MAIWE

Managed Industrial Ethernet Switch

WEB User Manual

——Applied for MBN8000 Series

Wuhan Maiwe Communication Co., Ltd.

Version: V2.2

Trademark

is the brand and registered by Wuhan Maiwe Communication Co., Ltd.

Microsoft and **Windows** is registered trademark owned by Microsoft.

Copyright

Statement

1. This user manual is suitable for MaiweMBN8000 platform series products, including ISM7112G /ISM7112GP series, MISCOM8028 series, MISCOM7028G/7020G/8028G/8020G series, MISCOM8028G-4XGF series and MISCOM7028GX /MISCOM8028GX/MISCOM8028GX-4XGF series.

2. This manual is a general manual, the interface and functions of different models of equipment are slightly different, and all are subject to the actual model used.

Important Statement

Any information provided by our company in this manual does not represent for corresponding authorization on these information.

Our company attempts to ensure the accuracy and applicability for the information provided in this manual, however our company does not assume any responsibility for the use of these information, and does not assume any joint responsibility for the use of these information. There may be a few technical or typographical errors in the product and manual. The company reserves the right to change all or part of this manual without prior notice.

Attention

Duo to continuous update and improvement of products and technology, the contents of this document may not be completely consistent with the actual products, appreciate for your understanding. If necessary to inquiry the updates of the product, please check our official website or contact our representative directly.

Revise History

Version No	Date	Revise record
V2.2	2021.11	Create file

Safe Use Instructions

This product performance is excellent and reliable in the designed range of use, but it's necessary to avoid man-made damage or destroy for the equipment.

- Read the manual carefully and keep this manual for reference if need afterwards.
- Do not put the device close to the water sources or damp places.
- Do not put anything on the power cable, it should be placed out of reach.
- To avoid causing fire, do not knot or wrap the cable.
- Power connector and other device connectors should be firmly connected with each other, frequently inspection is needed.
- Please keep the fiber socket and plug clean. Do not look directly at the fiber section when the equipment is working.
- Please keep the equipment clean and wipe it with a soft cotton cloth if necessary.
- Please do not repair the equipment by yourself, unless there is clear instructions in the manual.

Under the following circumstances, please cut off power immediately and contact us.

- Equipment water damage.
- The equipment is broken or the casing is broken.
- The equipment works abnormally or the performance has completely changed.
- The equipment produces odor, smoke or noise.

1. Configuration Preparation

1.1 Configure the switch

The MBN8000 platform managed industrial Ethernet switch has a built-in web server, and users can configure the switch by accessing the web server. Before accessing the Web, please configure the switch as follows:

- Configure the IP address of the VLAN 1.1 interface to ensure that the route between the PC and the switch VLAN 1.1 interface is reachable. The configuration commands are as follows:

  MBN8000#configure terminal

  MBN8000(config)#interface vlan1.1

  MBN8000(config-vlan1.1)#ip address 192.168.16.253/24

- To configure the user name, password and user authority level (level 3 is administrator authority), the configuration command is as follows:

  MBN8000#configure terminal

  MBN8000(config)#username xxx password xxx privilege <0-3>

Among them, <0-3> represents the user authority: 0-visitor, 1-observer, 2-operator, 3-manager. Privilege, the larger the value, the higher the user authority, and the third-level user has full access authority.

Statement

1.After the above configuration commands are executed, use the "write" command to save all configurations.
2.The web server is enabled by default when the switch leaves the factory.
3.The factory default IP address of the switch is 192.168.16.253, and the default user name/password is admin/admin.

1.2 PC Configure PC

To access the switch through the Web, the IP of the switch and the PC must be in the same network segment. For Windows users, please refer to the following steps:

Start→Control Panel→Network and Internet Connection→Network Connection→Local Connection→Properties→Internet Protocol (TCP/IP)

The specific operation page of Windows system is shown in Figure 1.

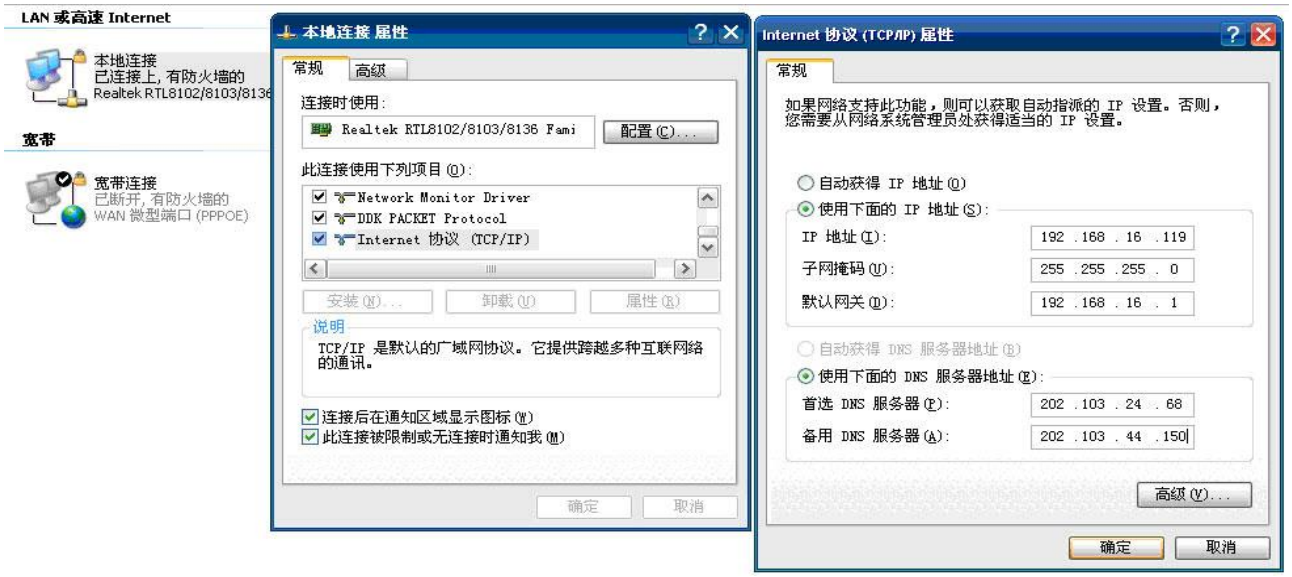


Figure 1 IP setting interface in Windows environment

The factory default IP address of the switch is 192.168.16.253. Follow the above operations to modify the IP address of the PC to 192.168.16.X (X is any valid value from 2 to 254 except 253). After the modification is successful, you can use this IP address to access the Web.

1.3 Ping Testing

After the switch and the PC are configured, you can use the Ping command to check whether the connection between the PC and the switch is normal. For Windows users, please refer to the following operations:

- **Start→Run→input "cmd" →click "OK"**
- **Enter the command "ping 192.168.16.253" in the command line program of the Windows system, as shown in Figure 2.**

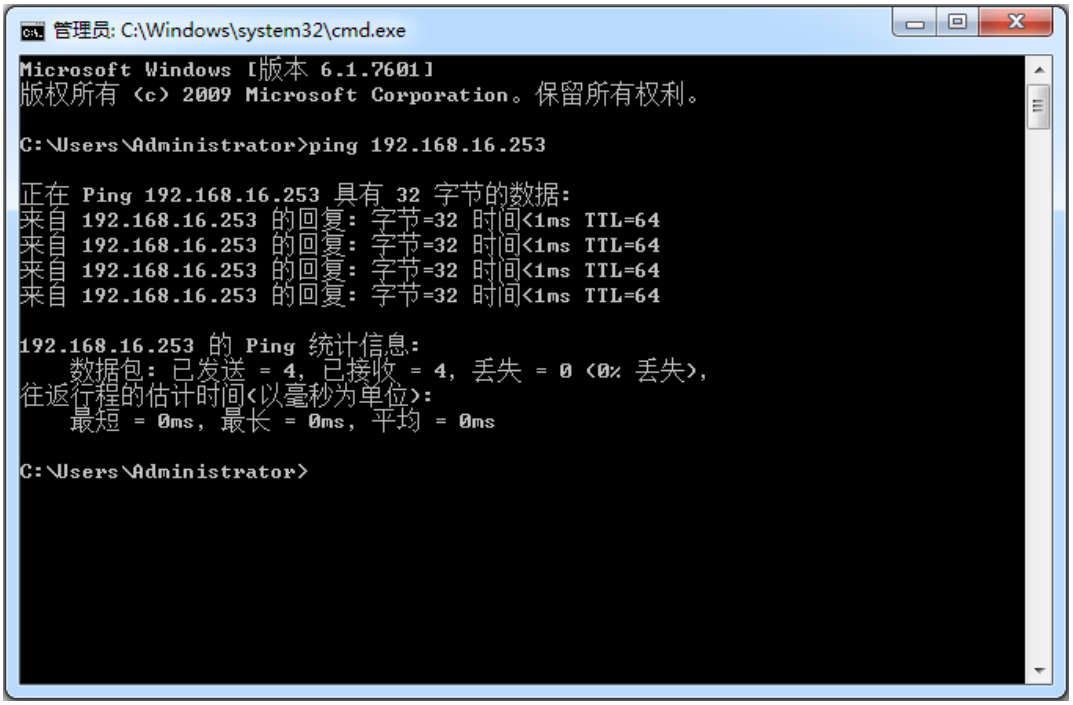


Figure 2 Using the ping command in Windows environment

If the ping is successful, it means that the PC and the switch are connected normally, otherwise, please check the network connection.

1.4 Login WEB

Open a browser and enter the default IP address of the switch in the address bar, as shown in Figure 3.

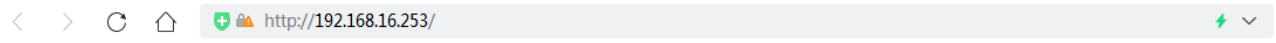
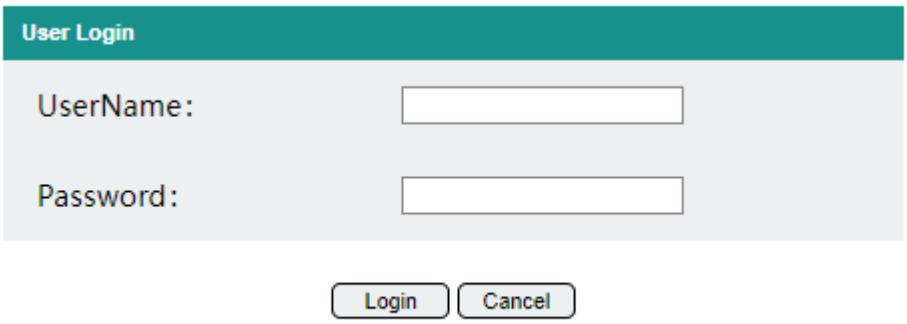


Figure 3 Entering the IP address interface in the address bar

Figure 4 will pop up, prompting the user to enter the user name and password.



Picture 4. Login WEB

Attention

1. It is recommended that users use Google, Firefox or IE7.0 and above browsers.
2. If the web page prompts "Web access has been disabled, please enable the web access function through the

command line!" after entering the IP address and redirecting, it means that the web function is not enabled normally. Please use the "web enable" command in the configuration mode of the command line to enable the web access function.

3. If the web page displays "Request timeout" after you enter the IP address, check whether the network connection is normal.

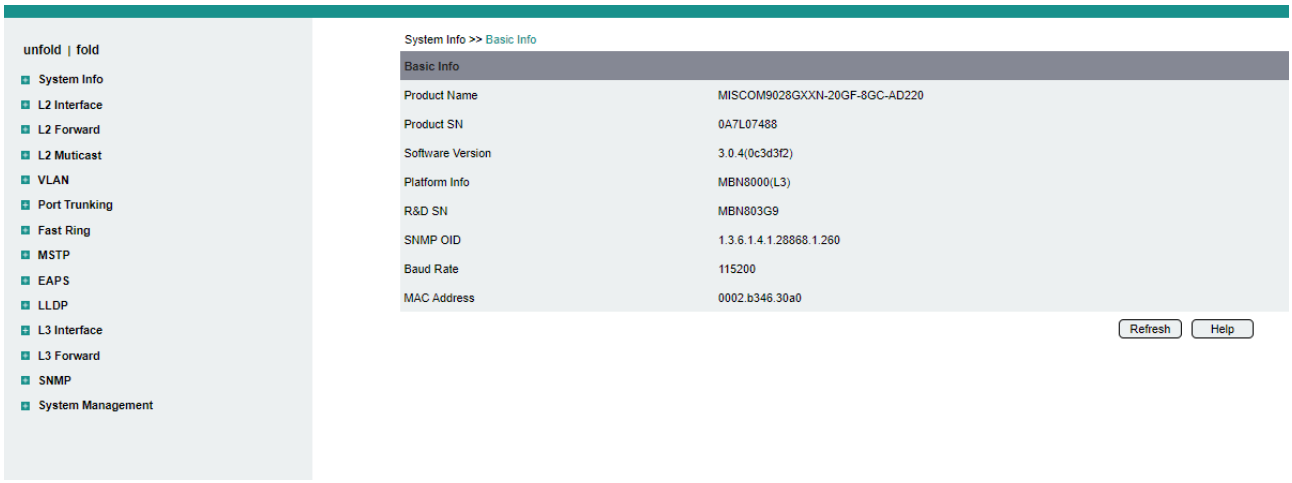
2 Web Interface Introduction

Statement

The pages and configurations of all the following functions are subject to the actual product

2.1 Overall Page

After the login verification is passed, enter the main web page. The title bar displays the product model of the current switch. The web page is divided into four areas. The upper part is the logo display area and the shortcut key area, the left side is the menu area, the right side is the main function display area, and the lower part is the copyright and browser information display area. As shown in Figure 5.



Picture 5 Overall page

2.2 Top Area

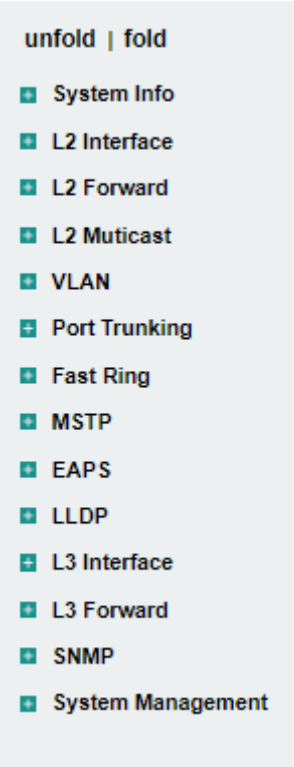
The left side of the top area is the Logo, and the right side is the shortcut key, which can switch between Chinese and English, save the configuration and exit. As shown in Figure 6.

Picture 6 Top area

2.3 Left menu area

The left area is the configurable function menu, where a three-level directory structure is used. The first-level directory is system information, port configuration, layer-2 features, ring redundancy, layer-3 features, advanced functions, and system management. Click "Expand" and "Collapse" to quickly expand and collapse all secondary menus. Click the sign in front of each level of directory to expand the corresponding submenu. As

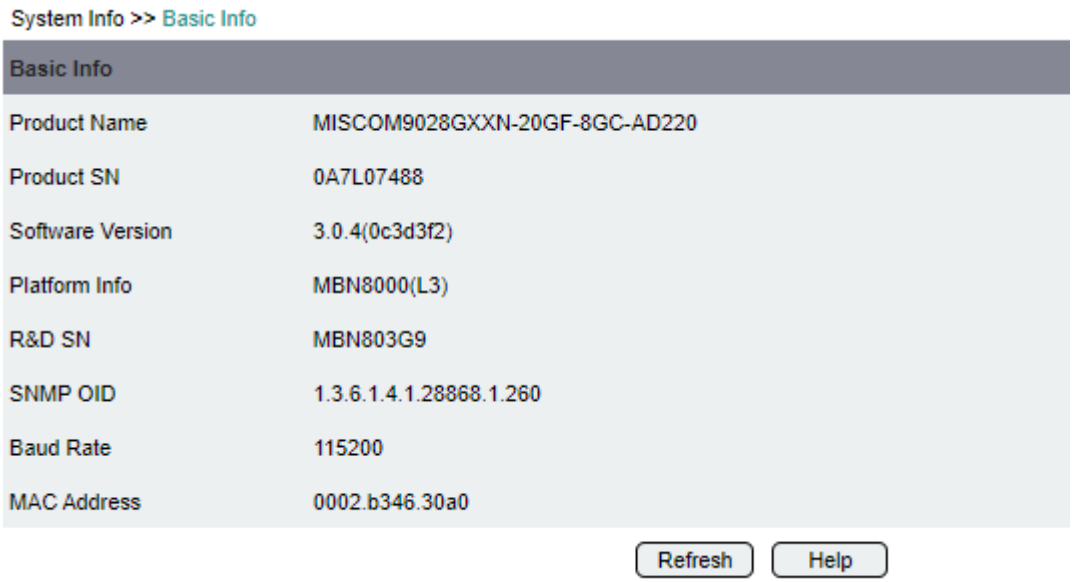
shown in Figure 7.



Picture 7.Left area menu

2.4 Right functional area

The right side is the function display area, which can view and configure various parameters of the function. As shown in Figure 8.



Picture8 Right function area

2.5 Bottom Area

The bottom area displays system copyright information and browser usage recommendations. As shown in Figure 9.

Picture9 Bottom area

2.6 Help Documentation

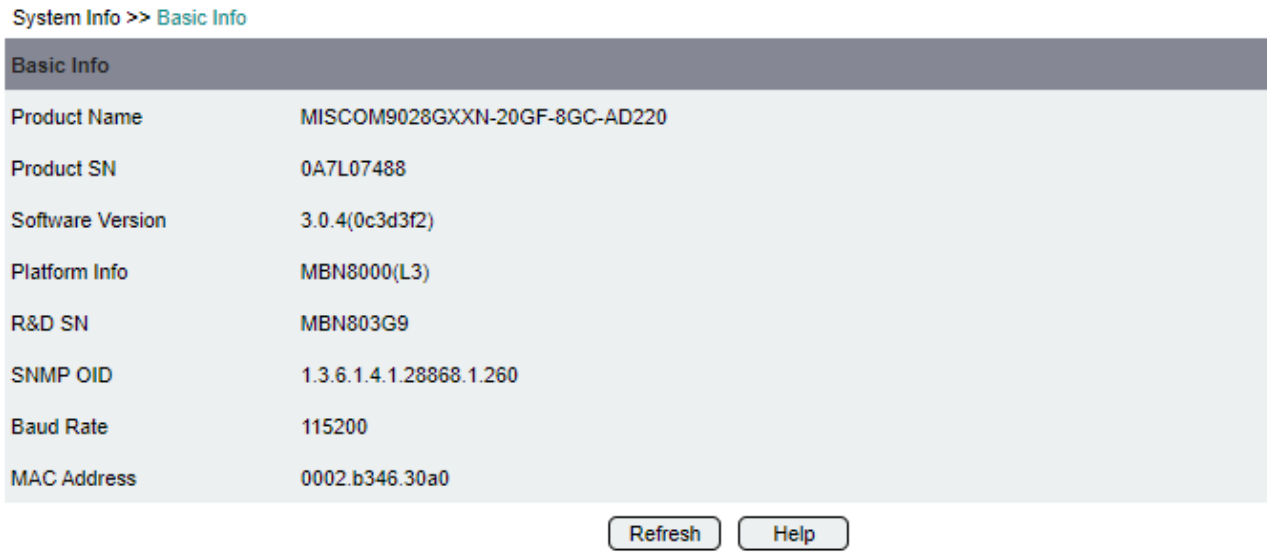
When accessing the function page, click the "Help" button below to pop up the help document corresponding to the function, as shown in Figure 10.

Picture 10 Help document

3 System Status

3.1 Basic Information

The basic information page displays the product name, product number, version information, platform information, R&D code, SNMP OID, baud rate, and MAC address information of the switch. As shown in Figure 11.

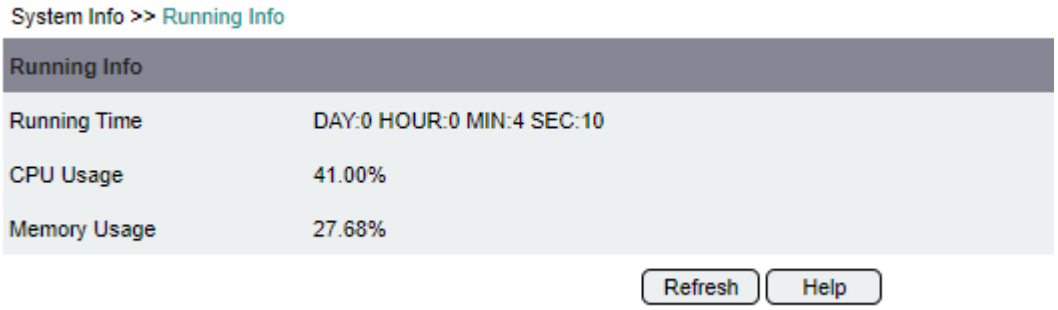


Picture11 Basic information area

3.2 Running Information

The Running Information page displays the switch's running time, CPU usage, and memory usage

information. As shown in Figure 12.



Picture12. Running information page

3.3 Port Status

The port status page can be automatically refreshed to display the connection status of each port in real time. When the port is connected, the port number will be highlighted. As shown in Figure 13.

Picture 13 Port statues page

3.4 Port Flow

The port flow page displays the traffic statistics of each port, including the number of bytes received, unicast packets received, non-unicast packets received, error packets received, bytes sent, unicast packets sent, non-unicast packets sent, Error packet sent. As shown in Figure 14.

System Info >> Port Flow Statistics

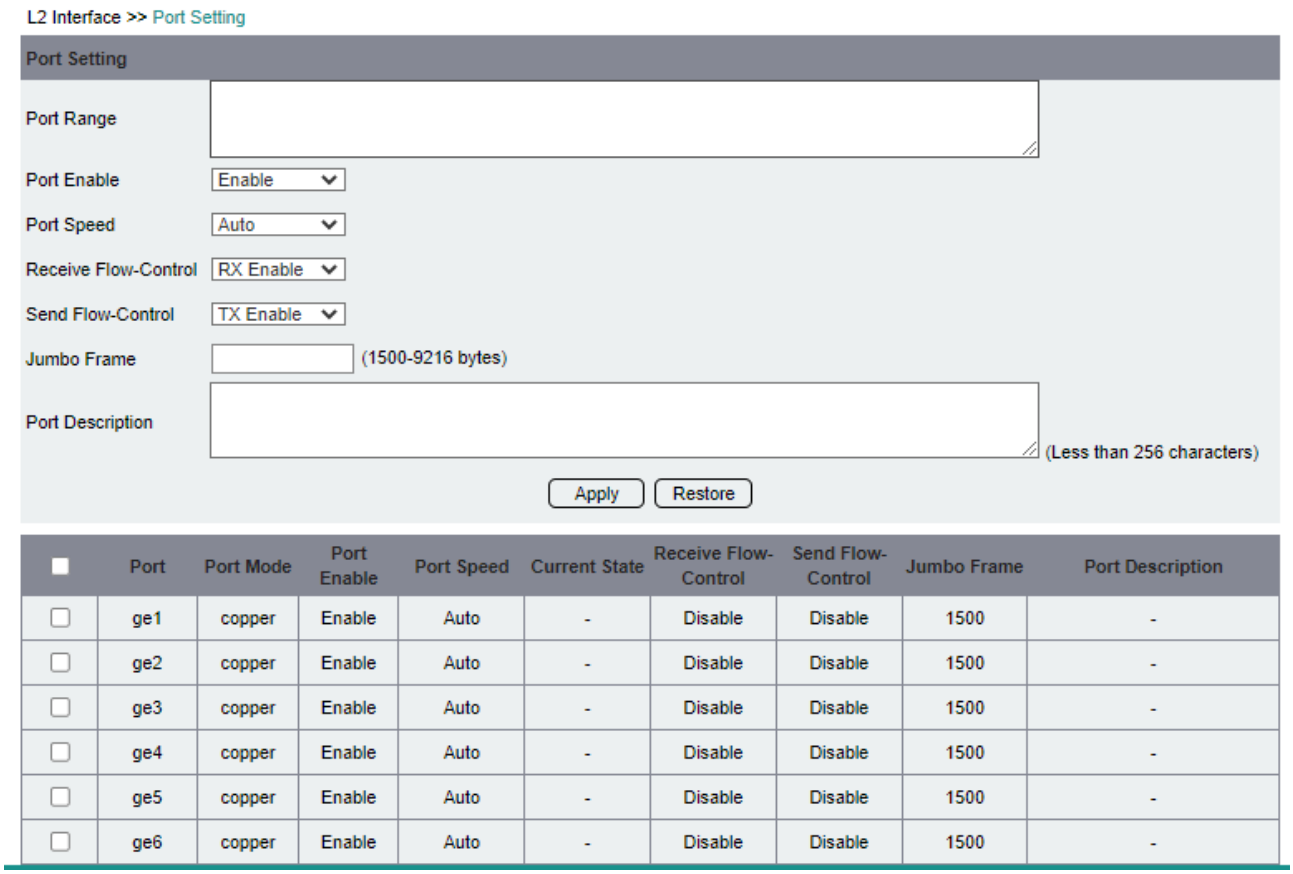
Port	Octects Received	Packets Received	Octects Sent	Packets Sent
ge1	0	0	0	0
ge2	0	0	0	0
ge3	0	0	0	0
ge4	0	0	0	0
ge5	0	0	0	0
ge6	0	0	0	0
ge7	0	0	0	0
ge8	0	0	0	0
ge9	0	0	0	0
ge10	0	0	0	0
ge11	0	0	0	0
ge12	0	0	0	0
ge13	0	0	0	0
ge14	0	0	0	0
ge15	0	0	0	0
ge16	0	0	0	0
ge17	0	0	0	0

Picture 15 Port flow page

4 Port Configuration

4.1 Port Configuration

The port configuration function is used to configure and display the enable, rate, flow control, jumbo frame, and description properties of the port. As shown in Figure 15.



	Port	Port Mode	Port Enable	Port Speed	Current State	Receive Flow-Control	Send Flow-Control	Jumbo Frame	Port Description
☐	ge1	copper	Enable	Auto	-	Disable	Disable	1500	-
☐	ge2	copper	Enable	Auto	-	Disable	Disable	1500	-
☐	ge3	copper	Enable	Auto	-	Disable	Disable	1500	-
☐	ge4	copper	Enable	Auto	-	Disable	Disable	1500	-
☐	ge5	copper	Enable	Auto	-	Disable	Disable	1500	-
☐	ge6	copper	Enable	Auto	-	Disable	Disable	1500	-

Picture 15 Port configuration page

This page is divided into two areas, the port is configured on the top, and the port parameter list is displayed on the bottom. When configuring the parameters of one or more ports, check the port list first, map the parameters of the selected ports to the upper configuration area for modification, and then click "Configure" to save.

The description of each configuration item is as follows:

Port Number: The label of the switch port. A port set whose properties need to be modified, it is automatically added to the text box after checking it.

Interface Type: Displays the type of the interface, such as: electrical port, optical port, and optoelectronic multiplexing port, etc.

Port Enable: Enable or disable the port, enabled by default.

Port Rate: Set the duplex status and speed mode of the port.

Ingress flow control: Enable/disable traffic congestion control in the ingress direction, disabled by default.

Egress flow control: Enable/disable traffic congestion control in the egress direction, disabled by default.

Jumbo frame length: Configure the maximum transmission unit of the port, the default value is 1500.

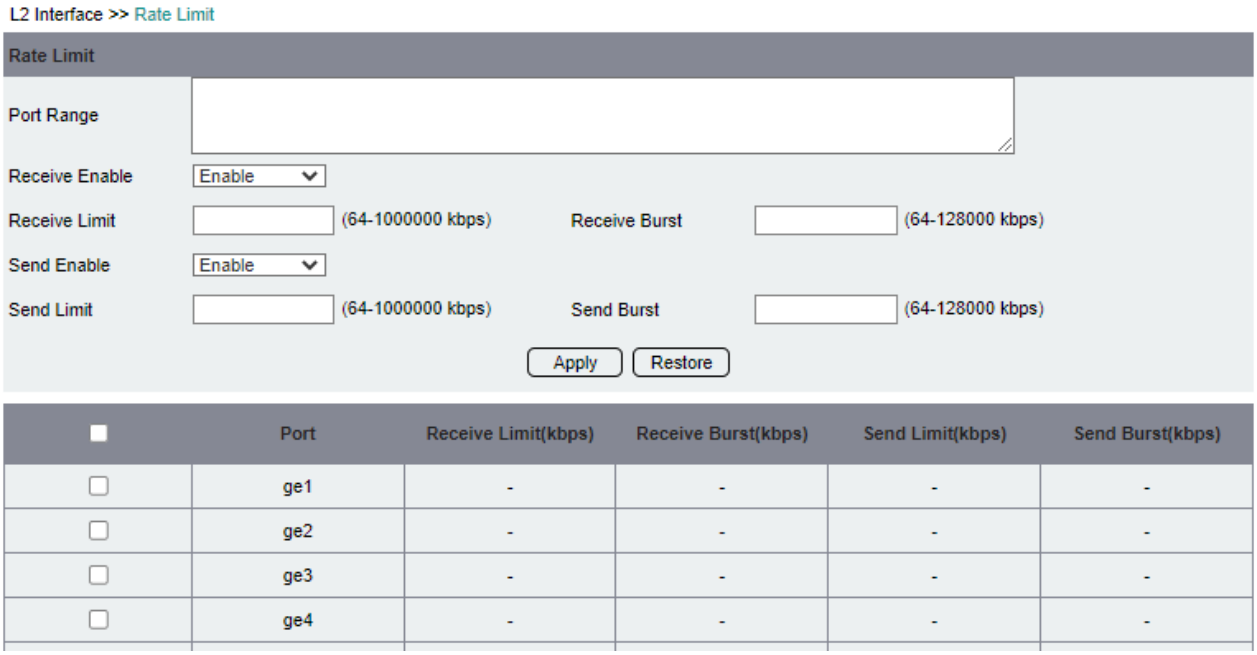
Interface description: Set the description information of the port, no more than 256 characters.

Attention

1. The reset button resets the attribute value of the selected port to the default value.
2. The port rate range, default rate mode and maximum jumbo frame length supported by different types of ports are different, and the specific model shall prevail.
3. The aggregate port cannot modify the port rate.

4.2 Port Rate Limiting

The port rate limit function is used to configure and display the rate limit and burst traffic of a switch port in the inbound and outbound directions. As shown in Figure 16.



Picture 16 Port rate limiting

This page is divided into two areas, the port is configured on the top, and the port parameter list is displayed on the bottom. When configuring the parameters of one or more ports, check the selection box in front of the port, the parameters of the selected port will be mapped to the upper configuration area, modify the parameters in the configuration area, and click "Modify" to save.

Each configuration item is described as follows:

Port Range: The port set whose properties need to be modified, it is automatically added to the text box after checking it.

Ingress Enable: Enable/disable configuration in ingress direction, disabled by default.

Ingress Rate Limit: Set the rate limit in the ingress direction.

Ingress Burst: Set the burst traffic in the ingress direction.

Outgress Enable: Enable/disable configuration in outgress direction, disabled by default.

Outgress Rate Limit: Set the rate limit in the outgress direction.

Outgress Burst: Set the burst traffic in the outgress direction.

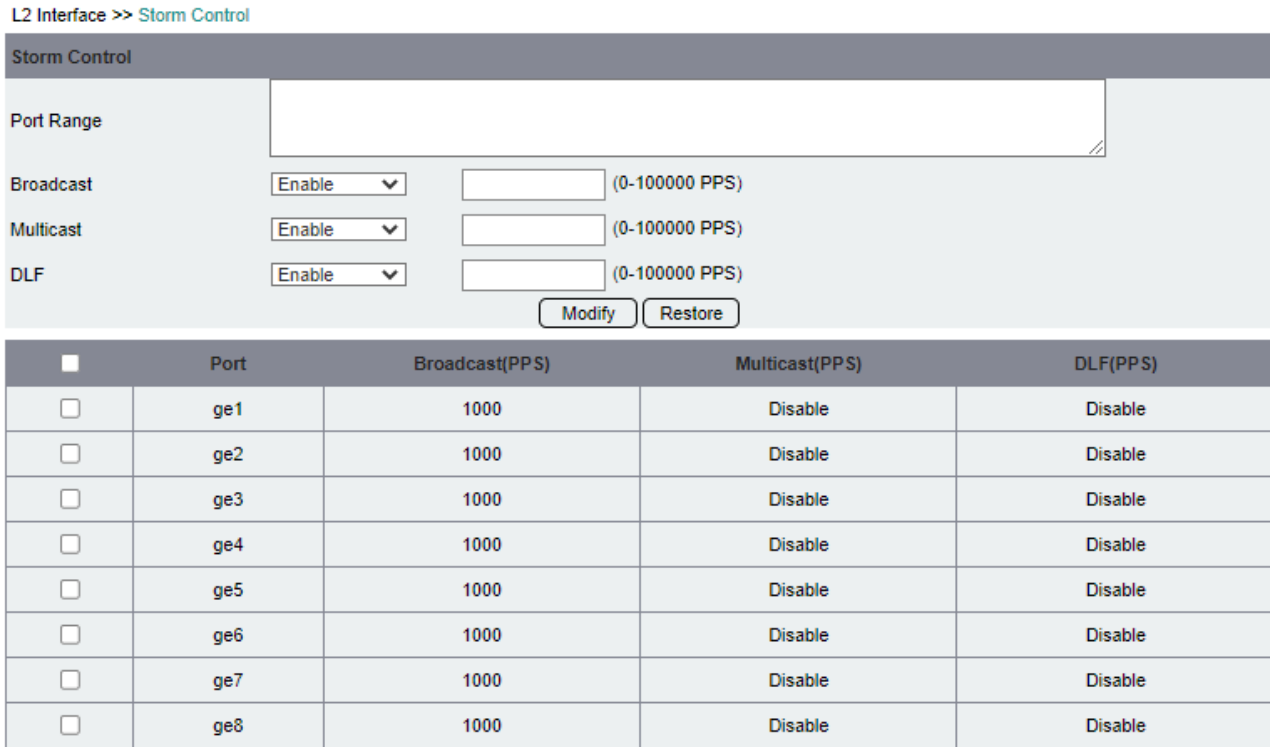
Attention

1. The aggregate port cannot be configured with port rate limit.
2. The rate limit value cannot exceed the maximum bandwidth of the port. If the port has been linked up, it cannot exceed the current rate.
3. The Reset button resets the attribute value of the selected port to the default value.

4.3 Storm Suppression

The device provides storm suppression function, which is used to prevent the port of the switch from being damaged by broadcast, multicast or unicast storms in the network.

The Storm Suppression page is shown in Figure 17.



Picture 17 Storm suppression setting interface

This page is divided into two areas, the port is configured on the top, and the port parameter list is displayed on the bottom. When configuring the parameters of one or more ports, check the selection box in front of the port, the parameters of the selected port will be mapped to the upper configuration area, modify the parameters in the configuration area, and click "Modify" to save.

Each configuration item is described as follows:

Port Range: Port set to be configured, which cannot be entered manually, but can only be selected below.

Broadcast data packets: broadcast data packets limit rate, unit pps, range 0~100000, default value 1000.

Multicast packets: The rate limit of multicast packets, in pps, range from 0 to 100000, the default value is disable.

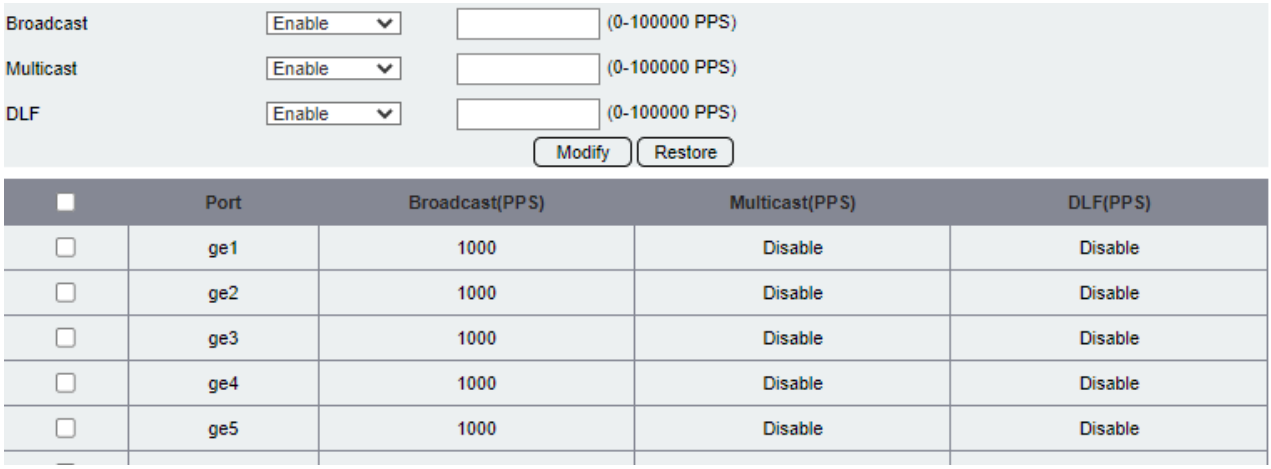
Unknown unicast packet: Unknown unicast packet rate limit, unit pps, range 0 to 100000, the default value is disable.

Attention

1. The reset button will reset the attribute value of the selected port to the default value.
2.Do not use port rate limiting and storm suppression at the same time.

4.4 Storm Detection

The storm detection function is used to configure the broadcast and multicast traffic thresholds that are allowed to pass through each port. When the broadcast and multicast traffic on the port exceeds the threshold, alarm and response actions are triggered to close or block the port to prevent LAN storms and ensure the normal operation of the network. As shown in Figure 18.



Picture 18 storm detection function

This page is divided into two areas, the port is configured on the top, and the port parameter list is displayed on the bottom. When configuring the parameters of one or more ports, check the selection box in front of the port, the parameters of the selected port will be mapped to the upper configuration area, modify the parameters in the configuration area, and click "Modify" to save.

Each configuration item is described as follows:

Port Range: Port set to be configured, which cannot be entered manually, but can only be selected below.

Broadcast Detection: Set the broadcast threshold, the unit is pps, the range is 0 to 1000000, and the default is disabled.

Multicast Detection: set the multicast threshold, the unit is pps, the range is 0~1000000, the default is disable

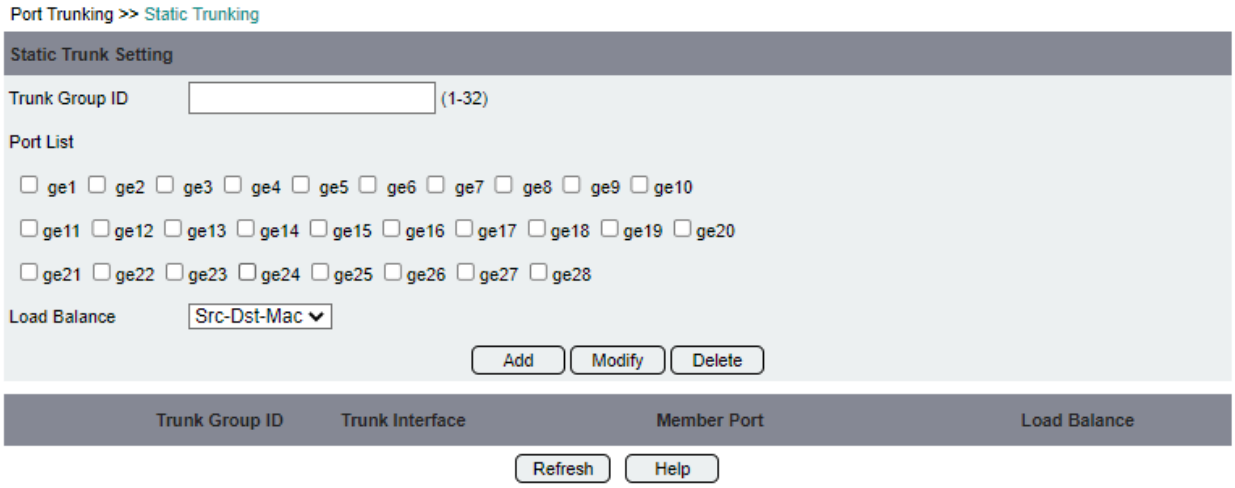
Trigger Action: The response action that exceeds the threshold, the default port is down.

Recovery Time: The recovery time of the controlled interface, the range is 3 to 36000s, and the default is 60s.

4.5 Port Aggregation

4.5.1 Static Aggregation

The static aggregation function binds multiple physical ports into one logical port, increasing the bandwidth between switches. Static aggregation does not allow ports in the aggregation group to be added or deleted automatically, and the aggregation group contains at least one port. As shown in Figure 19.



Picture 19 static aggregation

This page is divided into two parts. The group ID, member port and load balancing mode of the static aggregation group are configured on the top; the list of configured static aggregation groups is displayed below.

Each configuration item is described as follows:

Aggregation group ID: The ID of the static aggregation group. The specific range is subject to the actual model.

Aggregation interface: The interface name of the static aggregation group.

Member ports: List of ports added to the static aggregation group.

Load balancing: The load balancing mode of the static aggregation group is divided into six modes: src-mac, dst-mac, src-dst-mac, src-ip, dst-ip, and src-dst-ip.

4.5.2 LACP

LACP binds physical ports to logical ports, and only ports that pass the negotiation are allowed to bind, and others are not allowed. As shown in Figure 20.

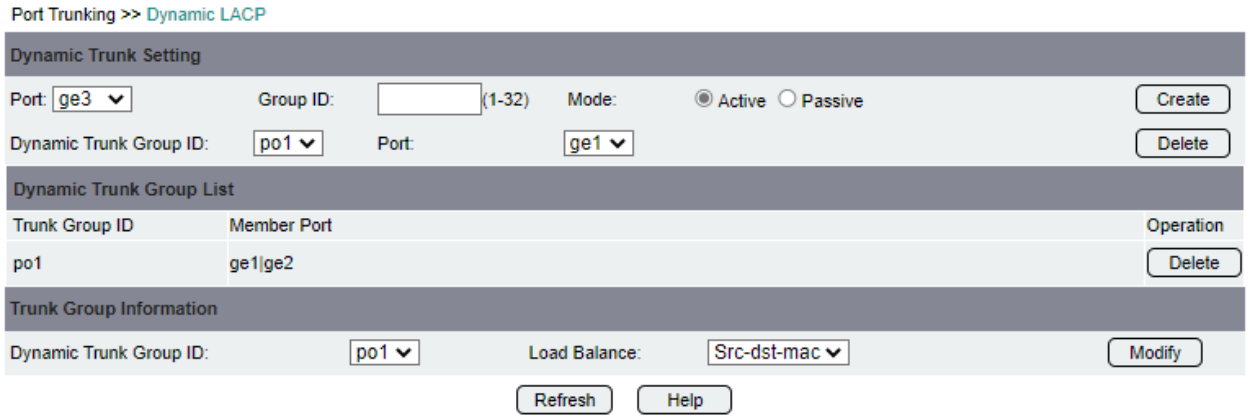


Figure 20 Dynamic LACP page

This page is divided into three parts: the first part creates a dynamic aggregation group, adds and deletes the member ports of the dynamic aggregation group; the second part deletes the dynamic aggregation group; the third part modifies the load balancing mode of the specified dynamic aggregation group, and checks the connection information.

Each configuration item is described as follows:

Port: The member port that joins the aggregation group.

Group ID: The ID of the dynamic aggregation group. The specific range is subject to the actual model.

Mode: The working mode of the port, divided into active and passive.

Load balancing: The load balancing mode of the dynamic aggregation group is divided into six modes: src-mac, dst-mac, src-dst-mac, src-ip, dst-ip, and src-dst-ip.

4.5.3 LACP Port Information

The LACP port information page displays the detailed configuration and status information of the member ports of the dynamic aggregation group, as shown in Figure 21.

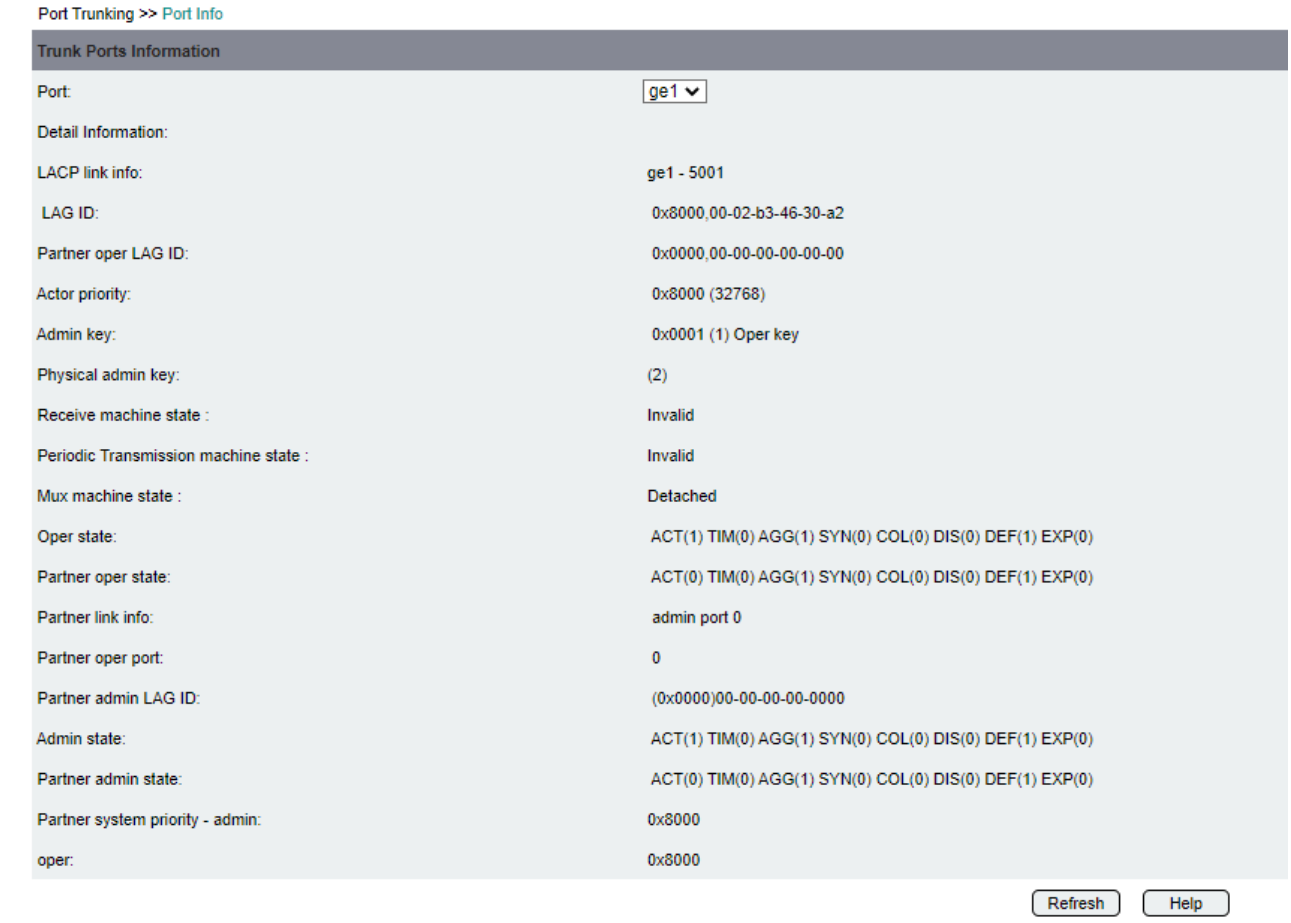


Figure 21 LACP port information page

4.6 Port mirroring

The port mirroring function is to copy the data in the specified direction of one or more mirrored ports to the monitoring port, and observe the data of the mirrored port through the monitoring port. Port mirroring is commonly used to troubleshoot, debug, and analyze networks. As shown in Figure 22.

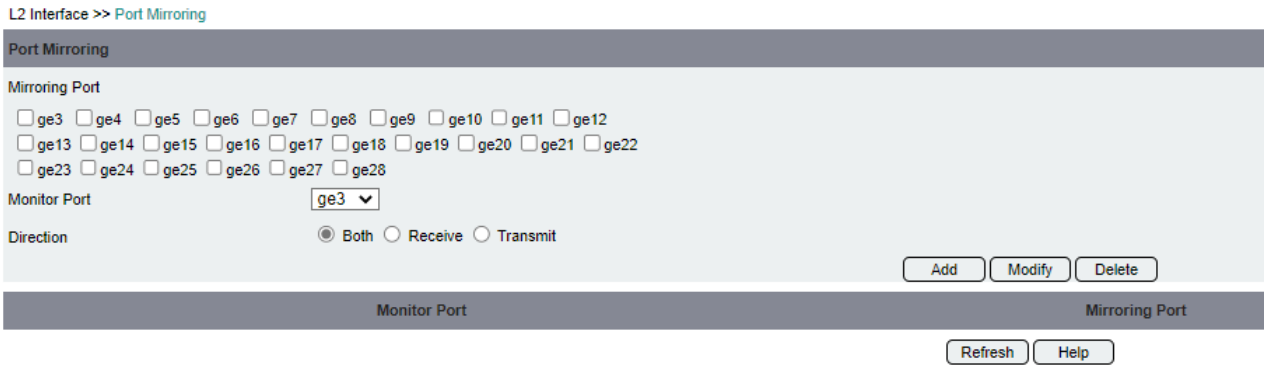


Figure 22 Port mirroring page

This page is divided into two parts, the mirroring rules are configured on the top, and the mirroring rules list is displayed below.

Each configuration item is described as follows:

Mirrored port: The monitored port can be one or more. The data in the specified direction is copied to the monitored port.

Monitoring port: The monitoring port, which can only be unique, monitors the data in the specified direction of the mirror port.

Direction: The data collection direction of the mirror port, divided into inbound direction, outbound direction and bidirectional.

Attention

1.It is allowed to configure multiple mirror groups, but there are restrictions on the number of directions, and the actual model shall prevail;

2.The mirror port cannot be the monitoring port at the same time;

3. Only the direction of port mirroring can be modified;

4. Port mirroring is mainly used for debugging and should be disabled under normal circumstances, otherwise er functions of the mirrored port may be unavailable.

4.7 Port Isolation

The port isolation function is used to prohibit data forwarding between different ports in a VLAN. Ports with isolation enabled cannot communicate; ports without isolation, or between isolated ports and un-isolated ports, can communicate normally.

After checking the ports in the list, you can configure whether port isolation is enabled or not.

Each configuration item is described as follows:

Port range: The set of Layer 2 ports whose properties need to be modified.

Port isolation enable: enable/disable port isolation, default is off

Attention

1.Port isolation can only be configured on Layer 2 interfaces

2. Port isolation cannot be configured on aggregation group or aggregation group member ports.

3. All ports share an isolation group.

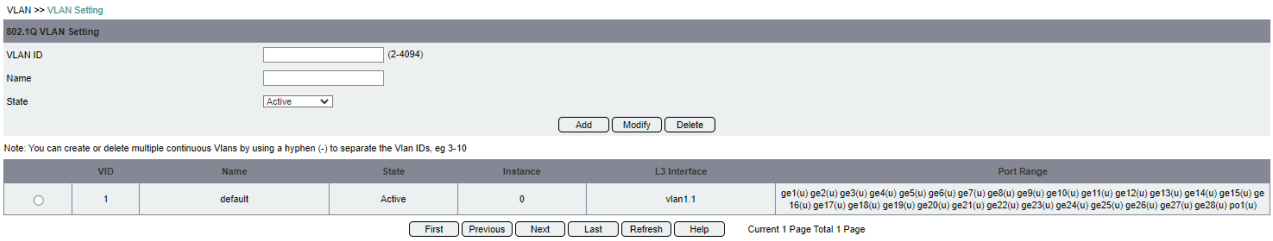
5 Layer 2 Features

5.1 VLAN

VLAN (Virtual Local Area Network) refers to the virtual local area network technology, which divides a physical LAN into multiple logical LANs, and each VLAN is a broadcast domain. Hosts in a VLAN exchange packets through traditional Ethernet communication. Hosts in different VLANs cannot communicate directly, and must use Layer 3 network devices.

5.1.1 VLAN Configuration

As shown in Figure 24.



This page is divided into two parts, the upper part configures the VLAN attribute, and the lower part displays the VLAN list. Each configuration item is described as follows:

VLAN ID: range from 2 to 4094. Use "-" to connect in batch configuration.

Name: The name of the VLAN.

Status: active or suspended, default active

Attention

1. A maximum of 100 consecutive vlans can be created or deleted in a batch at a time.

5.1.2 Port VLAN

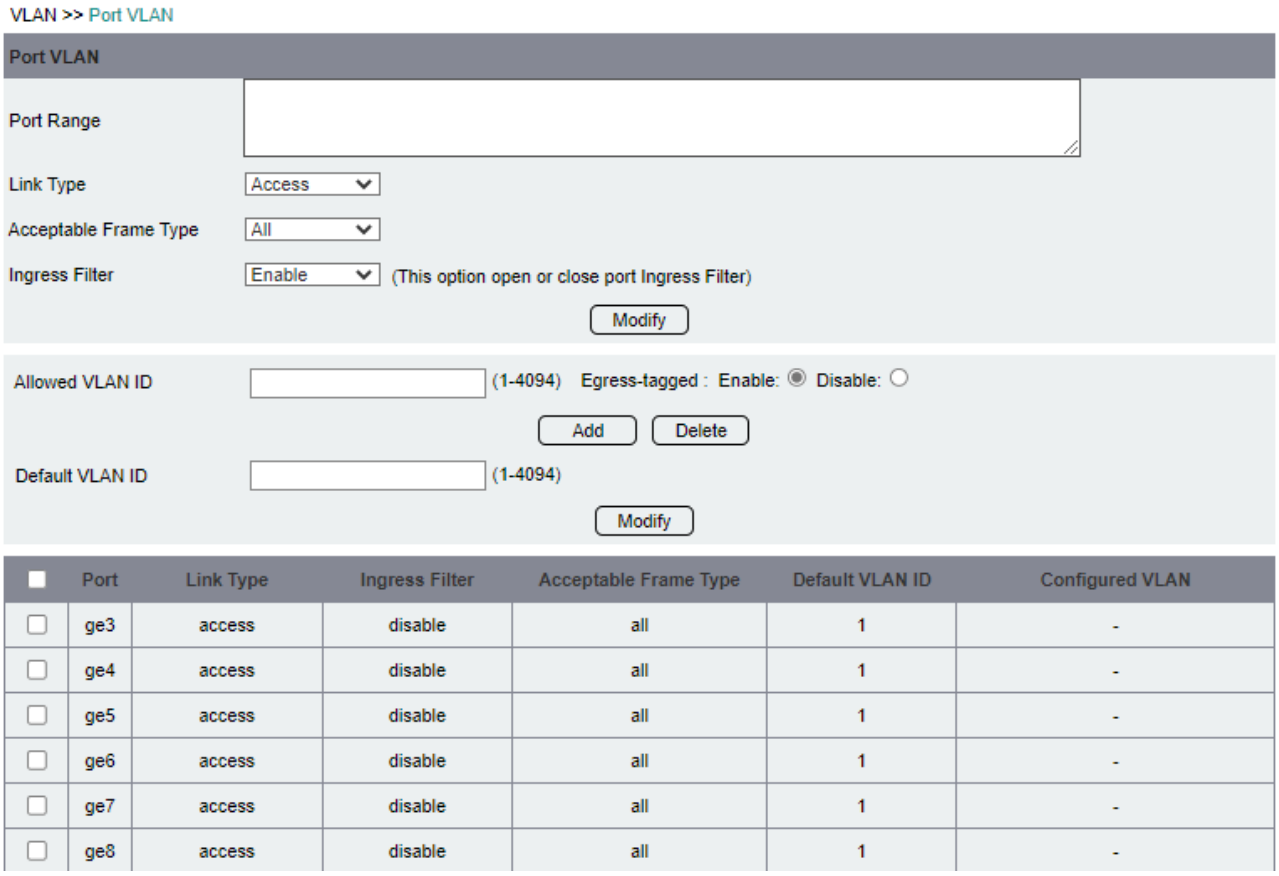


Figure 25 Port VLAN page

This page is divided into two parts. The upper part configures the port VLAN attributes, and the lower part displays the list of port VLAN attributes. Select the ports in the list, map them to the configuration area, and then modify their VLAN attributes.

Each configuration item is described as follows:

Port range: The set of Layer 2 ports whose properties need to be modified.

Link type: The optional link type is Access, Trunk or Hybrid, and the default is Access.

Acceptable frame types: All means receiving all packets, Vlan-untagged means only receiving packets without VLAN tags, Vlan-tagged means only receiving packets with VLAN tags, the default is All.

Ingress filtering: enable or disable, disabled by default.

Allow VLAN ID: Set the VLAN range that the port is allowed to pass through. Only Trunk and Hybrid ports can be set.

Egress tag: Set whether the packet is tagged with VLAN when going out of the port, only the Hybrid port can be set.

Default VLAN ID: Set the default VLAN ID of the port. The PVID of the trunk is fixed at 1 and cannot be modified.

Attention

1. The VLAN attributes of different types of ports cannot be set at the same time.
2.Allow VLAN ID, egress tag, and default VLAN ID can only be set by modifying the link type first.

5.1.3 MAC VLAN

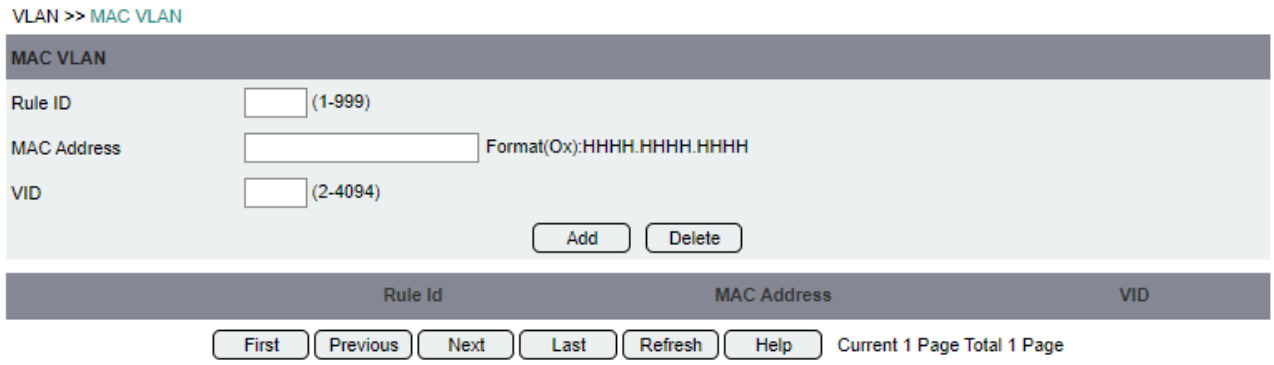


Figure 26 MAC VLAN page

This page is divided into two parts, the upper part configures the MAC VLAN rules, and the lower part displays the MAC VLAN rule list. Each configuration item is described as follows:

Rule ID: identifies the MAC VLAN rule, ranging from 1 to 999.

MAC Address: The MAC address to which the VID needs to be assigned.

VID: The VID to be allocated, ranging from 2 to 4094.

Attention

1. Only one rule can be configured per MAC, that is, only one VID can be assigned to each MAC.

5.1.4 Subnet VLAN

This page is divided into upper and lower parts. The upper part configures the subnet VLAN rules, and the lower part displays the subnet VLAN rule list. Each configuration item is described as follows:

Rule ID: identifies the subnet VLAN rule, ranging from 1000 to 1999.

IP address: The subnet network segment to which the VID needs to be assigned.

VID: The VID to be allocated, ranging from 2 to 4094.

Attention

1. Only one rule can be configured for each subnet segment, that is, only one VID can be assigned to each subnet segment.

5.1.5 Protocol VLAN

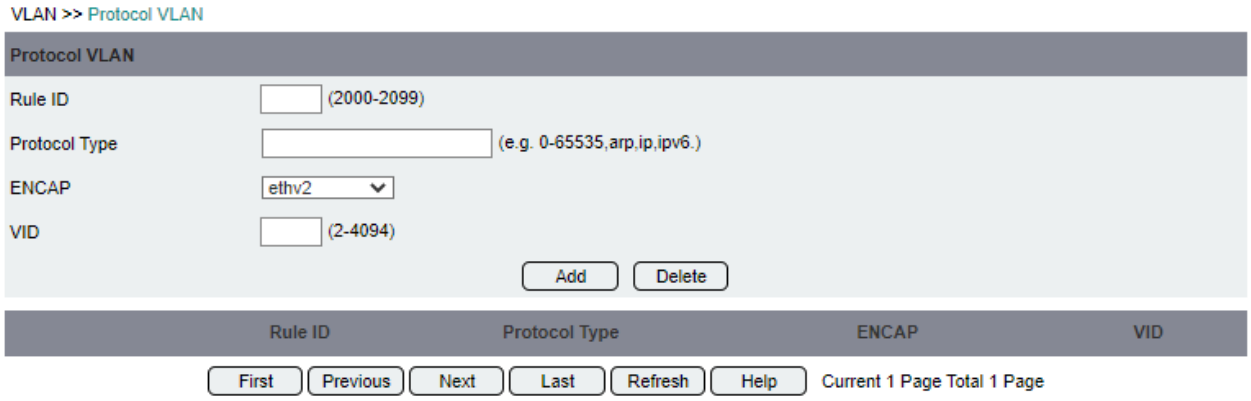


Figure 28 Protocol VLAN page

This page is divided into upper and lower parts. The upper part configures the protocol VLAN rules, and the lower part displays the protocol VLAN rule list. Each configuration item is described as follows:

Rule ID: identifies the protocol VLAN rule, ranging from 2000 to 2099.

Protocol Type: The protocol type for which VID needs to be assigned.

ENCAP: Layer 2 encapsulation type, supports three types: ethv2, nosnapllc and snapllc.

VID: The VID to be allocated, ranging from 2 to 4094.

Attention

1. Only one rule can be configured for each protocol, that is, only one VID can be assigned to each protocol.

5.1.6 VLAN Rules

Configure VLAN mapping rules for ports: including MAC, subnet and protocol-based VLAN rules. As shown in Figure 29.

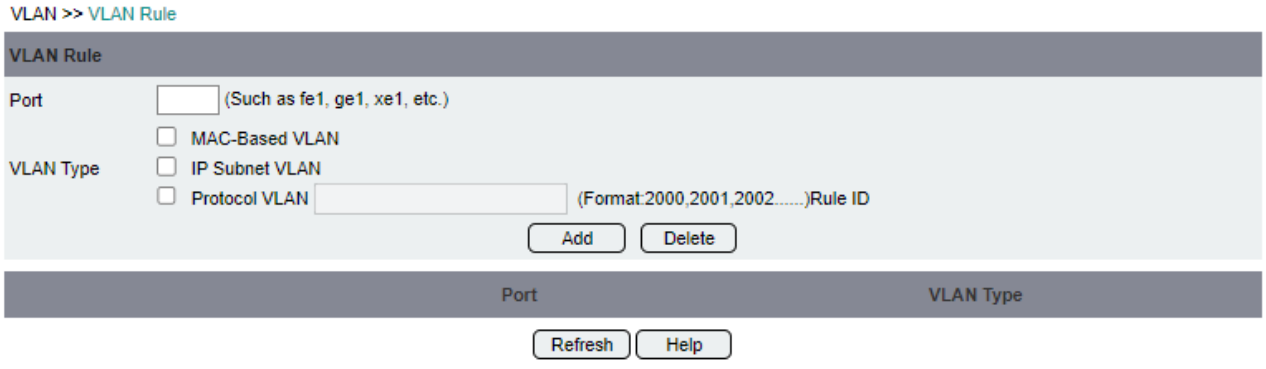


Figure 29 VLAN Rules page

This page is divided into upper and lower parts. The upper part configures the VLAN type used by the port,

and the lower part displays the list of port VLAN rules. Each configuration item is described as follows:

Port: The port to which the VLAN rule is applied.

VLAN classification: The VLAN type used by the port, there are three options: MAC VLAN, subnet VLAN and protocol VLAN.

Attention

1. VLAN rules based on MAC, subnet and protocol must be enabled to take effect.

5.1.7 GVRP Configuration

The GVRP protocol is used to maintain the dynamic VLAN attributes of the device. Through the dynamic distribution, registration and propagation of VLAN attributes, the VLAN information on a device is quickly spread to the entire network, effectively reducing the workload of manual configuration. As shown in Figure 30.

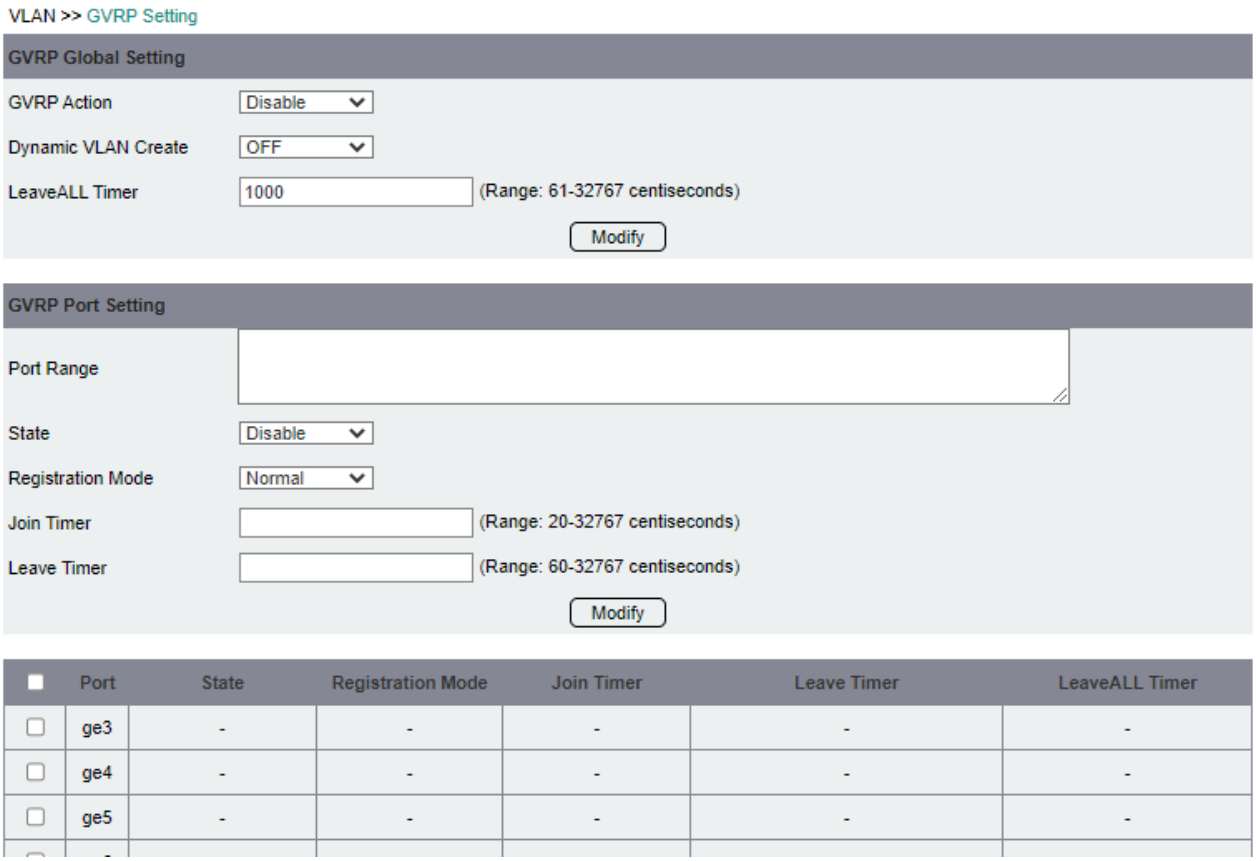


Figure 30 GVRP configuration page

This page is divided into two parts, the first part configures the global attributes of GVRP, and the second part configures and displays the port attributes of GVRP. When configuring GVRP port attributes, you need to check the list first, map the port attribute value to the GVRP port configuration area, and then modify it.

Each configuration item is described as follows:

GVRP function: enable or disable, disabled by default.

Dynamic VLAN Creation: Enable or Disable, disabled by default.

LeaveAll timer: the unit is centiseconds, the default value is 10000.

Port range: Configure the port set, which cannot be entered manually, but can only be automatically filled in by checking the list.

Status: Whether GVRP is enabled on the port, it is disabled by default.

Registration mode: Normal, Fixed and Forbidden are optional, the default is Normal.

Join timer: The unit is centiseconds, and the default value is 20.

Leave timer: The unit is centiseconds, the default value is 60.

Attention

1. The GVRP port must be a trunk port.

5.2 MAC

5.2.1 MAC Address Table List

The MAC address table is a port-based Layer 2 forwarding table and is the basis for fast forwarding of packets. The MAC address table contains several forwarding entries, and each forwarding entry has a corresponding destination MAC, port VID, and forwarding port. As shown in Figure 31.

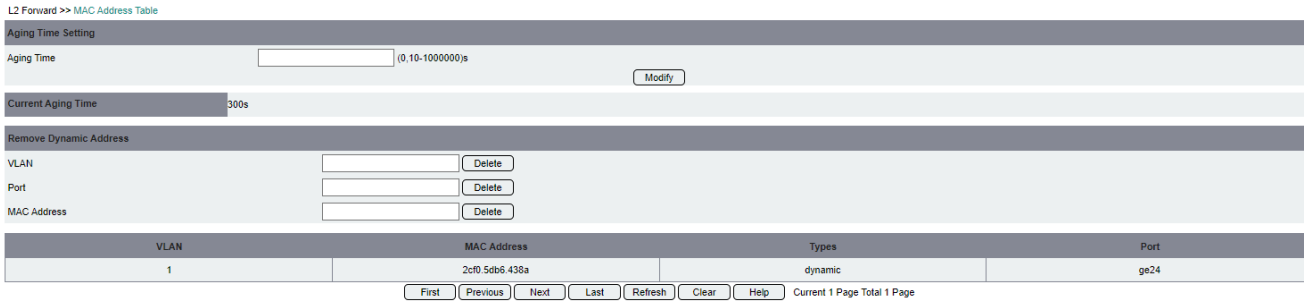


Figure 31 MAC address table page

This page is divided into four parts, the first part configures the MAC aging time, the second part displays the current MAC aging time, the third part deletes dynamic MAC entries based on VLAN, port or MAC, and the fourth part displays all dynamic and static MAC transfer Post items.

Each configuration item is described as follows:

Aging time: unit s, range 0, 10~100000, default 300s. 0 means no aging.

VLAN: Delete the dynamic forwarding entry of the specified VLAN.

Port: Delete the dynamic forwarding entry of the specified port.

MAC address: Delete the dynamic forwarding entry of the specified MAC address.

Attention

1. Delete and clear only for dynamic MAC entries.
2. The clear operation deletes all dynamic MAC entries.

5.2.2 Static MAC

The static MAC does not age, and the packets matching the MAC and VLAN in the static MAC forwarding table are forwarded to the specified port.

MAC filtering is a security mechanism that applies to all ports. Packets matching the MAC and VLAN in the MAC filtering list are filtered by all ports. As shown in Figure 32.

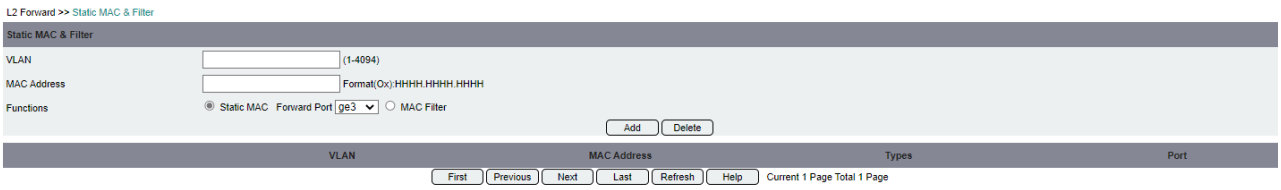


Figure 32 Static MAC page

This page is divided into upper and lower parts. The static MAC forwarding and filtering rules are configured on the top, and the static MAC rule list is displayed on the bottom. Each configuration item is described as follows:

VLAN: The VLAN to which the static MAC belongs.

MAC Address: Static MAC address.

Function selection: static MAC forwarding or MAC filtering, where static MAC forwarding must specify a port, and MAC filtering works on all ports.

Attention

1.MAC filtering, also known as black hole MAC, is a security mechanism that will cause specified packets to fail to pass through the switch. Please use it as appropriate.

2.Static MAC and black hole MAC do not age out automatically and can only be deleted manually.

5.2.3 MAC Binding

MAC binding binds the port to the specified MAC. Only the packets whose source MAC or destination MAC is equal to the binding MAC can be received and forwarded by the specified port, and all other packets are discarded. As shown in Figure 33.

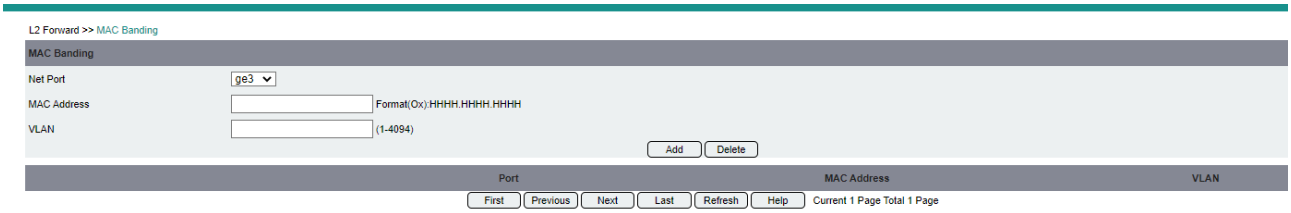


Figure 33 MAC Binding Page

This page is divided into two parts, the upper part configures the MAC binding rules, and the lower part displays the rule list. Each configuration item is described as follows:

Network Port: The port bound to the MAC.

MAC address: The MAC bound to the port.

VLAN: Bind the corresponding VLAN.

Attention

1. MAC binding binds the port to the MAC, which causes other packets to fail. Please use it with caution.

2. MAC binding is for the specified port, and MAC filtering is for all ports.

3. The bound MAC address does not age out automatically and can only be deleted manually.

5.2.4 MAC Automatic Binding

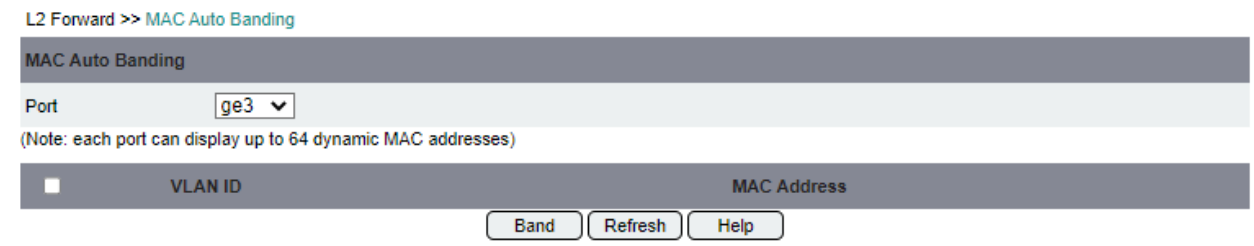


Figure 34 MAC automatic binding page

MAC auto binding is a complement to MAC binding. First select the port, and the page will display all dynamic MACs under the port; then select the entry and click "Bind" to automatically bind the MAC to the port.

5.2.5 MAC Learning Restrictions

MAC Learning Limit restrict the number of MAC learning for a port. When this value is exceeded, the port will no longer learn MAC dynamically. When a large number of forwarding entries exist in the MAC address table of a switch port, the forwarding performance of the port will be affected. The MAC learning limitation can solve this problem. As shown in Figure 35.

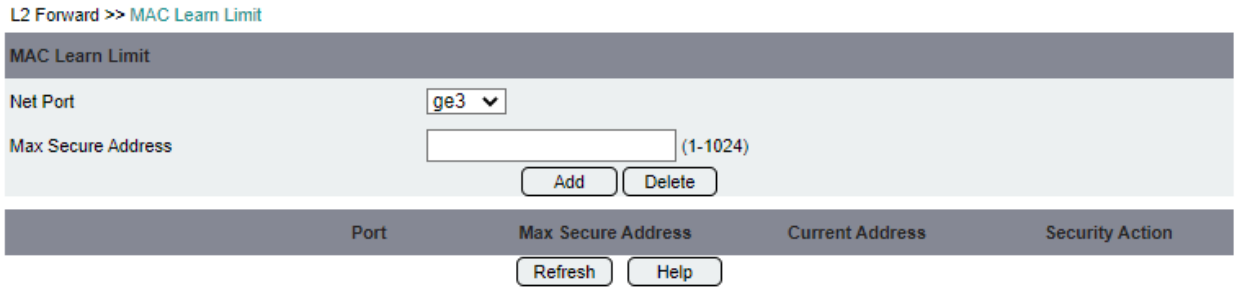


Figure 35 MAC Learning Restrictions page

This page is divided into upper and lower parts. The upper part configures the MAC learning restriction, and the lower part displays the port MAC learning restriction list. Each configuration item is described as follows:

Network Port: The physical port limited by MAC learning.

Maximum number of learning: The maximum number of MAC learning on the port, ranging from 1 to 1024.

5.3 Multicast

5.3.1 IGMP Snooping

The IGMP Snooping (Internet Group Management Protocol Snooping) function page is shown in Figure 36.

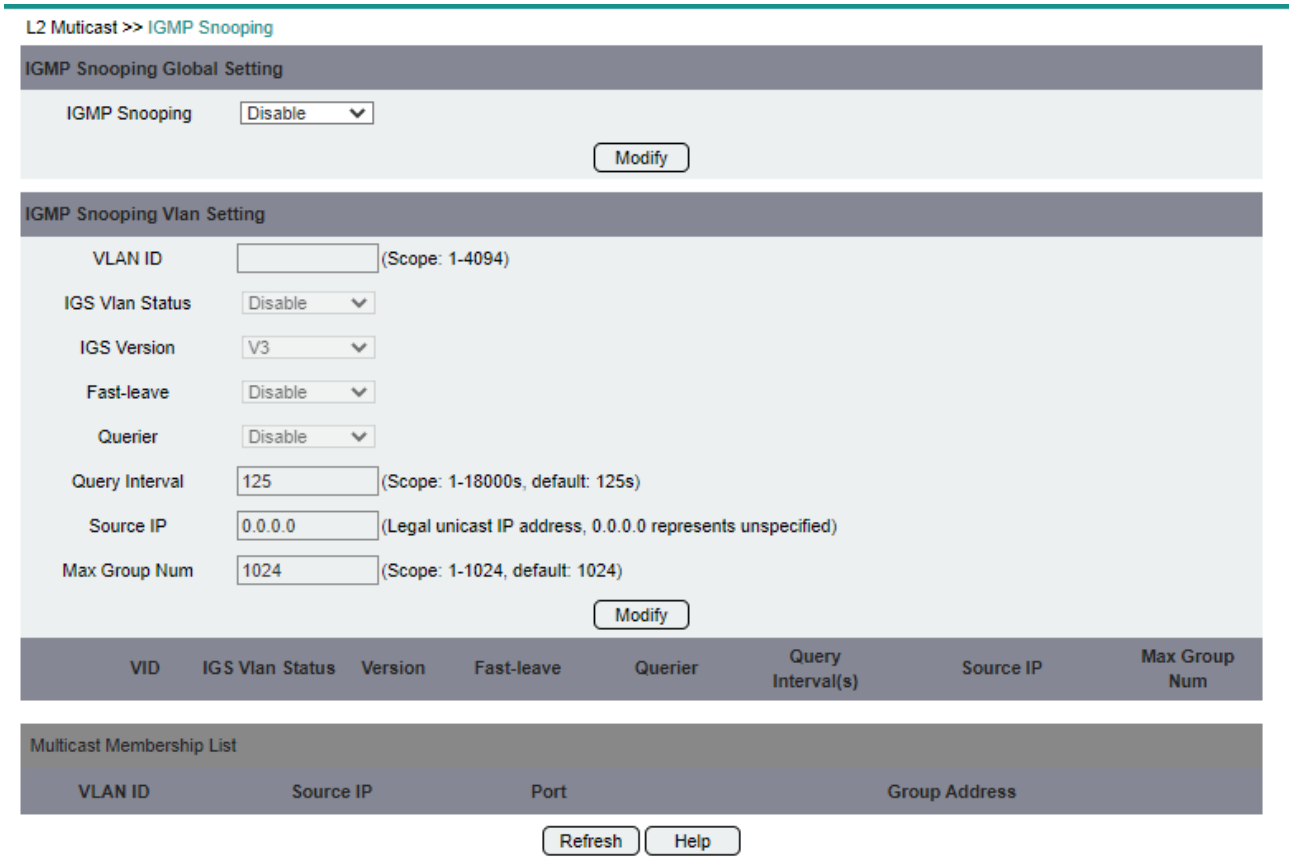


Figure 36 IGMP Snooping page

This page is divided into three parts, the first part configures the global IGMP Snooping enable switch, the second part configures and displays the detailed IGMP Snooping parameters of the VLAN, and the third part displays the list of all multicast members of the connected ports in the VLAN.

Each configuration item is described as follows:

IGMP Snooping: Enable/disable global IGMP Snooping, disabled by default.

VLAN ID: VLAN ID of IGMP Snooping, range: 1 to 4094.

IGS Vlan status: enable/disable the IGMP Snooping function in the vlan, disabled by default.

IGS version: The version of the IGMP protocol in the vlan, the default version is V3.

Quick leave group: Enable/disable IGMP quick leave group in vlan, disabled by default.

Querier: Enable/disable the IGMP querier within the vlan, disabled by default.

Query interval: The time interval for sending general query packets within the vlan, the range is 1 to 18000 seconds, and the default is 125 seconds.

Query packet source IP: The source IP of the query packet in the vlan must be a valid unicast IP. The default value of 0.0.0.0 means not specified.

Maximum number of multicast groups: the maximum number of groups allowed in the vlan, the range is 1 to 1024, and the default is 1024.

Multicast Member List: Displays the list of all static and dynamic multicast members learned by the active port.

Attention

1.The querier's query packet source IP must be a valid unicast IP. When the querier is disabled, the default value is 0.0.0.0.

5.3.2 Static Multicast

Static multicast is used to configure and display static multicast groups within a vlan. After the port joins the static multicast group, it will always receive the data of the multicast group. As shown in Figure 37.

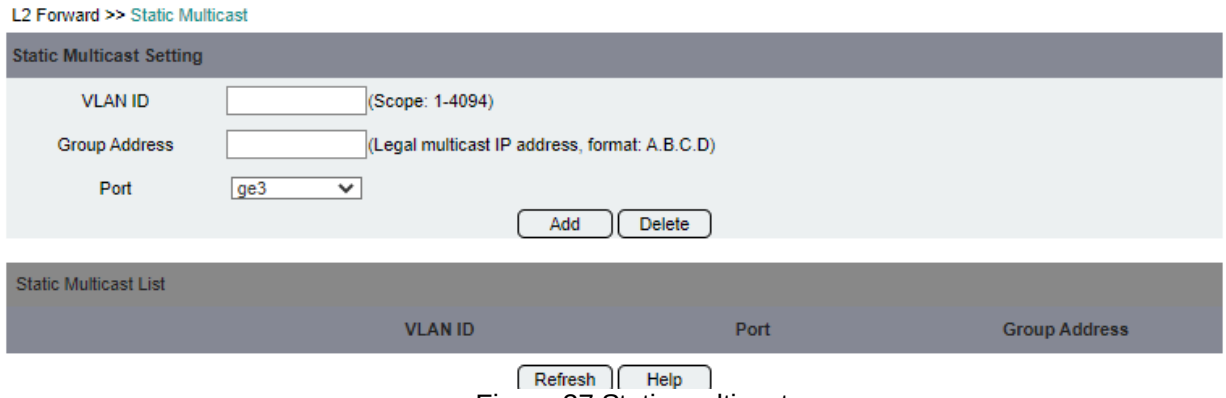


Figure 37 Static multicast page

This page is divided into upper and lower parts. The static multicast group in the vlan is configured in the upper page, and the list of all configured static multicast groups is displayed in lower page.

Each configuration item is described as follows:

VLAN ID: Static multicast VLAN ID, range: 1 to 4094.

Group Address: The statically added multicast group address, ranging from 224.0.1.0 to 239.255.255.255.

Port: The physical port bound by static multicast.

Static Multicast List: Display the list of static multicast groups.

Attention

1. The static multicast table of the VLAN can be configured only after IGMP Snooping of the VLAN is enabled.
2. Disabling IGMP Snooping of VLAN will clear the static multicast table of VLAN.
3. The static multicast table does not age and can only be deleted manually.
4. The list of multicast members for active ports in the static multicast table is also displayed in the list of multicast members for IGMP snooping.

5.4 LLDP

LLDP Link Layer Discovery Protocol is a neighbor discovery protocol that defines a standard method for Ethernet network devices, such as switches, routers, and wireless LAN access points, to advertise their presence to other nodes in the network, and save discovery information for nearby devices.

5.4.1 LLDP Configuration

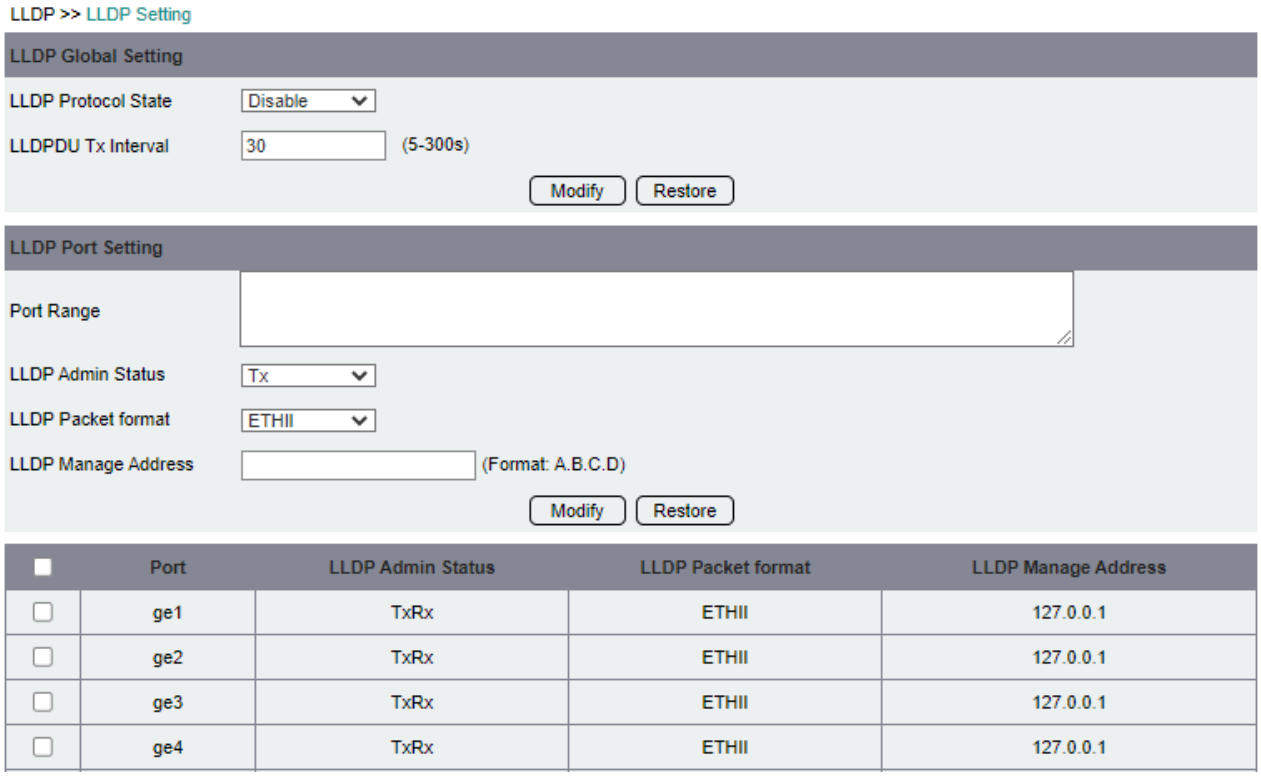


Figure 38 LLDP configuration page

The page is divided into two parts. The upper part configures the global parameters of LLDP, and the lower part configures and displays the port parameters of LLDP.

Each configuration item is described as follows:

LLDP protocol status: enable/disable global LLDP, the default is disabled.

LLDPDU sending interval: The interval for sending global LLDP packets, the range is 5 to 300 seconds, and the default is 30 seconds.

Port Range: LLDP port range, which can only be checked from the list.

LLDP working mode: Tx/Rx/TxRx/Disable, the default is TxRx.

Packet encapsulation format: EthernetII/SNAP, the default is EthernetII.

LLDP management address: The management IP advertised in LLDP packets, in the format of A.B.C.D.

Attention

1. In the working mode of LLDP, Tx means only sending but not receiving, Rx means only receiving but not sending, TxRx means both sending and receiving, Disable means neither sending nor receiving.
2. If the port is not configured with an LLDP management address, the primary IP of the VLAN with the smallest VLAN ID value that is allowed to pass through the port is preferentially selected as the LLDP management address. if the VLAN to which the port belongs is not configured with a primary IP or the port is disconnected, the LLDP management of the port is performed. The default address is the loopback address 127.0.0.1.

6 Ring Redundancy

6.1 Loopback Detection

A loop in the network will cause the device to repeatedly send broadcast, multicast, and unknown unicast packets, resulting in wasted network resources or even network paralysis. In order to detect loops in the Layer 2 network in time and avoid serious impact on the entire network, loopback detection provides a detection function, so that when a loop occurs in the network, users can be notified to check the network connection and configuration in time, and make the problematic interface under control.

Loopback detection periodically sends detection packets to check whether the packets are returned to the device,and then determines whether there is a loop between the interface, the network connected to the device, or the dual interfaces of the device. After a loop is found, the loopback detection sends an alarm and records a log to the NMS, and processes the interface according to the configuration, so that the interface is in a controlled state, reducing the impact of the loop on the device and the entire network.

You need to check the ports in the list first, map them to the configuration area, and then modify their configuration.

Each configuration item is described as follows:

Port range: The set of ports to which loopback detection is applied, it will be added automatically after checking the list.

Detection VLAN: The VLAN ID corresponding to loopback detection.

Detection Interval: The interval for sending loopback detection packets.

Action: After loopback detection is enabled, the response action of the interface when a loop exists.

Auto-recovery time: The interface in the controlled state, after the auto-recovery time elapses, the state returns to up, and the loopback detection is restarted.

Attention

The recovery time should be greater than 3 times the detection packet sending period.

6.2 Fast Ring Network

6.2.1 MW-RingV2

MW-RingV2 is an upgraded version of MW-Ring, which belongs to the company's private fast ring network technology. When the network connection is interrupted, the ring network redundancy mechanism immediately enables the backup link to quickly restore the network communication. As shown in Figure 40.

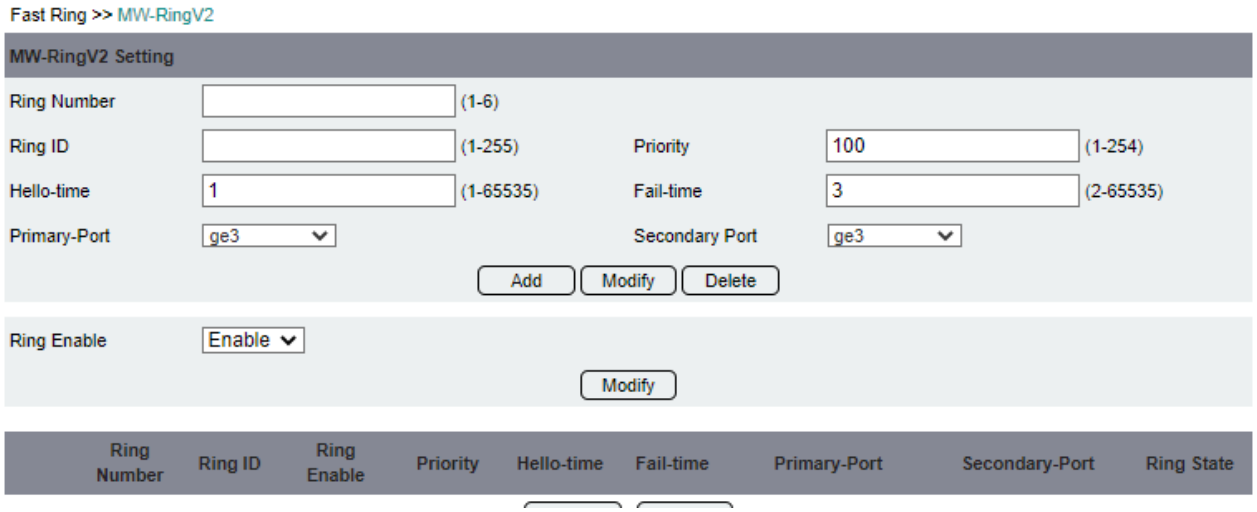


Figure 40 MW-RingV2 page

The page is divided into two parts. The upper part are the parameters of the MW-RingV2 and the enabled ring network. The bottom pat is list of the MW-RingV2 ring network displayed list.

Each configuration item is described as follows:

Ring number: The number of the ring network group. Up to 6 groups of fast ring networks can be enabled on each switch.

Ring ID: The network ID of the ring, ranging from 1 to 255.

Priority: The priority of the ring node, the value ranges from 1 to 254, and the default value is 100.

Hello-time: The interval for sending hello packets on the ring network. The value ranges from 1 to 65535 seconds. The default value is 1 second.

Fail-time: Delay of the fail timer of the ring node. The value ranges from 2 to 65535 seconds. The default value is 3 seconds.

Primary port: the priority forwarding port of the ring network node.

Slave port: The priority blocking port of the ring network node.

Attention

1. The switches in the same ring network group use the same ring network ID.
2. Switches in different ring groups use different ring IDs.
3. When modifying the parameters of the ring network group, the ring network must be disabled first, and then enabled after the modification is completed.
4. A switch can be designated as the master node by configuring the priority. The smaller the value, the higher the priority.
5. The Fail-Time of the ring network must be greater than the Hello-Time.
6. The master port and slave port cannot be the same port.
7. It is recommended not to enable fast ring/EAPS/MSTP/port aggregation functions at the same time.

6.3 EAPS

ERPS (Ethernet Ring Protection Switching), the Ethernet multi-ring protection technology, is a layer-2

network redundancy protection method. It can prevent the broadcast storm caused by the loop when the Ethernet ring is complete, and can quickly restore the pass link of each node on the ring network when the Ethernet link fails, and has a high convergence speed.

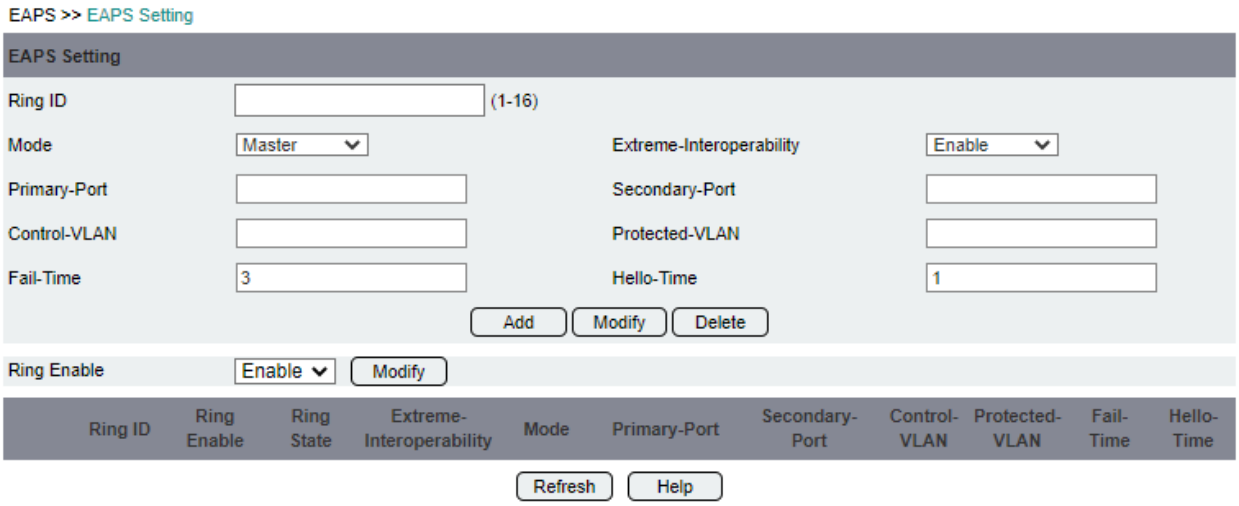


Figure 41 EAPS page

The page is divided into two parts. The upper part configures the EAPS parameters and enables the ring network, and the lower part displays the EAPS ring list.

Each configuration item is described as follows:

Ring Network ID: indicates the ID of the ring network. The value ranges from 1 to 16.

Node mode: indicates the mode of the switch in the ring, Master or Transit.

Extreme-Interoperability: whether to enable edge nodes.

Primary Port: indicates the primary port of the node.

Secondary Port: Secondary port of the node.

Control VLAN: Control VLAN of the ring network. It is used to transmit protocol packets. The value ranges from 2 to 4094.

Data VLAN: indicates the ring network data VLAN used to transmit service data. The value ranges from 1 to 4094.

Fail-Time: The unit is s. The value ranges from 2 to 65535.

Hello-Time: The unit is s. The value ranges from 1 to 65535.

Ring Network Enable: Enables or disables the ring network. This function is enabled by default.

Attention

1. The primary port and secondary port cannot be the same.
2. Control VLAN and data VLAN cannot be the same.
3. The value of Fail-Time must be greater than the value of Hello-Time.
4. When modifying the parameters of the ring network, the ring network must be disabled first, and then enabled after the modification is completed.

6.4 ERPS

ERPS (Ethernet Ring Protection Switching), the Ethernet multi-ring protection technology, is a layer-2 network redundancy protection method. It can prevent the broadcast storm caused by the loop when the Ethernet ring is complete, and can quickly restore the pass link of each node on the ring network when the Ethernet link fails, and has a high convergence speed.

The page is divided into two parts, on which the ERPS parameters are configured, as well as enabling and switching, and the ERPS ring list is displayed below.

Each configuration item is described as follows:

Ring ID: Uniquely identifies an ERPS ring, ranging from 1 to 255.

Node Mode: The node type of the switch in the ring, including:

Normal node: receive and forward protocol packets and service packets in the link;

RPL Owner node: The function is to block or open the RPL link (Ring Protection Link, that is, the link between the Owner node and the Neighbor node) to prevent the formation of loops.

RPL Neighbor node: The node directly connected to the Owner node on the RPL link is the Neighbor node, which blocks and opens the RPL port on this node together with the Owner node.

Ring type: Major (main ring) or Sub (sub ring). The main ring is a closed ring, and the subring is a non-closed ring. The ERPS ring can be composed of a single main ring, or a multi-ring structure can be formed by the main ring and sub-rings.

East port/west port: In the main ring, each node has 2 member ports, which are called east and west ports; in the sub-ring, the node connected to the main ring is called the interconnection node, and the sub-ring interconnection node There is only one member port, and only one of the east and west ports needs to be configured during configuration, and the other is configured as none.

RPL port: When the node type is Owner/Neighbor, the RPL port indicates which port is used as the port on the RPL link, and either east or west port can be selected. When the node type is Normal, this item is not configurable.

MW-ring: When the node type is the main ring, this item cannot be configured; when the node type is sub-ring, you need to configure the ID of the main ring to which the sub-ring node belongs. It must exist on the current node for the configuration to succeed.

Switchback mode**:** When the ERPS link returns to normal, you can decide whether to block the RPL link again by setting the switchback/non-switchback mode of the ERPS. Except for special needs, the configuration should be kept in failback mode.

 Switchback: If the faulty link recovers, after the WTR time, the RPL link will be blocked again, and all nodes will be stable in the Idle state.

 No switchback: If the faulty link recovers, the blocked link remains on the original faulty link, the

RPL link will not be blocked again, and all nodes are stable in the Pending state.

WTR timer: In switchback mode, the WTR timer is used to prevent frequent switchover protection operations when frequent link failures are detected. Before the timer expires, the RPL link keeps forwarding, and the port that recovers from the fault remains blocked. During this period, if the Owner node receives the SF protocol packet, it means that there is still a fault in the ring network, the timer is turned off, and the RPL link remains on. Otherwise, after the timer expires, the RPL link is blocked, and the Owner node sends (NR, RB) packets to notify the failure recovery node, release the temporarily blocked port, and refresh the MAC address table.

Guard timer: This timer is started after the node detects the fault recovery or executes the Clear command. It is used to prevent the old R-APS packets caused by the forwarding delay in the ring network from causing unnecessary oscillation to the network. Before this timer expires, any R-APS messages received, except event messages, will be ignored. Note that the duration of this timer should be greater than the delay for the R-APS packet to reach all nodes in the ring, but the longer the duration, the longer the node misses processing new requests from other nodes.

HoldOff timer: This timer is started when the node detects a fault, and the fault is not reported immediately. After the timer expires, if the fault still exists, it will be reported, which provides the service layer with the opportunity to repair the link. Note that the length of this timer will affect the reporting speed of the link failure, and ultimately affect the switching performance of the link.

Ring network enable: Enable or Disable the ring network. Generally, after the configuration is successful, the ring network is disabled by default and needs to be manually enabled.

Switching mode: ERPS can manually select the blocking state of the port by manually issuing switching commands, including FS (forced switching), MS (manual switching), and Clear (clearing operation).

FS (Forced Switching): You can choose any one of the east port or west ports. The port that is forced to switch will be blocked immediately, regardless of whether there is a faulty link in the ring.

MS (manual switching): any one of the east port or west port can be selected. When the ring state is Idle or Pending, the port that is manually switched will be blocked. If the link fails at this time, the ring will switch from MS state to Protection state, protection switching is performed.

Clear (clear operation): It can be used to clear the locally configured FS or MS operation, or use the Clear command to restore the node to the Idle state in advance before the WTR timer expires.

Attention

1. The east port and the west port should be the physical ports of the switch and cannot be the same.
2. A port can only belong to one ERPS ring. The control vlans of nodes in the same ERPS ring must be the same.
3. The control VLAN of ERPS must be a created VLAN, and cannot be configured on other ports except the east port or west port of the ring.

4. In addition to the control VLAN and the protection VLAN, it is better not to have other VLANs on the group ring port.

5. ERPS, EAPS, and private ring functions are mutually exclusive.

6.5 Spanning Tree

The MSTP (Multi Spanning Tree Protocol) protocol eliminates Layer 2 loops by selectively blocking redundant links in the network, and also has a link backup function. MSTP can make up for the shortcomings of STP and RSTP. It can not only converge quickly, but also forward traffic of different VLANs along their own paths, thus providing a better load sharing mechanism for redundant links.

6.5.1 MSTP Configuration

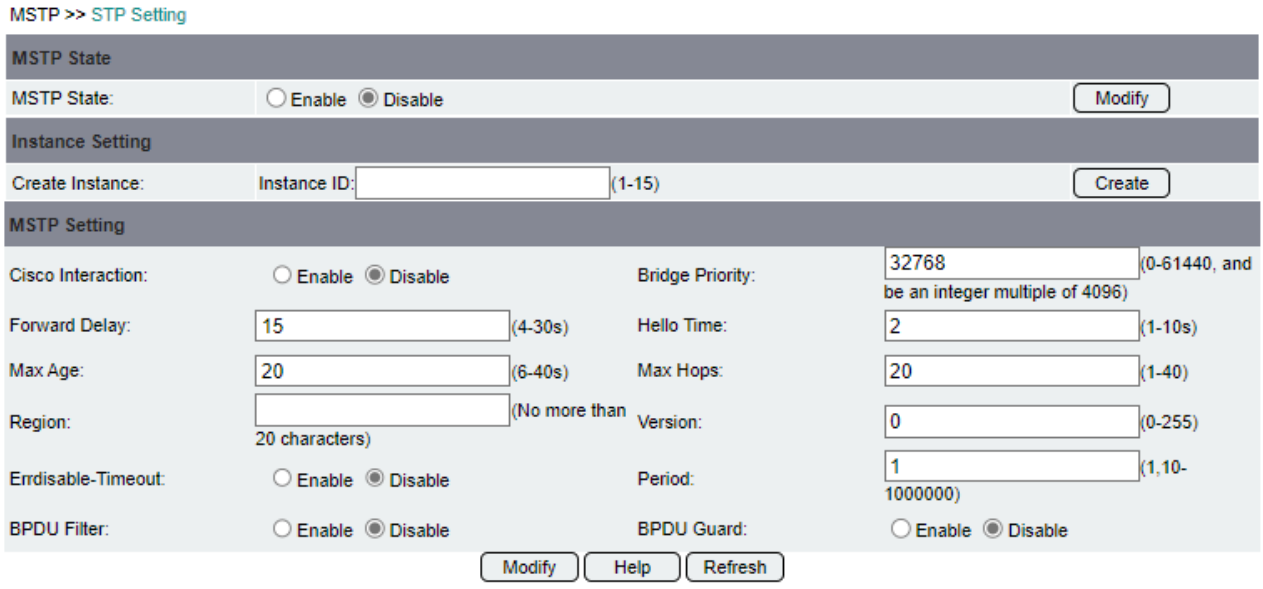


Figure 43 MSTP configuration page

The page is divided into three parts, the first part is the MSTP global switch, which can enable or disable MSTP; the second part creates an instance and configures VLAN; the third part configures MSTP global parameters, such as priority, forwarding delay, etc.

Each configuration item is described as follows:

MSTP switch: Enable or disable the MSTP function, disabled by default.

Instance ID: The ID of the created MSTP instance.

VLAN: Configure the VLAN parameters of the instance.

MSTP configuration: Configure the global parameters of MSTP, including Cisco interaction, priority, and forwarding delay.

6.5.2 MSTP Port Configuration

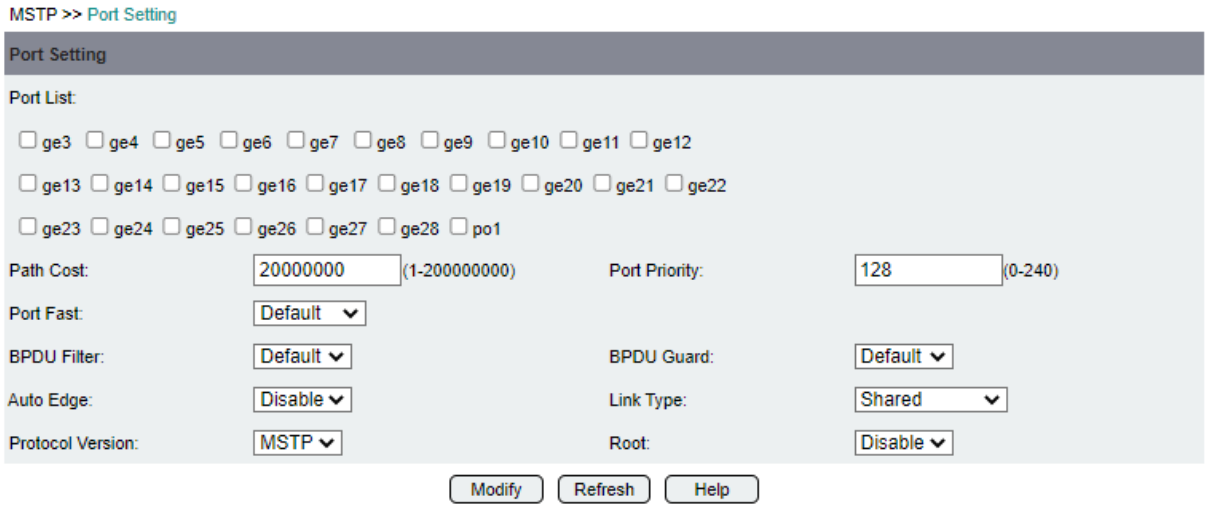


Figure 44 MSTP port configuration page

This page configures MSTP port parameters, including path cost, priority, BPDU filtering, etc. After the configuration is complete, click "Modify" to save the configuration. Users can view the specific configuration results of each port on the port information page of the MSTP module.

6.5.3 MSTP Basic Information

The MSTP domain configuration information is displayed, as shown in Figure 45.

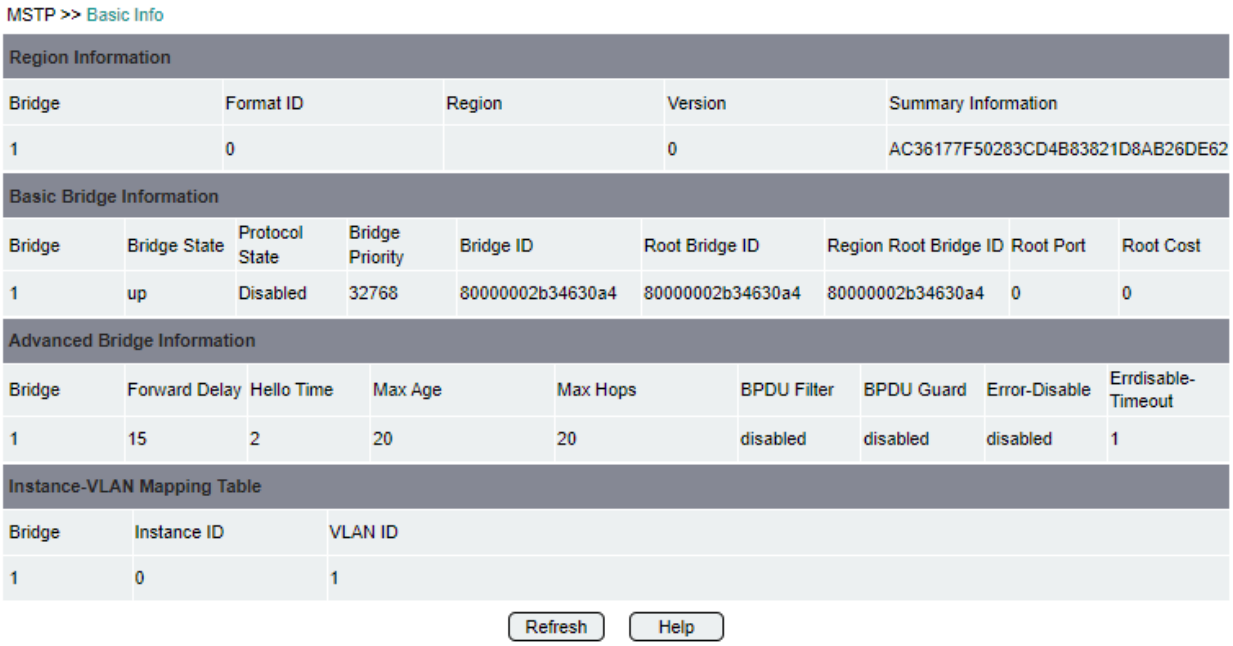


Figure 45 MSTP basic information page

6.5.4 MSTP Port Information

Displays the MSTP configuration and status information for the port, as shown in Figure 46.

MSTP >> Port Info

Port Info			
Port:	ge3		
Basic Port Information:			
Port:	ge3	Index:	5003
Port ID:	33675	Port Priority:	128
Role:	Disabled	State:	Discarding
Cost:	20000000	Acceptable Frame Type:	None
Outgoing Frame Type:	STP	Forward Transitions :	0
Port References:	1	Add Types:	Explicit
Port configuration information:			
Port:	ge3	Bridge:	1
Portfast Features:	OFF	Edge Port:	OFF
BPDU Guard:	OFF	BPDU Filter:	OFF
Root:	OFF	Link Type:	Shared
Protocol Version:	MSTP		
Priority Vector			
Port:	ge3	Root Bridge ID :	0000000000000000
External Path Cost:	0	Region Root ID:	0000000000000000

Figure 46 MSTP port information page

6.5.5 MSTP Instance Information

Displays instance bridge information, port and instance mapping information, as shown in Figure 47.

MSTP >> Instance Info

Instance Info						
Instance ID	Bridge	Instance Brige Priority	Instance Root Port	Instance Root Cost	Root Bridge ID	Instance Bridge ID
1	1	32768		0	8001000000000000	8001000000000000

Refresh Help

Figure 47 MSTP instance information page

6.5.6 MSTP Port Instance Information

Displays the role status information of the MSTP port in the instance, as shown in Figure 48.

MSTP >> Port Instance Info

Port Instance Info		
Instance:	1	No port exsit in the executive instance!

Refresh Help

Figure 48 MSTP port instance information page

6.5.7 MSTP Port Instance Relationship

Figure 49 MSTP port instance relationship page

7 Layer 3 Features

The content in this chapter is only applicable to our MBN8000 platform layer3 managed switch series products.

7.1 Layer3 Interface

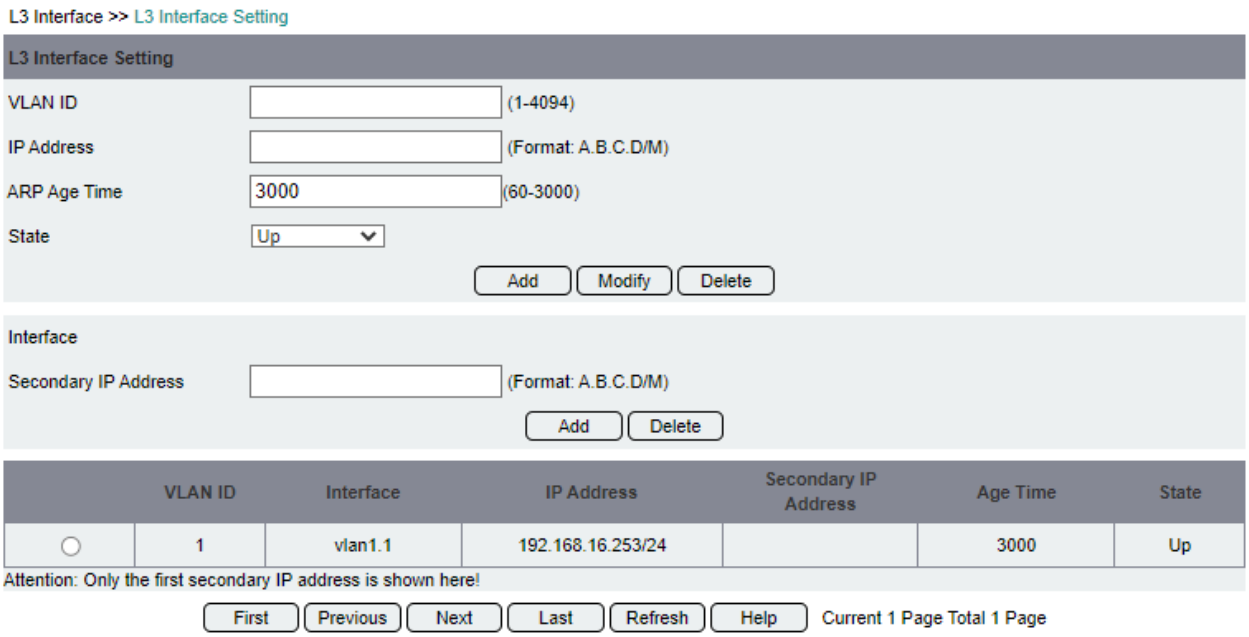


Figure 50 Layer 3 interface page

The page is divided into two parts. The Layer 3 interface parameters are configured on the top, and the Layer 3 interface list is displayed on the bottom.

Each configuration item is described as follows:

VLAN ID: The VID of the Layer 3 interface.

IP address: The primary IP address of the Layer 3 interface.

ARP aging time: The ARP aging time of a Layer 3 interface, in seconds, and the default value is 3000.

Management status: The status of the Layer 3 interface, Up or Down, the default is Up.

Interface: The name of the Layer 3 interface.

Slave IP address: The slave IP of the Layer 3 interface.

Attention

1.You must create a Layer 3 interface and configure the primary IP address, and then select the Layer 3 VLAN interface in the list before configuring its secondary IP address.

2.You must delete all secondary IP addresses on the Layer 3 interface before deleting the primary IP address.

3.A Layer 3 interface can be configured with multiple slave IPs, but only the first one can be displayed on the web page.

7.2 ARP

Static ARP specifies the mapping relationship between IP and MAC and is not affected by aging time. As shown in Figure 51.

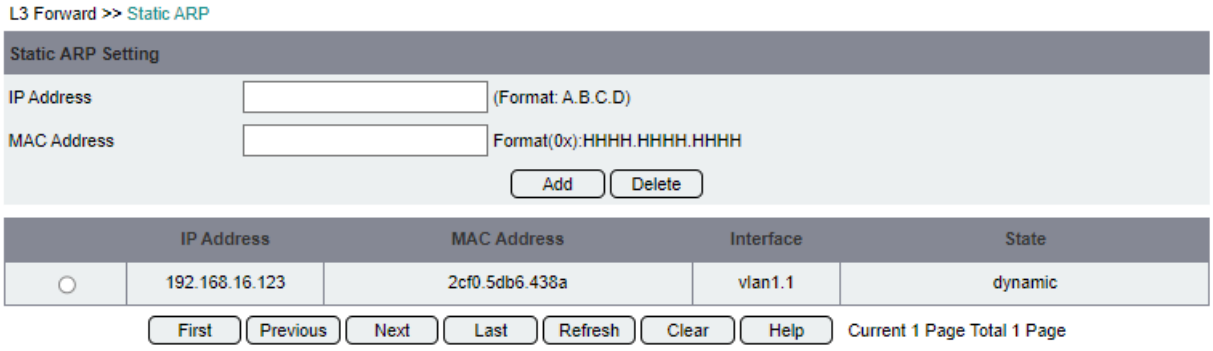


Figure 51 ARP page

The page is divided into two parts, the static ARP is configured on the top, and the dynamic and static ARP lists are displayed on the bottom. Each configuration item is described as follows:

IP address: The IP in the static ARP entry.

MAC address: The MAC corresponding to the IP in the static ARP entry.

Attention

1. Static ARP is not affected by aging time.

2. The "Clear" button can only delete all dynamic ARP; select the static ARP entry and click "Delete" to delete the static ARP.

7.3 Static Routing

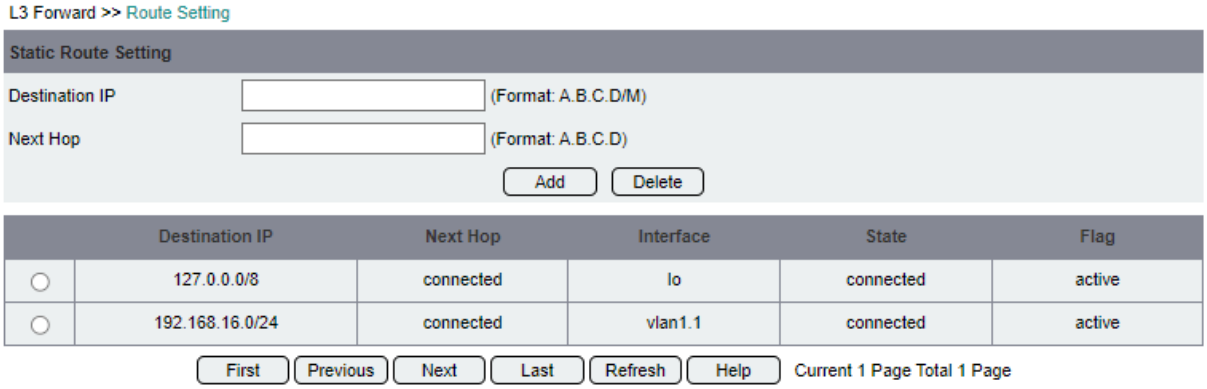


Figure 52 Static routing

.

Each configuration item is described as follows:

Destination IP address: The destination network segment of the static route.

Next-hop IP address: The next-hop address of the static route.

Attention

1. The static routing page can only add and delete static routes, but you can view all routing information.
2. The next hop IP cannot be the local interface IP.

8 Advanced Functions

8.1 SNMP

8.1.1 SNMP Configuration

Configure the administrator ID and device location, as shown in Figure 53.

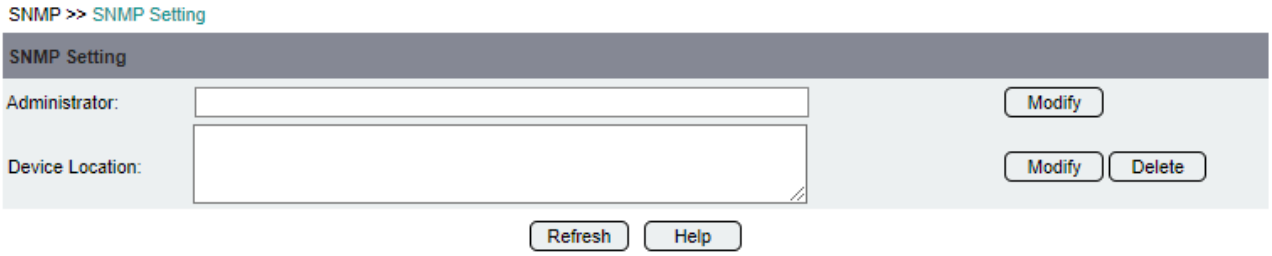


Figure 53 SNMP configuration page

8.1.2 Group Configuration

Figure54 Group configuration page

8.1.3 Trap Configuration

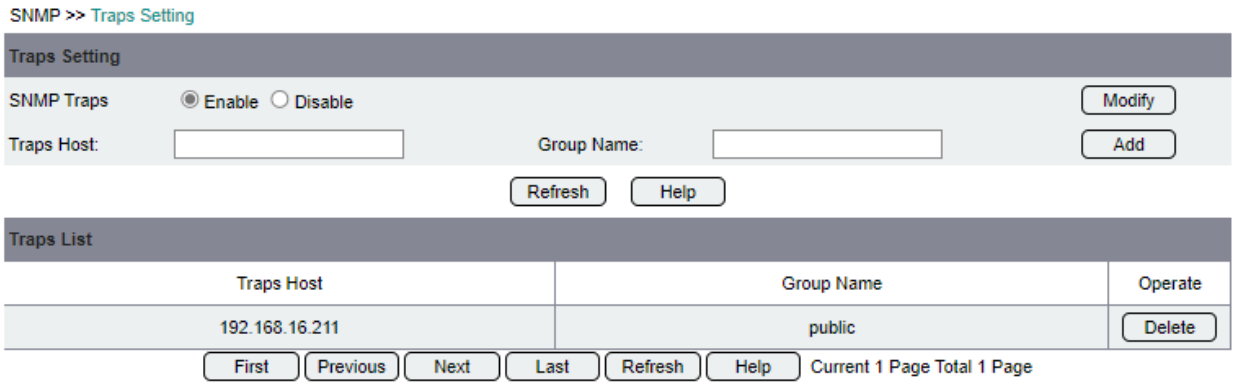


Figure 55 Traps configuration page

The page is divided into two parts. The upper part configures the SNMP Traps global switch, version, trap host and community name. The lower part displays the Trap list and its delete button.

8.2 ACL

ACL (Access Control List) implements packet filtering by configuring matching rules and processing operations for packets. The matching rules include the source address, destination address, and port number of the data packet.

An ACL consists of a series of entries, called an access control list entry (Access Control Entry: ACE). Each ACL entry declares the matching conditions and behaviors that satisfy the entry.

8.2.1 MAC ACL Configuration

MAC ACL formulates matching rules based on the source/destination MAC address and Ethernet II type of packets.

This page is divided into two parts. The upper part configures the MAC ACL parameters, and the lower part displays the MAC ACL list.

Each configuration item is described as follows:

ACL name: consists of letters, numbers or underscores, cannot be pure numbers, and is less than 20 in length.

Action: The processing action of the packet matching, allow or deny.

Source MAC address: HHHH.HHHH.HHHH or any (0000.0000.0000).

Source MAC mask: HHHH.HHHH.HHHH or host (FFFF.FFFF.FFFF) or any (0000.0000.0000).

Destination MAC address: HHHH.HHHH.HHHH or any (0000.0000.0000).

Destination MAC mask: HHHH.HHHH.HHHH or host (FFFF.FFFF.FFFF) or any (0000.0000.0000).

Data frame type: Decimal or hexadecimal representation, the value range is 0x0001~0xFFFF.

Add: Add an ACL rule.

Delete ACE: Delete the selected ACL rule entry.

Delete ACL: Delete a set of ACLs with the specified name.

Attention

1.* Indicates that it must be configured when adding ACL rules.

2. The name of the MAC ACL cannot be a pure number.

3. Creating a MAC ACL will automatically add an ACE at the end: deny any any, which can be replaced with permit any any.

4.ACE: deny any any /permit any any cannot be deleted with [Delete ACE], but can only be cleared with [Delete ACL].

8.2.2 IP ACL Configuration

IP ACL formulates matching rules based on Layer 3 and Layer 4 information of packets.

Each configuration item is described as follows:

ACL type:

Basic ACL: Make matching rules based on the source IP of packets.

Advanced ACL: According to the source/destination IP, source/destination port, IP protocol type and other Layer 3/4 information of the packet, the matching rules are formulated.

ACL number:

The number range of the basic ACL is 1 to 99 and 1300 to 1999.

The number range of an advanced ACL is 100 to 199 and 2000 to 2699.

Action: The processing action of the packet matching, allow or deny.

IP Protocol Type: The IP protocol type carried by the packet, ranging from 0 to 255, or the IP protocol name.

Source IP address: The source IP address of the packet, in the format *.*.*.* or any (0.0.0.0).

Source IP wildcard mask: The format is *.*.*.* or host (0.0.0.0) or any (255.255.255.255).

TCP/UDP packet source port number: The value ranges from 1 to 65535, or the TCP/UDP packet port name.

Destination IP address: The format is *.*.*.* or any (0.0.0.0).

Destination IP wildcard mask: the format is *.*.*.* or host (0.0.0.0) or any (255.255.255.255).

Destination port number for TCP/UDP packets: the value ranges from 1 to 65535, or the port name for TCP/UDP packets.

Add: Add an ACL rule.

Delete ACE: Delete the selected ACL rule entry.

Delete ACL: Delete a set of ACLs with the specified name.

Attention

1. Indicates that it must be configured when adding ACL rules.

2. The IP wildcard mask is expressed in dotted decimal, binary 0 means match, 1 means don't care, the opposite of subnet mask.

3. IP protocol names include: ahp, eigrp, esp, gre, icmp, igmp, ip, ipinip, ospf, pcp, pim, tcp, udp.

4. The TCP packet port names include: ftp, ftp-data, pop3, smtp, telnet, www.

5. UDP packet port names include: rip, snmp, snmp-trap, tftp.

6. Creating a basic ACL will automatically add an ACE at the end: deny any, which can be replaced with permit any.

7. Creating an advanced ACL will automatically add an ACE at the end: deny ip any any, which can be replaced with permit ip any any.

8. ACE: deny/permit any and deny/permit ip any any can only be cleared by [Delete ACL].

8.2.3 Applying ACLs to Ports

Applying an ACL to a port means applying an ACL rule to an interface to filter the packet flow received by the interface.

Each configuration item is described as follows:

ACL Port: The port to which the ACL is applied.

ACL group: any group of ACLs configured previously.

ACL direction: the application direction of the port ACL, in or out.

Attention

Before applying an ACL to a port, you must configure an ACL rule.

8.3 Network Diagnostics

8.3.1 Ping

The Ping function is used to detect whether the network connection is normal, as shown in Figure 59.

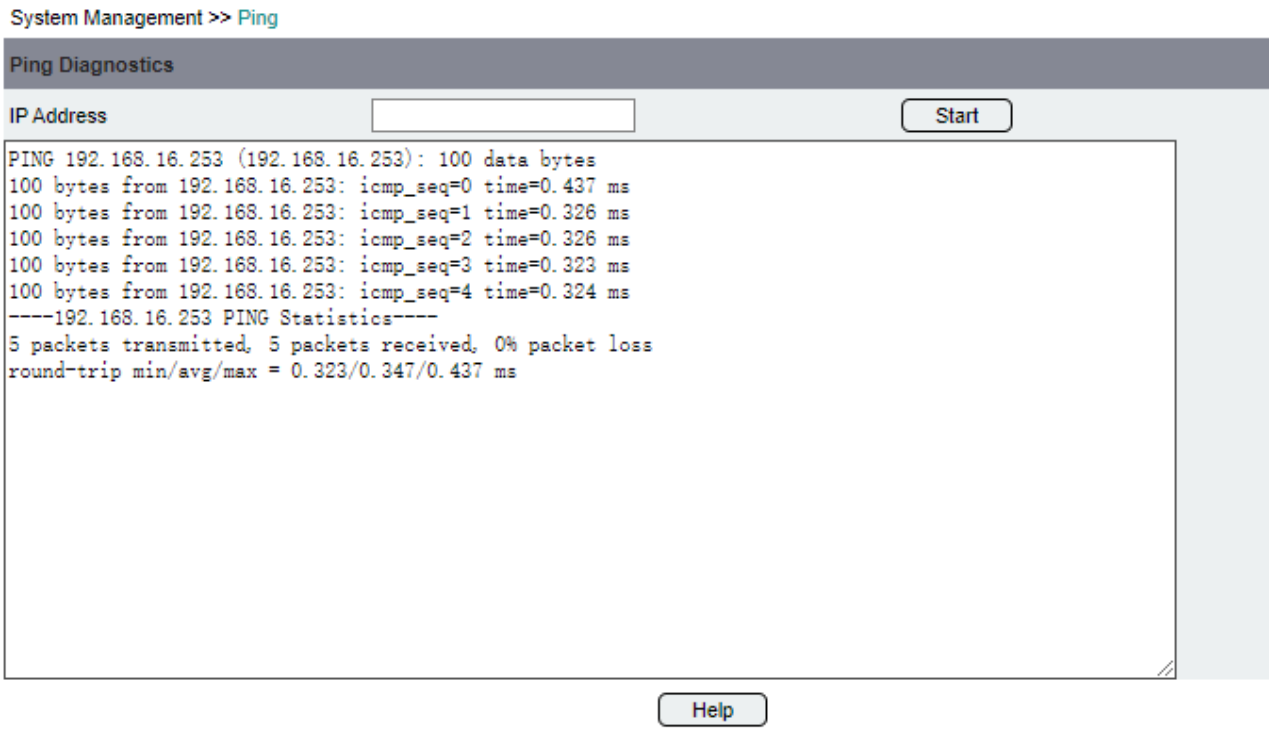


Figure 59 Ping page

8.3.2 Tracert

The tracert function is used to detect the path taken to reach the IP, as shown in Figure 60.

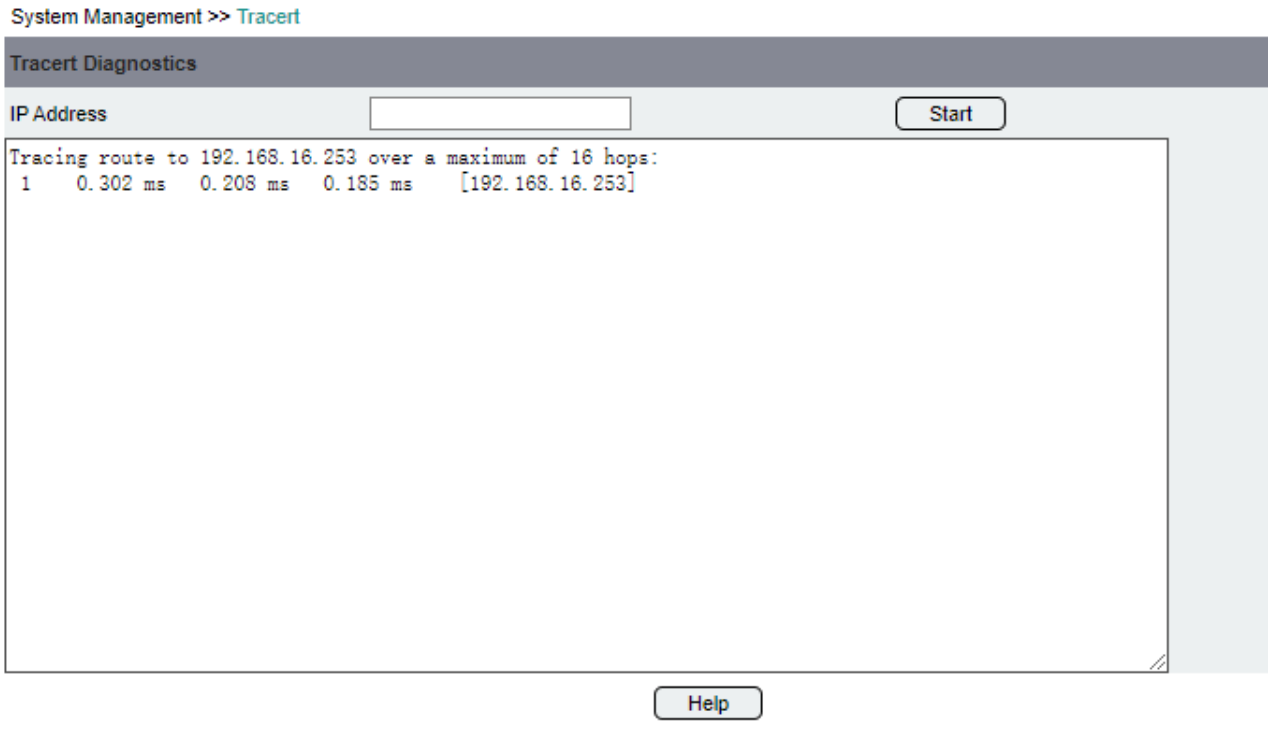


Figure 60 Tracert page

9 POE Management

This chapter only applies to our MBN8000 platform managed switch products with POE function.

PoE (Power over Ethernet, also known as remote power supply) It means that the device is connected to some IP-based external PD devices (Powered Device, such as IP phones, wireless APs, network cameras, etc.) through the Ethernet interface. , the technology of remote DC power supply while transmitting data signals.

9.1 POE Global Configuration

Each configuration item is described as follows:

Maximum power: The maximum total output power of POE, the unit is mW, the range is 1W~ 300W, the default is 300000mW.

Maximum overload: the percentage of the maximum allowable overload power to the total output power, the range is 0%~5%, and the default is 5%.

Reserved power: The percentage of the reserved power to the total output power, the range is 0%~10%, and the default is 10%.

9.2 POE Port Configuration

This page is divided into two parts, the POE port parameters are configured on the top, and the POE port parameter list is displayed below. You need to check the list first, map the attribute value of the POE port to the configuration area on the bottom, and then modify its parameter configuration.

Each configuration item is described as follows:

Port Enable: Enable and disable the POE power supply function of the port, which is enabled by default.

Maximum power: The maximum power that the port can provide externally, in mW, ranging from 1W to 30W, and the default is 30000mW.

Port priority: port power supply priority, the default is low, including:

Critical: highest priority

High: The next highest priority

Low: Lowest priority

10 System Management

10.1 Device Address

The content in this section is only applicable to our MBN8000 platform L2 managed switch products.

10.1.1 Static IP

Configure the IP address and default gateway, as shown in Figure 63.

Figure 63 Static IP page

10.2 System Time

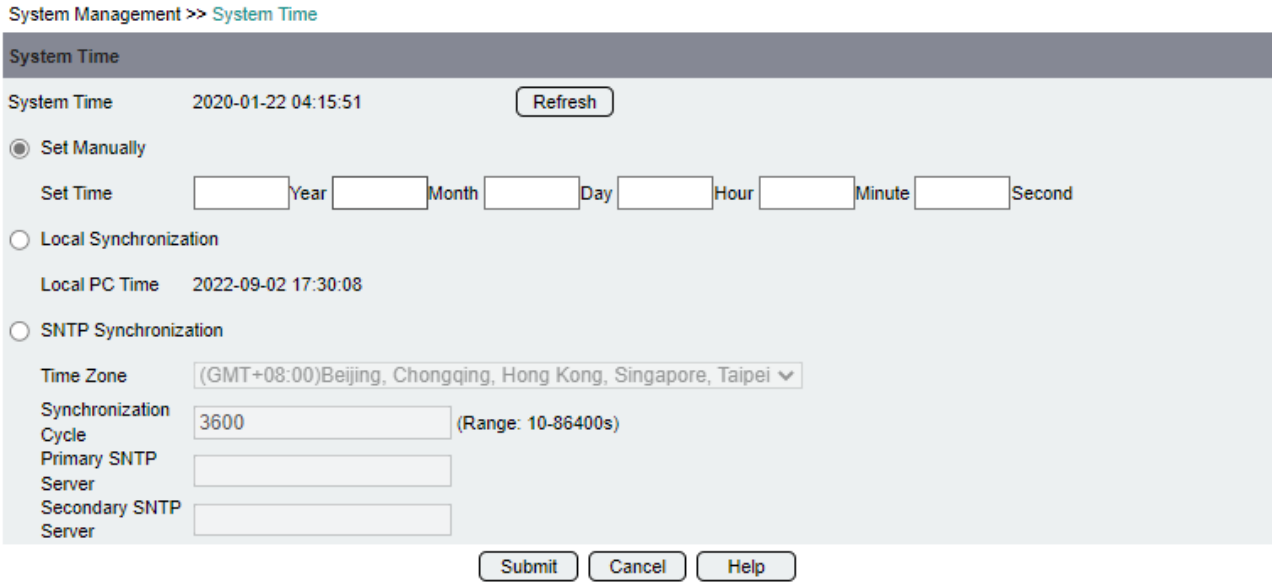


Figure 64 System time page

Attention

1. If you choose Manual Configuration or Local Synchronization, the configured system time will take effect immediately, and it can be saved when the switch battery has power. 2. If SNTP synchronization is selected, the system time of the switch will be synchronized with the time of the SNTP master server by default; when the SNTP master server is not set or disabled, it will automatically synchronize with the time of the SNTP slave server; only when all SNTP servers are not set or disabled In the case of all failures, the current system time is obtained according to the user's manual time configuration.

10.3 User Management

Add or delete users, and modify the passwords and permissions of the selected users, as shown in Figure 65.

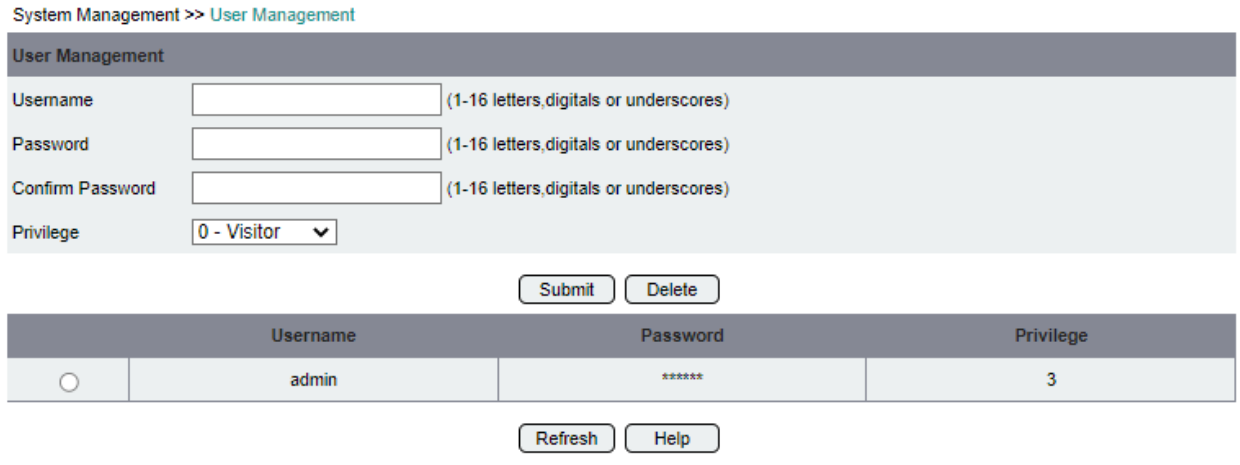


Figure 65 User management page

Attention

1. Only the user's password and authority can be modified, but the user name cannot be modified.
2. You cannot modify the authority of the currently logged-in user on the command line, and cannot delete the currently logged-in user on the command line.
3.The length of the password must be less than 16 characters and cannot contain spaces. The new password and the confirmation password must be the same.

10.4 Log Information

Configure the host IP of the remote log server, and display, clear, and export local log information. As shown in Figure 66.

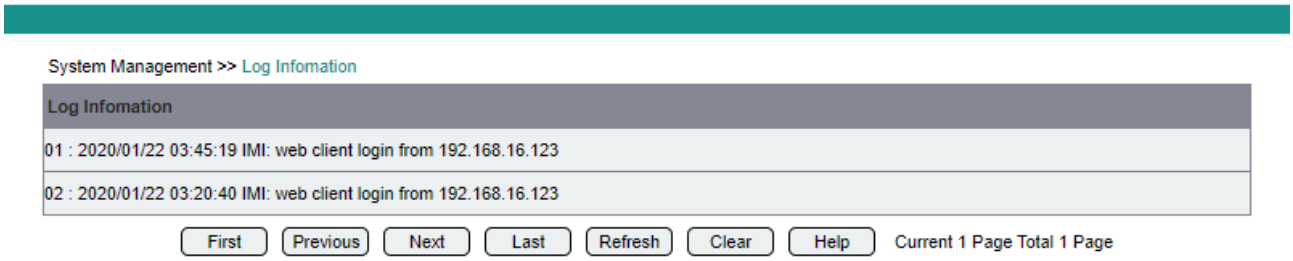


Figure 66 Log information page

Each configuration item is described as follows:

Log host IP address: The host IP of the remote log server.

Clear: Clear the local log information.

Export: Export local log information.

10.5 Restart the Switch

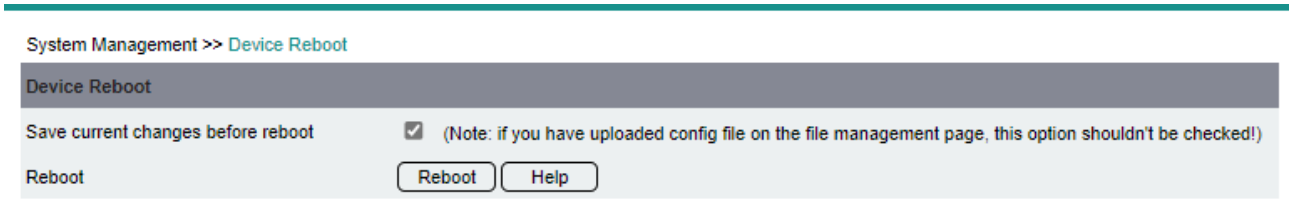


Figure 67 Restart switch page

Attention

1. It is recommended to save the current configuration before restarting the system, otherwise the unsaved configuration will be cleared after restarting.
2. If a new configuration is uploaded, do not select "Keep current configuration", otherwise the current configuration will overwrite the uploaded configuration.

10.6 Restore Factory Configuration

Figure 68 Restore factory configuration page

10.7 File Management

File management includes version upgrade, configuration file upload and download, running status file download, and configuration save. As shown in Figure 69.

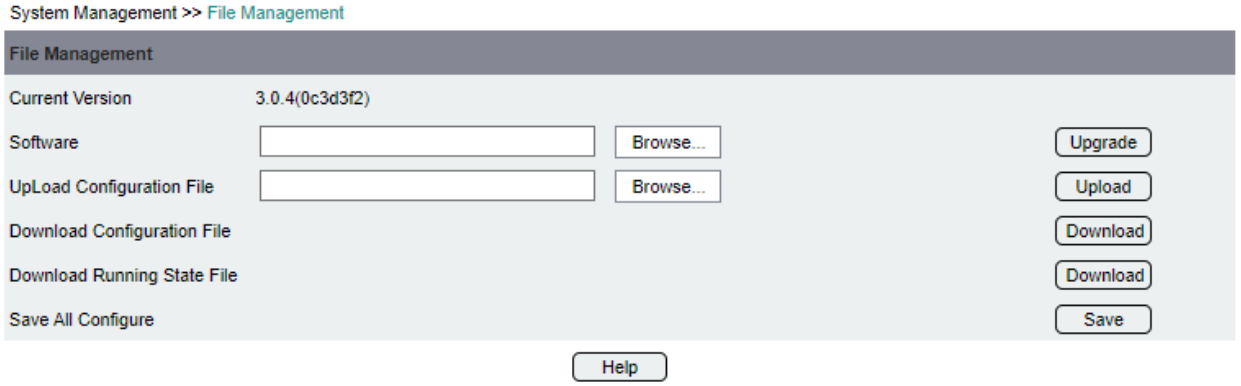


Figure 69 File management page

Attention

In order to prevent errors in the application of the old configuration, it is strongly recommended to manually restore the factory configuration after the upgrade is completed.

10.8 Exit the System

Log out of the web and return to the login page. As shown in Figure 70.

Figure 70 Exit the system page