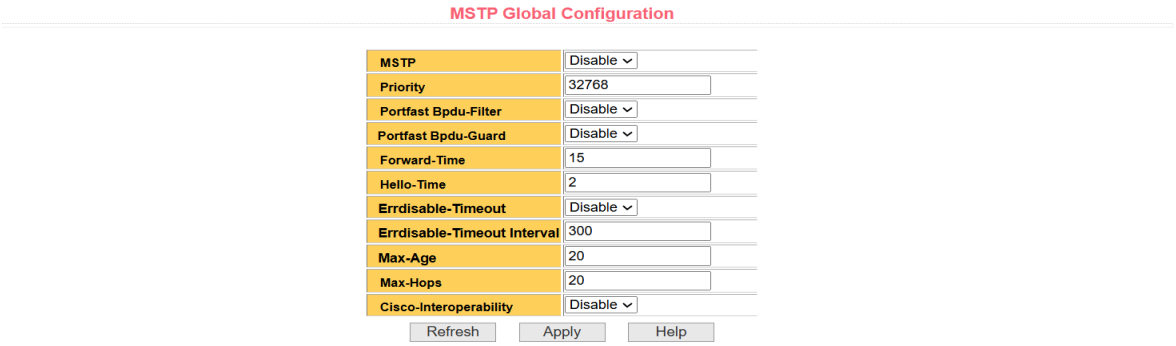


Figure 12-1 MSTP Global Configuration Page

(2) Port configuration

Figure 12-2 shows the MSTP port configuration page, through which the user can configure the port MSTP parameters.

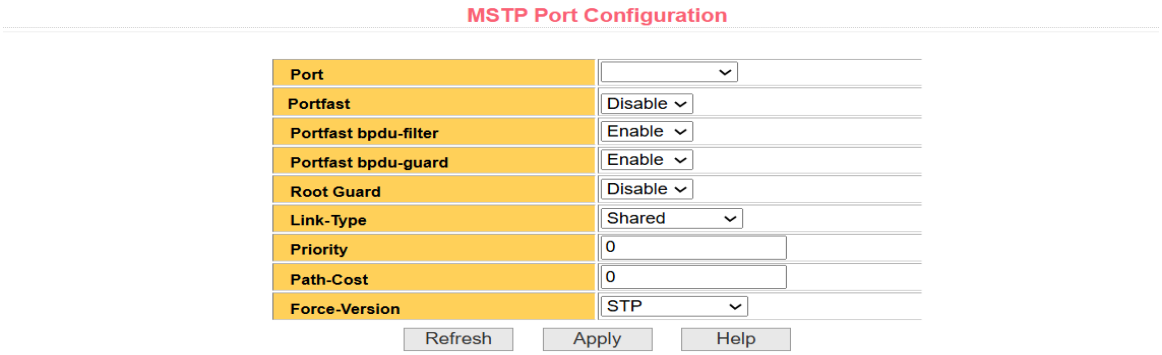


Figure 12-2 MSTP Port Configuration Page

(3) Port information

Figure 12-3 is the MSTP port information page, through which the user can view the specific status of the port MSTP.

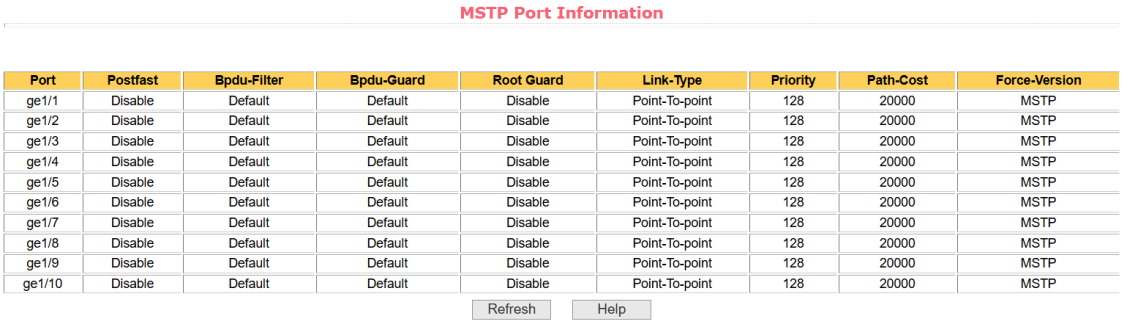


Figure 12-3 MSTP Port Information Page

13. IGMP SNOOPING configuration

(1) IGMP SNOOPING Configuration

Figure 13-1 shows the IGMP SNOOPING configuration page, which allows the user to enable IGMP SNOOPING.

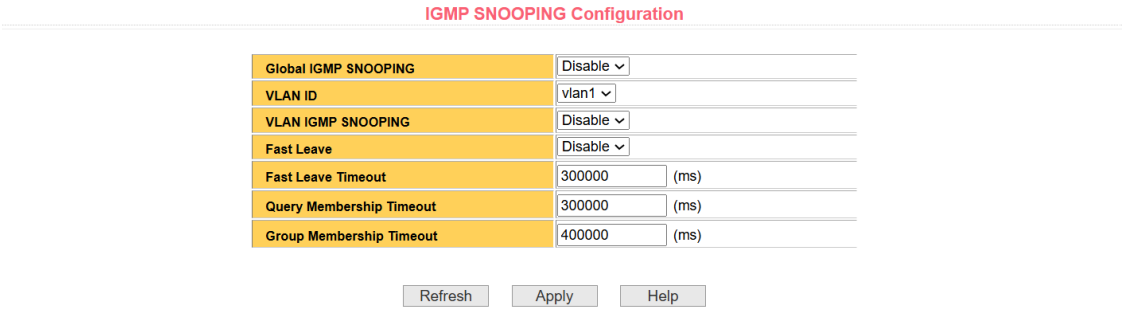


Figure 13-1 IGMP SNOOPING Global Configuration Page

(2) Multicast group information

Figure 13-2 is the multicast group information page, through which the user can view the IGMP snooping multicast program information.

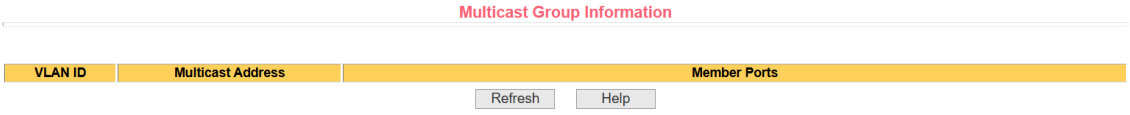


Figure 13-2 Multicast Group Information Page

14. GMRP Configuration

(1) GMRP Global Configuration

Figure 14-1 shows the GMRP global configuration page, which allows the user to enable GMRP.

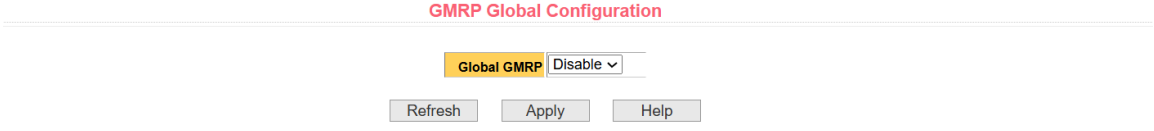


Figure 14-1 GMRP Global Configuration Page

(3) GMRP Ports Configuration

Figure 14-2 shows the GMRP port configuration page, through which the user can enable the port GMRP and view the port information.

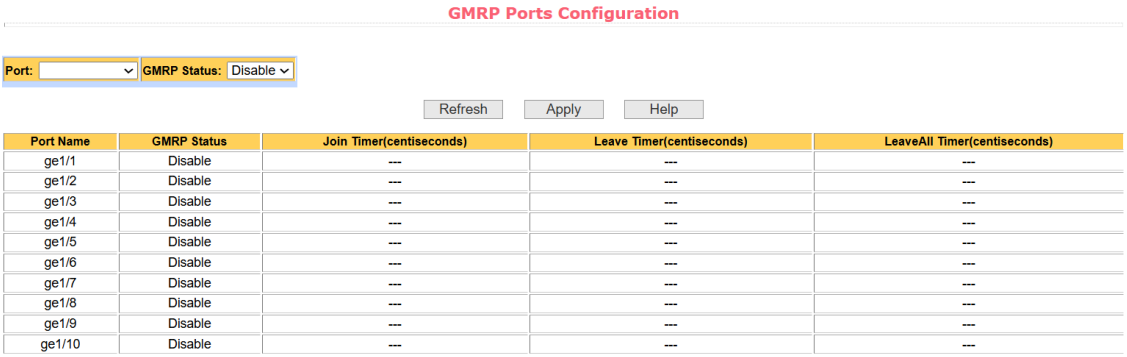


Figure 14-2 GM RP Ports Configuration Page

(3) GMRP State Machine

Figure 14-3 is the GMRP state machine page, through which the user can view the state machine information established by GMRP.

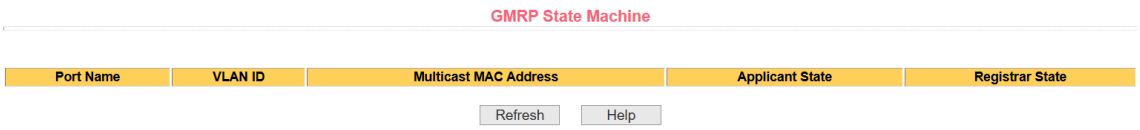


Figure 14-3 GMRP State Machine Page

15. GVRP Configuration

(1) GVRP Global Configuration

Figure 15-1 shows the GVRP global configuration page, which allows the user to enable GVRP.

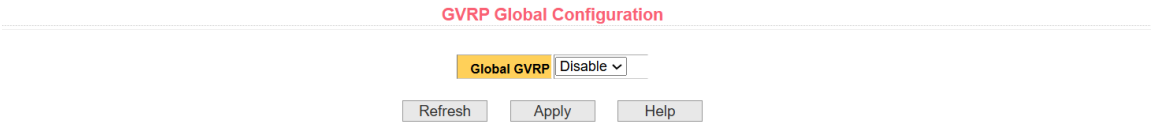
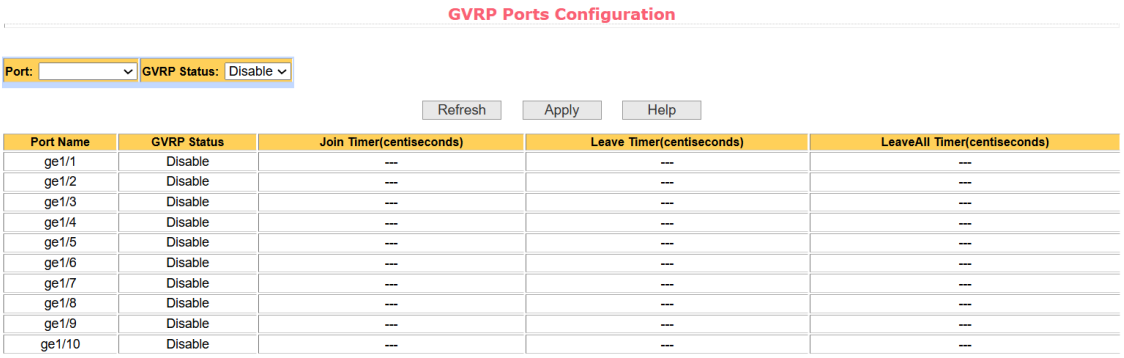


Figure 15-1 GVRP Global Configuration Page

(1) GVRP Ports Configuration

Figure 15-2 shows the GVRP port configuration page, through which the user can enable port GVRP and view port information.



Port Name	GVRP Status	Join Timer(centiseconds)	Leave Timer(centiseconds)	LeaveAll Timer(centiseconds)
ge1/1	Disable	---	---	---
ge1/2	Disable	---	---	---
ge1/3	Disable	---	---	---
ge1/4	Disable	---	---	---
ge1/5	Disable	---	---	---
ge1/6	Disable	---	---	---
ge1/7	Disable	---	---	---
ge1/8	Disable	---	---	---
ge1/9	Disable	---	---	---
ge1/10	Disable	---	---	---

Figure 15-2 GVRP Ports Configuration

(1) GVRP state machine

Figure 15-3 is the GVRP state machine page, through which the user can view the state machine information established by GVRP.

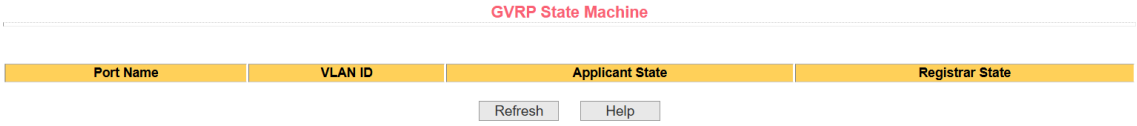


Figure 15-3 GVRP State Machine

16. EAPS Configuration

(1) EAPS Configuration

Figure 16-1 This page is used to create and configure EAPS information. It can also be used 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. If not created, you need to create first.

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

Master port EAPS master port, e.g. fe1/1, ge1/1 Alternate

port: EAPS second port

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

VLAN: EAPS ring protected VLAN

Hello Time Interval The time interval between the sending of Hello messages. 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 Disable state.

Enable Status: Displays whether EAPS is enabled or disabled.

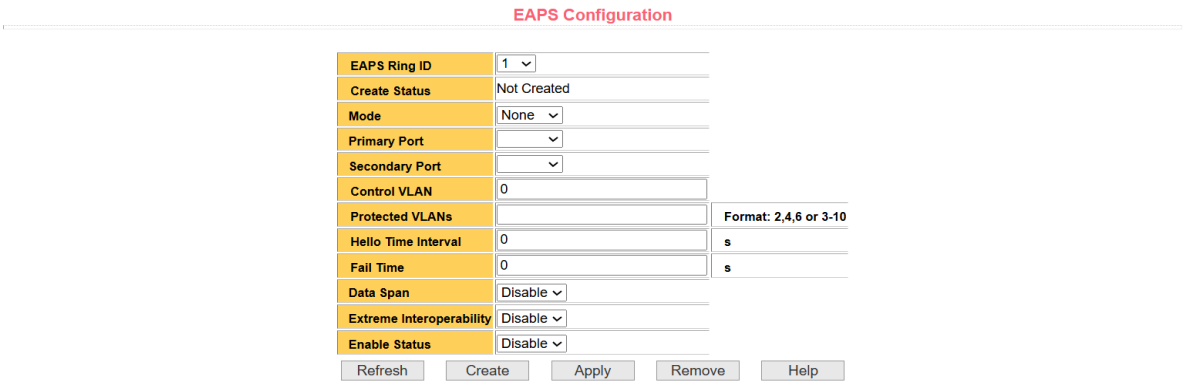


Figure 16-1 EAPS Configuration Page

(1) EAPS Information

Figure 16-2 shows the EAPS information page, through which the user can view the EAPS configuration information.

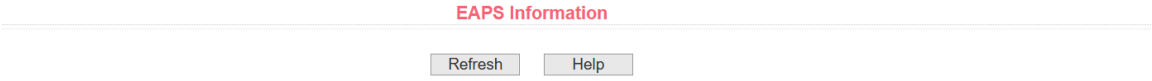


Figure 16-2 EAPS Information Page

17. RMON Configuration

(1) Statistics Configuration

Figure 17-1 shows the RMON Statistics Group Configuration page, which allows the user to configure the RMON Statistics Group. Select a port from the drop-down list to view the RMON statistics group configuration that configures that port. When it is not configured, the index number is 0. Fill in the correct index number (range is 1 to 100). The owner is optional. You can configure the RMON statistics group for this port. The Statistics table displays port statistics from the time the configuration was

successful.

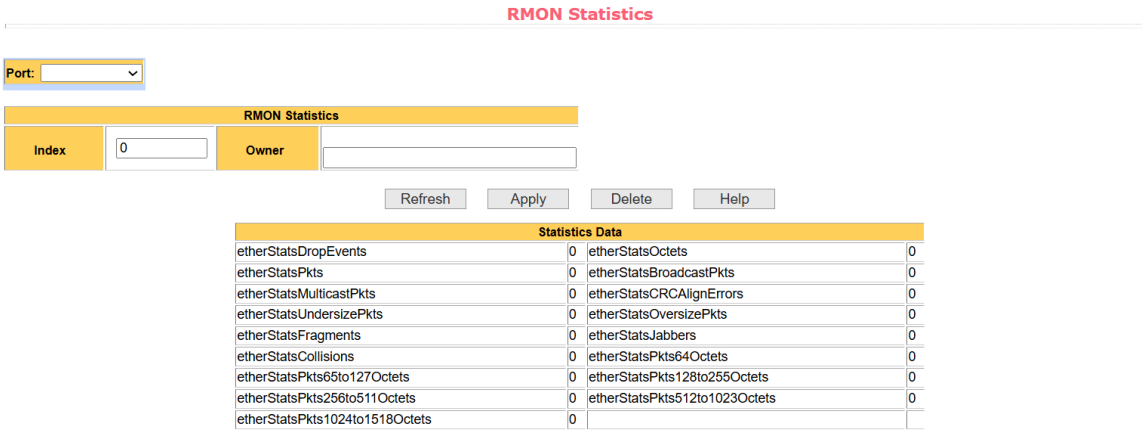


Figure 17-1 RMON Statistics Group Configuration Page

(1) History Configuration

Figure 17-2 shows the RMON history group configuration page, through which the user can configure the RMON history group. Select a port from the drop-down list to view the RMON History Group configuration that configures that port. If it is not configured, the index number is 0. Fill in the correct index

number (the range is 1 to 100). Interval, Request Buckets, and Owner are optional. You can configure the RMON history group for this port. Interval refers to the time interval for collecting data, in seconds, ranging from 1 to 3600. Request Buckets is the allocated storage size, indicating how many records are stored, ranging from 1 to 100. The statistics table displays the historical data that has been collected since the successful configuration.

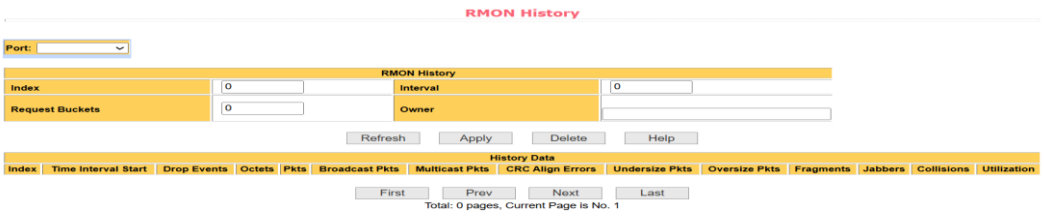


Figure 17-2 RMON History Group Configuration Page

(1) Alarm Configuration

Figure 17-3 shows the RMON Alert Group Configuration page, which allows the user to create or modify RMON Alert Groups. Select a configured alert group from the drop-down list to view/configure its information, or select New to create one. The index number range is 1 to 60, the interval range is 1 to 3600, and the unit is second. The monitoring object must fill in the MIB node. The comparison method can be absolute (absolute value) or delta (delta). In addition, the upper and lower threshold values and the event index must be filled in. The owner is optional. The alarm value is read-only and displays the sampled value when the alarm was last raised. The event index refers to the index number of the RMON event group, which must be configured in advance.

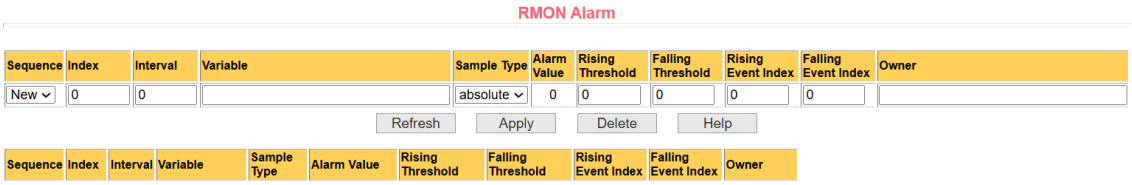


Figure 17-3 RMON Alarm Group Configuration Page

(1) Event Configuration

Figure 17-4 shows the RMON Event Group Configuration page, which allows users to create or modify RMON event groups. Select a configured event group from the drop-down list to view/configure its information, or select New to create one. The index number range is 1 to 60. The description is in the form of a string. The action can select none, log, snmp-trap, or log-and-trap. The community name has no effect in this device. The owner is optional. Last Sent Time is read-only and displays the last time the event was sent.

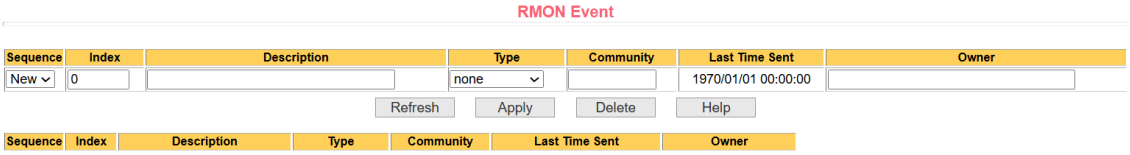


Figure 17-4 RMON Event Group Configuration Page

18. Cluster Management

(1) NDP configuration

Figure 18-1 shows the NDP configuration page, through which the user can configure the NDP. The information that can be set includes: selecting the port, enabling the port NDP function, enabling the global NDP function, the time interval for sending NDP messages, and the aging time of NDP messages on the receiving device.

Port selection: select the port as required and enable the NDP function of the port. For NDP to function properly, both global and port NDP functions must be enabled.

Configure the aging time of NDP message sent by the equipment on the receiving equipment. The effective time range is 1-4096 seconds, and the default configuration is 180 seconds.

Configure the time interval for sending NDP message. The effective time range is 1-4096 seconds, and the default configuration is 60 seconds.

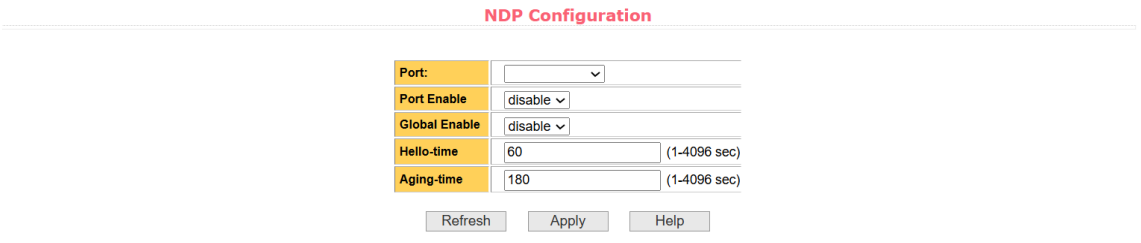


Figure 18-1 NDP Configuration Page

(2) NTDP Configuration

Figure 18-2 shows the NTDP configuration page, which allows the user to configure NTDP. Information that can be set includes: selecting a port, enabling the port NTDP function, enabling the global NTDP function, the scope of topology collection, the time interval for timing topology collection, the delay time for forwarding a packet on the first port, and the delay time for forwarding a packet on other ports.

Port selection: select the port as required and enable the NTDP function of the port. For NTDP to function properly, both the global and port NTDP features must be enabled.

Configure the range of topology collection. The valid range is 1-6. In the default configuration, the farthest device in the collected topology has a maximum hop count of 3 from the topology collection device.

Configure the time interval for scheduled topology collection. The valid range is 0-65535 minutes. The default configuration is 1 minute.

Configure the delay time for the first port to forward the message. The effective range is 1-1000 milliseconds, and the default configuration is 200 milliseconds.

Configure the delay time for the first port to forward the message. The effective range is 1-100 milliseconds, and the default configuration is 20 milliseconds.

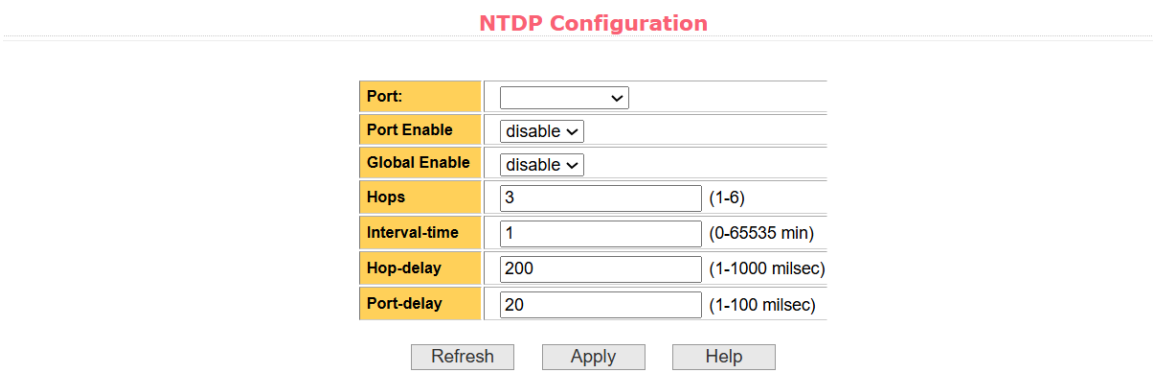


Figure 18-2 NTDP Configuration Page

(3) Cluster configuration

Figure 18-3 shows the cluster configuration page, which allows the user to configure the cluster and view the cluster member table. Information that can be set includes: enabling the cluster function, configuring the management VLAN, the address pool of the cluster, the time interval for sending the handshake message, the effective retention time of the device, the cluster name, the way to join the cluster, and deleting the cluster.

Enable the cluster feature. The cluster feature must be enabled for it to function properly.

Configure the management VLAN. The valid range is 1-4094. The default configuration is vlan1.

Configure the private IP address range used by the member devices in the cluster. The valid range of the IP address is 0.0.0.0 ~ 255.255.255.255, and the valid range of the mask length is 0~32.

Configure the time interval for sending the handshake message. The effective range is 1-255 seconds, and the default configuration is 10 seconds.

Configure the valid retention time of the device. The valid range is 1-255 seconds. The default configuration is 60 seconds.

To establish a cluster, you need to configure the cluster name and select the way to join the cluster. There are two ways to join the cluster: manual and automatic. After the cluster is established, automatic can be switched to manual, but manual cannot be switched to automatic. The cluster name can be changed manually.

After the cluster is established, member devices and candidate devices can be viewed in the cluster member table, and member devices can be deleted or candidate devices can be added to member devices according to roles.

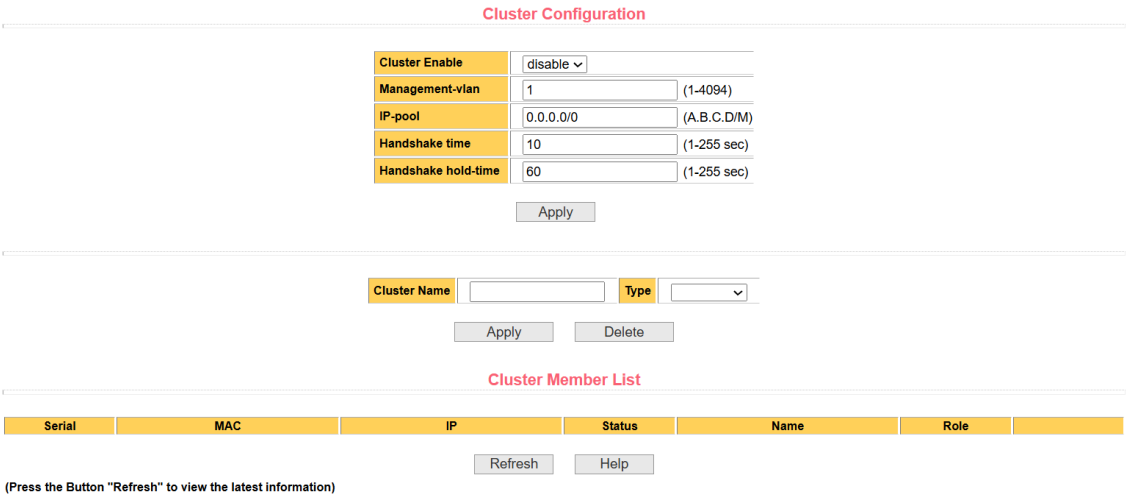


Figure 18-3 Cluster Configuration Page

19. ERPS Configuration

(1) ERPS Configuration

Figure 19-1 is the ERPS configuration page. Users can use this page to enable ERPS functions, configure ERPS parameters, create and delete ERPS instances, ERPS rings and other applications.

ERPS instances: creating and deleting ERPS instances (< 1-8 >)

ERPS Instance Node Role: Configure the role of the node in the ERPS ring, interlink node or non-interlink nodes

ERPS Ring Numbers: Creating and Deleting ERPS Rings (< 1-32 >) Ring mode: configure the ERPS ring mode, the main ring or the sub-ring Ring node mode: configure the ERPS ring node mode, RPL owner node, RPL neighbor node, or normal ring node

Protocol VLAN: Configure and delete the ERPS ring protocol VLAN (< 2- 4094 >)

Data VLAN: Configure the ERPS ring data VLAN (< 1-4094 >)

Ring port: configure and delete ERPS ring port, RPL port or normal ring port

Recovery behavior: Configure the recovery behavior of the ERPS ring, recoverable or non-recoverable

Hold-off time: configure ERPS ring hold-off time (< 0-10000 >), unit: ms, default: 0

Guard time: configure ERPS ring guard time (< 10-2000 >), unit: ms, default: 500

WTR time: configure the WTR time of ERPS ring (< 1-12 >), unit: min, default: 5

WTB time: configure the WTB time of ERPS ring (< 1-10 >), unit: sec, default: 5

Protocol message sending time: configure the ERPS ring protocol message sending time (< 1-10 >), unit: sec, default is 5

Enable ERPS ring: Turn ERPS ring on or off

Force switch ERPS ring port: Force, clear switch ERPS ring port Force

Manual ERPS Ring Port: Force, Clear Manual ERPS Ring Port

Manual recovery, manual recovery when unrecoverable behavior of ERPS ring is cleared, or manual recovery before WTR/WTB expires

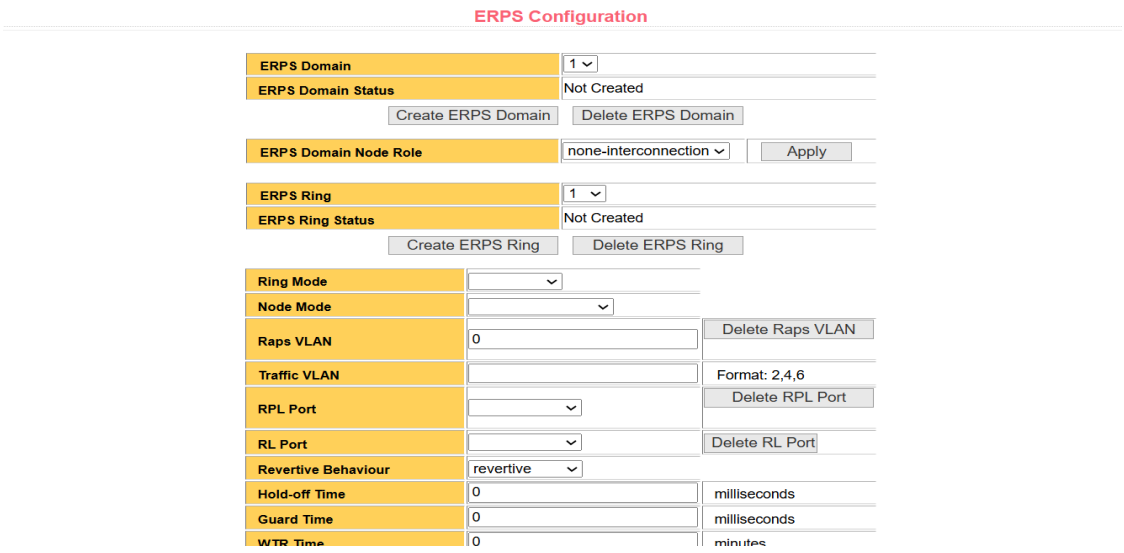


Figure 19-1 ERPS Configuration Page

(2) ERPS Information

Figure 19-2 is the ERPS information page that allows users to view ERPS configuration information.

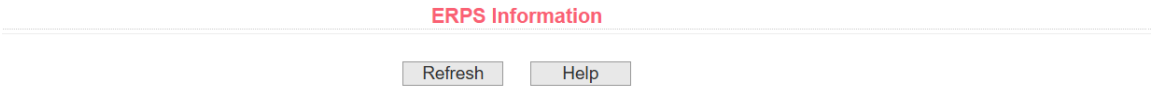


Figure 19-2 ERPS Information Page

20. LLDP Configuration

(1) LLDP global configuration

Figure 20-1 shows the LLDP global configuration screen, which is used to display and configure global LLDP parameters.

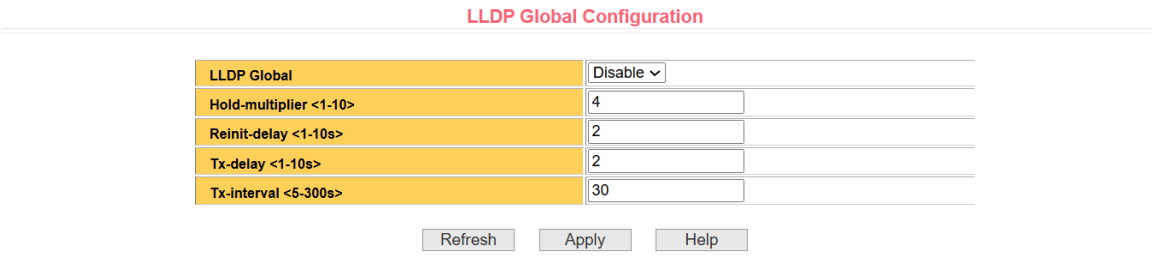


Figure 20-1 LLDP Global Configuration Part

(1) LLDP Ports Configuration

Figure 20-2 shows the LLDP port configuration screen, which is used to display and configure LLDP port parameters.

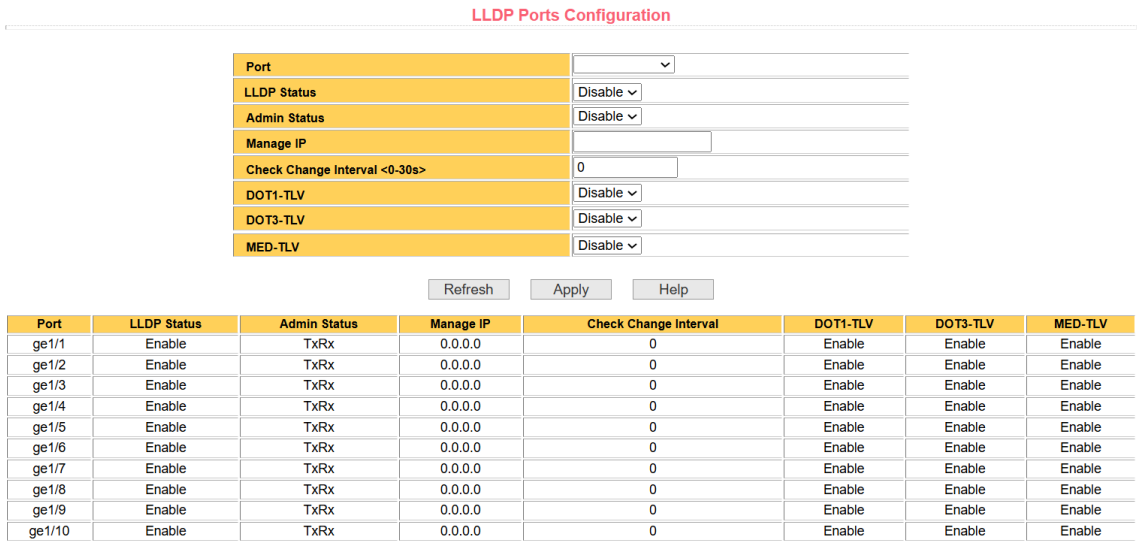


Figure 20-2 LLDP Ports Configuration Part

(1) LLDP Neighbor

Figure 20-3 This page is LLDP information. This page is used to display and configure LLDP port parameters.

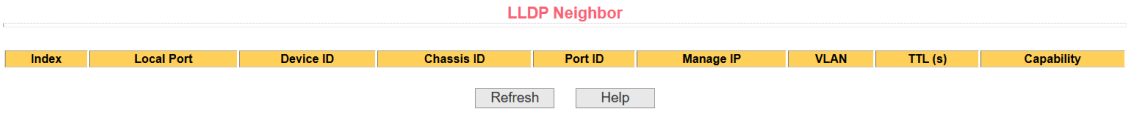


Figure 20-3 LLDP Neighbor Table Part

21. Log Management

(1) Log Configuration

Figure 21-1 shows the log information page through which the user can view the log. Select the log priority from the drop-down list to view the log of this level. Click Refresh to view the latest log.

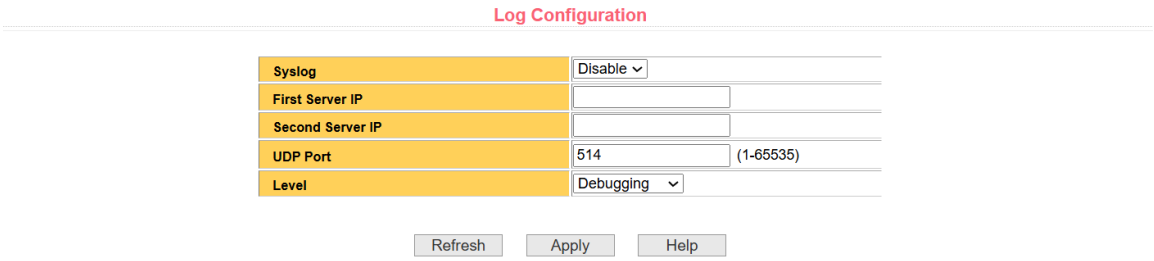


Figure 21-1 Log Configuration Page

(1) Log Information

Figure 21-2 shows the log information page through which the user can view the log. Select the log priority from the drop-down list to view the log of this level. Click Refresh to view the latest log.

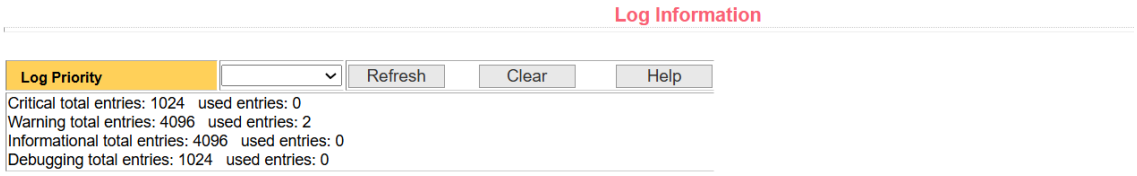


Figure 21-2 Log Information Page

22. POE Port Configuration

(1) POE Port Configuration

Figure 22-1 is the POE port configuration page, through which you can configure 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

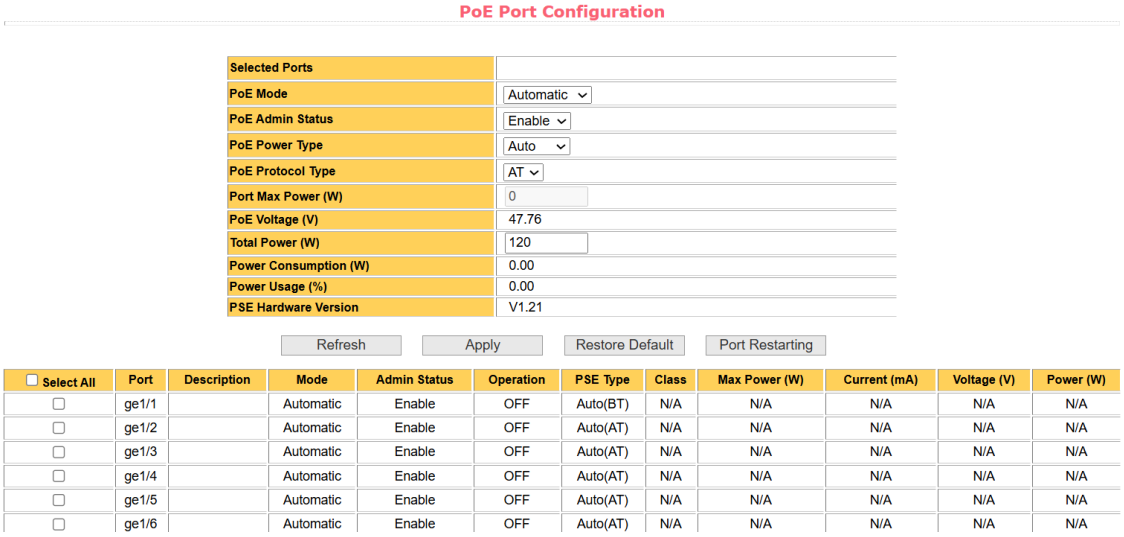


Figure 22-1 POE Port Configuration Page

(1) POE Policy Configuration

Figure 22-2 is the POE policy 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

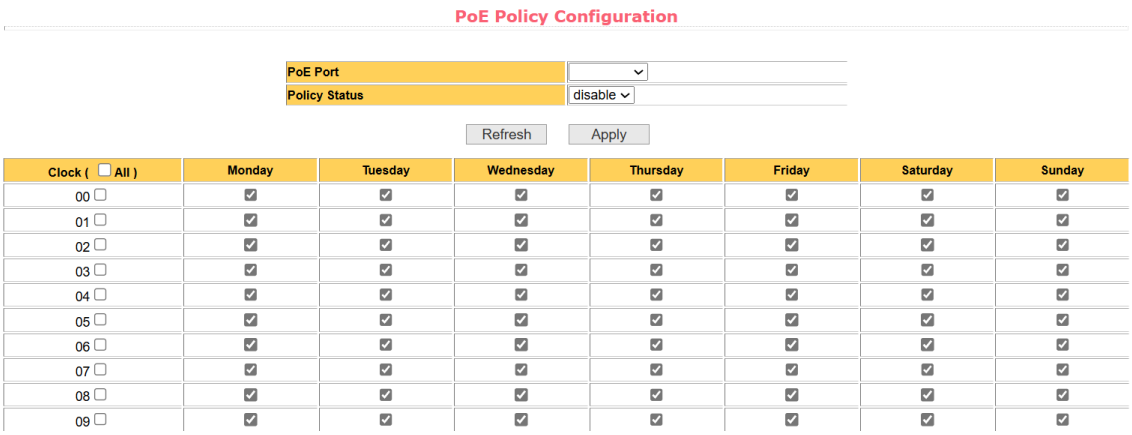


Figure 22-2 POE policy Configuration Page

(1) PD Query Configuration

Figure 22-3 shows the PD query configuration page, through which the PD online device status detection can be realized.

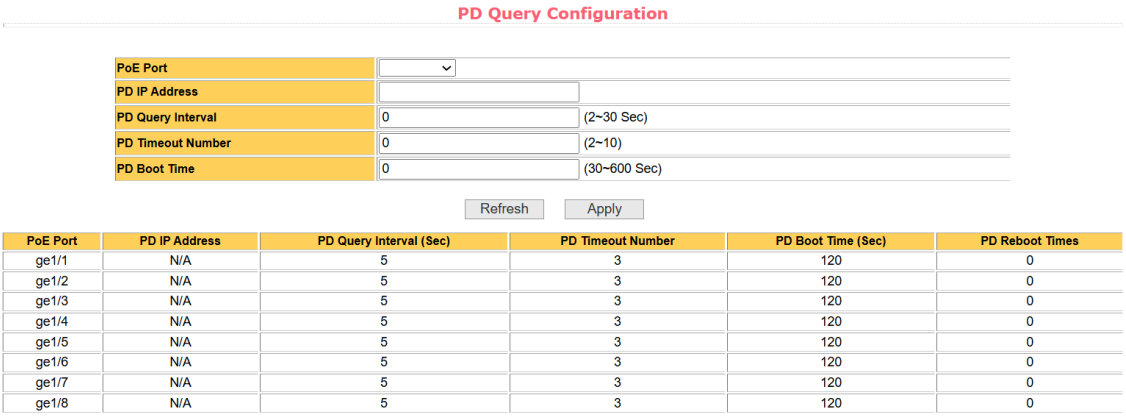
POE port: used to select the port to be queried and connected to the PD device

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 (120 seconds by default)



PoE Port	PD IP Address	PD Query Interval (Sec)	PD Timeout Number	PD Boot Time (Sec)	PD Reboot Times
ge1/1	N/A	5	3	120	0
ge1/2	N/A	5	3	120	0
ge1/3	N/A	5	3	120	0
ge1/4	N/A	5	3	120	0
ge1/5	N/A	5	3	120	0
ge1/6	N/A	5	3	120	0
ge1/7	N/A	5	3	120	0
ge1/8	N/A	5	3	120	0

Figure 22-3 PD Query Configuration Page