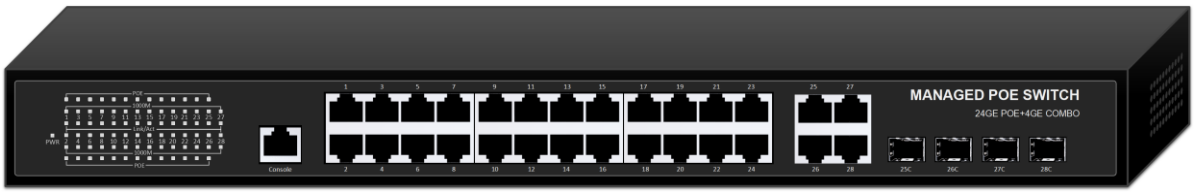
FLEXPORT TECNOLOGIA QUE CONECTA

Layer 2 Network Management

WEB Operation Guide



Ver 1.0.1

TEL: (19) 3876-1901
(19) 3876-5038
EMAIL: vendas@flexport.com.br
SITE: www.flexport.com.br

Declaration

Version Update

Ver 1.0.1

User experience optimization

Resolves known issues and provides faster response.

Perfect support for one-key conversion between Chinese and English.

Related functions are optimized to make management easier.

CONTENT

Figure Content

Product Introduction

The all-gigabit managed Ethernet switch is independently designed and developed by our company, 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 802.3q, IEEE 802.3q/p
- Supports IEEE 802.1w, IEEE 802.1d, EEE 802.1S
- Support 16K 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 EPPS 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 Snoping
- 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

1. Overview of WEB

1.1. 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-gigabit managed Ethernet 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.

1.2. System requirements for WEB browsing:

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®, WindowsVista®, Windows7®, Windows8®, Windows10® Windows11®, MAC, Linux, Unix-like operating system

Table 1: The system requirements for Web browsing

Note : Microsoft®, Windows95®, Windows98®, WindowsNT®, Windows2000®, WindowsXP®, Windows ME®, WindowsVista®, 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.

1.3. Login WEB

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

a. The switch has been configured for IP.

- **The default IP address for VLAN1 is 192.168.0.1**
- **The subnet mask is 255.255.255.0**

b. A host with a Web browser has been connected to the network and is able to ping to the switch.

c. Enter the IP address

d. Enter the user name and password.

- **The default user name: admin**

- **The default user password: admin**

Passwords are case-sensitive, and passwords can be up to 16 characters.

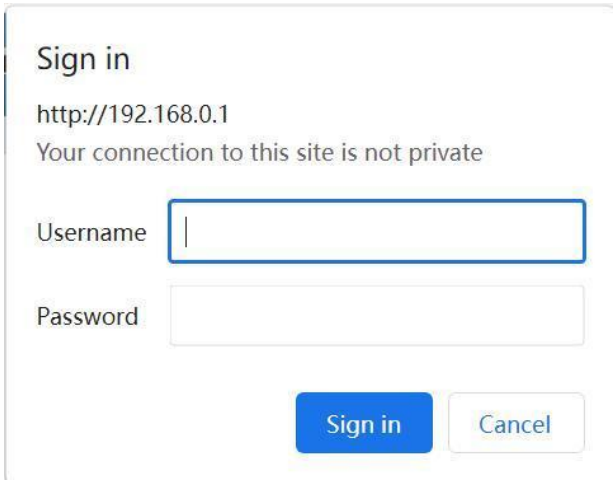


Figure 1: Login page for WEB browsing session

1.4. WEB page structure

There are 3 areas on the page: title area, navigation tree area and main area.

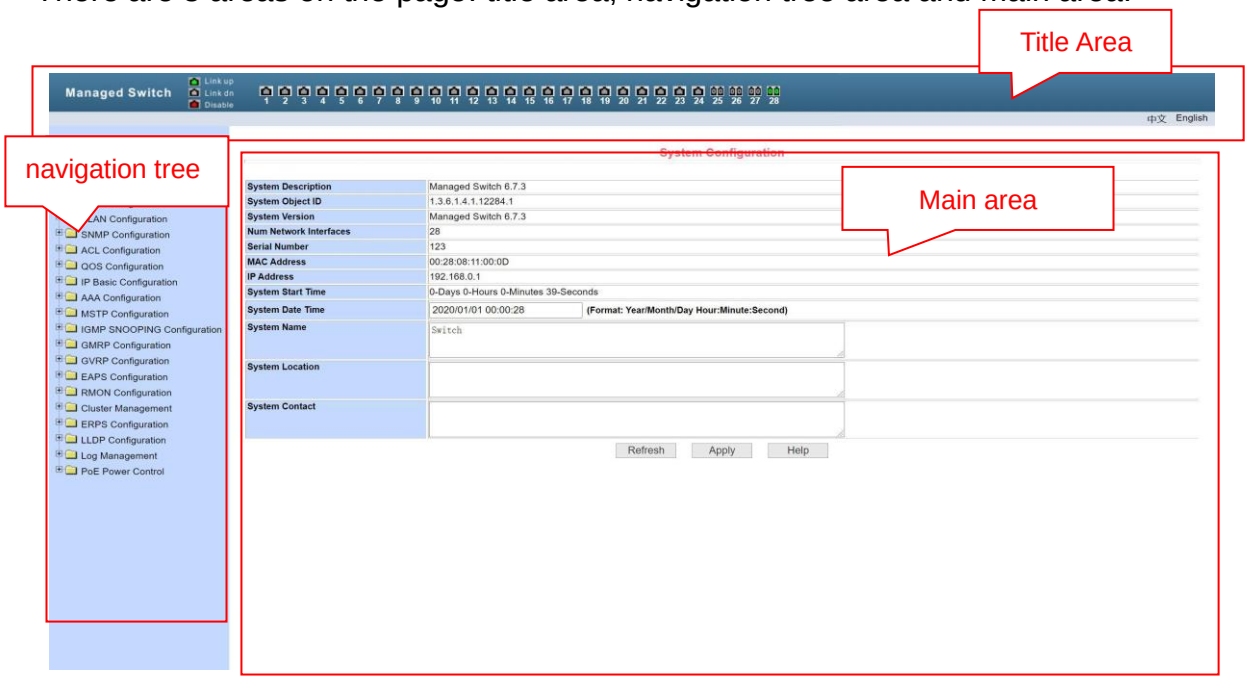


Figure 2: WEB page structure

Title area: used to display the logo and the real-time port status

Figure 3: Title area

- 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)

Navigation Tree: Refer to 1.5.
Main Area: Displays the page that the user selects from the navigation tree.

1.5. Navigation Tree Structure

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.

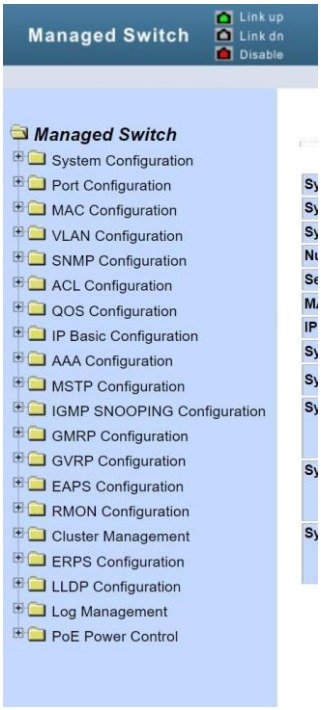


Figure 4: Organization page of the switch navigation tree

1.6. Introduction to Page Button

There are some common buttons on different pages, and the function is the same.

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

1.7. Error Message

If an error occurs while the switch 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 5: Error Information Page

1.8. Entry Field

Some pages have an entry field in the leftmost column of the table, 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 6: Entry Domain Page

1.9. State Field

Some pages have a status field in the rightmost column of the table, 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 7: Status Field Page

2. WEB configuration

2.1. Language switching

Language switching: via the language switching button in the upper right corner, you can easily switch between Chinese and English system interfaces.

Figure 8: 2.3.Language switching

2.2. System configuration

2.2.1. Basic Information

Figure 9: Basic Information

- 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.

2.2.2. Serial Information

Through this page, you can view the configuration information of the switch serial port.

Figure 10: Serial Port Configuration

2.2.3. User Management

Enable / Disable multi user management function

The multi user management function is disabled by default.

The default user “admin” doesn’t work when multi user management function is enabled.

- Telnet:
  Enable multi user management function by adding user name;
  Disable multi user management function by deleting all user names.
- WEB:
  Enable multi user management function by adding privilege user name;
  Disable multi user management function by deleting all privilege user names.

Change the password

Enter the new password twice, and click the “apply” button, the new password is activated.

Figure 11: Multi-user Management Configuration

2.2.4. Safe management

The administrator can enable or disable the network management services TELNET, WEB and SNMP, link the service to the IP standard ACL group , and control the access of the source IP addresses.
By default, the TELNET, WEB, and SNMP services are enabled without ACL filtering. All hosts can access these three services of the switch.

You can allow only specific host to access one or more of these services by configuring the ACL group of the services. You need to create the ACL group firstly before entering the group number (1-99) here.

If the WEB service is disable, you can not log in WEB. If you want to log in WEB again, you need to

log in the switch by other methods and enable WEB service here.

Figure 12: User Safety Configuration

2.2.5. SNTP configuration

You can set and view the system clock here.

Figure 13: SNTP Configuration

2.2.6. Jumbo Frame Configuration

You can configure the switch frame. The frame number range from 1522 to 16383) .

Figure 14: Jumbo Frame Configuration

2.2.7. Save Current configuration

You can view and safe the current configuration.

By clicking “save” button, you can save the current configuration of the system to the configuration file. It will take some while for this process. Don’t exit the page when saving.

Click save button if you want to keep the current configuration after restart the switch.

Figure 15: Current Configuration

2.2.8. Configuration file

You can download and delete the configuration file.

You can view the initial configuration of the system stored in FLASH. When there is no configuration file in FLASH, the default configuration is used when the system is started.
The delete button is used to delete the configuration file in FLASH. Click the delete button, and a dialog box will pop up in which you need to confirm to delete the configuration file.
The download button is used to download the configuration file to the PC. Click the download button, a dialog box will pop up, and you need to select the directory path and save the configuration file. The file name of the downloaded configuration file is the “switch.cfg”.

Figure 16: Configuration File

2.2.9. File upload

You can upload configuration files or firmware files to the switch.
Click “choose file” button, and choose the file from the PC.
Click “Upload” button to upload the file.
The suffix of the configuration file must be *.cfg.
The firmware file must be provided by the manufacturer and the suffix of the file name must be *.img.
DO NOT exit the page or power off the switch when the file is uploading. Otherwise, the file transferring will fail and the system will crash.

Figure 17: File Upload

2.2.10. System Reboot

Click “Reboot” button to reboot the switch.
Click “Reboot Factory” button to reboot the switch to the initial configuration.

Figure 18: System Reset Page

2.3. Port configuration

2.3.1. Common configuration

You can 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.

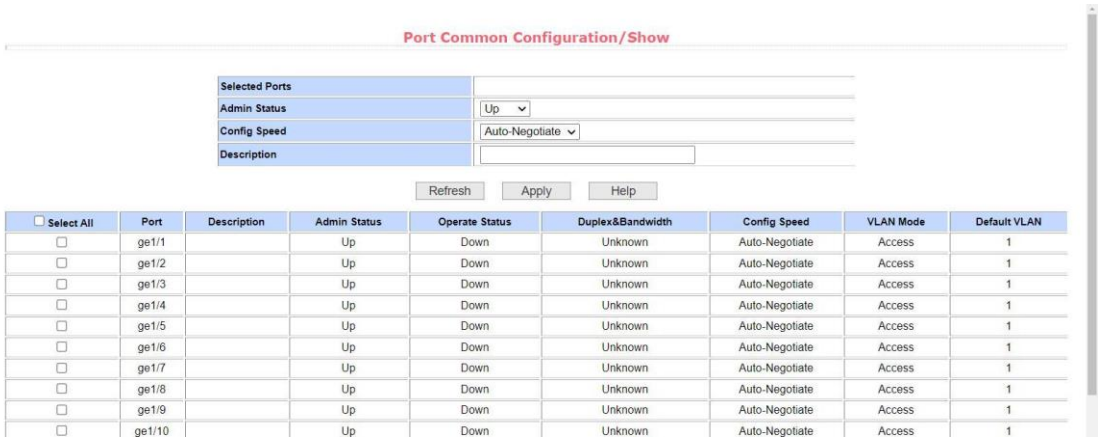


Figure 19: Port Configuration and Port status

2.3.2. Port Statistics

You can view the statistics of packets sent and received by the port.
To view a particular port by select the appropriate port name from the drop-down menu.

Figure 20: Port Statistics

2.3.3. Flow Control

You 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 21: Flow Control

2.3.4. Broadcast Storm

You can 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.

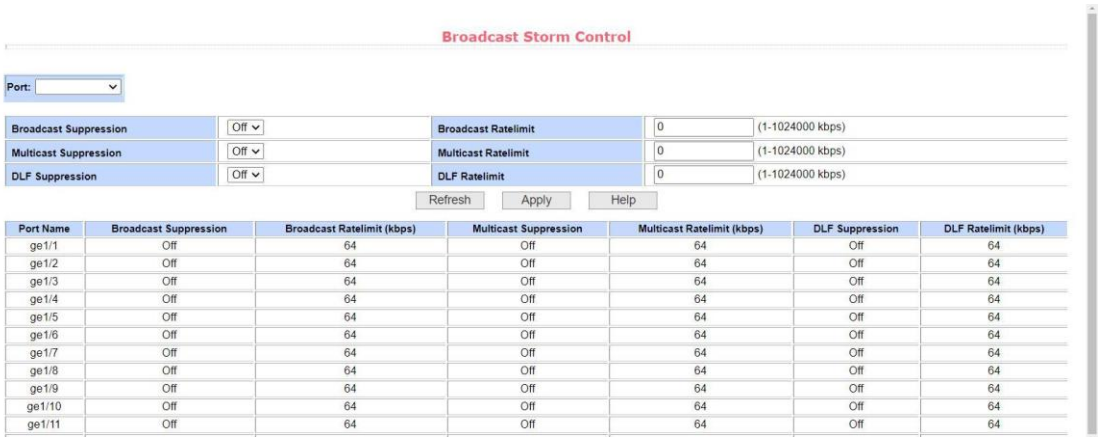


Figure 22: Broadcast Storm Control

2.3.5. Port rate limit

You can configure the sending and receiving rate of the port.

Select the port to be configured from the drop-down bar of the port. The bandwidth 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 23: Port Speed Limit Page

2.3.6. Protection Port

You can set the port to be the protectd port. The protected ports cannot communicate with each other, only with unprotected ports.

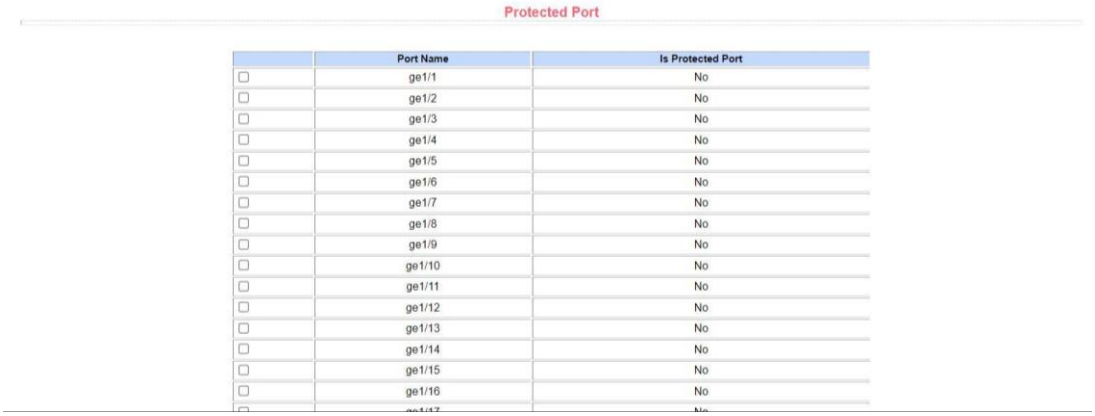


Figure 24: Protection Port Page

2.3.7. Learn limit

You can 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.

Figure 25: Port Learning Limit Page

2.3.8. Port Trunking

This page consists of four sections: trunk group ID, trunk method, able configurable ports, and member port.

Create trunk group

- Select the trunk group ID (1~8),
- click “create Trunk Group” button.

The status of “created” or “uncreated” shown along each group ID
Maximum 8 trunk groups be created.

Set the trunk method

- Select the created group ID,
- Select an aggregation method from the drop-down box,
- Click the button “Set Aggregation Method”.

There 6 trunk methods available:

- 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,
- Based on source and destination IP address

Each trunk group can configure its own port aggregation method.

Add port to Trunk group

- Select the created group ID,
- Select the port
- Click “Member Port” button

Each trunk group can add maximum 8 ports.

Remove port from Trunk group

- Select the created group ID,
- Select the port
- Click “Unmember Port” button

Delete the trunk group

- Select the created group ID,
- Remove all the ports in the group,
- Click “Delete the Group” button.

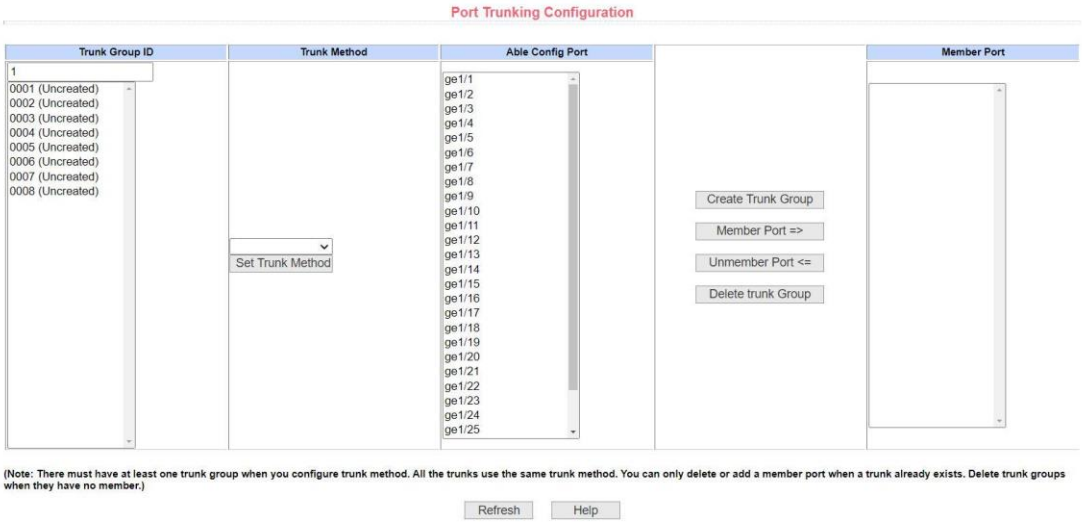


Figure 26: Port Aggregation Configuration

2.3.9. Mirror

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. 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.

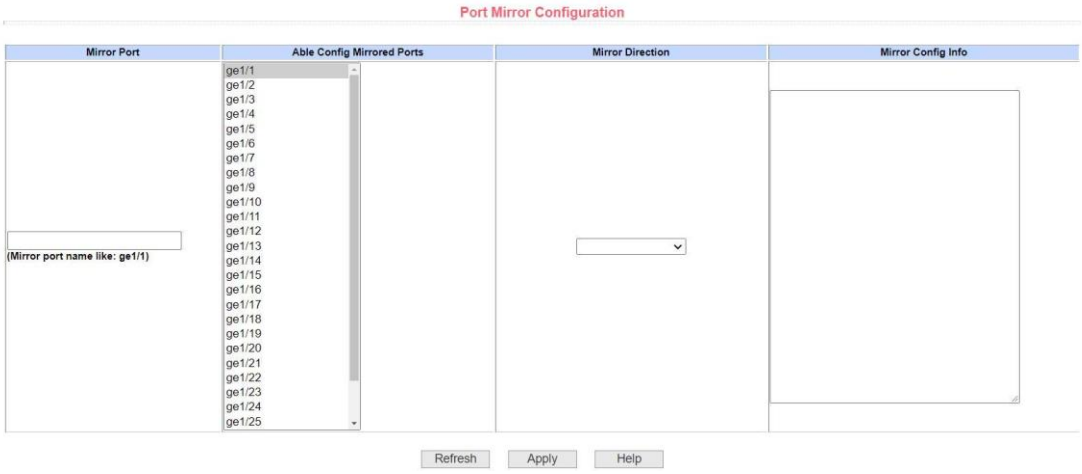


Figure 27: Port Mirror Configuration

2.3.10. DDM information

You can view the corresponding information of the optical module.

Figure 28: DDM information viewing interface

2.4. MAC Configuration

2.4.1. MAC table

You will view the MAC address of the VLAN corresponding to the port.

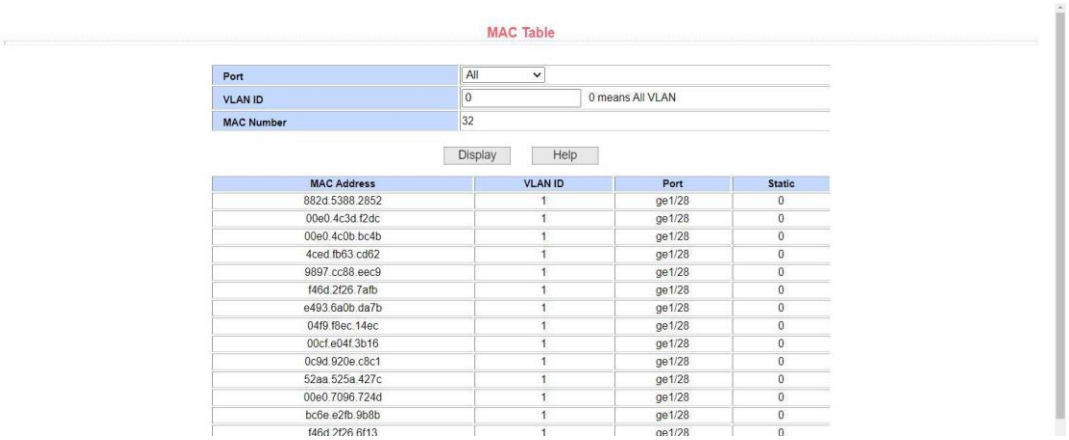


Figure 29：MAC Table

2.4.2. MAC Binding

You can bind the port and MAC address manually.

- Select the port from the drop-down menu,
- Enter the MAC address,
- Enter VLAN ID which MAC address belongs to,
- Click “Apply” button.

Figure 30：MAC Binding Configuration

2.4.3. MAC auto binding

You can bind the port and MAC address automatically.

- Select the port from the drop-down menu,
- Enter the MAC address and VLAN ID from the table,
- Click “Apply” button.

Figure 31: MAC Auto Bind

2.4.4. MAC Filter

You can bind the port and MAC filtering manually.

- Select the port from the drop-down menu,
- Enter the MAC address,
- Enter VLAN ID which MAC address belongs to,
- Click “Apply” button.

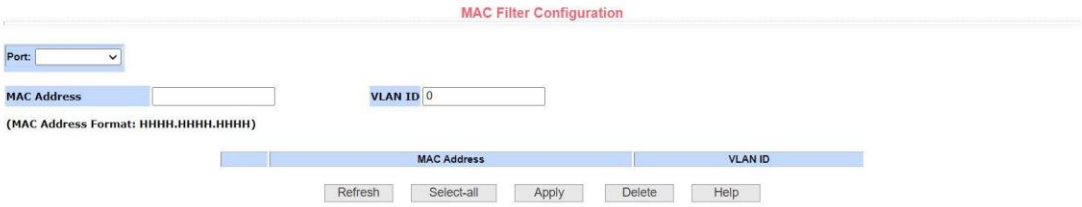


Figure 32: MAC Filtering Configuration

2.4.5. MAC auto filter

You can bind the port and MAC address automatically.

- Select the port from the drop-down menu,
- Enter the MAC address and VLAN ID from the table,
- Click “Apply” button.

Figure 33: MAC Auto Filter

2.5. VLAN Configuration

2.5.1. VLAN information

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 34: VLAN Information Page

2.5.2. VLAN Configuration

To create a new VLAN, the user enters a VID in the active line from 2 to 4094. 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.

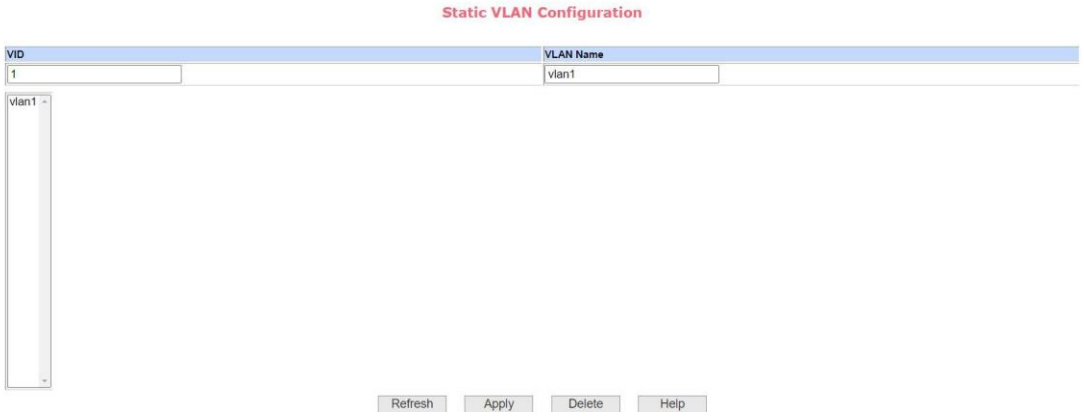


Figure 35: VLAN Configuration

2.5.3. VLAN Port Configuration

Select the port from the drop-down menu to configure VLAN.

Set VLAN mode:

Select the mode from the drop-down menu

- ACCESS mode: the port is an untagged member of VLAN1, and the default VLAN of port is 1;
- HYBRID mode: the port is an untagged member of VLAN1, and the default VLAN of port is 1;
- TRUNK mode: the port is an tagged member of VLAN1, and the default VLAN of port is 1.

Set the VLAN the port belonging to

- Select one VLAN ID shown in the “Current VLAN” column,
- Click “Default” button.

Set member characteristic of port in VLAN

- Select on or more VLAN IDshown in the “Current VLAN” column,
- Click “tagged” button setting the port to be the tagged member of selected VLAN(s); or
- Click “untagged” button setting the port to be the untagged member of selected VLAN(s).

Remove the Port from VLAN

- Select on or more VLAN IDshown in the “Current VLAN” column,
- Click “UnMember” button.

The meaning of the symbols shown in the “Port Members” column:
p=default VLAN of the port
t=tagged member of VLAN
u=untagged member of VLAN

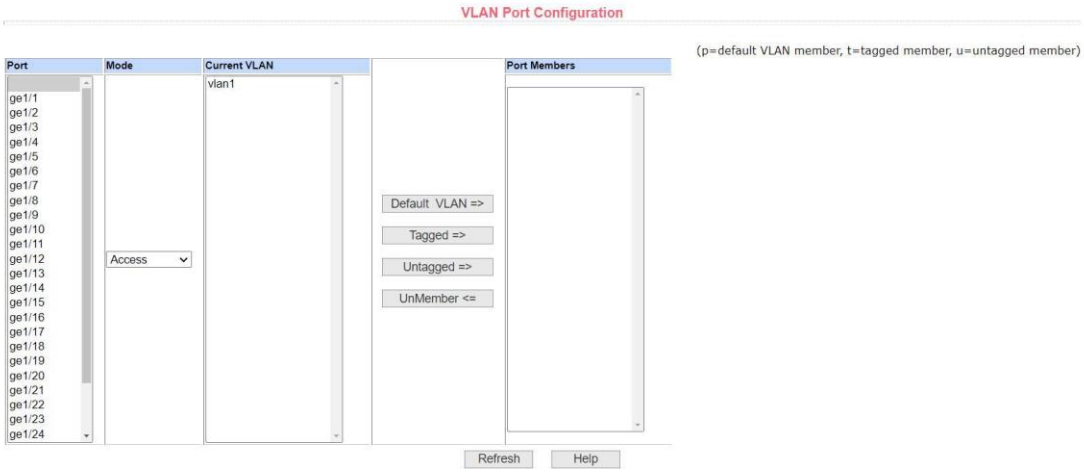


Figure 36: VLAN Port Configuration

2.6. SNMP Configuration

2.6.1. Community Name

By default, the switch has a read-only community with the name of “public”. When you need to manage the switch through SNMP, you need to set a read and write community.
There are maximum 8 communities are created.

- Enter community name,
- Select read/write permission by drop-down menu,
- Click “Apply” button,
- The state shows “Active”.

SNMP Community Configuration

2.6.2. TRAP Target

- You can set the switch to send the TRAP packet to the destination IP address on the situation like linkup, link-down offers.
- Enter name of TRAP,
- Enter the destination IP address which TRAP packet is sent to in “Transmit IP Address”,
- Select the SNMP version of TRAP target from the drop-down box,
- Click “Apply” button,
- The state shows “Active”.

TRAP Target Configuration

2.7. ACL Configuration

2.7.1. Standard IP

You can create rules of standard IP int the VLAN group .

- Select ACL Extended IP Group number from the drop-down menu (1-99, or 1300-1999),

You can create one or more rules in a group.

- In each rule, match the source IP address(with mask), and source wildcard.
  Both the source IP address and the destination IP address need to be masked.
  The rules can match a set of IP addresses. The mask of the address is expressed in reverse code. 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.
- Set the filter mode: permit or deny,
- Click “Add” button

When a user creates a rule in a rule group, the system will automatically assign a rule number to it.
When a rule in a rule group is deleted, other rules will be automatically sorted in a rule group.
You can click “Select-all” button and then “Delete” button to delete the whole rule group

Figure 37: ACL Standard IP Configuration

2.7.2. Extended IP

You can create rules of extended IP int the VLAN group .

- Select ACL Extended IP Group number from the drop-down menu (100-199, or 2000-2699), You can create one or more rules in a group.
- In each rule, match the source IP(with mask), source wildcard, destination IP (with mask), destination wildcard, protocol type (ICMP, TCP, UDP, etc.), source port and destination port (valid only for TCP and UDP protocols), and TCP control flags.
  Both the source IP address and the destination IP address need to be masked.
  The rules can match a set of IP addresses. The mask of the address is expressed in reverse code. For example, If the rule wants 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.
- Set the filter mode: permit or deny,
- Click “Add” button

When a user creates a rule in a rule group, the system will automatically assign a rule number to it.
When a rule in a rule group is deleted, other rules will be automatically sorted in a rule group.
You can click “Select-all” button and then “Delete” button to delete the whole rule group

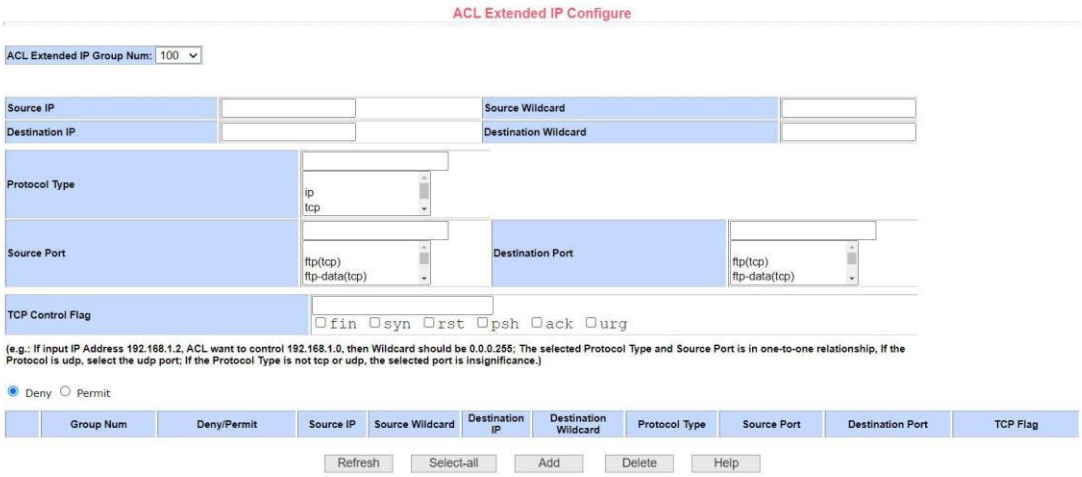


Figure 38: ACL Extended IP Configuration

2.7.3. MAC IP

You can create rules of ACL MAC IP .

- Select ACL MAC IP Group number from the drop-down menu (700-799),

You can create one or more rules in a group.

- In each rule, match source MAC address (with wildcard), source IP address (with wildcard), destination IP address (with wildcard), VLAN ID.

All the source MAC address, source IP address, and destination IP address must all have an address wildcard.

The rules 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.

- Set the filter mode: permit or deny,
- Click “Add” button

When a user creates a rule in a rule group, the system will automatically assign a rule number to it. When a rule in a rule group is deleted, other rules will be automatically sorted in a rule group.

You can click “Select-all” button and then “Delete” button to delete the whole rule group

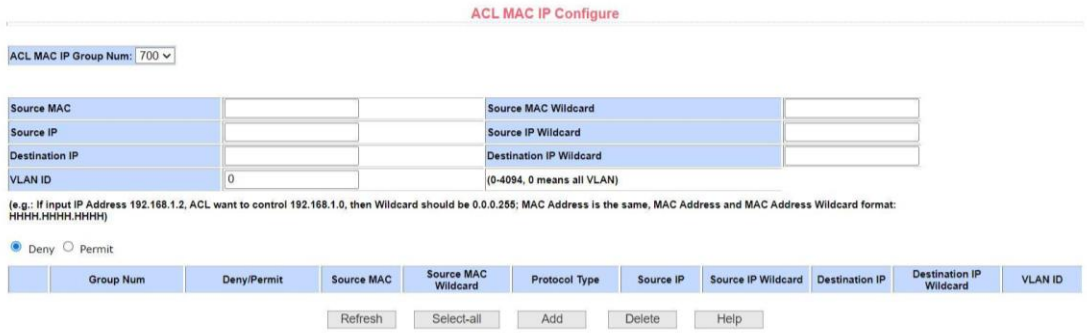


Figure 39: ACL MAC IP Configuration

2.7.4. MAC ARP

You can create rules of ACL MAC ARP .

- Select ACL MAC ARP Group number from the drop-down menu (1100-1199),

You can create one or more rules in a group.

- In each rule, match the sending MAC address (with wildcard) and the sending IP address (with wildcard).

Both the sending MAC address and the sending IP address need to have the address wildcard.

The rules can match a 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.

- Set the filter mode: permit or deny,
- Click “Add” button

When a user creates a rule in a rule group, the system will automatically assign a rule number to it. When a rule in a rule group is deleted, other rules will be automatically sorted in a rule group.

You can click “Select-all” button and then “Delete” button to delete the whole rule group

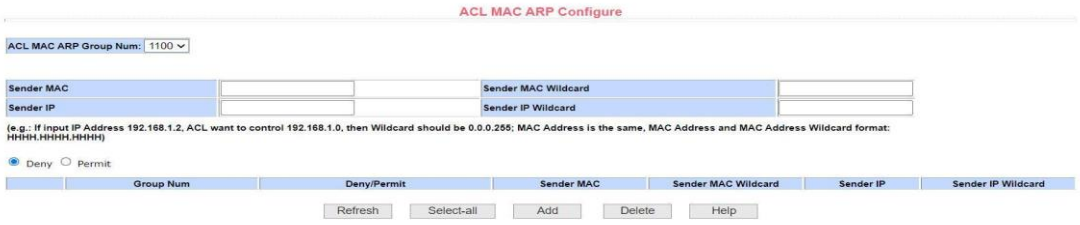


Figure 40：ACL MAC ARP Configuration

2.7.5. ACL Information

It displays all the rules and references configured in the current ACL.

Figure 41: ACL Resource Library Information Page

2.7.6. ACL Reference

You can select an ACL rule group for a port. By writing the ACL group rules into the port hardware logic, the port performs ACL filtering to the received packets accordingly.

Add the ACL reference

- Select the port from the drop-down menu
- Select the ACL group rules from the list shown in “All ACL Group” column

All ACL groups including standard IP, extended IP, MAC IP and MAC ARP can be selected

- Click “Add’ button

Delete the ACL reference

- Select the port from the drop-down menu
- Select the ACL group rules from the list shown in “Referenced ACL Groups” column
- Click “Delete’ button

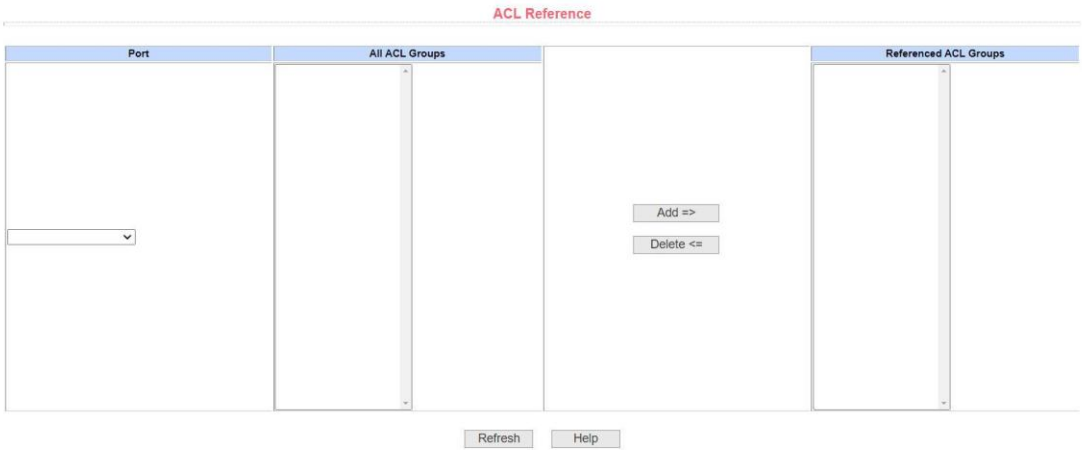


Figure 42: ACL Reference Configuration

2.8. Qos configuration

2.8.1. Qos apply

You can set and view QoS type and user priority of the port.

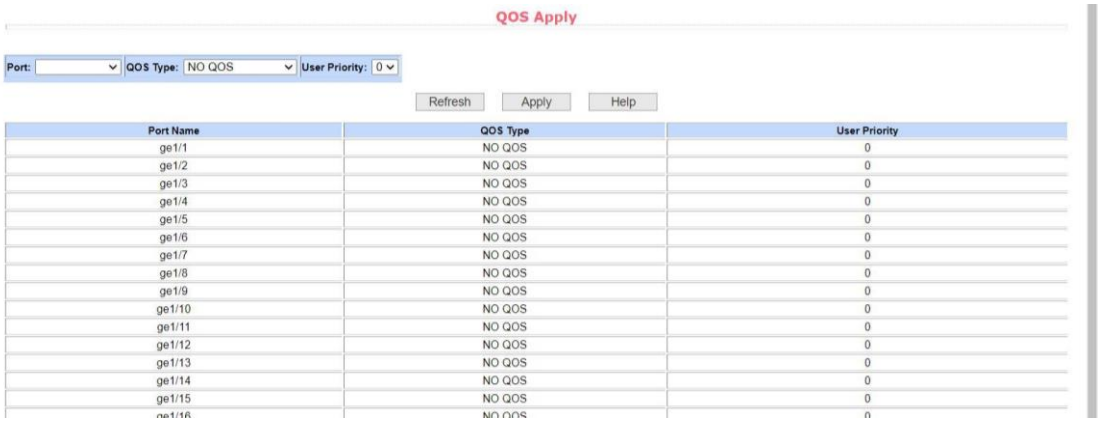


Figure 43: Qos Apply

2.8.2. Qos Schedule

You can set and view the Qos scheduling mode and the priority weight value of the queue of the port .

Qos Scheduling

2.9. IP Basic Configuration

2.9.1. VLAN interface

You can create VLAN Interface, delete the VLAN interface, set the IP address, delete the IP address, and view information of the interface.

There is a default VLAN interface “VLAN 1” which is not allowed to delete.

One VLAN only be allowed to have one interface.

Figure 44: VLAN Interface Configuration

2.9.2. ARP configuration and display

Set static ARP item

- Enter the IP address and MAC address,

The MAC address must be a unicast MAC address.

- Click “Add’ button

Delete ARP item

- Select deleted item,

You can delete a single IP ARP item, a network segment ARP item, all ARP items, all dynamic ARP items, or all static ARP items

- Enter the specified IP address or IP network segment in the input box
- Click “Delete” button.

Changed dynamic ARP list item into static ARP t list item

- Select ARP List item

The dynamic ARP list item in a certain network segment or all the dynamic ARP list items can be changed into the static ARP list item.

- In the case of a certain network segment, you need to enter the specified network segment in the input box.
- Click “Apply” button.

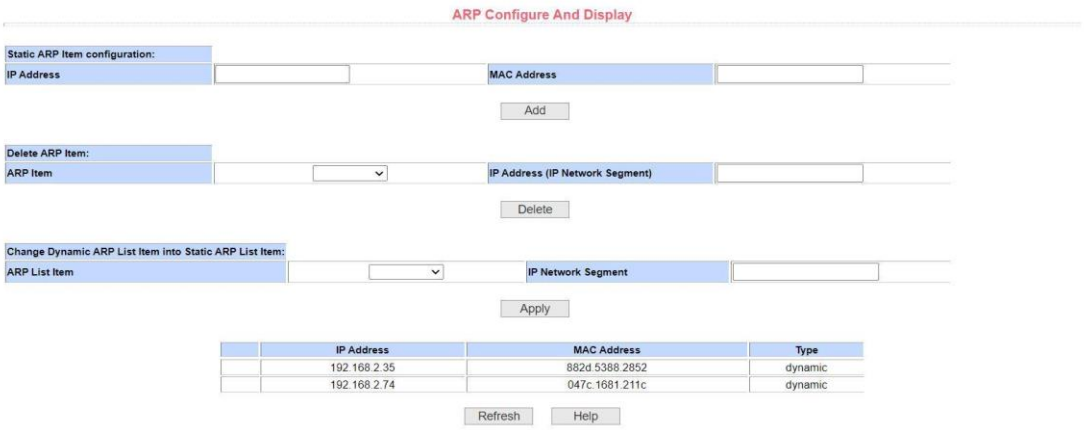


Figure 45: ARP Configuration and Display

2.9.3. Host static route configuration

You can add or delete the host static route of the switch. The switch is not configured with a host static route by default. You can set a default route which prefix of its destination address/subnet is 0.0. 0.0/0.

Figure 46: Host Static Route Configuration

2.10. AAA Configuration

2.10.1. AAA Authentication

You can select the authentication type.

Figure 47: AAA Authentication Configuration

2.10.2. Tacacs + Configuration

You 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 48: Tacacs + Configuration

2.10.3. Radius Configuration

Figure 11-3 is the Radius Configuration. 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.

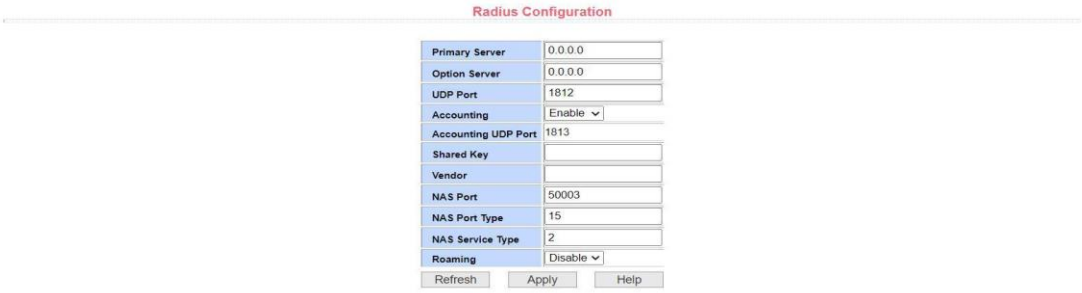


Figure 49: Radius Configuration

2.10.4. 802.1x configuration

You 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.

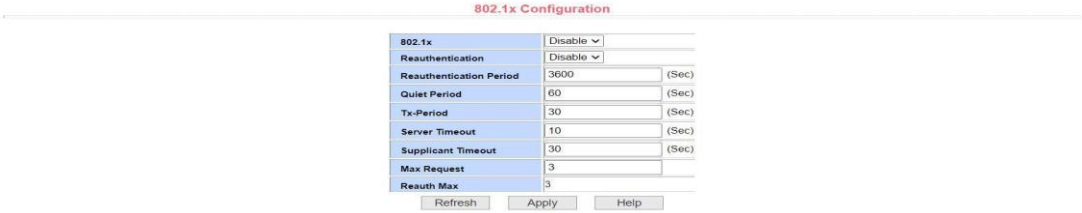


Figure 50: 802.1x Configuration

2.10.5. 802.1x Port Configuration

You 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.

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.

Figure 51: 802.1x Port Configuration

2.10.6. 802.1x user authentication information

You can view the status information of all users connected to a port

Figure 52: 802.1x User Authentication Information

2.11. MSTP configuration

2.11.1. Global Configuration

You can configure global MSTP parameters.

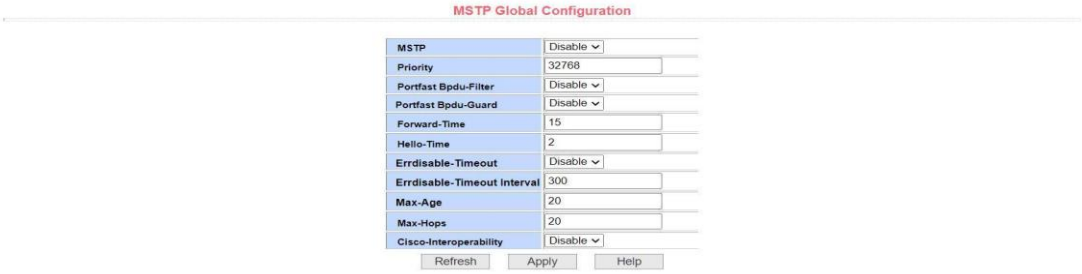


Figure 53: MSTP Global Configuration

2.11.2. Port configuration

You can configure the port MSTP parameters.

Figure 54: MSTP Port Configuration

2.11.3. Port information

You can view the specific status of the port MSTP.

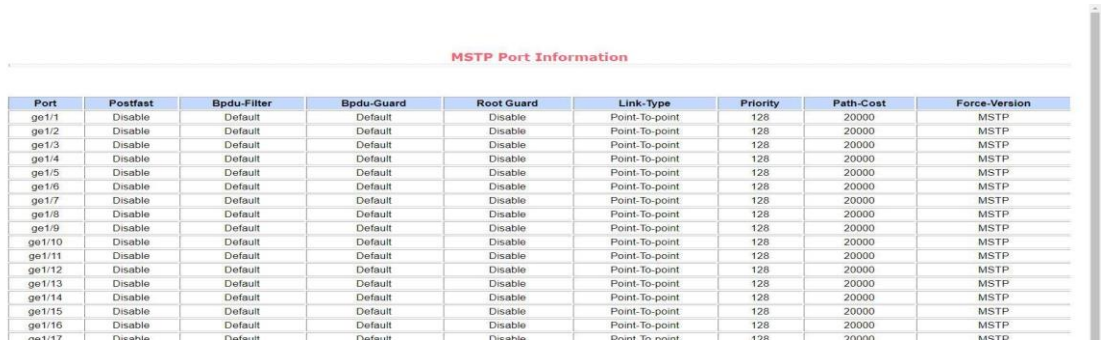


Figure 55: MSTP Port Information Page

2.12. IGMPSNOOPING configuration

2.12.1. IGMP SNOOPING Configuration

You can enable or disable IGMP SNOOPING.

Figure 56: IGMP SNOOPING Global Configuration

2.12.2. Multicast group information

You can view the IGMP snooping multicast program information.

Figure 57: Multicast Group Information Page

2.13. GMRP Configuration

2.13.1. GMRP Global Configuration

Enable/Disable GMRP.

Figure 58: GMRP Global Configuration

2.13.2. GMRP Ports Configuration

You can enable or disable the port GMRP and view the port information.

Figure 59: GM RP Ports Configuration

2.13.3. 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 60: GMRP State Machine Page

2.14. CVRP Configuration

2.14.1. GVRP Global Configuration

Enable or disable GVRP.

Figure 61: GVRP Global Configuration

2.14.2. GVRP Ports Configuration

You can enable or disable port GVRP and view port information.

Figure 62: GVRP Ports Configuration

2.14.3. GVRP state machine

You can view the state machine information established by GVRP.

Figure 63: GVRP State Machine

2.15. EAPS Configuration

2.15.1. EAPS Configuration

You can create and configure EAPS information, 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

Nable state, last EAPS loop enable condition

Figure 64: EAPS Configuration

2.15.2. EAPS Information

You can view the EAPS configuration information.

Figure 65: EAPS Information Page

2.16. RMON Configuration

2.16.1. Statistics Configuration

You can 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.

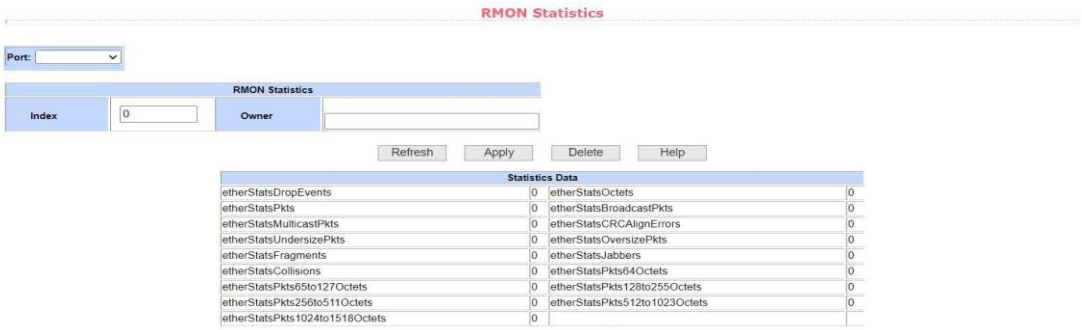


Figure 66: RMON Statistics Group Configuration

2.16.2. History Configuration

You 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 67: RMON History Group Configuration

2.16.3. Alarm Configuration

You can 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 68: RMON Alarm Group Configuration

2.16.4. Event Configuration

You can 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 69: RMON Event Group Configuration

2.17. Cluster Management

2.17.1. NDP configuration

You 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 70: NDP Configuration

2.17.2. NTDP Configuration

You can 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 71: NTDP Configuration

2.17.3. Cluster configuration

You can 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.

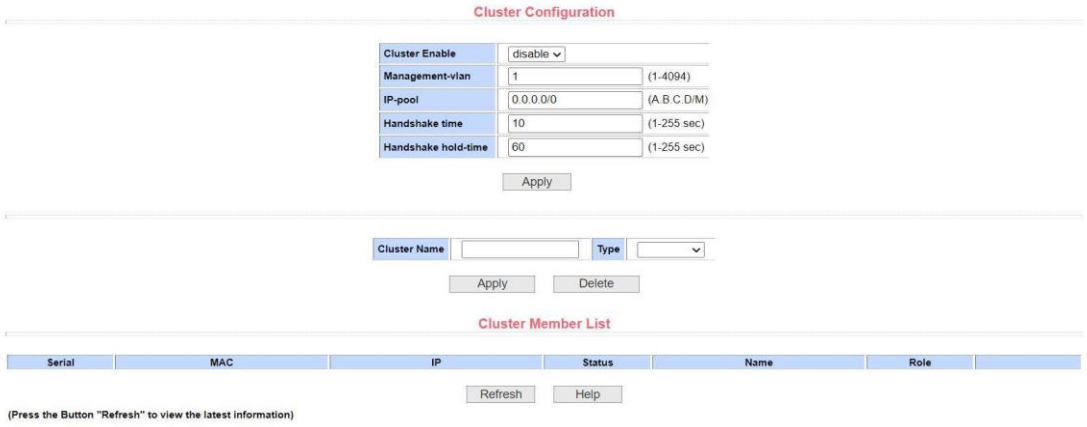


Figure 72: Cluster Configuration

2.18. ERPS Configuration

2.18.1. ERPS Configuration

You can enable or disable 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 73: ERPS Configuration

2.18.2. ERPS Information

You can view ERPS configuration information.

Figure 74: ERPS Information Page

2.19. LLDP Configuration

2.19.1. LLDP global configuration

You can view and configure global LLDP parameters.

Figure 75: LLDP Global Configuration Part

2.19.2. LLDP Ports Configuration

You can view and configure LLDP port parameters.

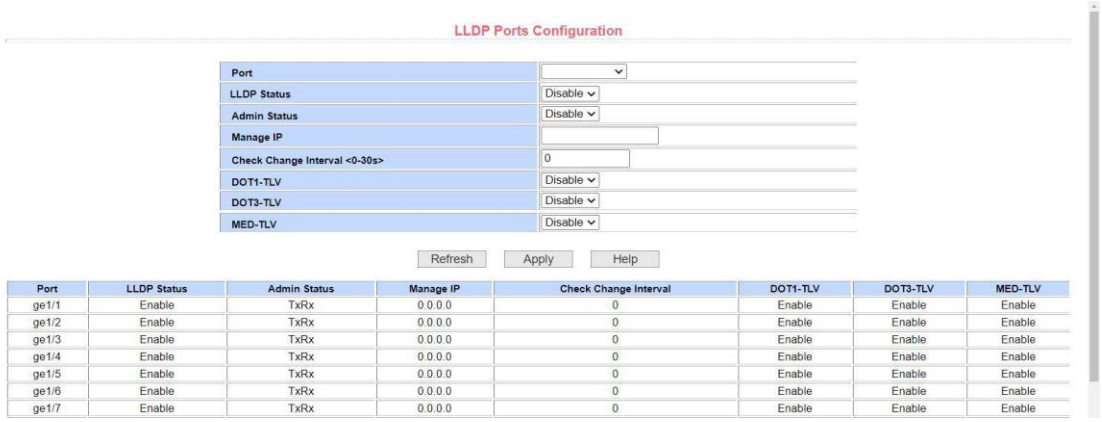


Figure 76: LLDP Ports Configuration Part

2.19.3. LLDP Neighbor

You can view and configure LLDP port parameters.

Figure 77: LLDP Neighbor Table Part

2.20. Log Management

2.20.1. Log Configuration

You 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.

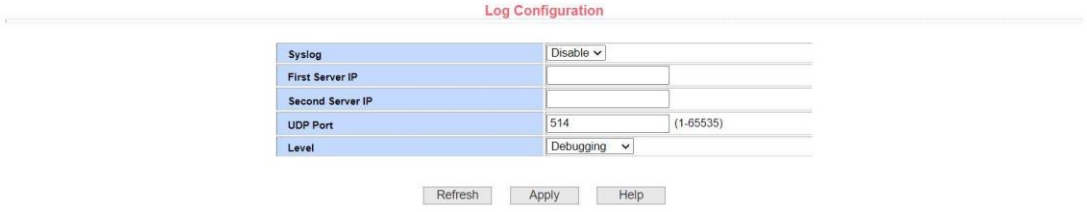


Figure 78: Log Configuration

2.20.2. Log Information

You 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 79: Log Information Page

2.21. POE Port Configuration

2.21.1. POE Port Configuration

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

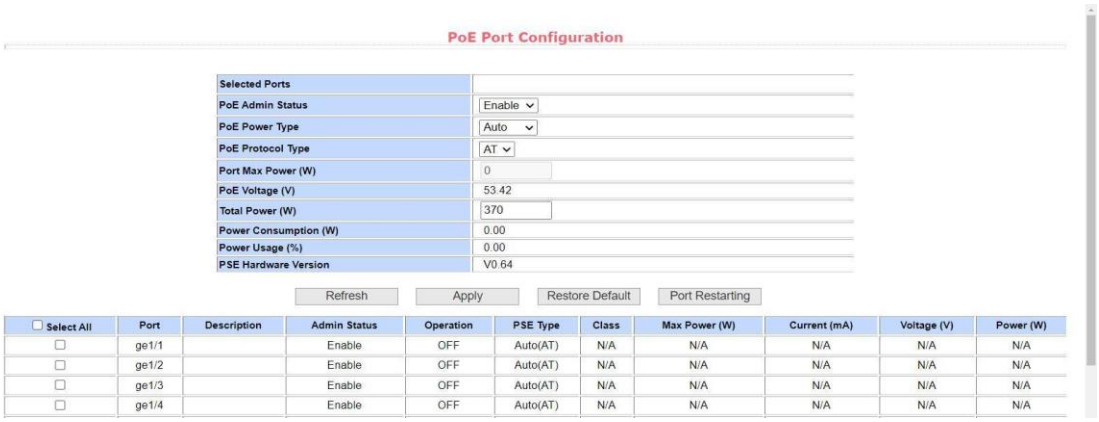


Figure 80: POE Port Configuration

2.21.2. POE Policy Configuration

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

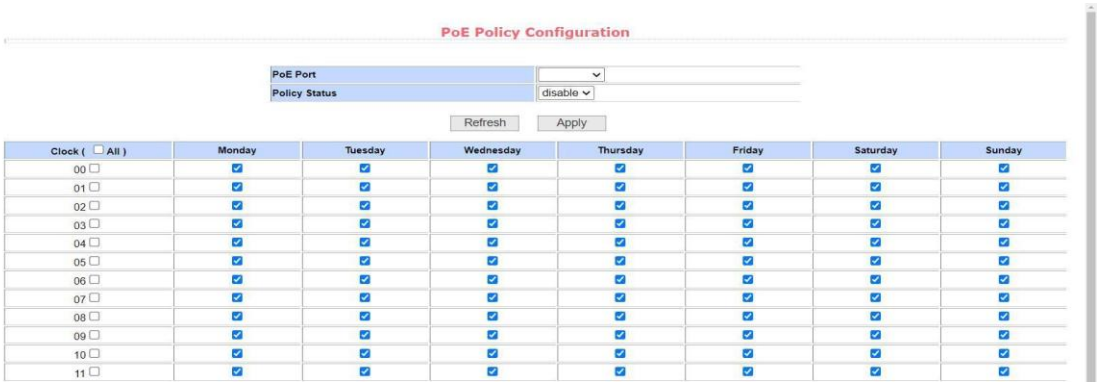


Figure 81: POE policy Configuration

2.21.3. PD Query Configuration

It shows the PD query Configuration, through which the PD online device status detection can be realized.

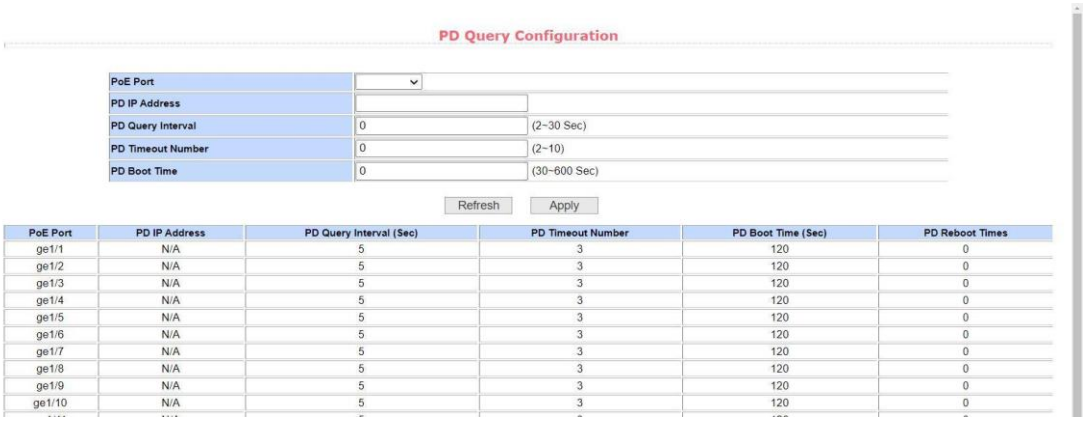
POE port: used to select the port to be queried and connected to the PD device

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
ge1/9	N/A	5	3	120	0
ge1/10	N/A	5	3	120	0

Figure 82: PD Query Configuration